IEC 62853

Edition 1.0 2018-06

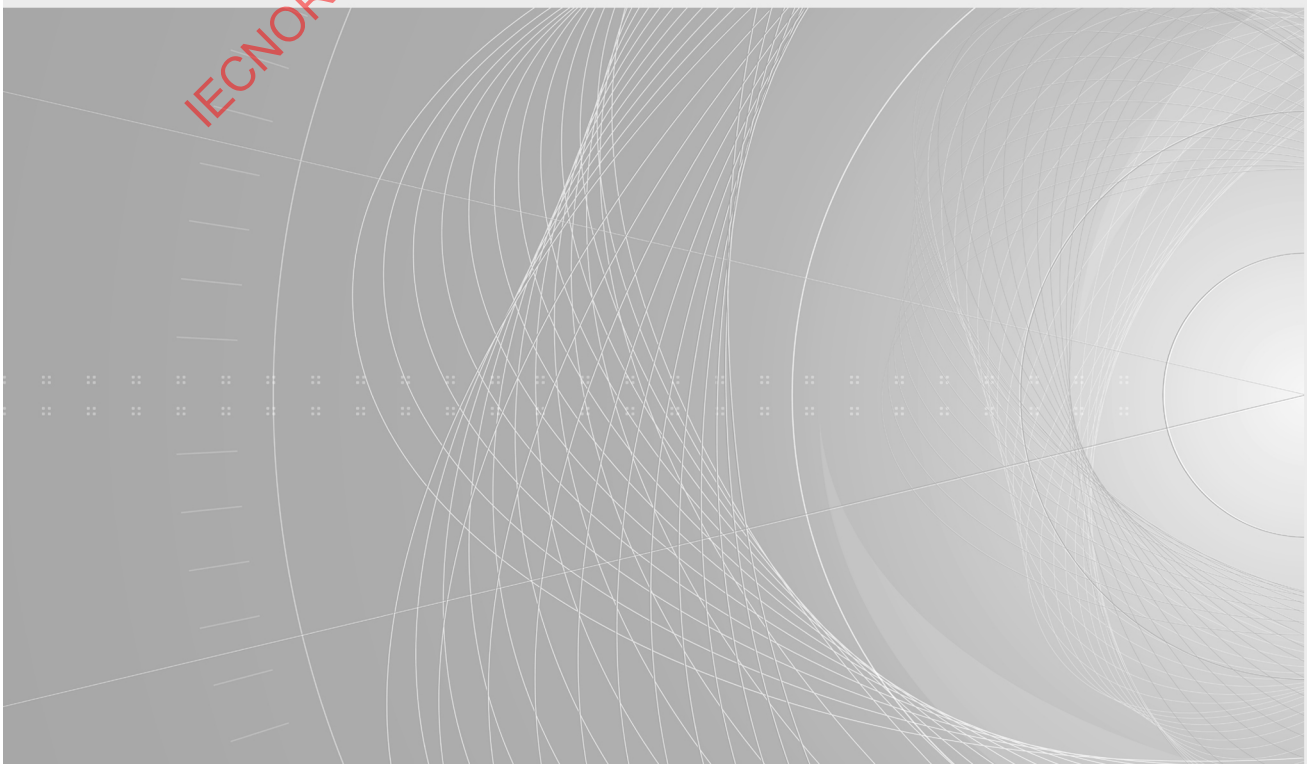
INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Open systems dependability

Sûreté de fonctionnement des systèmes ouverts



IEC 62853:2018-06(en-fr)

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

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

IEC 62853

Edition 1.0 2018-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Open systems dependability

Sûreté de fonctionnement des systèmes ouverts

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.100.40; 03.120.01; 21.020

ISBN 978-2-8322-5789-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

OPEN SYSTEMS DEPENDABILITY

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) 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 62853 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
56/1772/FDIS	56/1776/RVD

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

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

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

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

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

INTRODUCTION

Open systems are systems whose boundaries, functions and structure change over time and which are recognized and described differently from various points of view. The dependability of open systems is a key attribute for the life cycle of a system that operates for an extended period of time in a real-world environment. Open systems dependability is the ability of open systems to accommodate changes in purpose, objectives, environment and actual performance and to continuously maintain accountability from stakeholders, in order to provide expected services as and when required. The attributes of dependability, including availability, reliability, maintainability and supportability, are the same for open systems as conventional systems but they have to be considered in the context that no single stakeholder has a full understanding of the system or its risks.

For open systems, security is especially important since the systems are much exposed to attack by malware. Since an open system changes continuously through its life, the design process, e.g. modelled by the spiral product development model, will to some extent continue during the whole lifetime of the system.

This document elaborates on IEC 60300-1 by providing additional guidance for dependability management of open systems.

This document provides guidance on open systems dependability by using the four process views, each of which selects and combines system life cycle processes, activities and tasks of ISO/IEC/IEEE 15288: 2015.

- Change Accommodation process view;
- Accountability Achievement process view;
- Failure Response process view;
- Consensus Building process view.

A dependability case that assures these process views is crucial for stakeholders to understand and agree on the boundaries of their responsibilities, to assign accountability for implementation and to duly manage changes in achieving open systems dependability.

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

OPEN SYSTEMS DEPENDABILITY

1 Scope

This document provides guidance in relation to a set of requirements placed upon system life cycles in order for an open system to achieve open systems dependability.

This document elaborates on IEC 60300-1 by providing details of the changes needed to accommodate the characteristics of open systems. It defines process views based on ISO/IEC/IEEE 15288:2015, which identifies the set of system life cycle processes.

This document is applicable to life cycles of products, systems, processes or services involving hardware, software and human aspects or any integrated combinations of these elements.

For open systems, security is especially important since the systems are particularly exposed to attack.

This document can be used to improve the dependability of open systems and to provide assurance that the process views specific to open systems achieve their expected outcomes. It helps an organization define the activities and tasks that need to be undertaken to achieve dependability objectives in an open system, including dependability related communication, dependability assessment and evaluation of dependability throughout system life cycles.

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/)

IEC 60300-1, *Dependability management – Part 1: Guidance for management and application*

ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes*

3 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
accountability
state of being answerable for decisions and activities to the organization's governing bodies, legal authorities and, more broadly, its stakeholders

Note 1 to entry: Accountability includes answerability to society in general.

Note 2 to entry: Description in ISO 26000:2010 [1]: Accountability involves an obligation on management to be answerable to the controlling interests of the organization and on the organization to be answerable to legal authorities with regard to laws and regulations. Accountability for the overall impact of its decisions and activities on society and the environment also implies that the organization's answerability to those affected by its decisions and activities, as well as to society in general, varies according to the nature of the impact and the circumstances.

Note 3 to entry: The definition in ISO 15489-1:2001 [2]: principle that individuals, organizations and the community are responsible for their actions and may be required to explain them to others.

[SOURCE: ISO 26000:2010, 2.1, modified – Notes to entry have been added.]

3.2
assurance case
reasoned, auditable artefact created that supports the contention that its top-level claim (or set of claims) is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s)

Note 1 to entry: An assurance case contains the following and their relationships:

– one or more claims about properties;
– arguments that logically link the evidence and any assumptions to the claim(s);
– a body of evidence and possibly assumptions supporting these arguments for the claim(s);
– justification of choice of top-level claim and the method of reasoning.

Note 2 to entry: An assurance case can be understood as a reasoned and compelling argument, supported by a body of evidence, that a system, service or organization will operate as intended for a defined application in a defined environment and defined lifetime.

[SOURCE: ISO/IEC 15026-1:2013 [3], 3.1.3, modified – Note 2 to entry has been added.]

3.3
change accommodation
set of activities which modify and adapt a system to changes in its purpose, objectives, environment or actual performance that require re-establishment of stakeholders' consensus on the system

3.4
consensus
general agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments

Note 1 to entry: Consensus need not imply unanimity.

[SOURCE: ISO/IEC Guide 2:2004 [4], 1.7]

3.5
dependability case
evidence-based, reasoned, traceable argument created to support the contention that a defined system does and/or will satisfy the dependability requirements

Note 1 to entry: A dependability case is an assurance case whose top-level claim is about dependability.

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

3.6
dependability communication
continual and iterative process that a stakeholder conducts to provide, share or obtain information, and to engage in dialogue with other stakeholders regarding the management of dependability

Note 1 to entry: The role of dependability communication in the management of open systems dependability is not unlike that of risk communication in risk management.

Note 2 to entry: See the definition of the term “communication and consultation” in ISO Guide 73:2009 [5], 3.2.1.

3.7
environment
<system> context determining the setting and circumstances of all influences upon a system

[SOURCE: ISO/IEC/IEEE 42010:2011 [6], 3.8]

3.8
failure response
set of activities initiated immediately when a failure is predicted or detected in order to prevent the failure or minimize its effect, to analyse its causes and prevent its recurrence and to fulfil accountability

3.9
frame of reference
set of conventions for the construction, interpretation and use of documents describing a common understanding of and explicit agreements on a system, its purpose, objectives, environment, actual performance, life cycle and changes thereof

3.10
interaction error
error that occurs due to the interactions between items despite each item’s performance meeting the specification

3.11
monitoring
determining the status of a system, a process or an activity

Note 1 to entry: To determine the status there may be a need to check, supervise or critically observe.

[SOURCE: ISO 22301:2012 [7], 3.29]

3.12
open system
system whose boundaries, functions and structure change over time and is recognized and described differently from various points of view

Note 1 to entry: Changes include not only adaptation with specific purpose but also spontaneous evolution. For example, they include spontaneous and uncoordinated changes within a system that spans multiple domains with different authorities.

Note 2 to entry: An open system’s boundaries, functions and structure are not only changing with time but can be vague at any point in time and recognized differently by different stakeholders. This refines the definition of system in IEC 60050-192 for a given level of abstraction and a given viewpoint. A boundary can have a clear definition at one level of abstraction, but it could become more vague at a more detailed level. The level of details necessary for a purpose or for a stakeholder need not be predetermined nor guaranteed to be attainable.

Note 3 to entry: An open system exchanges resources over its boundary with other systems or the environment, possibly changing the boundary itself.

Note 4 to entry: Every substantial system has aspects of both an open system and of a conventional system. The term open system is not used for classification of systems. The term applies to a system when its open aspects are significant for the discussion at hand about the system.

Note 5 to entry: The fact that a software system can be “open source” is irrelevant to being an open system, except that being open source software necessarily brings in aspects of open systems such as lack of centralized authority.

3.13
open systems dependability
ability to accommodate changes in purpose, objectives, environment and actual performance and to achieve accountability continually, so as to provide expected services as and when required

3.14
process
set of interrelated or interacting activities that use inputs to deliver an intended result

Note 1 to entry: Whether the “intended result” of a process is called output, product or service depends on the context of the reference.

Note 2 to entry: Inputs to a process are generally the outputs of other processes and outputs of a process are generally the inputs to other processes.

Note 3 to entry: Two or more interrelated and interacting processes in series can also be referred to as a process.

Note 4 to entry: Processes in an organization are generally planned and carried out under controlled conditions to add value.

Note 5 to entry: A process where the conformity of the resulting output cannot be readily or economically validated is frequently referred to as a “special process”.

Note 6 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified to prevent circularity between process and output, and Notes 1 to 5 to entry have been added.

[SOURCE: ISO 9000:2015 [8], 3.4.1]

3.15
process view
collection of processes, activities and tasks that provides a focus for a stakeholder’s particular concern about a system in a manner that cuts across all or parts of the life cycle

3.16
resilience
adaptive capacity in a complex and changing environment

Note 1 to entry: The definition of resilience in UNISDR Terminology on Disaster Risk Reduction [9]: the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions.

Note 2 to entry: The definition in [10]: the persistence of service delivery that can justifiably be trusted, when facing changes.

[SOURCE: ISO Guide 73:2009, 3.8.1.7, modified – The definition has been made applicable to items other than organizations and Notes to entry have been added.]

3.17
stakeholder
individual or organization having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations

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

Note 1 to entry: Some stakeholders can have interests that oppose each other or oppose the system.

Note 2 to entry: The term ‘interested party’ constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. This document uses the admitted term ‘stakeholder’, following ISO/IEC/IEEE 15288:2015.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.44, modified – Note 2 to entry has been added.]

4 Open systems dependability

4.1 Open systems

Open systems have the following characteristics [11].

– They are large, complex and interconnected.

– They can include black box components.

NOTE 1 A black box component is a component whose users do not know its implementation details and cannot control its functionality and interface.

– Their purpose, objectives, environment and actual performance are not determined and change through their lives. Unpredictable changes of user requirements, service objectives, services received via network, black box components, technological basis, etc., are commonplace.

– Their boundaries, functions and structure are ever-evolving and perceived differently by different stakeholders. Preventing them from becoming vague requires particular effort.

– Accountability is vital in their system life cycle and for risk control, but it needs particular effort to establish because of lack of effective central control.

– Understanding of the systems and their risks by their stakeholders is neither complete nor certain at any given time.

– The possibility of failures due to an incomplete understanding of the systems, unanticipated events and changes cannot be eliminated or predicted. Systems need to be resilient, need to have risk controls including error proofing, need to be able to recover from failures and need to be able to adapt to prevent recurrence.

– Achievement of dependability requires an iterative approach and depends on integration of the system operation and development. Performing dependability activities throughout the system life cycle and iterating them as often as needed is particularly important for open systems.

NOTE 2 Some of these features are shared with so-called “system of systems” [12], [13] and “unbounded or weakly bounded systems”.

NOTE 3 Depending on a particular point of view, most systems have these features to some, possibly negligible, degree. A system is an open system when these features of the system are significant for the discussion at hand regardless of its being a system of systems.

A system necessarily exchanges services with a wide variety of other interconnected, independently managed systems. These surrounding systems are managed according to their own principles and stakeholders, and their interfaces are subject to change for various reasons. The system must serve diverse stakeholders. Each stakeholder has different objectives and there might be no single authority over the system; moreover, the objectives of the system and the surrounding systems change with time. The conditions for the system, such as requirements and constraints, change frequently and unpredictably. Thus, there are uncertainty and incompleteness about these conditions and they cannot be understood completely at any given time.

Since an open system changes continuously through its life, the design process, as modelled by the spiral product development model, will to some extent continue during the whole lifetime of the system.

Moreover, uncertainty and incompleteness are also present within the system itself, such as with respect to its functions, internal structure, and the boundary. Its subsystems are often managed by different parties and those involved in integration and coordination of the system boundaries might not have complete knowledge and control of them. Services and components might be added to or removed from the system during its operation by/for various stakeholders. This dynamic nature makes the system boundary, functions and structure ambiguous in practice, even if there is no ambiguity in theory at any specific time from a specific point of view.

For these reasons, as well as the sheer complexity and scale of the system, it is very difficult for any stakeholder to specify, comprehend or control the system and its management to any sufficient completeness and certainty. Unanticipated changes and failures of various degrees are a part of the system's nature. The use of the term open systems emphasises this aspect of systems.

The true, implicit expectations for the system are always relative to the context of other surrounding systems and stakeholders. The objectives of the various levels of systems surrounding the target system should be taken into account. As the context changes, and as incompleteness and uncertainty are resolved in one way or the other, the system should adapt to the corresponding changes in the requirements and assumptions. These changes cannot be fully anticipated or specified in advance.

4.2 Dependability issues specific to open systems

Open systems dependability aims to achieve service continuity over extended periods of time notwithstanding changes and failures. Achieving service continuity places requirements on the entire life cycle of the system and iteration thereof aided by enhancement activities.

Dependability management provided by IEC 60300-1 generally applies to open systems and this document shall be used together with IEC 60300-1. IEC 60300-1 requires that sustained improvement be ensured via planning and control of enhancement activities and appropriate reviews of progress. Open systems dependability elaborates on this for open systems where dependability directly depends on improvement with respect to frequent unpredictable changes. An iterative approach to the life cycle can be applied to accommodate such changes; see Annex A.

The scope of dependability management of an open system is not trivial because of characteristics explained in 4.1. Merely conforming to explicit agreements is not sufficient because agreements cannot adequately cover all aspects of the system of interest, as no open systems can be completely defined. Stakeholders need to be prepared to act beyond the agreements based on a common understanding of the system and its environment. As a principle, open systems dependability strives for confidence and trust in the system even under broken assumptions, requirements invalidated by changes, and eventual system failures.

The argument above highlights the importance of processes that continually review and revise the scope of dependability management and that provide explicit documentation and an agreement on the scope. The agreement on the scope by stakeholders needs to be backed by agreements on accountability.

Unanticipated causes cannot be prevented. What can be done is to identify key functions, anticipate possible consequences of losing the key functions and protect the key functions so that they can be recovered quickly or covered by redundancy.

4.3 Objective

The objective of open systems dependability is to sustain a degree of service continuity of a system in the context of surrounding systems, stakeholders and the environment, so far as practicable under unanticipated events and changes due to incompleteness and uncertainty of knowledge by stakeholders.

Systems are no longer taken as definite, but as open systems of which our knowledge cannot be complete or certain. A system with open systems dependability should have the ability:

– to continuously remove factors which have the potential to cause failures and hence improve itself;

– to take quick and appropriate action when a failure occurs;

– to prevent, minimize and mitigate damage;

– to continuously provide the services anticipated by stakeholders as much as possible (graceful degradation);
– to maintain the activities and tasks to achieve accountability for the system operations and processes;
– to help understand and communicate the assumptions made when describing the system, documenting these assumptions explicitly, and determining the system's dependability through the documentation and the authority for accepting it.

These abilities are expected for any dependable system even though they have particular importance for an open system that has increased likelihood of being affected by changes in other systems connected to it. Specificity of open systems dependability arises from the incompleteness and uncertainty under which the stated abilities are to be attained. The characteristic of open systems dependability lies in the process of achieving the stated ability, and the open systems dependability is not different from conventional dependability.

4.4 Achieving open systems dependability

For an open system to be dependable, its life cycle should enable stakeholders to do the following.

a) Establish a frame of reference understood by all stakeholders for addressing the system, its purpose, its operation, its environment and changes thereof, and then establish a common understanding and explicit agreements on those matters in that frame of reference.
b) Make transparent the relationship between a failure to fulfil an item in the stakeholder agreement and its implications for stakeholders and society in general, including accountable stakeholders' obligations to provide remedies, so as to motivate best efforts to honour the agreement and to secure availability of remedies for potential damage.
c) Plan and execute immediate actions against failures to provide expected services as much as possible, with least possible disruption and damage, in the manner most expedient in the context.
d) Organize activities that arise when adapting the system to changes in its environment, purpose, agreement, etc., and to gain from experience with failures, so as to improve dependability continuously.

These four practices work together and each depends on the others. Item a) provides the basis of b), c) and d). Item b) helps to enforce the agreement in a) and promotes public confidence and trust in the system by communicating the plans and activities executed according to c) and d). Item c) gives necessary information to b), and triggers item d) for prevention of failure recurrence. Item d) restarts a) to reflect time-dependent changes in the common understanding and explicit agreements of a), which is always a provisional snapshot in need of continuous updating.

The ways in which these four practices are combined and collaborate can be represented in life cycle models. Annex A provides examples. An example of applying open systems dependability to a concrete open system is given in Annex C.

4.5 Relationship to resilience and fault tolerance

The concept of resilience is very similar for open and conventional systems. Traditional resilience (3.16 and its Note 1 to entry) emphasizes the ability to get back to normal operation after disturbances, while open systems dependability embraces the fact that even the definition of "normal operation" varies from time to time or from one point of view to another. A more recent concept of resilience (Note 2 to entry in 3.16) considers a broader range of changes and adaptations and shares the goal with open systems dependability. The difference is that open systems dependability focuses on cases where changes and a need to adapt stem from openness of systems, and hence on consensus and accountability in a system life cycle approach.

The idea of fault tolerance, on the other hand, differs between conventional and open systems. In a conventional system, it is assumed possible, at least in principle, to enumerate all significant potential faults. A fixed, concrete procedure for getting back from deviation to normal operation is given to achieve fault tolerance, where deviation and normal operation are explicitly defined. Open systems dependability concerns the situation where those cannot be explicitly defined.

5 Conformance

For a system life cycle to support open systems dependability, a dependability case [14], [15] demonstrating the following should be provided:

a) that the system life cycle achieves the requirements of all the process views specified in Clause 6;

b) that the adequacy of these requirements for achieving open systems dependability for the target system has been considered.

NOTE 1 The dependability case is required in order to ensure that stakeholders understand and agree on the boundaries of their responsibilities, assign accountability for implementation and management of changes appropriately.

NOTE 2 By its nature, open systems dependability is not shown by a fixed set of sufficient conditions. Each application of this document is assessed for conformance considering the quality of additional consideration in b) with respect to the specifics of the target at hand.

An informative template of a dependability case that demonstrates the above claims is given in Annex B.

6 Process views for achieving open systems dependability

6.1 General

Clause 6 describes the four process views that address the four practices of the open systems dependability 4.4 a) to d). Some of the activities and tasks required for implementing these processes are selected from ISO/IEC/IEEE 15288:2015.

Each practice of open systems dependability needs a set of activities and tasks that cut across many life cycle processes. The concept of a process view is introduced in order to gather a group of related activities in a single place as described in ISO/IEC/IEEE 15288:2015, Annex E.

Clause 6 specifies the four process views conforming to the process viewpoint provided in ISO/IEC/IEEE 15288. A process view is defined by providing the following information:

a) process view name;

b) process view purpose;

c) process view outcomes;

d) identification and description of the processes, activities and tasks that implement the process view and references to the sources for these processes, activities and tasks in other standards.

Clause 6 specifies each of the four process views by providing the above items a) to d).

The four process views work together to achieve the objective of open systems dependability. Together with other system life cycle processes and process views, they form a system life cycle model as is required for each application of ISO/IEC/IEEE 15288:2015 as indicated in Annex A.

NOTE 1 ISO/IEC/IEEE 15288 details processes and their activities and tasks. Selected sets of these processes can be applied throughout the life cycle for managing and performing the stages of a system's life cycle.

NOTE 2 The penultimate paragraph of 4.4 outlines the relationship among the four process views. Clause A.2 provides the detailed relationship in an example life cycle model.

In the rest of Clause 6, each subclause (i.e. 6.*i*) provides a process view and is organized as follows.

The title of 6.*i* is the name of the process view (a).

6.*i*.1 "Purpose" provides the process view purpose (b). The first paragraph is the core statement of the purpose and the following paragraphs add some explanation.

6.*i*.2 "Outcomes" lists the process outcomes (c). In some cases, outcomes are arranged hierarchically. Annex B provides a template argument structure for a dependability case using the outcomes. This provides some rationale for the selection of outcomes.

6.*i*.3 "Processes, activities and tasks" constitutes the principal part of this document. The list of ISO/IEC/IEEE 15288 processes, activities and tasks (d) that implement the process view is provided, together with advice specific to realization of open systems dependability. For each ISO/IEC/IEEE 15288 process, an optional paragraph that describes its relevance to the process view is followed by a list of more detailed descriptions of the related activities and tasks, with indications of the related outcome of the process view. Descriptions in 6.*i*.3 shall be used together with those in ISO/IEC/IEEE 15288:2015 that provide definitions and contexts of the related processes, activities and tasks.

In 6.*i*.3, clauses of ISO/IEC/IEEE 15288:2015 and clauses of this document are both referred to. They are distinguished in the following way. Angle brackets (<>) are used to refer to the subclause number of a process in ISO/IEC/IEEE 15288:2015 and the list item label of an activity or a task within that process. For example, "<6.4.2> Stakeholder Needs and Requirements Definition process" refers to 6.4.2 of ISO/IEC/IEEE 15288:2015 and, within the context of <6.4.2>, "<a)1)>" refers to the task "1) Identify the stakeholders who have an interest in the system throughout its life cycle" within the activity "a) Prepare for Stakeholder Needs and Requirements Definition". For a two-level list, a reference to a level-1 list item, say "<a)>", refers to all of the level-2 items <a)1)>, <a)2)>, …, <a)n)> that make up the level-1 item <a)>. Square brackets ([]) are used to refer to the list item label of a process view outcome in 6.*i*.2 of this document.

6.2 Consensus Building process view

6.2.1 Purpose

The purpose of the Consensus Building process view is to establish and maintain a common understanding with explicit agreements about the system, its purpose, objectives, environment, actual performance, life cycle and changes thereof.

NOTE 1 Unlike explicit agreements, the common understanding of the system is not necessarily documented explicitly and includes the attitude, beliefs, perceptions and values shared among stakeholders.

The Purpose should be achieved with the following understanding.

It should be ensured that the same understanding is shared by all stakeholders so that the inevitably remaining discrepancy of interpretations is acceptable. Explicit agreements include those covering stakeholders' benefits and responsibilities in developing and operating the system, as well as those on assumptions made.

Establishment of the common understanding and explicit agreements provide a generic preventive measure against unanticipated events.

NOTE 2 For some stakeholders, it might be sufficient to understand that other stakeholders ensure the desired outcomes, without the need to understand the technical details involved.

Achievement of the Purpose consists of the following:

– establishment of a common understanding and explicit agreements among stakeholders [6.2.2 outcomes a)1) to a)7)];
– maintenance of the understanding and agreements [b)1) to b)5)].

The relationship between the purpose and the outcomes is described in Clause B.2.

6.2.2 Outcomes

a) A common understanding and explicit agreements among stakeholders are established.
   1) Stakeholders of the system are identified.

   NOTE 1 The list of stakeholders changes with time and points of view.

   2) A frame of reference understood by all stakeholders is established. The frame includes the vocabulary and basic assumptions on the environment of the system.
   3) The system's purpose, objectives, environment, actual performance, life cycle and changes thereof are understood in the frame of reference by each stakeholder in a same way. This includes the assumptions concerning the system and stakeholder's responsibilities.
   4) An arbitration process is pre-agreed for situations when consensus cannot be reached so that conflicts of interest can be resolved.

   NOTE 2 Conflicts of interest can include those related to intellectual property rights.

   5) Explicit agreements are developed based on the understanding in 3) and are documented. The records include accounts of their development and the reasoning why the various components of the agreements are considered appropriate and feasible.
   6) The differences of interpretation of the agreement documents are within an acceptable range.
   7) The outcomes above are achieved in a way that is fair and equitable for all stakeholders.

   NOTE 3 Fairness and mindfulness contribute to resilience against unanticipated events. Lack of fairness and mindfulness eventually leads to problems that affect all stakeholders.

   NOTE 4 Extortion of opinions and requirements, for instance, is not fair nor mindful, and has disproportionate long-term impact on the failure of large open systems to achieve their objectives.

b) The common understanding and explicit agreement among stakeholders is maintained.
   1) The policy on change management of agreements is established.

   NOTE 5 The policy applies in all phases, including initial identification of service requirements and revision of them.

   2) Stakeholder consensus is maintained when the business objectives, stakeholder needs, system or environment changes.

   NOTE 6 Such changes might be necessitated by post-failure treatment.

   NOTE 7 Maintaining stakeholder consensus means revising, validating and renewing it so that it reflects the new objectives, needs, system and environment after a change.

   3) Processes for achieving consensus are reviewed when the business objectives, stakeholder needs, system or environment changes.

   NOTE 8 Consensus can be limited to a part of the activities, or some of the stakeholders, while the rest of the activities or stakeholders are not influenced. Stakeholders can also by passive acceptance choose not to involve themselves in matters that are of no or limited importance to them. Often an activity is controlled by a small group of dedicated stakeholders while the rest of the stakeholders accept this as long as the performance is acceptable and their vital interests are not affected.

   NOTE 9 Actions for stakeholder involvement are described in IEC 60300-1:2015, 5.3 (the third item of the itemized list).

   4) Responsibility for producing and approving the dependability case is defined.

5) The achievement of consensus, an account of its development and the reasoning why the consensus is considered appropriate and feasible are recorded in the dependability case (see IEC 62741 [15]).

6.2.3 Processes, activities and tasks

The Consensus Building process view should be implemented using the activities and tasks of the following processes provided by ISO/IEC/IEEE 15288.

NOTE 1 In the following, angle brackets (<>) are used to refer to subclause numbers and list item labels in ISO/IEC/IEEE 15288:2015. Square brackets ([]) are used to refer to the list item label of a process view outcome in this document. See the last paragraph of 6.1 for details.

<6.1.1> The Acquisition process establishes and maintains an agreement between an acquirer and a supplier, which is a part of the explicit agreements referred to in [a), b)]. The acquirers should take into account the concerns of parties other than the acquirers and the suppliers such as end users, the local community and regulators [a)].

– <a)1)>: The acquisition strategy should clarify tactics to achieve the common understanding and explicit agreements in [a)].
– <c)1), c)4)>: Development and change negotiation of the agreement between the acquirer and the supplier should be done in a fair and mindful manner [a)7)].
– <d)>: Monitoring of the agreement is a part of the policy and aims to maintain the explicit agreement [b)1), b)2), b)3)].
– <d)1)>: Assessment of the execution of the agreement should include assessment of its fairness and mindfulness [a)7)].

<6.1.2> The Supply process establishes and maintains an agreement between the acquirer and the supplier, which is a part of the explicit agreements in [a), b)]. The suppliers should take into account concerns of parties other than the acquirer and the suppliers such as end users, local community and regulators [a)].

– <a)1)>: Identification of the acquirers is a part of stakeholder identification [a)1)].
– <a)2)>: The supply strategy should clarify tactics to achieve [a)].
– <c)1), c)4), d)1)>: Negotiation on an agreement and its execution should be done in a fair and mindful manner [a)7)].
– <d)2)>: Assessment of the execution of the agreement should include assessment of its fairness and mindfulness [a)7)].

<6.2.1> The Life cycle model management process should specify the linkages among life cycle processes that enable achievement of all outcomes of this process view [a), b)].

<6.2.5> The Quality management process formulates aspects of the common understanding and explicit agreements as managed qualities. It also manages the quality of the common understanding and explicit agreements [a), b)].

– <a)1)>: The quality management policies, objectives and procedures should address the extent of the common understanding and the extent of consent to the explicit agreements [a), b)]. Stakeholders should develop a common understanding and explicit agreements on quality management taking into account that, in general, there is no central organization that manages quality of the whole system [a), b)].
– <a)2), a)3)>: The common understanding of quality management should recognize that definitions of responsibilities and evaluation criteria are not perfect and are subject to change, and that stakeholders should be prepared to act, when necessary, beyond their defined responsibility for the sake of total quality [b)].
– <a)3)>: Evaluation criteria should be fair and mindful [a)7)].

<6.2.6> The Knowledge management process provides a source of the common understanding.

– <a)1), b)1), c)1)>: The knowledge management strategy, classification for sharing knowledge and a taxonomy to organize knowledge should provide a frame of reference understood by all stakeholders [a)2)].

– <d)>: Maintenance of knowledge should be integrated with maintenance of the common understanding and explicit agreements [b)].

<6.3.1> The Project planning process embodies the common understanding and explicit agreements as plans [a), b)].

– <a), b)1) to b)6)>: Definition and planning of the project (objectives, constraints, scope, life cycle model, work breakdown structure, schedule, achievement criteria for life cycle stages, costs and budget, roles, responsibilities, accountabilities, etc.) should reflect the common understanding and explicit agreements and in turn deepen and clarify them, forming the basis of their maintenance [a)2), a)3), a)5), a)6), b)1), b)2), b)3)].

– <b)4)>: Responsibility for the dependability case should be defined in the project plans [b)4)].

– <b)7)>: Communicating and reviewing plans should form a part of developing and maintaining explicit agreements; the review should provide and record the rationale for the agreements [a)5), b)2), b)5)].

<6.3.2> The Project assessment and control process governs the maintenance of the common understanding and explicit agreements when changes occur.

– <b), c)>: Assessment and control of the project includes assessment and control of (i) stakeholder consensus with respect to its changing context and (ii) the performance of relevant processes with respect to the required outcomes of this process view [b)1), b)2), b)3)].

<6.3.3> The Decision management process resolves conflicts arising in establishing and maintaining the common understanding and explicit agreements, and also manages decisions to accept unopposed opinion [a), b)].

– <a)1)>: The decision management strategy should include a pre-agreed arbitration process [a)4)].

– <a)3)>: Besides stakeholders with conflicting interests, those affected by the decision should be identified and involved [a)1), a)7)].

– <b)2)>: The desired outcome and selection criteria should be determined in a fair and mindful manner by recursive application of the Consensus Building process view [a)6), a)7)].

– <c)2), c)3)>: A record of resolutions, decisions rationale and assumptions, tracking and evaluation should provide an account of consensus building and evidence for its fairness and mindfulness [a)7), b)5)].

NOTE 2 Invocations of the Consensus Building process view and those of Decision Management process are mutually recursive. Consensus building requires decisions to be made and each decision requires consensus on the desired outcomes and selection criteria.

<6.3.6> The Information management process generates, obtains, confirms, transforms, retains, retrieves, disseminates and disposes of information about the common understanding, the explicit agreements and their management.

– <a)1), a)5)> The strategy for information management and information maintenance actions should include the policy on the change management of agreements [b)1)], maintenance of stakeholder consensus [b)2)], review of processes for achieving consensus [b)3)]. They should reduce differences of interpretations [a)6)] and support the fairness and equitability for all stakeholders [a)7)].

– <a)2)>: Information items to be managed should include the list of identified stakeholders [a)1)], the frame of reference [a)2)], the understanding of the system's purpose, etc. [a)3)], the agreed arbitration process [a)4)], the explicit agreements [a)5)], the dependability case [b)4)] and the account of development of consensus and the reasoning behind it [b)5)].

– <a)3)>: Designation of authorities and responsibilities for information management includes that for the dependability case [b)4)].

– <a)4)>: The formats and structure of information items are parts of the frame of reference [a)2)] and their contents should reflect the common understanding [a)3),a)5)].

– <b)1)>: Development of information on explicit agreements should adopt the agreed arbitration process to resolve conflicts of interest [a)4)]. The frame of reference established in [a)2)] should be used for transforming information into useable information for stakeholders.

– <b)5)>: Disposal of information, particularly the account of the development of explicit agreements and the reasoning behind it [b)5)], should be done only after careful consideration of the value it has for change accommodation and accountability achievement at a later time, including when those arise from failure response.

<6.3.8> The Quality assurance process provides confidence that the common understanding and explicit agreements are established and maintained with sufficient quality and that their contents represented as quality requirements are fulfilled.

– <b), c)>: Evaluation of product or service and process should form a part of the maintenance of the common understanding and explicit agreements [b)1), b)2)].

– <d)>: A record of quality assurance activities should provide an account of consensus building [b)5)].

– <e)>: The treatment of problems should consider whether their causes require update of the common understanding and explicit agreements and that of the processes [b)1), b)2), b)3)].

<6.4.1> The Business or mission analysis process provides the frame of reference and starts building the common understanding of environments, etc., in that frame. Application of the process should take into consideration that the system might lack an organization encompassing all stakeholders.

– <a)2), b)2)>: The analysis strategy and the problem space definition should clarify the frame of reference and the common understanding in that frame to be shared; they should also be fair and mindful [a)2), a)3), a)7)].

– <b)1)>: After the problem analysis, confirmation should be obtained that all stakeholders share the same understanding of the scope, basis or drivers of the problems or opportunities addressed in <b)1) NOTE 1> [a)2), a)3), a)6)].

– <c)1)>: Identification of major stakeholder groups should take into account that stakeholders might change with time and that each stakeholder may perceive differently which entities are the major stakeholder groups of the system; each stakeholder should be identified together with his/her roles [a)1)]; preliminary operational concepts should include policies on services that express the common understanding [a)2)].

– <c)2)>: The solution classes identified should be shared among all stakeholders and each stakeholder should be able to examine the solutions from his/her own viewpoint for fairness and mindfulness [a)3), a)7)].

– <d)>: The evaluator and the method of evaluation should be identified and agreed among the stakeholders [a)7)].

– <e)1)>: The traceability between the analysis results before and after changes should be maintained, in addition to traceability between the analysis result and other artefacts in one iteration of a life cycle [b)2), b)5)] (cf. <6.4.1.1 NOTE 2>).

<6.4.2> The Stakeholder needs and requirements definition process develops the common understanding and explicit agreements on the system purpose, etc., as stakeholder needs and requirements definitions [a)3), a)5)].

– <a)1)>: Identification of stakeholders should take into account that stakeholders might change with time and that each stakeholder may perceive differently which entities are the stakeholders of the system; each stakeholder should be identified together with his/her roles [a)1)].
– <a)2)>: The stakeholder needs and requirements definition strategy should provide for fair and mindful resolution of different opinions and conflicts that help ensure system assurance and integrity [a)4), a)7)] (cf. <6.4.2.3 a)2) NOTE>); the strategy should address how to achieve the common understanding of policies on the system's service [a)3)].
– <b)1)>: The definition of context of use should resolve differences in presuppositions held by stakeholders in a fair and mindful manner [a)2), a)3), a)7)].
– <b)2), b)3), b)4)>: Elicitation of explicit and implicit needs should pay particular attention to <b)2) NOTE 1>; stakeholders needs should be elicited together with their presuppositions about the system and its environment; it should be taken into account that differences in the presuppositions might become apparent only after some period of operation; differences hinder dependability communication among stakeholders, can be an obstacle to consensus building and can lead to inappropriate decisions [a)2), a)3)]; elicitation, identification, selection and definition of stakeholder needs should be fair and mindful [a)7)].
– <c)>: The operational concept should include policies on the system's service that reflects the common understanding [a)2)].
– <f)>: Changes to the stakeholder needs and requirements definition should be managed [b)].

<6.4.3> The System requirements definition process transforms stakeholder consensus to concrete system requirements. This facilitates maintenance as well as assessment of the outcomes of this process view [a), b)].

– <b), c)>: Before a particular set of technical requirements is chosen, stakeholders should reach consensus on the anticipated consequences and risks of the choice in their own terms [a)5), a)6), a)7)].

<6.4.4> Definition of architecture provides a part of the frame of reference and explicit agreements [a)2), a)5)].

– <b)1)>: The architecture viewpoint should form the frame of reference in [a)2)].
– <f)2)>: Explicit acceptance of the architecture should form a part of the explicit agreements [a)5)].

<6.4.9> The Verification process is a part of assessment of the explicit agreement [a)6), b)2)].

– <c)3)>: The stakeholder agreement that the system meets requirements is a part of the explicit agreements referred to in [a)5)].

<6.4.11> The Validation process is a part of assessment of the explicit agreements [a)6), b)2)].

6.3 Accountability Achievement process view

6.3.1 Purpose

The purpose of the Accountability Achievement process view is to establish the relationship between a breach of an explicit agreement and its implications for stakeholders and society in general. This includes accountable stakeholders' obligations to provide remedies, so as to improve the chance of realizing consensus on the system, to sustain confidence and trust in the system and to secure the availability of remedies for potential damage.

NOTE 1 A breach of agreement includes the case where a stakeholder is unable to keep the agreement because of an unforeseeable harmful event.

NOTE 2 Agreements need to be explicit to the extent necessary to clarify for what each stakeholder is to be held accountable. The explicit agreement needs to refer to implicit agreements such as industry codes of practice when necessary.

The Purpose should be achieved taking the following into account.

The Accountability Achievement process view provides accountability to society in general. Accountability is the overall responsibility for decisions and actions taken in any part of the life cycle of a system. Accountability includes outward responsibility for providing information to the users and other stakeholders, and inward responsibility for monitoring and maintaining controls over identified risks. Since there is no central control for open systems, it is difficult to identify the party that is accountable for a decision, an action or a particular control.

Accountability has an immediate impact on people's confidence and trust in the system, and such subjective properties of the system are essential for dependability. Lack of accountability prevents some systems from resuming services after technical recovery from a failure, because of regulatory requirements, public opinion and other social reasons.

Accountability is necessary to achieve dependability of the system and strengthens the overall dependability of interconnected, independently managed systems. Impacts of failures of a system can be mitigated by the surrounding interconnected systems that share information on the failure.

Achievement of the Purpose consists of the following:

– establishment of the relationship between a breach of an agreement and its implications, which include accountable stakeholders' obligations to provide remedies, before events for which accountability is required [6.3.2 outcomes a) to e)];
– the performance of actions that anticipate and respond to events for which accountability is required [f) to h)];
– provision of adequate information to stakeholders and society in general [i)1) to i)5)].

The relationship between the purpose and the outcomes is described in Clause B.3.

6.3.2 Outcomes

a) Key decisions controlling the system life cycle and risks in the system life cycle are identified, including those controlling the outcomes of the processes and process views.

NOTE 1 Key decisions include those decisions made at the life cycle stage decision gates and those that have a large influence on later progress of the system life cycle.

b) A person or an entity accountable for each key decision controlling the system life cycle and risks in the system life cycle is identified.

c) For each item of each explicit agreement, the key decisions that can cause its failure or breach are identified.

NOTE 2 For a breach of an agreement caused by factors outside the system, contributing key decisions include acceptance of the risk and acceptance of risk analysis result that is insufficient.

NOTE 3 The stakeholders accountable for a breach of agreement are those who are accountable for the key decisions identified as possible causes of the breach.

d) For each breach of each explicit agreement, its impacts on the non-accountable stakeholders and society in general are assessed.

NOTE 4 Assessment includes analysis of the controllability of impacts by the accountable stakeholders with given authority and resources.

NOTE 5 Each item of each explicit agreement is formulated so that such examination is possible.

e) For each breach of each explicit agreement, its implications for the accountable stakeholders and the remedies for the non-accountable stakeholders and society in general are agreed.

NOTE 6 The implications for the accountable stakeholders include obligations to provide the agreed remedies for the non-accountable stakeholders and society in general. The Consensus Building process view is invoked to revise the original agreement so that accountable stakeholders' control is sufficient for fulfilling the obligations.

NOTE 7 The agreement on the implications and remedies for a breach of the base agreement includes consideration of the case where it is caused by disruptive changes not considered in a) to d).

f) Anticipated and unanticipated outcomes from decisions broadly across the system are monitored and assessed. This includes monitoring of breach of agreements.

g) Feedback loops that inform decision makers and other stakeholders about the outcomes of decisions and actions are established.

NOTE 8 Feedback loops recognize unintended outcomes and initiate actions to address them.

NOTE 9 Feedback loops improve understanding of system behaviour and interactions among decision makers responsible for different parts of the system. Good feedback loops are crucial since parties making decisions do not have a full understanding of the whole system; hence decisions can have unintended consequences in other parts of the system.

NOTE 10 Decision management is particularly difficult for open systems. It relates to both the Consensus Building process view and the Accountability Achievement process view. Issues arise when implementing a consensus decision, feeding back the results of the decision and addressing its unintended outcomes in other parts of the system. The feedback loops help resolve these issues.

h) When a breach of an agreement occurs, the stakeholders accountable for it provide in a timely manner the remedies for the non-accountable stakeholders and society in general.

i) Adequate and pertinent information is provided by the accountable stakeholders to non-accountable stakeholders and society in general in a timely manner.

NOTE 11 There are some cases where information from multiple life cycle processes needs to be integrated.

NOTE 12 Information is adequate and pertinent when (1) it is comprehensive; (2) the recipients understand it with ease; (3) it enables each recipient's own mitigation of the harm from failure and (4) the recipients have justified confidence and trust in its adequateness and validity.

1) Prompt, valid and adequate responses are given to legitimate requests by a stakeholder for information about the system.

2) The stakeholders have justifiable confidence and trust in the information provided about the system.

3) Following a failure, adequate and pertinent information is chosen and given to stakeholders of the system, stakeholders of the interconnected systems and general public.

NOTE 13 Information is given by the Failure Response process view.

4) Information on changes to requirements of the system, to expectations of the system, to descriptions of the system and to performance of the system is chosen and given to stakeholders of the system, stakeholders of the interconnected systems and general public.

5) Information on gaps between requirements, expectations, descriptions and performance of the system, when found, is chosen and given to stakeholders of the system, stakeholders of the interconnected systems and general public.

6.3.3 Processes, activities and tasks

The Accountability Achievement process view should be implemented using the activities and tasks of the following processes provided by ISO/IEC/IEEE 15288.

<6.1.1> Acquisition process

– <c)>: The establishment of the agreement between the acquirer and the supplier (including acceptance criteria and the acquirer's obligations) involves key decisions controlling the system life cycle [a)]; its non-fulfilment is a breach of the agreement and key decisions leading to it, etc., should be identified [b), c), d), e)].

– <d)>: Monitoring of the agreement is a part of the feedback loops [f), g)].

<6.1.2> Supply process

– <c)>: The establishment of the agreement between the acquirer and the supplier including acceptance criteria and the acquirer obligations involves key decisions controlling the system life cycle [a)]; its non-fulfilment is a breach of the agreement and key decisions leading to it, etc., should be identified [b), c), d), e)]. Maintenance of the agreement should enable outcomes [f), g)], too.

– <e)4)>: Responsibility for the product or service should be transferred in a manner that ensures continuous achievement of outcomes [f), g), h), i)].

<6.2.1> Life cycle model management process

– <a)3)>: Establishment of the roles, etc., should include the identification of a person or an entity accountable for each key decision [b)].

– <a)4)>: Definition of the business criteria and how it controls life cycle stages involve key decisions [a), b)]. Accounts of their development should be documented [i)].

– <a)5)>: The established standard life cycle models should specify the linkages among life cycle processes that enables all outcomes of the Accountability Achievement process view [a) to i)].

<6.2.3> The Portfolio management process should identify key decisions controlling the interface between the system life cycle of a system and that of other systems [a)].

– <a)3)>: Definition of accountabilities and authority is a part of achieving [a), b)] and should consider [c), d), e)] together.

– <a)5)>: Allocation of resources to a person or an entity accountable for it involves key decisions [a), b)].

– <c)1)>: Cancellation and suspension of the project should be accounted in a timely manner [i)].

<6.2.5> Quality management process

– <a)1), a)3)>: Establishment of quality management policies, etc., and the definition of quality evaluation criteria and methods involve key decisions [a)] and outcomes [b), c), d), e), h)] should be considered together. Each identification or definition should be accompanied by assignment of its accountability.

– <a)2)>: Defining responsibilities and authority for quality management implementation is a part of achieving [b)].

– <b)>: Customer satisfaction assessment is a part of achieving [d), f), g)].

– <c)>: Planning corrective and preventive actions is a part of the obligations of accountable stakeholders [e), h)]; this is a part of the feedback loops [g)].

<6.2.6> The Knowledge management process should be performed in the context where knowledge is to be shared among multiple organizations [f), g), i)]. Adequate information in [i)] should include the ‘lessons learned’ from past experiences that accountable stakeholders utilized in their decisions.

<6.3.1> Project planning process: All definitions and identifications made in this process involve key decisions [a)] and should be considered together with [b), c), d), e), h)].

– <a)4)>: The work breakdown structure should be accompanied by assignment of accountability and identification of pertinent information to be disseminated [b), i)].

– <b)4)>: The defined accountability should include identification of information to be disseminated in the case of system failure [i)].

– <b)6)>: Planning acquisition involves key decisions [a)] and should be considered together with [b), c), d), e), h)].

<6.3.2> Project assessment and control process

– <a)1)>: Definition of the project assessment and control strategy involves key decisions [a)] and should be considered together with [b), c), d), e), h)].
– <b)>: Project assessment should include the assessment in [d)]. The result should be provided in accountability information [i)].
– <c)>: The controls over the project should include the feedback loops referred to in [g)], initiation of corrective actions [h)] and provision of accounting information [i)].

<6.3.3> Decision management process: The accountability for making and managing decisions includes responsibility to show that accountable stakeholders considered all relevant information and followed the Decision management process properly.

– <a)1), c)3)>: The decision management strategy should provide good feedback loops [g)].
– <c)2), c)3)>: The record of decisions should include evidence that accountability for making and managing decisions is achieved [i)].

<6.3.4> Risk management process: The accountability for managing identified risks, i.e. monitoring and maintaining control of them, is particularly important. It needs to be clearly defined even for risks that are not well understood [b), e), f), h)].

– <a)1), d)>: Definition of the risk management strategy and decisions on risk treatment involve key decisions [a)] and should be considered together with [b), c), d), e), h)].

<6.3.5> Configuration management process

– <b), c)>: Identification of configuration items and their change management in Configuration management process involve key decisions [a)] and should be considered together with [b), c), d), e), h)].
– <d), e)>: The configuration status, accounting, and configuration evaluation should provide a part of adequate information in [i)] that helps to gain the trust and confidence of stakeholders in information given about the system [i)2)].
– <e)4), e)5)>: Assessment of configuration should be performed as a part of monitoring of breach of agreements [f)] and the feedback loops that inform decision makers [g)].

<6.3.6> The Information management process should manage and provide adequate information referred to in [i)]. In particular, justifiable confidence and trust by the stakeholders should be achieved [i)2)]. Cooperation of multiple life cycle processes should be considered in providing the information.

– <a)1)>: The information management strategy should support provision of feedback loops about the outcome of decisions to decision makers [g)].
– <a)2)>: All processes should invoke the Information Management process in order to collect and manage log data and other evidence that would establish and justify the adequateness and validity of the accountability information; the objective representation of justification should be provided [i)2)].
– <b)1)>: Information items should be collected and utilized together with evidence of their authenticity in a form verifiable by receivers of information [i)2)].
– <b)3)>: Publication, distribution or provision of access to information should be done so as to realize [i)].
– <b)5)>: Disposal of information involves key decisions. It should be done only after careful consideration of its effect in future on accountability achievement [a) to i)].

<6.3.7> The Measurement process should form a part of the feedback loops [g)].

– <a)3)>: Information needs for monitoring unanticipated outcomes should be considered for the feedback loops [f), g)].

<6.3.8> Quality assurance process

– <a)1)>: Definition of the quality assurance strategy involves key decisions [a)] and should be considered together with [b), c), d), e), h)].

<6.4.1> Business or mission analysis process

– <c)>: Characterization of solution space should include accountability for each identified major stakeholder [b)].

<6.4.2> Stakeholder needs and requirements definition process

– <a)1), b), c), d)>: Identification of stakeholders, definition of stakeholder needs, definition of the operational concept and other life cycle concepts and definition of stakeholder requirements involve key decisions [a)] and should be considered together with [b), c), d), e), h)].
– <b)2), d)3)>: Needs of stakeholders should be identified together with their accountability [b), c), d), e), h)].
– <c)>: The operational concept and other life cycle concepts should include definition of accountability of major stakeholder groups identified in <6.4.1>. Analysis of scenarios should identify key decisions taken by stakeholders within the scenarios and analyse potential impacts and consequences of those decisions [a), b), c), d), e), h)].
– <e)>: Accepting the result of stakeholder needs analysis as appropriate is a key decision and the person responsible for the Stakeholder needs and requirements definition process is accountable for the decision [a), b), c), d), e), h)].
– <e)3)>: Feeding back the analysed requirements to applicable stakeholders is a part of the feedback loops [g)].
– <f)1)>: The explicit agreement on stakeholder requirements should identify the accountability for each item of the agreement [c), d), e), h)].
– <f)2)>: Assignment of accountability should be traced [b)]. Traceability should be maintained in a manner suitable to achieve [c), d), e), i)]. Stakeholder requirements should be traced to requirements for system monitoring [f), g)].
– <f)3)>: An account of the selection of the key information items for baselines should be recorded for use in achieving [i)].

<6.4.3> System requirements definition process

– <a)1), b)2), b)4), d)3)>: Definition of the functional boundary, implementation constraints, system requirements and selection of the key information for baselines involve key decisions [a)] and should be considered together with [b), c), d), e), h)].
– <a)1)>: The functional boundary should be defined together with the boundary of accountability [a), b), c), d), e), h)].
– <b)1)>: Functions should be defined together with accountability for their fulfilment [a), b), c), d), e), h)].
– <b)3)>: Risk-related and critical system requirements should be identified together with accountability for them [c), d), e)].
– <b)4)>: Definition of stakeholder requirements and rationale should clarify the key decisions that influenced the definition and accountability for the requirements [a), b), c), d), e), h)].
– <c)>: Accepting the result of the system requirements analysis as appropriate is a key decision and the person responsible for the System requirements definition process is accountable for this decision [a), b), c), d), e), h)].
– <c)3)>: Feeding back the analysed requirements to applicable stakeholders is a part of the feedback loops [g)].
– <d)2)>: Assignment of accountability should be traced [b)]. Traceability should be maintained in a manner suitable to achieve [c), d), e), i)].

<6.4.4> Architecture definition process

– <a)1), a)2), a)4), b), d)1), d)2), e)3), f)2)>: The following involve key decisions [a)] and should be considered together with [b), c), d), e), h)]: identification of key drivers, identification of stakeholder concerns, definition of evaluation criteria, definition of architecture viewpoint, identification of system elements, definitions of the interfaces and interactions between the system elements and with external entities, selection of the architecture and acceptance of the architecture.
– <a)4)>: The evaluation criteria for architectures should include that of the accountability described in candidate architectures.
– <c)>: Models and views that clarify how outcomes [a), b), c), d), e), h)] are achieved should be developed.
– <d)>: The relation between architecture and design should include mapping of accountability.
– <f)6)>: Assignment of accountability should be traced [b)]. Traceability should be maintained in a manner suitable to achieve [c), d), e), i)].
– <f)7)>: An account of the selection of the key information items for baselines should be recorded for use in achieving [i)].

<6.4.5> Design definition process

– <b)1), b)2), b)5), c), d)4)>: The following involve key decisions [a)] and should be considered together with [b), c), d), e), h)]:
  - allocation of system requirements to system elements;
  - transformation of architectural characteristics into design characteristics;
  - definition of the interface between the system elements and with external entities;
  - identification of Non-Developmental-Items (assessment of alternatives for obtaining system elements);
  - selection of the key information items for baselines.
– <b)1)>: Allocation of system requirements to system elements should allocate accountability as well [b), c), d), e), h)].
– <b)2)>: When architectural characteristics are transformed to design characteristics accountabilities for these should also be assigned. [b), c), d), e), h)].
– <b)5)>: Interfaces of system elements should be defined together with the scope of accountabilities for them [b), c), d), e), h)].
– <c)>: The accountability for Non-Developmental-Items should be clarified [b), c), d), e), h)].
– <d)3)>: Traceability of accountabilities should also be maintained [b), c), d), e), h), i)].
– <d)4)>: An account of the selection of the key information items for baselines should be recorded for use in achieving [i)].

<6.4.6> System analysis process: Accounts of the following should be recorded for use as adequate information in [i)]:

– <a)1)>: identification of the problem that requires system analysis;
– <a)2)>: identification of the stakeholders of the system analysis;
– <a)3)>: definition of the scope, objectives, and level of fidelity of the system analysis;
– <b)1)>: identification of assumptions;
– <b)4)>: establishment of analysis conclusion(s);
– <c)2)>: selection of key information item for baselines.

<6.4.7> Implementation process

– <a)1), a)2)>: Definition of the implementation strategy, identification of implementation constraints and implementation technology involve key decisions [a)] and should be considered together with [b), c), d), e), h)].
– <c)>: Accounts of establishment of the criteria used to discern anomalies and selection of key information items for baselines should be recorded for use in achieving [i)].
– <c)2)>: Traceability of the accountability for implemented system elements should also be maintained [b), c), d), e), h), i)].

<6.4.8> Integration process

– <a)5)>: The system constraints to accommodate integration should be incorporated into the system requirements, architecture or design as a part of the feedback [g)].
– <c)1), c)3)>: Accounts of how the criteria used to discern anomalies were established and selection of the key information items for baselines should be recorded for use in achieving [i)].
– <c)2)>: Traceability of the accountability for integrated system elements should also be maintained [b), c), d), e), h), i)].
– <b)1), b)3)>: Accepting the implemented system elements and judging that results from checking interfaces, etc., are satisfactory, are key decisions [a)] and should be considered together with [b), c), d), e), h)].

<6.4.9> Verification process

– Accounts of the following should be recorded for use as adequate information in [i)]:
  - <a)1)>: identification of the verification scope and corresponding verification actions;
  - <b)>: performance of verification;
  - <c)1)>: how the criteria used to discern anomalies were established;
  - <c)3)>: obtaining the stakeholder agreement that the system or system element meets the specified requirement;
  - <c)5)>: selection of key information items for baselines.
– <a)5)>: The system constraints to accommodate verification should be incorporated into the system requirements, architecture or design as a part of the feedback [g)].
– <c)3)>: Confirming that the system or system element meets the specified requirements is a key decision [a)] and should be considered together with [b), c), d), e), h)].
– <c)4)>: Traceability of the accountability for verified system elements should also be maintained [b), c), d), e), h), i)].

<6.4.10> Transition process

– The following involve key decisions [a)] and should be considered together with [b), c), d), e), h)]:
  - <a)1)>: definition of the transition strategy;
  - <a)2)>: identification of needed facility or site changes;
  - <a)3)>: identification of necessary training of operators, users and other stakeholders;
  - <b)10)>: the decision to commission the system for operation.
– Accounts of the following should be recorded for use as adequate information in [i)]:
  - <b)4)>: judgement that the system is properly installed;
  - <b)6)>: judgement that the check-out of the installed system validates the fulfilment of stakeholder requirements in the operational environment;
  - <b)7)>: judgement that the capability of the installed system to deliver required functions is demonstrated;

- <b)8)>: judgement that the sustainability of the installed system by the enabling systems is demonstrated;
- <b)9)>: judgement that the operational readiness is demonstrated by the review;
- <c)1), c)2)>: establishment of the criteria used to discern anomalies, operational incidents and problems;
- <c)3)>: selection of key information items for baselines.

– <a)1)>: The transition strategy should include assignment of accountability [b), c), d), e), h)].

– <a)3)>: Identification of necessary training of operators, etc., should include identification of their accountability [b), c), d), e), h)].

– <a)4)>: The system constraints to accommodate transition should be incorporated into the system requirements, architecture or design as a part of the feedback [g)].

– <b)5)>: Training of operators, etc., should include communication of their accountability [b), c), d), e), h)].

– <b)9)>: Review of the operational readiness should review the prospect of accountability achievement in the installed environment [b), c), d), e), h)].

– <c)3)>: Traceability of the accountability for transitioned system elements should also be maintained [b), c), d), e), h), i)].

<6.4.11> Validation process

– Accounts of the following should be recorded for use as adequate information in [i)]:
  - <a)1)>: identification of the validation scope and corresponding validation actions;
  - <b)>: performance of validation;
  - <c)1)>: establishment of the criteria used to discern anomalies;
  - <c)3)>: obtaining the stakeholder agreement that the system or system element meets the stakeholder needs;
  - <c)5)>: selection of key information items for baselines.

– <b)3), c)3)>: Confirming that the system or system element meets the stakeholder needs is a key decision [a)] and should be considered together with [b), c), d), e), h)];

– <b)3)>: Review of the validation results should review the prospect of accountability achievement [b), c), d), e), h)].

– <c)4)>: Traceability of the accountability for transitioned system elements should also be maintained [b), c), d), e), h), i)].

<6.4.12> The Operation process is at the core of the Accountability Achievement [f), g), h), i)].

– The following involve key decisions [a)] and should be considered together with [b), c), d), e), h)]:
  - <a)1)>: definition of the operation strategy;
  - <a)2)>: identification of system constraints from operation to be incorporated in the system requirements, architecture, or design;
  - <a)3)>: identification of and planning for the necessary enabling systems or services needed to support operation;
  - <a)6)>: assignment of trained, qualified personnel to be operators;
  - <b)3)>: definition of monitored data-items;
  - <b)5)>: decision whether or not to perform contingency operations.

– Accounts of the following should be recorded for use as adequate information in [i)]:
  - <b)4)>: definition of the acceptable parameter ranges of service performance;
  - <c)1), c)2)>: establishment of the criteria used to discern anomalies, operational incidents and problems;

- <c)4)>: selection of the key information items for baselines;
- <d)3)>: determination of the degree to which delivered system services satisfy the needs of the customers.

– <a)1)>: The operation strategy should clarify the assignment of accountability for monitoring and customer support [b), c), d), e), f), g), h), i)].

– <a)3)>: Identification of the enabling systems for operation should include identification of the boundary of accountability between the system and enabling systems [b), c), d), e), h)].

– <a)6)>: Training and qualification of operators includes their awareness of accountability [h)].

– <b)3)>: Monitoring of system operation should cover anticipated and unanticipated outcomes from decisions broadly across the system [f)]. Monitoring should form a part of the feedback loops [g)]. Monitoring should enable prompt identification of accountable stakeholders and provision of accountability information upon anomalies and failures [h), i)]. Traceability between monitoring actions and breach of agreement in [6.3.2] should be established through the chain of accountability maintained in <6.4.5 d)3), 6.4.7 c)2), 6.4.8 c)2), 6.4.9 c)4), 6.4.10 c)3), 6.4.13 d)4)>.

– <b)4)>: Operational anomalies in relation to agreements, stakeholder requirements and organizational constraints should be identified, analysed and recorded using the System analysis process [h), i)].

– <b)5)>: Contingency operations should include initiation of corrective actions by accountable stakeholders [h)] and a timely provision of accountability information [i)3)].

– <c)2)>: Resolution of operational incidents and problems should be tracked to accountable stakeholders and actions they took [h), i)].

– <c)3)>: Traceability of accountability for operations elements should also be maintained [b), c), d), e), h), i)].

– <d)1), d)2)>: Customer support should provide trustworthy information upon request promptly [i)1), i)2)], upon failures [i)3)], when changes occur [i)4)], and when a performance gap is found [i)5)].

– <d)3)>: Determination of the degree of customer satisfaction should be performed as a part of the feedback loops. Satisfaction of stakeholders should be monitored together with the degree of their accountability achievement [f), g)].

<6.4.13> Maintenance process

– The following involve key decisions [a)] and should be considered together with [b), c), d), e), h)]:
  - <a)1)>: definition of the maintenance strategy;
  - <a)2)>: identification of the system constraints from maintenance;
  - <b)1)>: identification of future corrective, adaptive, perfective and preventive maintenance needs;
  - <b)5)>: decision whether or not to perform preventive maintenance;
  - <b)6)>: identification of failures;
  - <b)7)>: identification of needs for adaptive or perfective maintenance;
  - <c)5)>: confirmation that logistics actions include supportability requirements that are planned, resourced, and implemented;
  - <d)3)>: identification of trends of incidents, problems, and maintenance and logistics actions.
– Accounts of the following should be recorded for use as adequate information in [i)]:
  - <a)3)>: identification of trades for the system, maintenance and logistics actions;
  - <d)1), d)2)>: establishment of the criteria used to discern anomalies, operational incidents and problems;

- <d)6)>: determination of the degree of customer satisfaction with system and maintenance support;
- <d)5)>: selection of key information items for baseline.

– <a)2)>: The system constraints to accommodate maintenance should be incorporated into the system requirements, architecture or design as a part of the feedback [g)].

– <b)1)>: Review of incidents and problems for identification of future maintenance needs should examine obtained degree of achievement for [b), c), d), e), h)].

– <b)2), d)2)>: Resolution of maintenance and operational incidents should be tracked to accountable stakeholders and their actions [h), i)].

– <d)4)>: Traceability of the accountability for maintenance elements should also be maintained [b), c), d), e), h), i)].

– <d)6)>: Determination of the degree of customer satisfaction should be performed as a part of the feedback loops; satisfaction of stakeholders should be monitored together with the degree of their accountability achievement [f), g)].

<6.4.14> Disposal process

– The following involve key decisions [a)] and should be considered together with [b), c), d), e), h)]:
  - <a)1)>: definition of the disposal strategy;
  - <a)2)>: identification of system constraints from disposal to be incorporated in the system requirements, architecture, or design;
  - <a)5)>: specification of containment facilities, storage locations, inspection criteria and storage periods (if the system is to be stored);
  - <a)6)>: definition of preventive methods to preclude disposed elements and materials that should not be repurposed, reclaimed or reused from re-entering the supply chain;
  - <b)1)>: decision to deactivate the system or system element to prepare it for removal;
  - <b)3)>: selection, in order to be recorded, of operating knowledge relevant to safety, security, privacy and environmental standards, directives and laws;
  - <c)1)>: confirmation that no detrimental health, safety, security and environmental factors will exist following disposal.

– <c)3)>: An account of the selection of information to be archived should be recorded for use in adequate information in [i)].

– <c)>: Finalization of disposal should confirm that no accountability issues remain for the disposed system [i)].

6.4 Failure Response process view

6.4.1 Purpose

The purpose of the Failure Response process view is to continue the provision of the service as much as possible, with the least possible disruption and damage, in the manner most expedient in the context.

The Purpose should be achieved taking the following into account.

Failures might be unforeseen, or foreseen but deemed too improbable or costly to prevent, or foreseen and dealt with but not prevented due to unanticipated events.

No remedies specific to unanticipated events causing failures can be prepared. However, generic measures can be prepared in advance to enable their expeditious execution. These include procedures to quickly form countermeasures specific to the failure in the context at hand, changing the context if necessary. Guarding against conceivable forms of failures, regardless of their causes, also leads to such generic measures.

Human intervention plays a key role since not all failures can be prevented or mitigated by preprogramed means. For quick and appropriate response, human intervention should be supported by computers for decision-making and implementation of decided actions.

The Failure Response process view prepares ex post facto means to manage damaging consequences of system operations. These post-failure actions include measures against identified consequences for which no causes can be imagined at the time of identifying the consequences. Preparation for such consequences is possible but only through preparing what to do after such consequences manifest themselves.

The Failure Response process view identifies actions taken against faults, errors, failures and their precursors. Failure response includes failure prevention following detection of precursors, contingency operations upon detection of failures and corrective and preventive maintenance.

Achievement of the Purpose consists of the following:

– preparation for failure response [6.4.2 outcomes a)1) to a)8)];
– performance of failure response upon failures [b)1) to b)8)];
– achieving accountability regarding failures and failure response [c)1) to c)4)];
– improving the system life cycle with experience from failures [d)1), d)2)].

The relationship between the purpose and the outcomes is described in Clause B.4.

6.4.2 Outcomes

a) Failure response is prepared.
   1) Key functions to be protected in order to ensure service continuity are identified.
   2) Goals for protection of the key functions necessary for continuous provision of service are identified.
   3) Faults, errors, failures and their precursors that impact the key functions are identified.

   NOTE 1 There are unidentified faults, errors, failures and their precursors including those that are not foreseen and have not been recognized by any of the stakeholders.

   NOTE 2 Interaction errors are addressed in the identification and detection of faults, errors, failures and their precursors.

   4) Consequence analysis and likelihood analysis of the identified faults, errors, failures and their precursors are performed.

   NOTE 3 Assumptions made for the analysis at the preparation time are checked before responding to actual failures, etc. See b)2) below.

   5) For the identified faults, errors, failures and their precursors, the goals of treatment necessary for continuous provision of service are defined and agreed.

   NOTE 4 The goals include those of damage prevention.

   6) Disposition towards the treatment of each identified fault, error, failure and their precursors is chosen from the following classes:
      i) to be monitored and to be prepared for in design;
      ii) to be monitored but not to be prepared for in design;
      iii) not to be monitored and not to be prepared for in design.

   NOTE 5 “prepared for in design” means that the system is designed to provide a set of specific responses to it that enables service continuity.

   7) Specific responses that protect the key functions from faults, errors, failures and their precursors in class a)6)i) and default responses to those in class a)6)ii) and a)6)iii) are developed.

   NOTE 6 The specific responses will be based on the result of consequence analysis and likelihood analysis. These responses are to be performed by the system, as well as by personnel relating to the system life cycle.

NOTE 7 The specific responses include post-failure actions.

NOTE 8 Failures of the post-failure actions are considered. Post-failure actions for such failures can be provided in several layers and applicable recursively to their own failures.

8) Generic measures to reduce the harm from failures with unidentified causes are developed.

NOTE 9 Generic measures include identification of faulty parts of the system promptly, isolation of the malfunctioning parts in order to protect other normally operating parts, sustainment of surviving services at a level agreed by stakeholder consensus, and recovery from failure.

b) Failure response is performed when necessary.

1) Faults, errors, failures and their precursors are detected.

2) Cause analysis and consequence analysis of the actual fault, error, failure or their precursor are performed.

NOTE 10 The consequence analysis after detection of failures, etc., examines the assumptions made in the analysis before detection against the actual situation at hand and confirm or modify the analysis results.

3) The goal of treatment for the detected faults, errors, failures and their precursors is refined for the situation at hand.

4) The specific responses to the faults, errors, failures and their precursors in the class a)6)i) and the default responses to those in the class a)6)ii) and a)6)iii) are performed when detected.

5) Responses to the actual faults, errors, failures and their precursors in the class a)6)ii) and a)6)iii) are devised after the event.

NOTE 11 Monitoring in the class a)6)ii) enables more prompt recognition of failures, etc., with more detailed data for formation of responses compared to the case of no monitoring in the class a)6)iii).

6) The responses to the faults, errors, failures and their precursors do not aggravate the harm and do not increase the risk of further harm.

NOTE 12 In some cases, mitigating activities cause new harm. It is to be expected that such activities do not cause more harm than would have occurred in the absence of such intervention.

7) Harm to the system of interest and the systems connected to it is reduced as a whole.

8) The responses to the detected failures are assessed with respect to the goal refined in b)3).

c) Failure response is accounted by the Accountability Achievement process view.

1) Damage caused by failures is compensated according to the established agreement.

2) Confidence and trust in the system is sustained.

NOTE 13 For example, this is achieved by dissemination, after each failure response, of (1) an assurance case assuring that the response achieved or will achieve its goals and (2) the revised assurance case for the system life cycle (Clause 5) assuring that future recurrences are prevented.

3) Stakeholders and society in general are informed of the account of the failure response. This information includes:

i) justification of the scope of the identified set of faults, errors, failures and their precursors;

ii) justification of the response plan for the detected faults, errors, failures and their precursors;

iii) the result of consequence analysis of detected fault, errors, failures or their precursors;

iv) the result of the failure response and its assessment.

4) Necessary information is provided to the Accountability Achievement process view.

NOTE 14 Disruptive changes can cause failures that have no accountable stakeholders as well as those that are impossible to respond to. Provision of the necessary information to the Accountability Achievement process view enables such disruptive changes to be recognized promptly and to be relayed to the Change Accommodation process view that addresses the disruptive changes.

d) The system life cycle is improved based on the experience from the actual failures after the failure response by the Change Accommodation process view.

1) The goal of improvement is defined and agreed.

NOTE 15 The goal includes prevention of recurrence of failure, improvement of the operation strategy, refinement of the system purposes, improvement of processes for fault identification and risk management. Defining the goal involves identification of actual failure consequences according to the consequence analysis, evaluation of harm, and that of value of the system's services.

2) Necessary information is provided to the Change Accommodation process view.

6.4.3 Processes, activities and tasks

The Failure Response process view should be implemented using the activities and tasks of the following processes provided by ISO/IEC/IEEE 15288.

<6.1.1> Acquisition process

– <c)1)>: The agreement between the acquirer and the supplier should identify key functions to be protected from failures and the goals of protection [a)1), a)2), a)5)].

– <d)1)>: Assessment of the agreement execution should confirm that the protection goals in <c)1)> and outcomes [b), c)] are achieved and assured.

<6.1.2> Supply process

– <c)1)>: The agreement between the acquirer and the supplier should identify key functions to be protected from failures and the goals of protection [a)1), a)2), a)5)].

– <d)2)>: Assessment of the agreement execution should confirm that the protection goals in <c)1)> and outcomes [b), c)] are achieved and assured.

<6.2.1> Life cycle model management process

– <a)5)>: The established life cycle models should specify the linkages among life cycle processes that enables achievement of all outcomes of the Failure Response process view [a), b), c), d)].

<6.2.4> Human resource management process

– <a)>: Skills to be identified include the skills necessary to understand the system purpose and skills necessary to apply the understanding of the system's purpose to devising human intervention that achieves outcomes [a)7), a)8), b)].

<6.2.5> Quality management process

– <b)>: Assessment of quality management should review whether it detects and treats the faults, errors, failures and their precursors identified in [a)3)] as anticipated [b), c)].

<6.3.2> Project assessment and control process

– <a)>: The project assessment and control strategy should reflect the common understanding established in [6.2.2 a)] to support

- development of the generic measures against failures not prepared for in design and failures with unidentified causes [a)8)],
- refinement of the failure treatment goals [b)3)],
- devising of responses to failures not prepared for in design [b)5)].

– <c)>: The project control should include adoption of the Change accommodation process view to adapt the system for failure recurrence prevention [d)].

<6.3.4> Risk management process

– <a)1), a)2), b)2), c), d)1), d)2), d)4), e)>: Processes and procedures for managing and assessing risk are given in ISO 31000 [16] and IEC 31010 [17]. In addition, the following should be identified [a), b)8)]:

  - means to communicate and consult about risks and their controls and treatments;
  - means to reduce the harm from failures with unidentified causes;
  - means to reduce harm from the system as well as other systems connected to it;
  - results of consequence analysis and likelihood analysis in an objective written form;
  - a list of harmful events that could happen, a list of harmful events that are judged to be improbable but decided to be monitored, and a list of harmful events that are judged to be improbable and decided not to be monitored;
  - objective description of the justification of the adequacy of the set of means to detect faults, errors, failures and their precursors;
  - means to adapt the system to the changes with regard to failures.

<6.4.2> Stakeholder needs and requirements definition process

– <b)2)>: Stakeholder needs should be identified together with the needs for protection from failures [a)1), a)2)]. Stakeholder needs should include the need not to cause harm to the system of interest and the systems connected to it as a whole [a)8), b)7)].

– <c)1)>: Analysis of the representative scenarios should help identifying key functions to be protected [a)1)]. It includes risk analysis of failures in order to define the needs for protection from failures [a)2)] and to analyse harm that the system of interest might cause to the systems connected to it [b)7)].

– <d)2)>: Identification of the stakeholder requirements and functions includes designation of the key functions to be protected from failures [a)1)] and the goal of protection [a)2)]. The stakeholder requirements should include the requirements that the system of interest does not cause harm to itself and the systems connected to it as a whole [b)7)].

– <e)1)>: Analysis of the complete set of the stakeholder requirements should include risk analysis of key function failures in order to define the goals for their protection [a)2)], to consider generic measures against failures with unidentified causes [a)8)] and to consider the harm that the system of interest might cause to any system connected to it [b)7)]. The analysis should identify faults, errors, failures and their precursors that impact the key functions and their consequences [a)4), a)5)].

– <e)2)>: Critical performance measures should include measures of degrees of protection for the key functions [a)2)] and of treatment for failures, etc. [a)5)].

– <f)1)>: The agreement on the stakeholder requirements should list the key functions to be protected [a)1)], the goals of protection of the key functions [a)2)] and the goals of treatment for failures, etc., that impact the key functions [a)5)].

<6.4.3> System requirements definition process

– <b)1)>: Definition of the key functions should include the following:

  - goals of protection from failures [a)2)];
  - identification of faults, errors, failures and their precursors that impact the function, including interaction errors [a)3)];
  - goals of treatment for the identified faults, etc. [a)5)];
  - classification of treatment for each identified fault, etc. [a)6)].

– <b)3)>: Identification of system requirements that relate to risks, etc., should enable identification of key functions to be protected from failures [a)1)]. The following should be identified:

  - requirements for protection of the key functions [a)2)];

- requirements for the treatment of relevant failures, etc. [a)5)];
- requirements that failure responses do not aggravate the harm from failures and do not increase the risk of further harm [b)6)];
- requirements for monitoring of failures, etc., to be detected [b)1)];
- requirements for any reduction of harm which the system of interest might cause to the systems connected to it [b)7)].

– <b)4)>: Definition of the system requirements and rationale should clarify the following:

- requirements for the key function protection [a)2)] and those for the treatment of failures, etc. [a)5)];
- traceability between the above requirements and their source functional requirements [c)].

– <c)1)>: Analysis of the complete set of system requirements should include consequence analysis of potential failures of the key functions [a)4)] that enables the following:

- definition of the goals for key function protection [a)2)] and the goals for treatment of identified faults, etc. [a)5)];
- development of generic measures against failures with unidentified causes [a)8)];
- avoiding aggravation of the harm and the increase of risk to further harm by failure responses [b)6)];
- reduction of harm that the system of interest might cause to any system connected to it [b)8)].

– <c)2)>: The critical performance measures should include measures of the degree of protection for the key functions [a)2)] and of treatment for failures, etc. [a)5)].

– <d)1)>: The agreement on system requirements should list the key functions to be protected [a)1)], the goals of protection of the key functions [a)2)] and the goals of treatment for failures, etc., that impact the key functions [a)5)].

– <d)2)>: Traceability between the requirements for monitoring and the requirements for the key functions should be maintained to enable the accountability of failure response [b)1), c)].

<6.4.4> Architecture definition process

– <a)2)>: The identified stakeholder concerns should be reflected in the goals of protection of the key functions [a)2)] and the goals of treatment for faults, etc. [a)5)] in iterations of the Architecture Definition process with the Stakeholder Needs and Requirements Definition process and the System Requirements Definition process. The stakeholders' concerns regarding harm to the system connected to the system of interest should be identified [b)7)].

– <c)>: Models and views should be developed that address the treatment of failures, etc. [a)5), a)6)], their detection [b)1)], and specific and generic failure responses [a)7), a)8)]. Interactions among failure responses and other system functions should be addressed to avoid aggravation of the harm by failure responses [b)7)].

– <c)2)>: Key architectural entities that relate to the key functions and to their protection should be identified [a)1), a)7)].

– <d)1)>: Key system elements that relate to key architectural entities for key function protection should be identified [a)1), a)7)].

– <d)2), d)3)>: Interaction errors, their detection, and specific and generic responses to them should be taken into consideration when defining interfaces between system elements and with external entities and when partitioning requirements to system elements [a)3), b)1), a)7), a)8)]. Interactions between failure responses and other system functions should be considered to avoid aggravation of the harm by failure responses [b)6)].

– <f)2)>: Acceptance of the architecture by stakeholders should include that of architecture for the treatment of failures, etc. [a)6)], specific failure responses [a)7)], generic responses [a)8)] and detection [b)1)].

– <f)6)>: Traceability between the goals of treatment for failures, etc. [a)5)] and the architecture for the treatment of failures, etc. [a)6)], specific failure responses [a)7)], generic

responses [a)8)] and detection [b)1)] to the goals of protection [a)2)] should be maintained for accounting of failure response [c)].

<6.4.5> Design definition process

– <a)2)>: Design characteristics related to the generic measures against failures with unidentified causes [a)8)] should be determined.
– <a)3)>: The principles for evolution of the design should provide guidance as to the Change Accommodation process view after failure response [d)].
– <b)1)>: The requirements for protection of the key functions [a)2)] and for treatment of faults, etc. [a)5)] should be allocated to system elements.
– <d)3)>: Traceability from design characteristics for the treatment of failures, etc. [a)6)], specific failure responses [a)7)], generic responses [a)8)] and detection [b)1)] to the architectural entities for key function protection [a)2)] and the goals of fault treatment [a)5)] should be maintained for accounting purposes [c)].

<6.4.6> System analysis process

– <c)1)>: Traceability of the system analysis results should be maintained in a manner that enables timely accounting of failure response [c)].

<6.4.7> Implementation process

– <c)2)>: Traceability from the following to design characteristics should be maintained for accounting of failure response [c)]:
  - implemented system elements for the treatment of faults, errors, failures and their precursors [a)6)];
  - specific failure responses [a)7)];
  - generic responses [a)8)];
  - detection of faults errors, failures and their precursors [b)1)];

<6.4.8> Integration process

– <a)1)>: The check points for the correct operation and integrity of the assembled interfaces and the selected system functions should include the following:
  - interfaces of the key functions identified in [a)1)];
  - interfaces of functions to protect the key functions [a)2), a)5), a)7), b)1), b)5)];
  - checking of interaction errors between system elements [a)2), a)8), b)7)];
  - checking of system-wide generic measures against failures [a)8), b)6), b)7)];
  - checking that failure responses do not aggravate the harm and do not increase the risk of further harm [b)6)];
  - checking of potential harm that the system of interest might cause to any systems connected to it [b)8)].
– <b)3)>: Checking of the interfaces, selected functions, and critical quality characteristics includes the following:
  - identification of potential interaction errors [a)3), a)7), b)7)];
  - checking effectiveness of the generic measures against failures [a)8)];
  - checking that failure responses do not aggravate the harm and not increase the risk of further harm [b)6)];
  - checking the potential harm which the system of interest might cause to any systems connected to it [b)8)].
– <c)2)>: Traceability of the integrated system elements should be maintained in a manner that enables prompt failure responses [b)] and timely accounting of failure responses [c)].

<6.4.9> Verification process

– <a)1)>: The verification scope and actions should include verification of achievement of the goals of key function protection [a)2)] and treatment for failures, etc. [a)5)].
– <c)2)>: Operational incidents should be recorded and tracked to resolutions in a manner that enables timely accounting of failure response [c)].
– <c)3)>: The agreement among stakeholders that the specified requirements are met should include an agreement that the goals of treatment for failures, etc., are met [a)5)].
– <c)4)>: Traceability of the verification results should be maintained in a manner that enables prompt failure response [b)] and timely accounting of failure response [c)].

<6.4.10> Transition process

– <b)5)>: Training of operators, etc., should be planned as a part of the generic responses and measures against failures [a)7), a)8)]. Training should also develop skills of stakeholders to achieve [b)] through human intervention.
– <b)9)>: Review of the operational readiness should confirm that the achievement of goals in [a)2), a)5), a)8), b)1) to b)7)] has been demonstrated.
– <c)2)>: Operational incidents should be recorded and tracked to resolutions in a manner that enables timely accounting of failure response [c)].
– <c)3)>: Traceability of the transitioned system elements should be maintained in a manner that enables prompt failure response [b)] and timely accounting of failure response [c)].

<6.4.11> Validation process

– <a)1)>: The validation scope and actions should include the following:
  - validation of the key function protection with respect to their goals [a)2)];
  - validation of the treatment for failures, etc., with respect to their goals [a)5)];
  - validation of the generic measures against failures with unidentified causes [a)8), b)1), b)4) to b)7)].
– <c)2)>: Operational incidents should be recorded and tracked to resolutions in a manner that enables timely accounting of failure response [c)].
– <c)4)>: Traceability of the validated system elements should be maintained in a manner that enables prompt failure response [b)] and timely accounting of failure response [c)].

<6.4.12> Operation process

– <a)1)>: The operation strategy should include the following procedures for [b)]:
  - procedures for detection of failures, etc. [b)1)] and for prediction of failures from their precursors;
  - procedures for monitoring failures, etc., in classes i) and ii) of [a)6)];
  - procedures for [b)3)] and [b)5)] that ensure readiness for prompt human intervention upon detection of failures, etc.
– <a)5)>: Training of personnel should be planned as part of the generic measures in [a)8)] and should develop the ability of stakeholders to achieve [b)] through human intervention that reflects understanding of the system purpose. The qualification requirements should include those for the aforementioned ability.
– <b)3)>: Monitoring of system operation should include monitoring of the faults, errors, failures and their precursors in class i) and ii) of [a)6)] so as to enable their detection [b)1)]. When failures, etc., are detected, procedures in the operation strategies that achieve outcomes [b)2) to b)7)] should be performed and the result should be assessed [b)8)].
– <b)4)>: Identification of unacceptable performance should include assessment of failure response [b)8)] and should invoke the Change Accommodation process view for system improvement [d)].

– <b)5)>: Goals of system contingency operations necessary for continuous provision of services and the condition that triggers the contingency operations should be included in the goals of key function protections in [a)2)] and the goals of treatment for failures, etc., in [a)5)].
– <c)1)>: Results of operations and anomalies should be recorded in a manner that enables accounting of failure response [c)] and system improvement [d)].
– <c)2)>: Operational incidents and problems should be recorded and tracked in a manner that enables accounting of failure response [c)] and system improvement [d)].
– <c)3)>: Traceability of the operations elements should be maintained in a manner that enables prompt failure response [b)] and timely accounting of failure response [c)].
– <d)>: Customer support should actively provide accounts of failure response [c)].

<6.4.13> Maintenance process

– <a)1)>: The maintenance strategy should reflect the goals of key function protection [a)2)] and the goals of treatment of failures, etc. [a)5), b)].
– <b)1)>: Identification of future maintenance needs should be integrated with identification and detection of faults, etc. [a)3), b)1)].
– <b)2)>: Maintenance incidents and problems should be recorded and tracked in a manner that enables accounting of failure response [c)] and system improvement [d)].
– <b)3), b)4)>: Treatment of random faults should be integrated in the Failure Response process view [a), b), c), d)].
– <b)5)>: Preventive maintenance may be chosen as a means to achieve the goal of treatment for identified faults, etc. [a)5), a)7)].
– <b)6)>: Failure identification actions are a part of achieving [b)1), b)2)].
– <c)>: Logistics support should be included in specific responses to failure precursors in [a)7), b)4)].
– <d)1)>: Maintenance results, logistics results and anomalies should be recorded in a manner that enables accounting of failure response and system improvement [c), d)].
– <d)2)>: Operational incidents and problems should be recorded and tracked in a manner that enables accounting of failure response and system improvement [c), d)].
– <d)3)>: Identification of trends of incidents and problems should be performed to promote improvement of the system life cycle [d)].
– <d)4)>: Traceability of the maintenance elements should be maintained in a manner that enables prompt failure response [b)] and timely accounting of failure response [c)].
– <d)6)>: Monitoring of customer satisfaction should be integrated with assessment of failure response [b)8)] and improvement of the system life cycle [d)].

<6.4.14> Disposal process

– <a)1)>: The disposal strategy should be defined so as to enable [b)7)].

6.5 Change Accommodation process view

6.5.1 Purpose

The purpose of the Change Accommodation process view is to maintain the ‘fit for purpose’ status of the system despite changes in requirements, environments, objectives and/or purpose.

The Purpose should be achieved with the following understanding.

The process view sustains the ability to continue services by genuine solutions to problems caused by changes and focuses on ensuring that failures of the same kind will not recur.

There are many kinds of changes that require adaptations. Changes occur in other systems connected to the system. Changes in technological, business, and social environments are more frequent now with the rapid pace of innovation. Any detection of unanticipated events signals a change in the assumptions, which are always incomplete and uncertain. Changes might not be explicitly evident; often they must be actively sought out by, for example, periodic reviews. Required adaptations need not necessarily be about the system itself. The whole set of life cycle processes needs to be reviewed and adapted when necessary. Even influencing and changing the environment could be an adaptation.

The Change Accommodation process view organizes activities that arise when adapting the system to changes including: detecting changes; analysing them; forming and performing actions so as to continue possibly changed services and, where changes cause failures, to prevent manifestation or recurrence of failures.

Care should be taken that plans are not so rigid that an organization loses the ability to be flexible in the event of an unplanned situation.

Achievement of the Purpose consists of the following:

– performance and assessment of adaptation when changes occur [6.5.2 outcomes a) to d)];
– continual improvement of the system life cycle and achievement of accountability with respect to adaptation to changes [e), f)].

The relationship between the purpose and the outcomes are described in Clause B.5.

6.5.2 Outcomes

a) Changes are recognized and identified.

   1) Changes in context, assumptions, risks, etc., that might require adaptation of the system are identified.

   NOTE 1 Items subject to such changes include: stakeholder requirements; connected systems; the technological, business and social environment; stakeholders' perception of services; stakeholders' understanding of the consensus.

   NOTE 2 Changes might not be evident; often they are actively sought out by, for example, periodical reviews.

   2) Upon detection of unanticipated events including failures, the change in the system and/or environment that caused them is identified. This identification may be triggered by the Failure Response process view.

   NOTE 3 Any detection of unanticipated events including failures is a detection of a change. The change might be factual or that of understanding of assumed facts.

   3) Disruptive changes are recognized and managed.

   NOTE 4 Disruptive changes are those for which meaningful adaptation of the system by existing stakeholders is impossible or impracticable. This includes the case where the cost of necessary adaptation exceeds the sustainable business parameters of stakeholders held accountable in the agreement currently in effect. Orderly management of such cases can be pre-planned as much as possible in advance in terms of, for example, introduction of new stakeholders, ejection of non-performing stakeholders, rebuilding consensus anew or early disposal of the system.

b) Adaptation of the system is prepared.

   1) The changes' impacts on the 'fit for purpose' status of the system are assessed and the relationship between the changes and their impacts is documented.

   NOTE 5 Assessment includes causal analysis.

   2) The goal of adaptation to maintain the 'fit for purpose' status of the system is defined. This includes the following.

      i) Stakeholders are informed of the needs for adaptation, the choices for adaptation and their consequences.

      ii) Stakeholders obtain necessary support in the negotiation of agreements under the changed circumstances.

iii) Adaptation triggered by the Failure Response process view prevents recurrence of the failures.

iv) The goal of adaptation is defined.

3) The goal of adaptation is agreed and is reflected in the updated stakeholder agreement by invoking the Consensus Building process view.

NOTE 6 This includes making the decision to adapt the system.

NOTE 7 Particular care is taken in case of adaptation to disruptive changes.

c) Adaptation of the system is performed.

NOTE 8 Adaptation can be technical or non-technical. The whole set of life cycle processes is reviewed and adapted when necessary. Adaptation is not necessarily about the system itself. Even influencing and changing the environment could be an adaptation.

NOTE 9 Consideration of adaptations includes prevention of interaction errors between the parts of system that would change after adaptations and the parts that would be left unchanged.

1) Technical support for needed adaptation is available.

2) The knowledge obtained from the past experience is used effectively.

3) An adaptation that realizes the goal is defined.

4) The adaptation is developed.

5) The adaptation is deployed so that disruptions to the system's existing service in operation and to other connected systems are kept to a minimum.

d) The adapted system is assessed with respect to the goal of adaptation.

e) The system life cycle is improved continually.

NOTE 10 Continual improvement is expected on the system life cycle's ability to maintain the 'fit for purpose' status of the system. This is distinct from pursuit of ever higher system performance, etc.

f) Adaptation is accounted by adopting the Accountability Achievement process view.

1) Traceability from changes in context, etc., to the adaptation is maintained.

2) Stakeholders and society in general are informed of the account of the development and the result of the adaptation.

6.5.3 Processes, activities and tasks

The Change Accommodation process view should be implemented using the activities and tasks of the following processes provided by ISO/IEC/IEEE 15288.

<6.1.1> Acquisition process

– <c)1), c)4)>: Necessary support should be provided to stakeholders in the negotiation of agreement between the acquirer and the supplier under the changed context [b)2)ii)].

– <c)2), c)5)>: Necessary changes to the agreement should be identified from the goal of adaptation. The goal of adaptation should be represented as an updated agreement [b)3)].

– <c)3)>: Evaluation results of impact of changes to the agreement should be fed back to the definition of adaptation goal [b)].

– <d)1)>: A large deviation of the actual progress of the agreement execution from the planned should be identified as a change that might require adaptation [a)1)].

<6.1.2> Supply process

– <c)1), c)4)>: Necessary support should be provided to stakeholders in the negotiation of the agreement between the acquirer and the supplier under the changed context [b)2)ii)].

– <c)2), c)5)>: The necessary changes to the agreement should be identified from the goal of adaptation. The goal of adaptation should be represented as an update to the agreement [b)3)].

– <c)3)>: Evaluation results of impact of changes to the agreement should be fed back to the definition of adaptation goal [b)].

– <d)2)>: A large deviation of the actual progress of agreement execution from the planned should be identified as a change that might require adaptation [a)1)].

<6.2.1> Life cycle model management process

– <a)5)>: The established life cycle models should specify the linkages among life cycle processes that enables achievement of all outcomes of the Change Accommodation process view [a) to f)].

– <c)2)>: 'Lessons learned' in one iteration of change accommodation should be incorporated in the process improvement to enable application to future changes [e)].

<6.2.2> Infrastructure management process: Changes in the project infrastructure and infrastructure requirements should be identified as changes that might require adaptation of the system [a)].

<6.2.3> Portfolio management process

– <a)1)>: Identification of potential new or modified capabilities or missions should be performed as part of change identification and assessment of its impact [a)1), b)1)].

– <a)2)>: Prioritizing, selecting and establishing new business opportunities, etc., should inform assessment of the 'fit for purpose' status of the system and definition of adaptation goals in relation to other projects in the organization's portfolio [b)1), b)2)].

– <a)3)>: Definition of the project concerning the system, accountabilities and authorities should be consistent with the goal of adaptation of the system [b)2), b)3)].

– <a)4)>: The anticipated goals, objectives and outcomes of the project should provide a basis for assessment of the 'fit for purpose' status of the system and the definition of the goal of adaptation in relation to other projects in the portfolio [b)1), b)2)].

– <a)8)>: Authorization to commence adaptation of the system with the defined goal should be given taking into account its impacts on other projects within the organization's portfolio [b)3), c)].

– <b)1)>: Evaluation of viability of the project should be performed as a part of change identification and assessment of the 'fit for purpose' status of the system [a)1), b)1)].

– <b)2)>: Actions to continue or redirect the project concerning the system include making decisions as to whether to adapt the system or not and defining the goal of adaptation [b)3), b)2)].

<6.2.5> Quality management process

– <a)>: Quality management should be planned taking into account that quality management objectives change when the purpose of the system, etc., changes [a) to d)].

– <b)1)>: Gathering and analysing quality assurance evaluation results should be performed as a part of recognition and identification of relevant changes [a)].

– <b)2)>: Assessment of customer satisfaction should be used in assessment of the 'fit for purpose' status of the system [b)1)].

– <b)4)>: Monitoring the status of quality improvements should be performed as part of recognition and identification of relevant changes [a)] and assessment of the adapted system [d)].

– <c)1), c)2)>: Planning of corrective and preventive actions on quality management should be integrated with the definition of the goal of adaptation [b)2)].

– <c)3)>: Monitoring of corrective and preventive actions should be used in the assessment of the adapted system with respect to the goal of adaptation [d)].

<6.2.6> The Knowledge management process should maintain 'lessons learned' information from one iteration of change accommodation in order to enable application to future changes [c)2), e)].

<6.3.1> Project planning process

– <a)1)>: The project objectives should be identified together with their rationale that provides a basis for assessment of the 'fit for purpose' status upon changes [b)1)] and definition of the goal of adaptation [b)2)].
– <a)2)>: The project scope should include activities to achieve all outcomes of this process view [a) to f)]. Planning of actions for controlling the project (see <a)2) NOTE>) should address the case where the project objectives change [a)]. Changes in activities within the scope should be recognized and identified [a)].
– <a)3)>: The life cycle model defined for the project should specify the linkages among life cycle processes that enables achievement of all outcomes of Change Accommodation process view [a) to f)].
– <b)2)>: The achievement criteria for the life cycle stage decision gates should include criteria for an exit decision gate from the utilization stage that initiates Change Accommodation process view [a)].
– <b)4)>: The roles, responsibilities, accountabilities and authority for the Change Accommodation process view should be defined in a manner that enables accounting of change accommodation [f)].
– <b)5)>: Changes in the infrastructure and services required for the project should be recognized and identified [a)].
– <b)7)>: Communication of the plan for adaptation should enable the agreement on the goal of adaptation [b)3)] and should be used in accounting of adaptation [f)].

<6.3.2> The Project assessment and control process should govern and enable all outcomes of Change Accommodation process view [a) to f)]. In particular, the process should address changes in the technical objectives, the requirements and overall business objectives. This includes support to developers to devise possible adaptations, identification of changes in context, assumptions, risks and others that require adaptation of the system, identification of technical or non-technical means for adaptation required for each change.

– <b)>: Assessment of the project should include recognition and identification of changes [a)]. The project should be assessed with respect to the possibly changed project context, objectives and plans in order to assess the 'fit for purpose' status of the system [b)1)] and to define the goal of adaptation [b)2)].
– <b)7)>: The project management, technical review, audits and inspection should determine the necessity and readiness to proceed to adaptation of the system [a), b)].
– <b)8)>: Monitoring of the critical processes and new technologies should be performed as a part of recognition and identification of changes [a)].
– <b)9)>: Analysis of measurement results should identify changes and make recommendations for the goal of adaptation [a), b)2)].
– <b)11)>: A large deviation of the actual progress from the plan should be identified as a change that might require adaptation [a)1)].
– <c)>: The project controls include initiation of system adaptation as needed [b), c)].
– <c)1)>: The actions to be initiated for the project control include definition of the adaptation goal [b)2)].
– <c)2)>: The project should be re-planned reflecting the agreed adaptation goals and the updated agreement [b)3)].
– <c)4)>: The project should be authorized to proceed to adaptation of the system with the defined goals [b)3), c)].

<6.3.3> Decision management process

– <a)1), c)>: The decision management strategy should address changes in decision criteria due to changes in context, assumptions, risks, etc. Management of decisions should review past decisions when changes are recognized and identified [b)1), b)2)].

<6.3.4> Risk management process: Procedures and processes for managing and assessing risk in general are given in ISO 31000 [16] and IEC 31010 [17]. In addition, the following should be considered.

– <a)1)>: The risk management strategy should address changes in the risk management context and include procedures to review current risk controls when changes are recognized and identified [a), b)1), b)2)].
– <a)2)>: The risk management context and risk identification process should consider the risks associated with changes in the following [a)]:
  - stakeholder requirements;
  - connected systems;
  - technological, business and social environment;
  - stakeholders' perception of services;
  - stakeholders' understanding of the consensus.
– <b)1)>: The risk thresholds and acceptance criteria for the risk associated with changes should reflect the impact of the changes on the 'fit for purpose' status of the system [b)1)].
– <b)3)>: Provision of the risk profile to stakeholders should be performed as a part of negotiation on the goal of adaptation and accounting of adaptation [b)2), f)2)].
– <c)1)>: Identification of the risk associated with changes should be performed as a part of recognition and identification of changes [a)1)].
– <c)2), c)3)>: Estimation of the consequences of the risk associated with changes and evaluation against the risk thresholds should be performed as a part of assessment of the 'fit for purpose' status of the system [b)1)].
– <c)4)>: Defining recommended treatment strategies and measures for the risks associated with changes that do not meet their risk threshold is a part of defining the goal of adaptation [b)2)] and defining the adaptation to be performed [c)3)].
– <d)1)>: Identification of recommended alternatives for treatment of the risk associated with changes is a part of defining the goal of adaptation [b)2)].
– <d)2)>: Determination by stakeholders that actions on the risk associated with changes should be taken should be recorded in the updated stakeholder agreement [b)3)]. Implementing the treatment of the risk associated with changes is a part of the adaptation to be performed [c)3)] and its performance [c)4)].
– <e)1)>: Continual monitoring of all risks and the risk management context for change and re-evaluation of risks when changes occur should be performed as a part of recognizing and identifying changes [a)1)] and assessment of the 'fit for purpose' status of the system [b)1)].
– <e)2)>: The measures to evaluate the effectiveness of risk treatments should enable assessment of the adapted system [d)]. Monitoring the measures is a part of recognition and identification of changes [a)].

<6.3.5> Configuration management process

– <b)1)>: Identification of configuration items is crucial for recognition and identification of changes within the system [a)]. System elements whose change might require system adaptation should be identified as configuration items. Configuration items might be black box components.
– <b)2)>: Identification of the structure of system information should take into account the likelihood that the system structure itself might change unintentionally due to uncertainty and incompleteness within the system or deliberately by adaptation [a), f)].
– <b)3)>: Establishment of configuration item identifiers should enable the traceability between the configuration items introduced or modified for adaptation and the change that required the adaptation [f)].
– <b)4)>: Baselining should enable recognition and identification of changes within the system throughout the system life cycle [a)].

– <b)5)>: The agreement between the acquirer and the supplier that establishes a baseline should be used to define the goal of adaptation for future changes as an update to the baseline [b)3)].
– <c)>: Configuration change management should include the following:
  - analysis of the changes' impact to 'fit for purpose' status of the system [b)1)];
  - informing relevant stakeholders of possible adaptations [b)2)i)];
  - supporting stakeholders in negotiating and agreeing on the goal of adaptation [b)2)ii), b)3)].
– <c)4)>: Tracking and managing approved changes should support accounting of adaptation [f)]. The rationale for adaptation should be recorded as 'lessons learned' to be used in future adaptations [c)2)].
– <d)>: Configuration status accounting should include maintenance of traceability of configuration items together with rationales for items' changes [f)].
– <e)2)>: Verification of the product configuration should support recognition and identification of unintentional changes within the system due to uncertainty and incompleteness of the system [a)].
– <f)1)>: Approval of a system release should confirm that the release will be done in a manner that minimizes disruptions to the system's existing service and other connected systems [c)5)].

<6.3.6> The Information management process should enable the following:

– recognition and identification of changes by making available past and present information on items subject to changes [a)];
– provision of information on possible adaptations of the system to the stakeholders [b)2)i)];
– provision of information on past experience in developing adaptations [c)2)];
– provision of accounting of adaptation to stakeholders [f)].

<6.3.7> Measurement process

– <a)3)>: Information needs should be identified for recognition and identification of changes [a)] and assessment of the 'fit for purpose' status of the system [b)1)].
– <b)4)>: Measurement results should inform stakeholders of the significance of changes [a), b)].

<6.3.8> Quality assurance process

– <b)>: Evaluation of products and services should be performed as part of assessment of the adapted system with respect to the goal of adaptation [d)].
– <c)1)>: Evaluation of project life cycle processes should enable continuous improvement of the system life cycle [e)].
– <e)>: For each treated incident and problem, consideration should be given to whether or not there is a change that might require system adaptation [a)2)].

<6.4.1> Business or mission analysis process

– <a) to e)>: The Business or mission analysis process should be adopted whenever necessary to achieve [a), b)] (cf. <6.4.1.1 NOTE 2>). The conditions for adoption include the following:
  - when changes are detected in Operation process and Maintenance process;
  - when the Failure Response process view defines the goal of life cycle improvement after failure response;
  - when changes in inputs to this process are identified.

NOTE 1 Inputs to the Business or mission analysis process that might change include organization strategy, identified problems and opportunities therein, organization goals and objectives, enabling systems or services to be used [a)1) NOTE 1].

The result of the Business or mission analysis process should include explicit agreements among stakeholders as to whether or not to initiate system adaptation and the possible goals of adaptation as in [b)3), b)2)].

– <a)1)>: The organization strategy should define triggers for periodical reviews of problems and opportunity in order to recognize changes, especially on the occasion of relevant organizational events [a)].

– <b), c)>: Definition of the problem and opportunity space and characterization of the solution space should form a basis for the analysis of the impact of changes on the 'fit for purpose' status of the system and should be a part of the possible goals of adaptation [b)1), b)2)].

– <d)>: Evaluation of the alternative solution classes should provide information for deciding whether or not to initiate system adaptation [b)3)] and for defining possible goals of adaptation as preferred alternative solution class(es) [b)2)].

– <e)1)>: Traceability between the business or mission analysis results before and after changes should be maintained, in addition to traceability between the business or mission analysis results and the artefacts in later life cycle stages [d), e), f)].

<6.4.2> Stakeholder needs and requirements definition process

– <a) to f)>: The stakeholder needs and requirements definition process should be adopted whenever necessary. The conditions for adoption are the same as Business or mission analysis process.

NOTE 2 Inputs to the Stakeholder needs and requirements definition process that might change include the output from the Business or Mission Analysis process, the set of identified stakeholders, stakeholders' needs and the environment considered for defining the representative scenarios.

– <a)1)>: Identification of the stakeholders should support management of disruptive changes where the existing list of stakeholders might need to be changed [a)3)].

– <a)2)>: Stakeholder needs and requirements definition strategy should include a plan for reviews that recognizes changes in the identified stakeholders and the defined stakeholder needs and requirements. Such reviews should be triggered periodically and whenever necessary [a)].

– <b), c)>: Definition of the stakeholder needs and rationale (<b)>) and development of the operational and other life cycle concepts (<c)>) should take into consideration that their outputs form a basis of the following when changes occur in future:

  - the analysis of change's impact on the 'fit for purpose' status of the system [b)1)];
  - decision on whether or not to proceed to system adaptation [b)3)];
  - the definition and agreement on the goal of adaptation [b)2), b)3)].

  The stakeholder needs and rationale should be recorded in a manner that helps future adaptation as 'lessons learned' [c)2)].

– <e)2)>: Critical performance measures that support the assessment of adaptation should be defined [d)].

– <e)4), f)1)>: The goal of adaptation and the agreement on it should be represented as updates to the definition of stakeholder requirements and the explicit agreement on the stakeholder requirements [b)3)].

– <f)2)>: Traceability between the system requirements before adaptation and the ones after should be maintained [f)1)].

<6.4.3> System requirements definition process

– <a) to d)>: The System requirements definition process should be adopted whenever necessary. The conditions for adoption are the same as those for Business or mission analysis process.

NOTE 3 Inputs to the System requirements definition process that might change include the stakeholder requirements, the context of use and operational scenarios, environment behaviour and the implementation constraints.

– <a)1), a)2), b), c)>: Definition of the functional boundary (<a)1)>), the system requirements definition strategy (<a)2)>), the system requirements (<b)>) and analysis of the system requirements (<c)>)should be performed such that their outputs support readily the analysis of the impact of future change on the 'fit for purpose' status of the system [b)1)] and the definition of the goal of adaptation [b)2)].

– <b)2)>: The implementation constraints should be monitored for changes in their status as a part of recognition of potential changes in Project assessment and control process [a)].

– <b)3)>: The system requirements that relate to the risk associated with changes should be identified [a), b)1)].

– <b)4)>: The goal of adaptation should be represented as an update to the definition of system requirements and rationale that reflects changes in the environment including the systems connected to the system of interest [b)2)]. The rationale should be recorded in a manner that supports assessment of the 'fit for purpose' status of the system [b)1)] and that helps future adaptation as 'lessons learned' [c)2)].

– <c)1)>: The goal of adaptation should be analysed together with the original set of system requirements in terms of potential disruption to the system's existing service and to the systems connected to the system of interest [c)5)] and effectiveness in preventing recurrence of failures [b)3)].

– <c)2)>: Critical performance measures that enable the assessment of the adapted system with respect to the goal should be defined [d)].

– <c)3)>: Feeding back the analysed requirements to applicable stakeholders should enable communication with stakeholders, support to stakeholders in the negotiation, and accounting of the adaptation [b)2)i), b)2)ii), f)].

– <d)1)>: The agreement to the goal of adaptation should be represented as an update to the explicit agreement on the system requirements [b)3)].

– <d)2)>: Traceability between the system requirements before the adaptation and after the adaptation should be maintained [f)].

<6.4.4> The Architecture definition process develops the adaptation to changes [c)4)].

– <a) to f)>: The Architecture definition process should be adopted whenever necessary. The conditions for adoption are the same as those for Business or mission analysis process.

NOTE 4 Inputs to the Architecture definition process that might change include the system requirements, market environment, regulatory and legal constraints, mission or business concept of operations, technology roadmaps, stakeholder concerns, interfaces of connected systems, and any other factors that impact the suitability of the system through its life cycle.

– <a)1), a)2), b), c)>: Identification of key drivers of the architecture and stakeholder concerns (<a)1), a)2)>), development of architecture viewpoints and models of candidate architectures (<b), c)>) should be performed such that their outputs support readily the analysis of future change's impact on the 'fit for purpose' status of the system [b)1)].

– <a)4), b), c), e)>: The defined evaluation criteria for architectures, the developed architecture viewpoints and models of candidate architectures, and the assessment result of architecture candidates should enable the definition of the goal of adaptation and agreement on it [b)2), b)3)].

<6.4.5> The Design definition process develops the adaptation to changes [c)4)].

– <a) to d)>: The Design definition process should be adopted whenever necessary. The conditions for adoption are the same as that for Business or mission analysis process.

NOTE 5 Inputs to the Design definition process that might change include the result of Architecture Definition processes, available technologies, stakeholder concerns, forecasting of obsolescence of system elements, interfaces with external entities, and available Non-Developmental-Items.

– <a)1), a)2), c)>: Determination of required technologies and necessary design characteristics types (<a)1), a)2)>) and assessment of alternatives for obtaining system elements (<c)>) should be performed such that their outputs support readily the analysis of future changes' impact on the 'fit for purpose' status of the system [b)1)].

– <b), c)>: The established design characteristics and design enablers and the result of assessment of alternatives for obtaining system elements should enable the definition of the goal of adaptation and agreement on it [b)2)].

<6.4.6> The System analysis process should be used for the assessment of the 'fit for purpose' status of the system [b)1)] and that of the adapted system with respect to the goal of the adaptation [d)].

<6.4.7> The Implementation process implements the adaptation to changes [c)4)]. The Implementation process is commenced when the Design definition process produced updated design after changes and when implementation errors are identified after failures in the Failure Response process view.

<6.4.8> The Integration process realizes the adaptation to changes [c)4)]. The Integration process is commenced when system elements implementation is updated after changes and when integration errors are identified after failures in the Failure Response process.

<6.4.9> The Verification process should be used for the assessment of the adapted system with respect to the goal of adaptation [d)] and for recognition and identification of changes [a)] in reviews done periodically or upon other events in the Project assessment and control process.

<6.4.10> The Transition process deploys the adapted service or system [c)5)], assesses the adapted system with respect to the goal of adaptation [d)] and accounts for the adaptation before operation [f)]. This includes identification of the responsible persons or entities, deployment of the revised service with least disruptions to existing service in operation and to other connected systems. The Transition process is commenced when the adapted system is integrated after changes, and when re-installation of the system is required after changes in the site of operation and other environment.

<6.4.11> The Validation process should be used for the assessment of the adapted system with respect to the goal of adaptation [d)] and for recognition and identification of changes [a)] in reviews done periodically or as the result of other events in Project assessment and control process.

<6.4.12> The Operation process monitors the system operation and the environment such as to ensure recognition and identification of changes that might require system adaptation [a)] and initiation of adaptation [b), c), d), e)] by adopting appropriate processes. This process accounts for the adaptation by adopting the Accountability Achievement process view [f)].

<6.4.13> The Maintenance process assists the Project Assessment and Control process in governing the Change Accommodation process view when the system design is stable and changes are largely predictable.

– The following should be performed as a part of recognition and identification of changes [a)]:
  - <a)2)>: identifying the system constraints to accommodate maintenance;
  - <b)1)>: reviewing incident and problem reports to identify future maintenance needs;
  - <b)6)>: failure identification actions, when a non-compliance has been detected;
  - <b)7)>: identifying when adaptive or perfective maintenance is required;
  - <d)1)>: identifying anomalies in maintenance and logistics results;
  - <d)3)>: identifying trends of incidents, problems. and maintenance and logistics actions;
  - <d)6)>: monitoring customer satisfaction with system and maintenance support.

– The following should be performed as a part of preparation for adaptation [b)]:
  - <a)2)>: identifying the system constraints to accommodate maintenance;
  - <a)3)>: identifying trade-offs for the system, maintenance and logistics actions;
  - <b)1)>: reviewing incident and problem reports to identify future maintenance needs;
  - <d)3)>: identifying trends of incidents, problems, and maintenance and logistics actions;
– <b)2), d)2)>: Maintenance problems and operational problems should be resolved by adopting appropriate processes [b), c), d), e)].

<6.4.14> Disposal process

– <b)3)>: The record of operating knowledge should be used in future change accommodation [c)2)] and for improvement of the life cycle [e)].
– <c)1)>: The confirmation that no detrimental health factors, etc., exist after disposal of obsolete system elements should be included in accounting of adaptation [f)].
– <c)3)>: The archived information gathered through the lifetime of the system should be included in accounting of adaptation [f)] and recorded to be used in future change accommodation [c)2)].

Annex A
(informative)

Example life cycle models with open systems dependability

A.1 General

This document provides four life cycle process views, but does not provide any life cycle models using these process views. Annex A suggests two example life cycle models: DEOS life cycle model and WCM life cycle model.

In Annex A, angle brackets (<>) are used to refer to the subclause number of a process in ISO/IEC/IEEE 15288:2015.

A.2 Dependable Engineering for Open Systems (DEOS) life cycle model

DEOS life cycle model ([11], therein called DEOS Process) considers the classes of stakeholders such as

– users of services or products (the whole society in the case of systems for social infrastructure),
– providers of services or products,
– certifiers (authorizers) of services or products, and
– providers of systems including
  - designers and developers,
  - maintainers, and
  - providers of hardware.

The DEOS life cycle model is organized into two iterative flows of works, called “cycles” in [11] (Figure A.1): the Change Accommodation Cycle (outer loop) and the Failure Response Cycle (inner loop). Each cycle implements the same-named process view by specifying the flow and/or order of works necessary for that process view. The two cycles also implement the parts of Consensus Building and Accountability Achievement process views regarding change accommodation and failure response, respectively. Both cycles are initiated from the Ordinary Operation Stage.

a) The Change Accommodation Cycle begins when the system is to be modified in response to changes in its purpose, objectives, environment or actual performance, and it comprises the Consensus Building Stage, the Development Stage, and the Accountability Achievement Stage.
b) The Failure Response Cycle begins when a failure has occurred or is predicted, and it consists of the Failure Response Stage and the Accountability Achievement Stage.
c) If deemed necessary after the cause of the failure has been analysed, the Failure Response Cycle can initiate the Change Accommodation Cycle in order to modify the system.
d) The agreement description database stores dependability cases and scripts (programs) that automate monitoring, failure response and accountability achievement based on the current dependability cases. Dependability cases and scripts are utilized in system operation. The system operation is integrated into the development processes and dependability cases are updated on an ongoing basis.

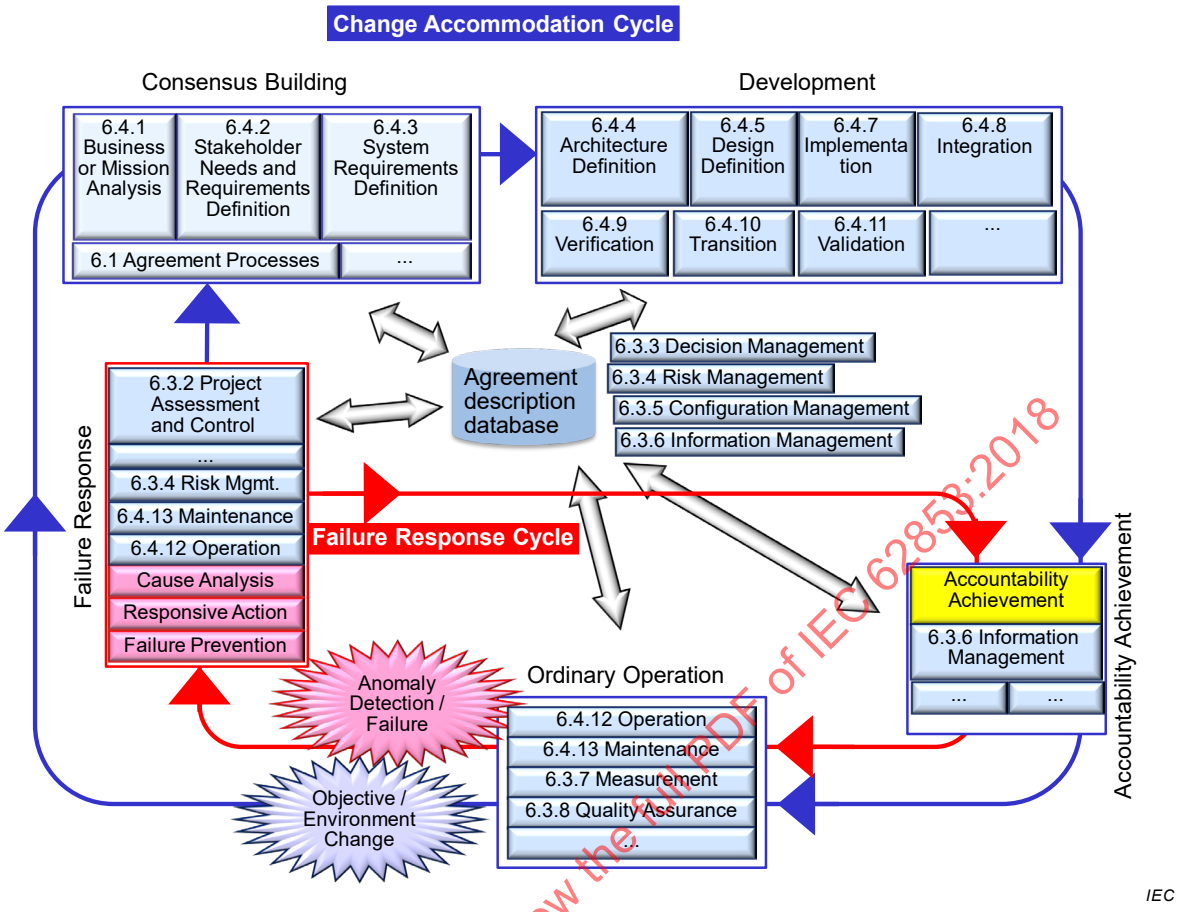


Figure A.1 – DEOS life cycle model ([11], adjusted)

The DEOS life cycle model has five stages. The following lists the process view outcomes in this document and the life cycle processes in ISO/IEC/IEEE 15288:2015 most relevant to each stage.

– Consensus Building Stage encompasses the following:
  - the Consensus Building process view (6.2.2 a), b));
  - the initial parts of the Accountability Achievement process view (6.3.2 a) to e), g));
  - the initial parts of the Failure Response process view (6.4.2 a)1), a)2)) and rebuilding of consensus after failures (6.4.2 d));
  - the initial parts of the Change Accommodation process view (6.5.2 a), b)).

  The relevant life cycle processes include <6.1.1> Acquisition Process, <6.1.2> Supply Process, <6.4.1> Business or Mission Analysis Process, <6.4.2> Stakeholder Needs and Requirements Definition Process, <6.4.3> System Requirements Definition Process.

  NOTE 1 The life cycle processes of ISO/IEC/IEEE 15288:2015 are applied concurrently, iteratively and recursively to a system and incrementally to its elements (see <1.3> and <5.7>). This point is particularly pertinent to open systems. Since an open system is continuously updated and changed, the processes mentioned above need to be repeated several times after the system has been taken into use.

– The Development Stage encompasses the following:
  - maintenance and monitoring of accountability as more detailed decisions are made and outcomes of decisions become available (6.3.2 all);
  - development of failure response (6.4.2 a)3) to a)8));
  - development and assessment of adaptation (6.5.2 c), d)).

The relevant life cycle processes include <6.4.4> Architecture Definition Process, <6.4.5> Design Definition Process, <6.4.7> Implementation Process, <6.4.8> Integration Process, <6.4.9> Verification Process, <6.4.10> Transition Process, <6.4.11> Validation Process.

– The Accountability Achievement Stage encompasses the following:
  - collection of necessary information including that on failure response and adaptation to changes (6.3.2 f), g), 6.4.2 c), 6.5.2 f));
  - fulfilment of accountable stakeholders' obligations to provide agreed remedies for non-accountable stakeholders (6.3.2 e), h));
  - provision of accounting information to stakeholders and society in general (6.3.2 i)).

  The relevant life cycle processes include <6.3.6> Information Management Process.
– The Ordinary Operation Stage encompasses the following:
  - detection of failures (6.4.2 b)1));
  - detection of changes (6.5.2 a));
  - monitoring for accountability (6.3.2 f)).

  The relevant life cycle processes include <6.4.12> Operation Process, <6.4.13> Maintenance Process, <6.3.7> Measurement Process, <6.3.8> Quality Assurance Process.
– The Failure Response Stage encompasses:
  - immediate response to detected failures (6.4.2 b));
  - provision of failure information for accountability achievement and for continual improvement (6.4.2 c), d)2)).

  The relevant life cycle processes include <6.3.2> Project Assessment and Control Process, <6.3.4> Risk Management Process, <6.4.12> Operation Process, <6.4.13> Maintenance Process.

NOTE 2 The listing above is a simplification and not exhaustive. Each stage affects process view outcomes not explicitly associated with the stage and each outcome depends on performance of stages not explicitly associated with the outcome.

Conformance by a concrete example of the DEOS life cycle model to this document can be established by a dependability case demonstrating that the four process views provided in Clause 6 are implemented by the set of relevant processes, activities and tasks shown in Figure A.1.

A.3 Warranty Chain Management (WCM) life cycle model

Warranty Chain Management (WCM) is management of a cyclic business process. One round of the cycle starts when a product fails, continues through analysis of all feedback data and root cause analysis (RCA), provides the customer with a revised product that fulfils expectations and restarts for the next round. Besides failures, WCM considers other events that occur in the field as well as in the development stage for starting a round, since an open system is continuously updated and changed. WCM includes proactive activities, which is intended to reduce future failures.

The life cycle processes subject to WCM are classified into four groups: Customer service, Failure analysis, Engineering and Supply chain.

Customer service is the continual operation of product maintenance services, which accepts claims from the customer, delivers repair service to the customer and records field information for further analysis. Failure analysis processes monitor field information and manage the identification of root causes and corrective actions. Engineering processes cover the technical management of the product, including product development, manufacturing technology and portfolio management. The Supply Chain covers sourcing, manufacturing and distribution and is responsible for producing and delivering products to the customer.

WCM connects the four life cycle processes by means of Shewhart/Deming's Circle: Plan-Do-Study-Act.

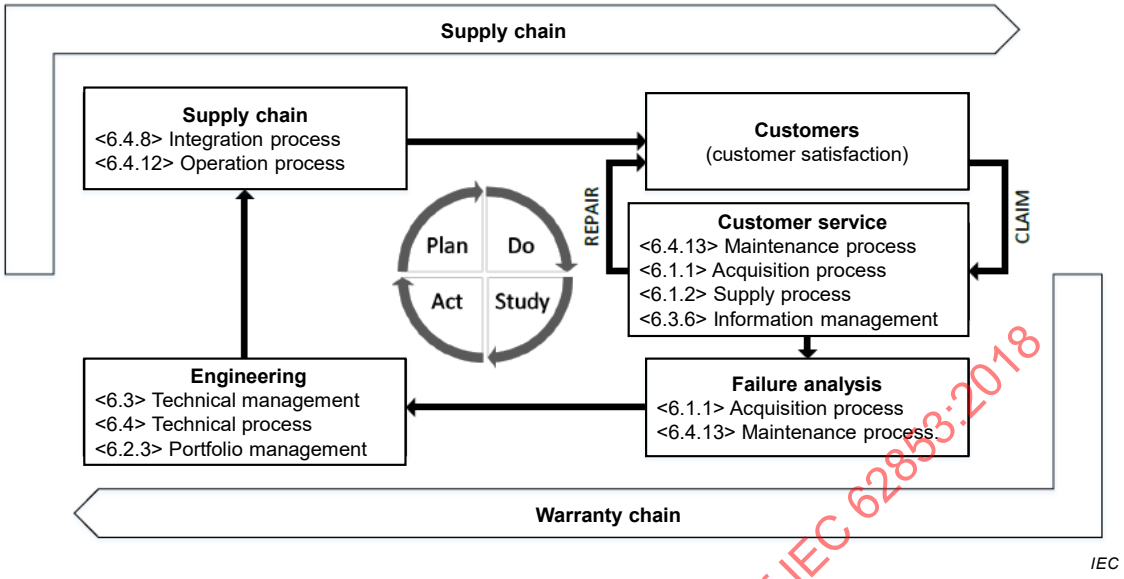


Figure A.2 – WCM life cycle model

The Customer service (the inner cycle of CLAIM-REPAIR) describes the parts of the Failure Response process view and the Accountability Achievement process view that face the customer directly (6.4.2 b), 6.4.2 c), 6.3.2 h) and 6.3.2 i)). The Failure analysis corresponds to the initial part of the Change Accommodation process view where changes in the form of unanticipated failures are detected, analysed and corrective action identified (6.5.2 a)2) and b)). Engineering develops adaptation (6.5.2 c)4)). The supply chain deploys the adaptation (6.5.2 c)5)) as well as realizing the Consensus Building process view (6.2.2) between the supplier and customer for the new adapted service. Similarly, the life cycle model provides targets to which other process view outcomes are mapped.

Conformance by a concrete example of WCM life cycle model to this document can be established by a dependability case demonstrating that the four process views provided in Clause 6 are implemented by the set of relevant processes, activities and tasks shown in Figure A.2.

Annex B
(informative)

An example template for dependability cases

B.1 Overview

The following is an example template argument structure for a dependability case claiming achievement of open systems dependability required in Clause 5. The argument structure is given in Goal Structuring Notation (GSN 0).

NOTE In Annex B, goals with dashed borders in some figures are those goals that are developed further in separate diagrams.

Process view outcomes are goals in the template structure; all goals that are not decomposed (leaf goals) are outcomes. Where outcomes have a hierarchical structure, higher level outcomes become intermediate goals. An intermediate goal that is not a higher-level outcome describes intended significance of the group of goals beneath it. Strategies describe the rationale of goal decomposition.

A concrete example of argument on a given target system life cycle is obtained by further developing and concretizing goals and providing evidence (solutions) to the resulting leaf goals. The description of goals and strategies should be examined for adequacy and sufficiency in the situation at hand and the argument structure should be modified and augmented as necessary. This example does not contain templates for context nodes and evidence, which also need to be added as necessary.

The top-level goal “Service continuity and accountability in an ever-changing system is achieved” is decomposed according to the four process views provided by this document. Decomposition of a goal means identification of a set of sub-goals, the achievement of which implies achievement of the goal. See Figure B.1 below.

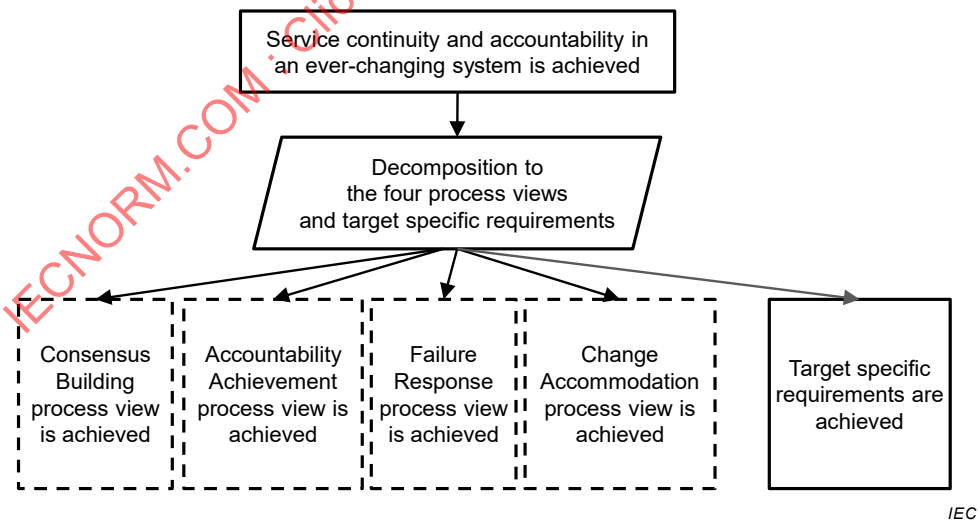


Figure B.1 – Overall argument

B.2 Consensus Building argument

The goal description “Consensus Building process view is achieved” means that the purpose of this process view is met, and thus expanded to the following statement, according to the first paragraph of 6.2.1.

> A common understanding with explicit agreements about the system, its purpose, objectives, environment, actual performance, life cycle and changes thereof are established and maintained.

The argument is divided into the establishment of understanding and agreements, and their maintenance (Figure B.2). Establishment is argued for from the viewpoint of preparation [6.2.2 a)1), a)2), a)4)], contents to be established [a)3), a)5)], and assessment of results [a)6), a)7)] (Figure B.3). Maintenance goals are divided into a group of those relating to actions necessary for maintenance [b)1), b)2), b)3)] and another of those securing linkages between maintenance action and maintenance of dependability case [b)4), b)5)] (Figure B.4).

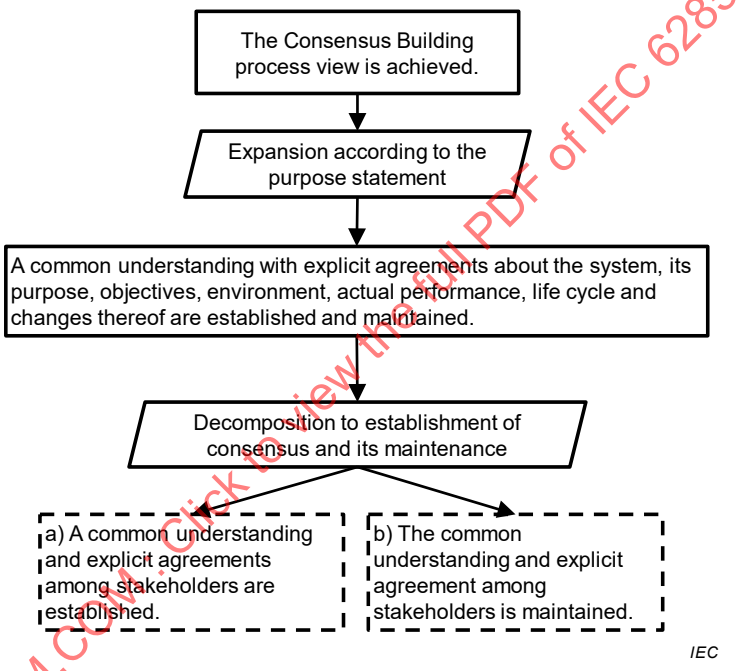


Figure B.2 – Consensus Building 1

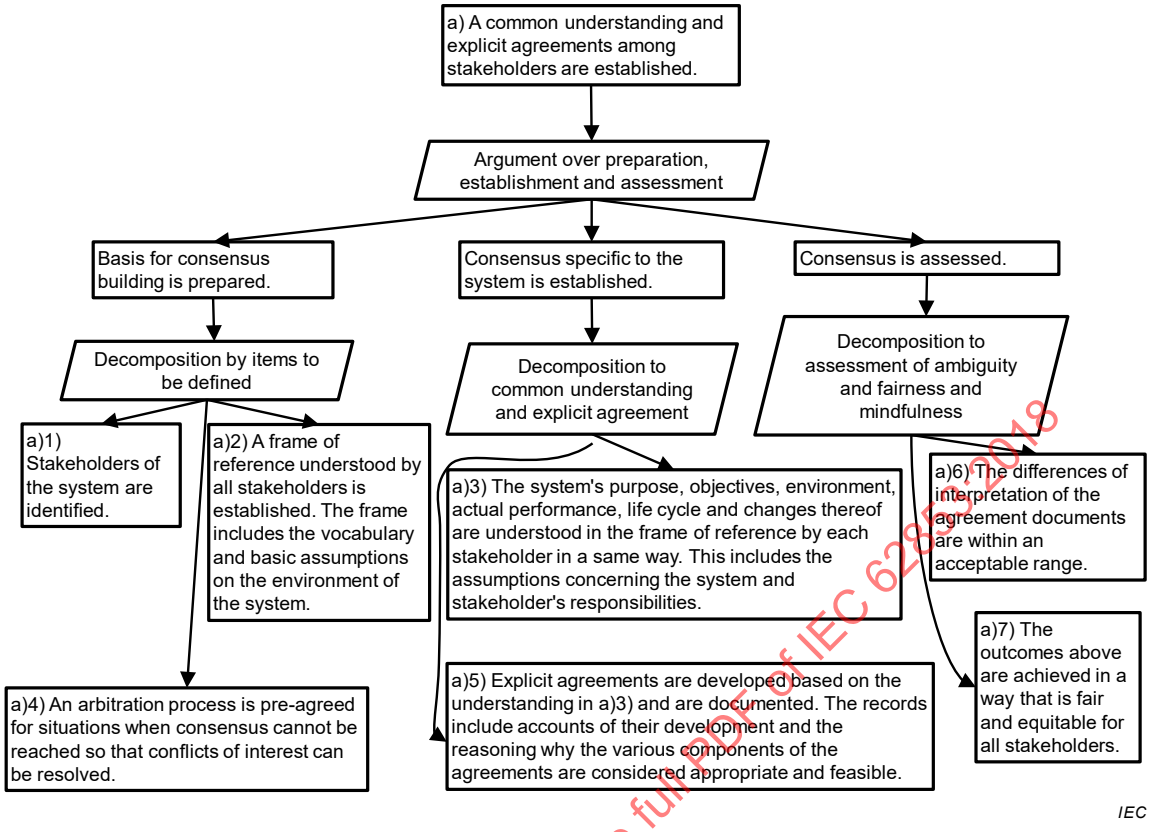


Figure B.3 – Consensus Building 2

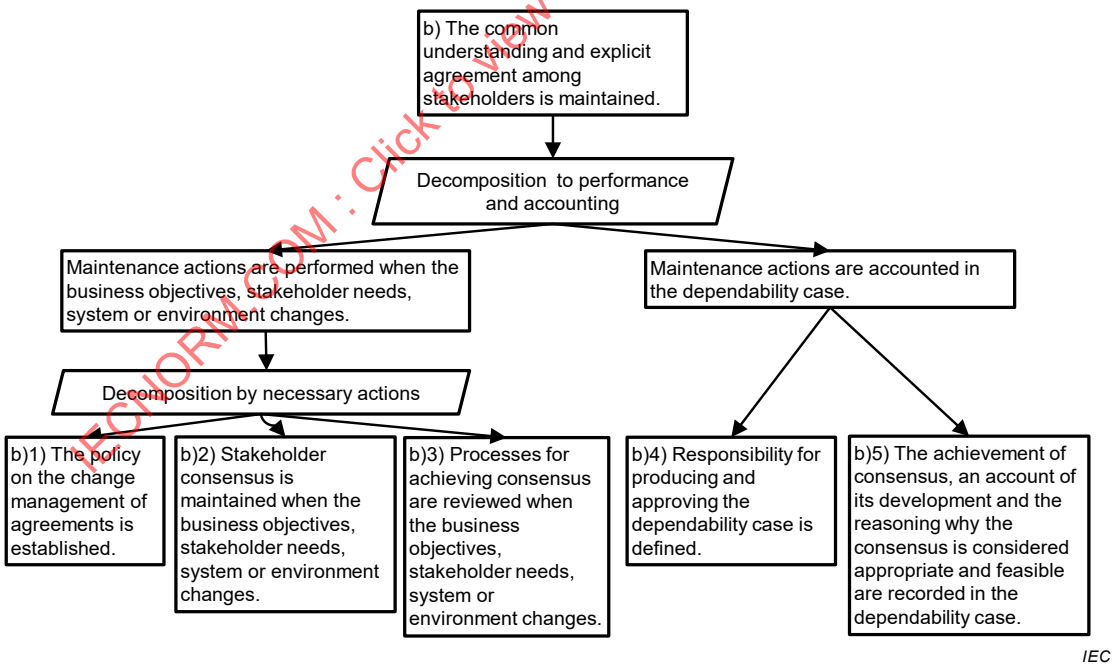


Figure B.4 – Consensus Building 3

B.3 Accountability Achievement argument

The goal “Accountability Achievement process view is achieved.” is expanded to the following statement, according to the purpose of the process view, i.e. the first paragraph of 6.3.1.

> The relationship is established between a breach of an explicit agreement and its implications for stakeholders and society in general. This includes accountable stakeholders’ obligations to provide remedies, so as to improve the chance of realizing consensus on the system, to sustain confidence and trust in the system and to secure the availability of remedies for potential damage.

This goal is argued for from the viewpoint of the preparation that occurs before events that need to be accounted and the actual performance when events occur, including monitoring (Figure B.5). The preparation, which determines what the relationship should be, amounts to identification and definition of necessary elements [6.3.2 a) to e)] (Figure B.6). The goals of performance are divided into two groups: goals to be achieved within the system [f) to h)] (Figure B.7) and goals to be obtained with respect to outside of the system [i), i)1), i)2), i)3), i)4), i)5)] (Figure B.8).

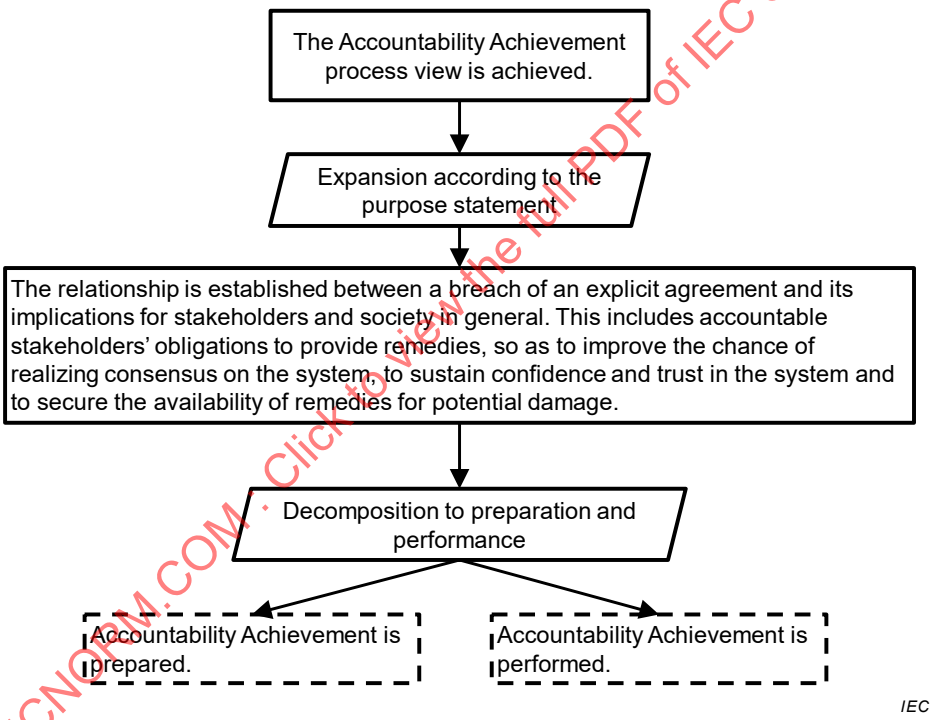


Figure B.5 – Accountability Achievement 1

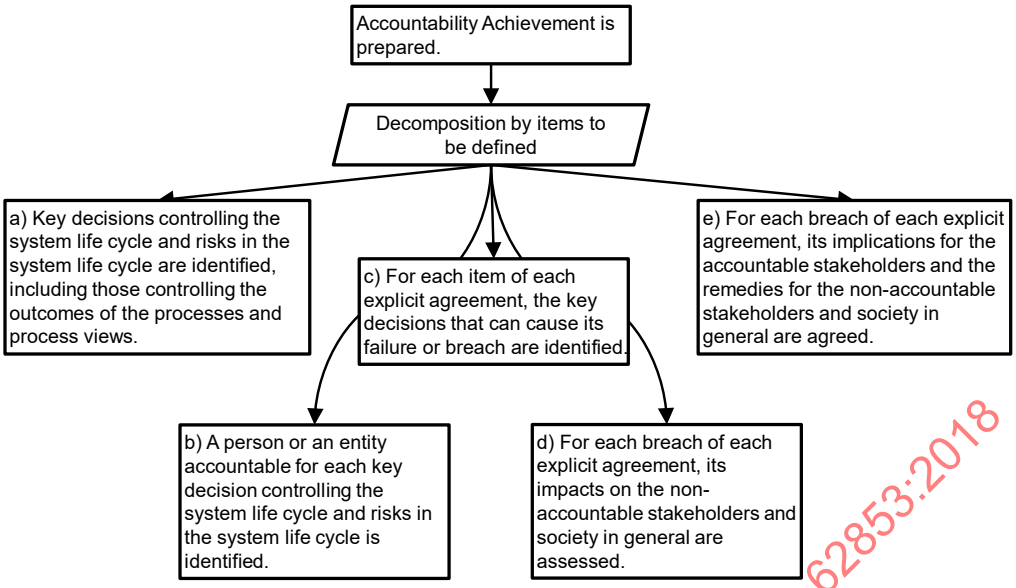


Figure B.6 – Accountability Achievement 2

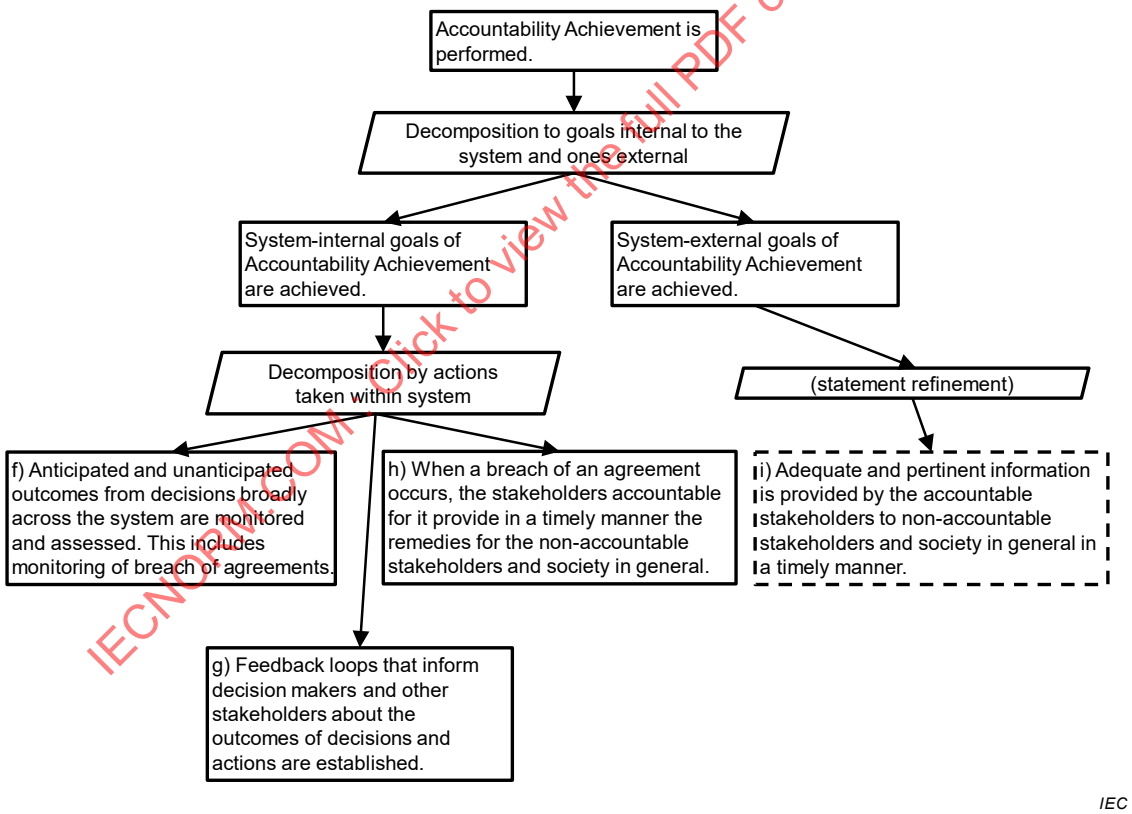


Figure B.7 – Accountability Achievement 3

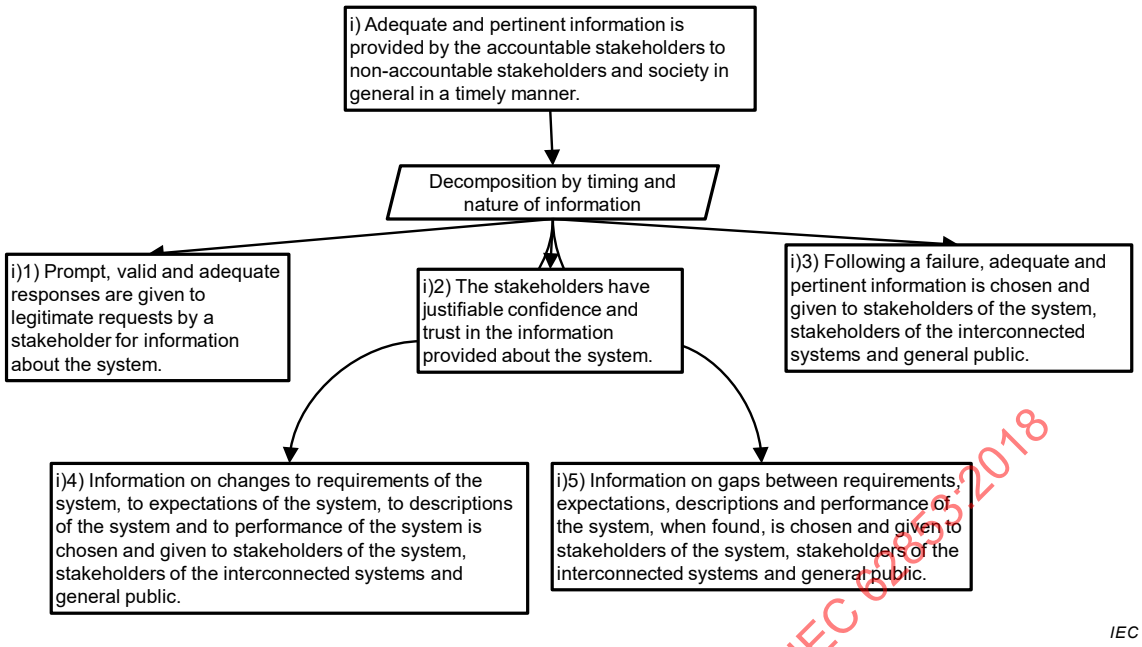


Figure B.8 – Accountability Achievement 4

B.4 Failure Response argument

The goal "Failure Response process view is achieved" is expanded to the following statement, according to the purpose, i.e. the first paragraph of 6.4.1.

> The provision of the service is continued as much as possible, with the least possible disruption and damage, in the manner most expedient in the context.

The goal is decomposed into the goal of mitigating immediate harm from failures and that of mitigating longer-term harm from failures (Figure B.9). Mitigation of immediate harm is argued for from the viewpoint of preparation before failure events [6.4.2 a)] and the actual performance when they occur [b)]. The preparation consists of the goal-setting of failure responses and the development of responses that achieve the goals set. The goal-setting of failure response includes identification of targets for protection, identification of failure causes, and definition of their goals for treatment [a)1) to a)5)] (Figure B.10). The development of failure responses considers both the case where failure causes are identified and the case where they are not. For the former case, development includes the decision for each identified failure cause as to whether a specific response to it is warranted or generic response is sufficient, and development proceeds accordingly [a)6), a)7)] (Figure B.11). For the case where failure causes are not identified, generic measures are developed [a)8)]. The goal of the performance of failure response is decomposed to the goal that responses are indeed performed and the goals on assessment of the responses. The performance of response is demonstrated from the following: failure detection, analysis, refinement of response for the situation at hand and actual responding [b)1) to b)5)]. The goals on assessment of the responses consider both the general assessment with respect to the purpose of the process view [b)6), b)7)] and the specific assessment with respect to the goal, set in the preparation [b)8)] (Figure B.12). The goal of mitigating longer-term harm from failures decomposes to sustainment of public confidence and trust in the system, which is an instance of accountability achievement [c)] and to continual improvement of the system life cycle, which is an instance of Change Accommodation [d)] (Figure B.9). The former is necessary for the process view purpose as explained in 6.3.1, fourth paragraph, and consists of accountability goals after failure events [c)1) to c)4)] (Figure B.13). The latter consists of definition of improvement goals including failure recurrence prevention and appropriate invocation of the Change Accommodation process view [d)1), d)2)] (Figure B.14).

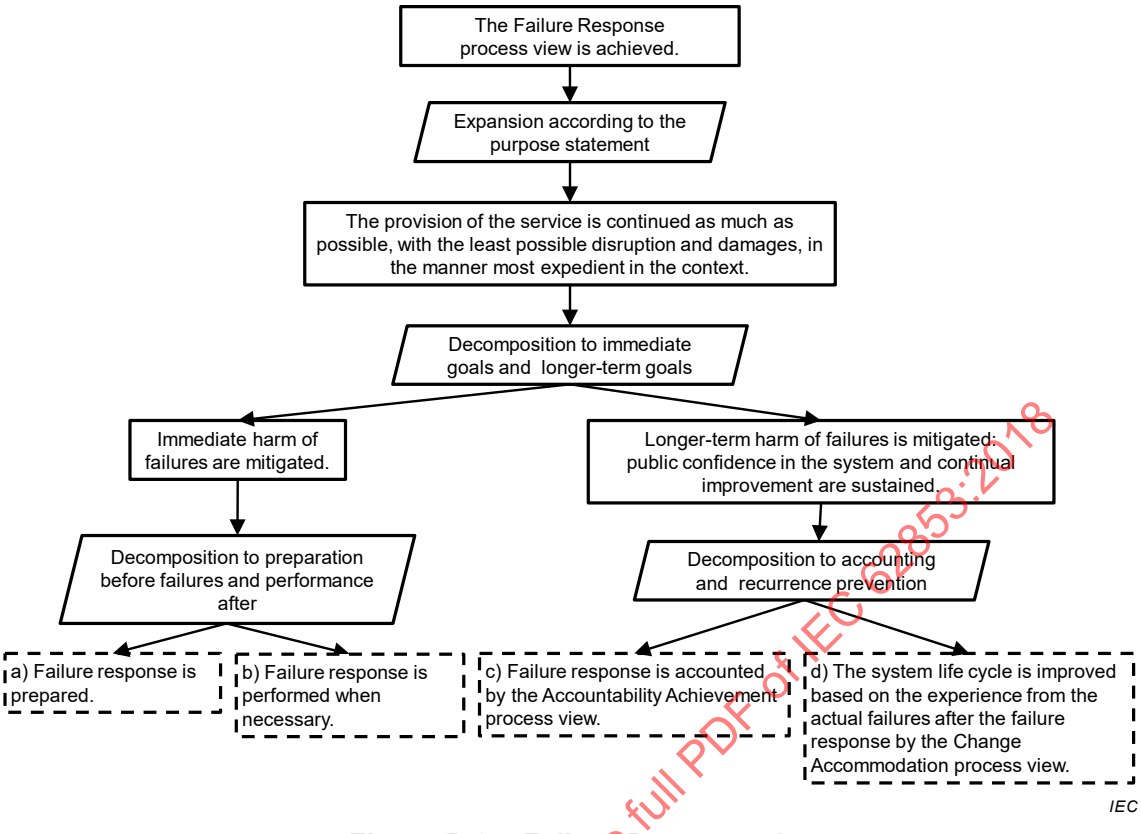


Figure B.9 – Failure Response 1

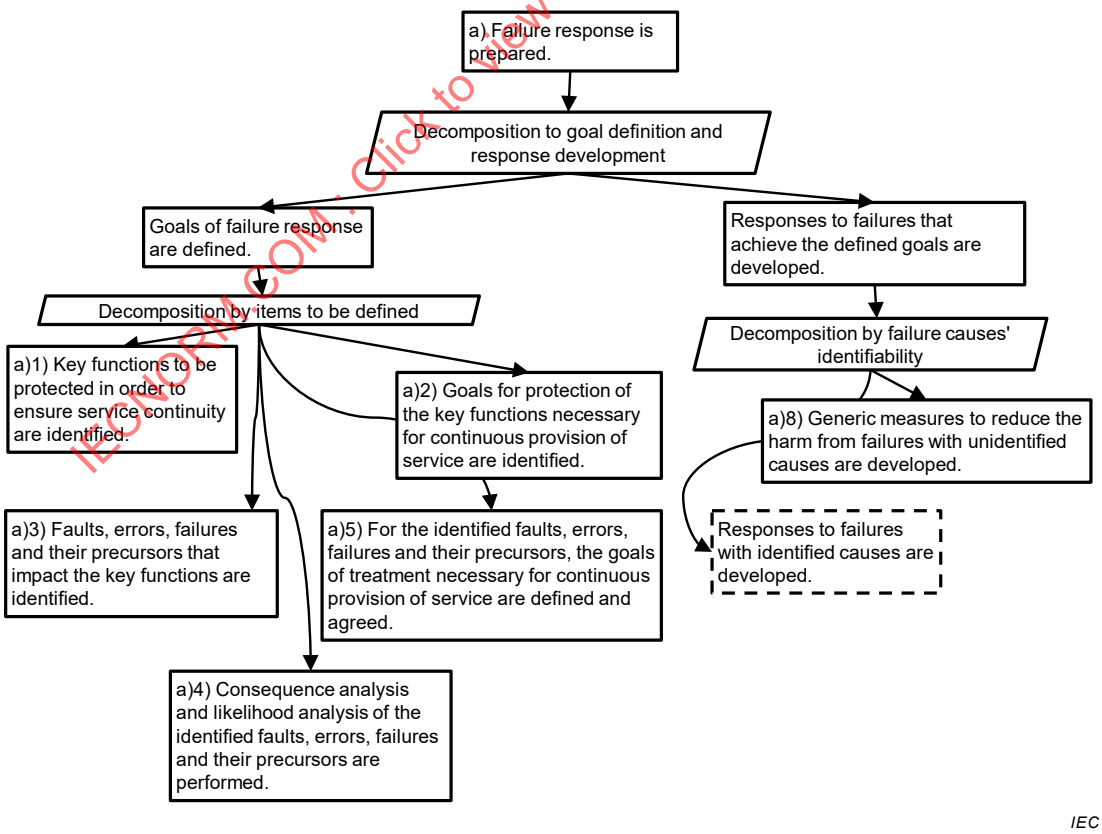


Figure B.10 – Failure Response 2

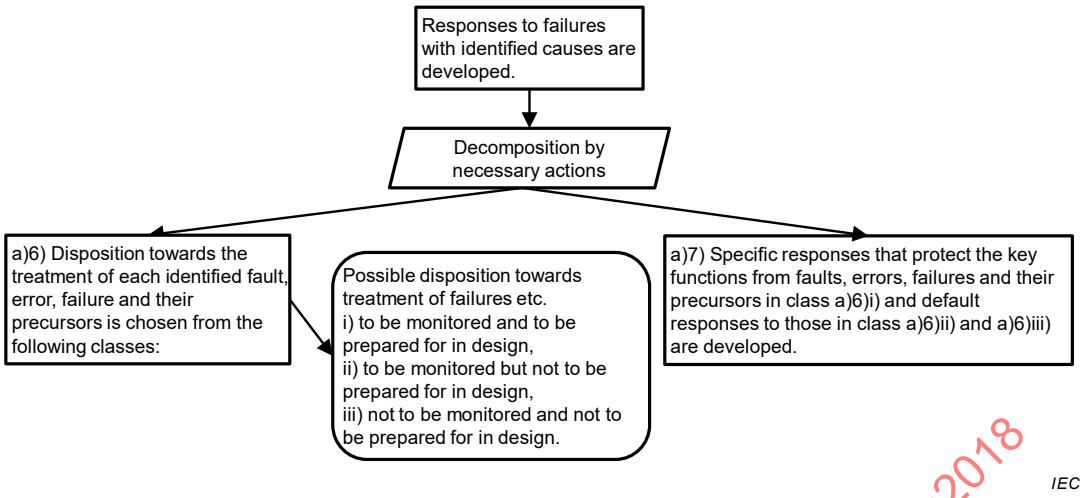


Figure B.11 – Failure Response 3

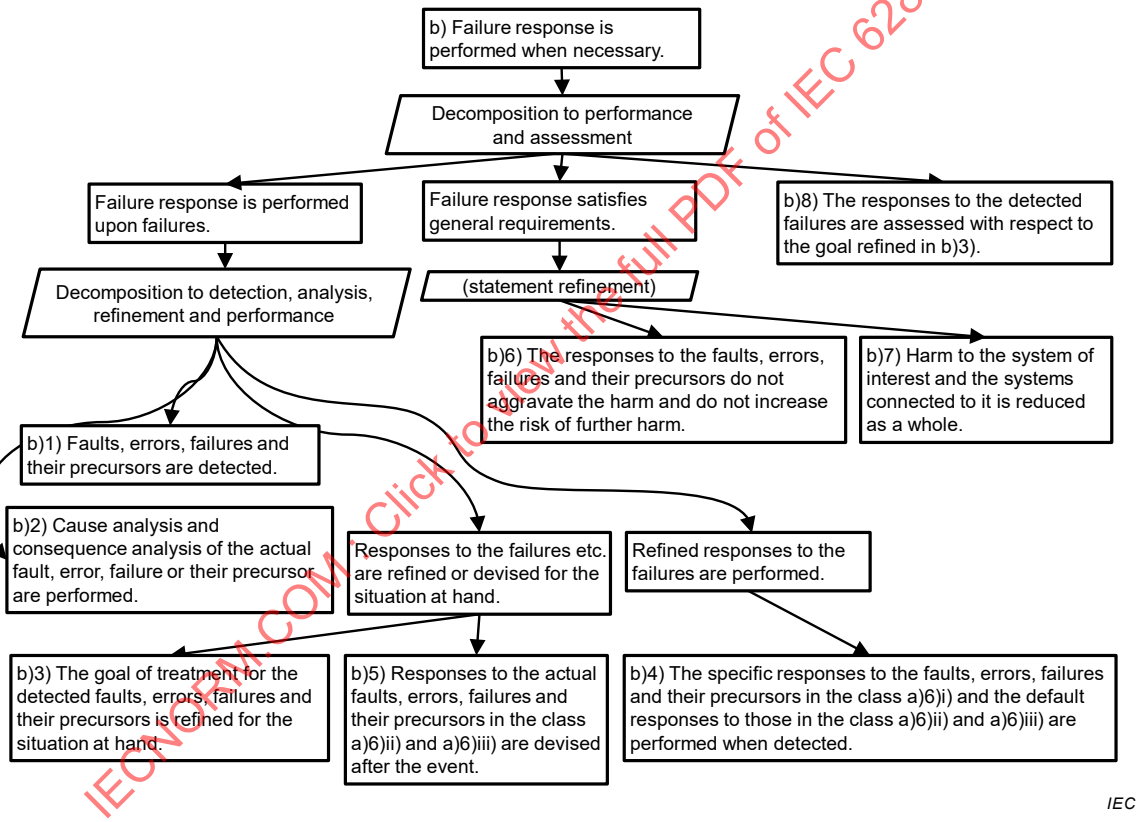


Figure B.12 – Failure Response 4

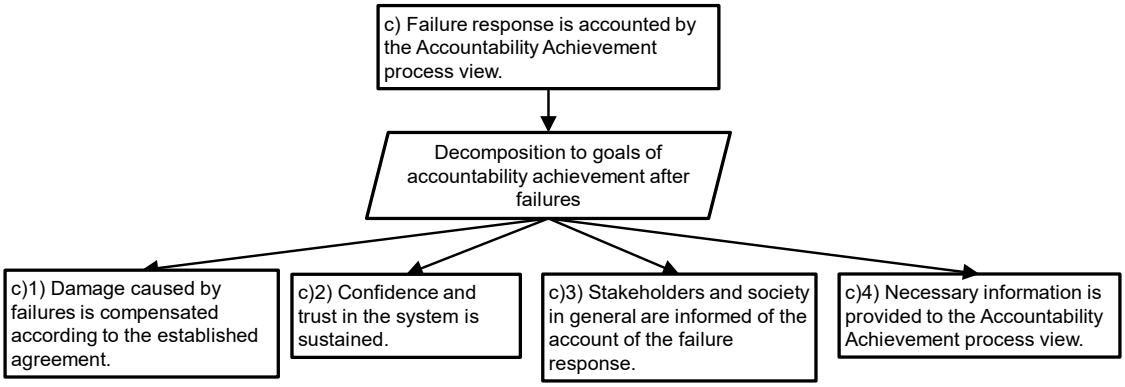


Figure B.13 – Failure Response 5

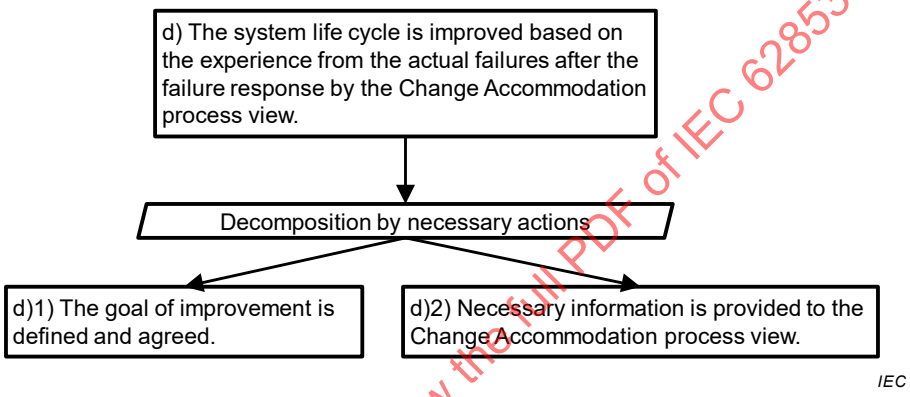


Figure B.14 – Failure Response 6

B.5 Change Accommodation argument

The goal “Change Accommodation process view is achieved” is expanded to the following statement according to the purpose given in 6.5.1.

> The ‘fit for purpose’ status of the system is maintained despite changes in requirements, environments, objectives and/or purpose.

This goal is decomposed to the direct goal of adapting the system to changes and to the longer-term goal of sustaining continual improvement of the system life cycle and public confidence and trust in the system. The direct goal is argued for from the viewpoint of identification of changes [6.5.2 a)], preparation for adaptation [b)], performance of adaptation [c)] and assessment [d)] (Figure B.15). The goal of change identification is decomposed to goals identifying the types of changes to watch for [a)1) to a)3)] (Figure B.16). The goal of preparation for adaptation is argued for from the viewpoint that necessary actions are taken [b)1) to b)3)] (Figure B.17). The goal of performing adaptation is examined from two viewpoints: whether the necessary support is available [c)1), c)2)] and whether the necessary adaptation actions are taken [c)3) to c)5)] (Figure B.18). Of the two parts of the longer-term goal, the goal of continual improvement is left undeveloped here but should be developed in the context of a concrete life cycle model detailing how one iteration of the Change Accommodation process view achieves lasting effects for future improvement. The other part of the longer-term goal, sustaining public confidence and trust in the system, is an instance of the accountability achievement for the adaptation [f)] and is argued for from the availability of inputs to the Accountability Achievement process view and that it achieves accounting of adaptation [f)1), f)2)] (Figure B.15).

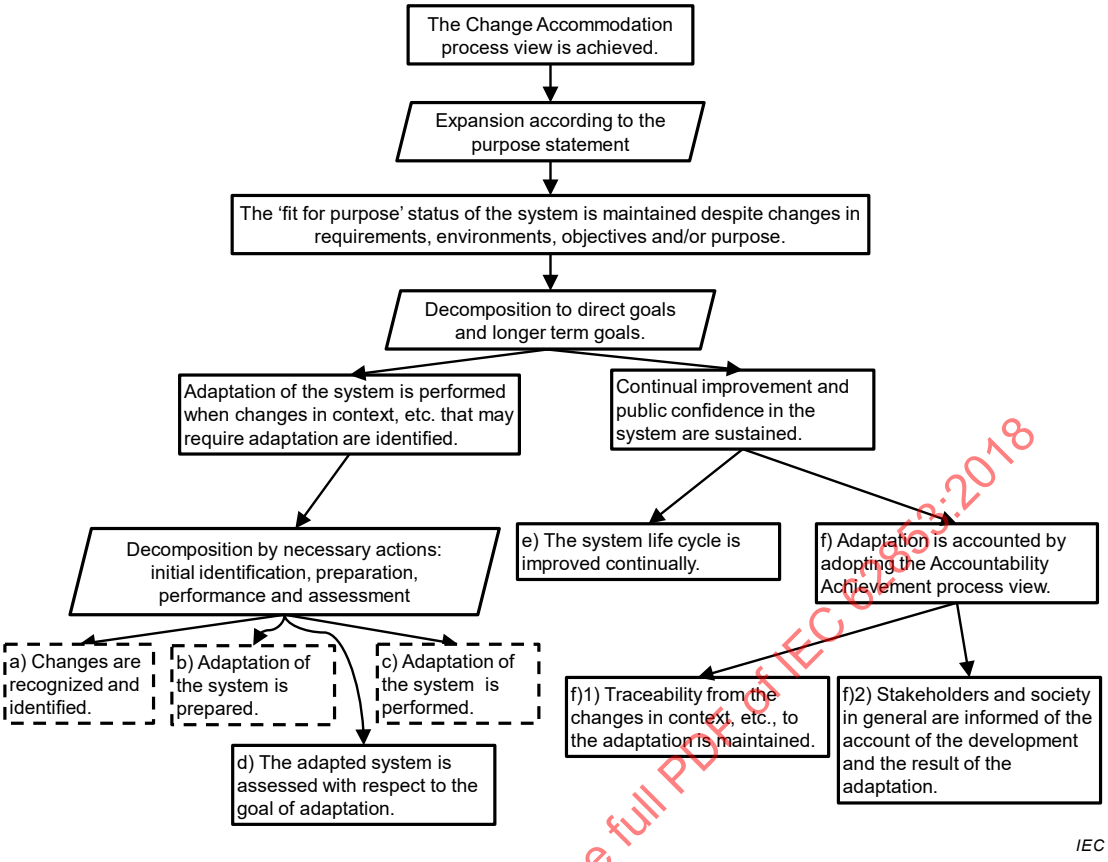


Figure B.15 – Change Accommodation 1

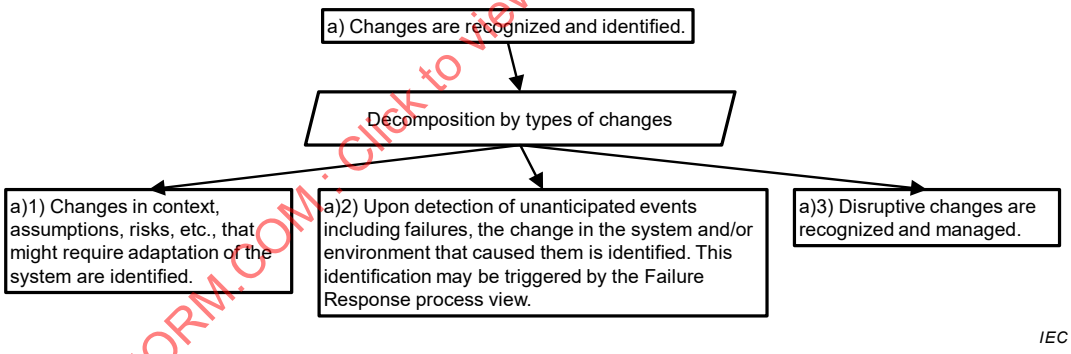


Figure B.16 – Change Accommodation 2

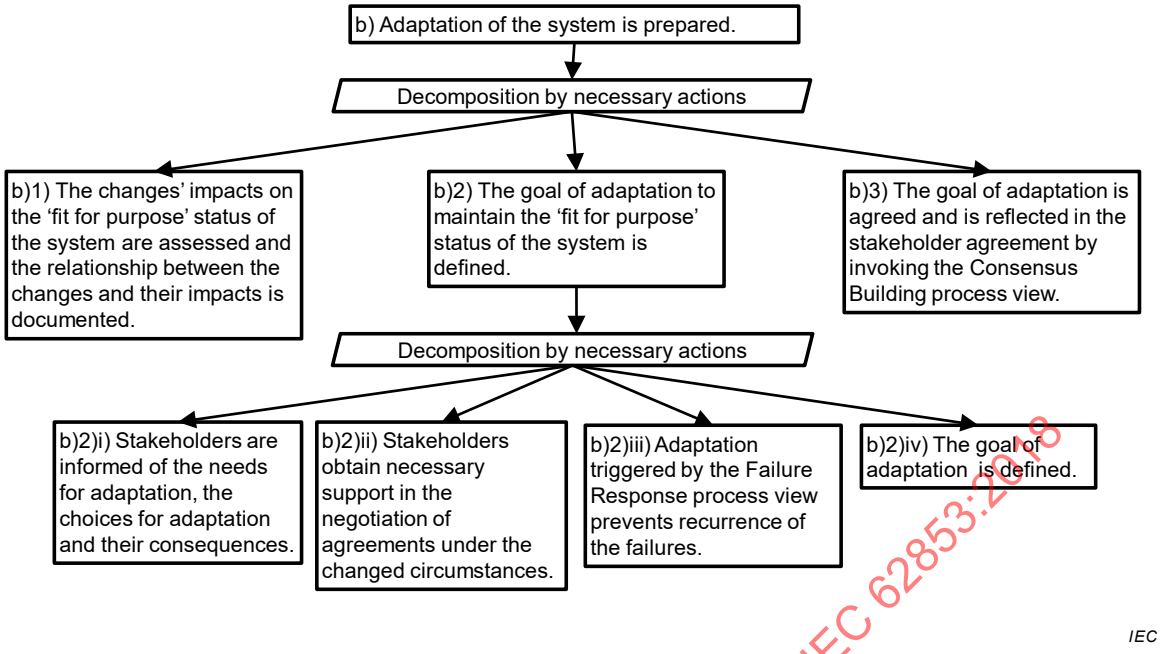


Figure B.17 – Change Accommodation 3

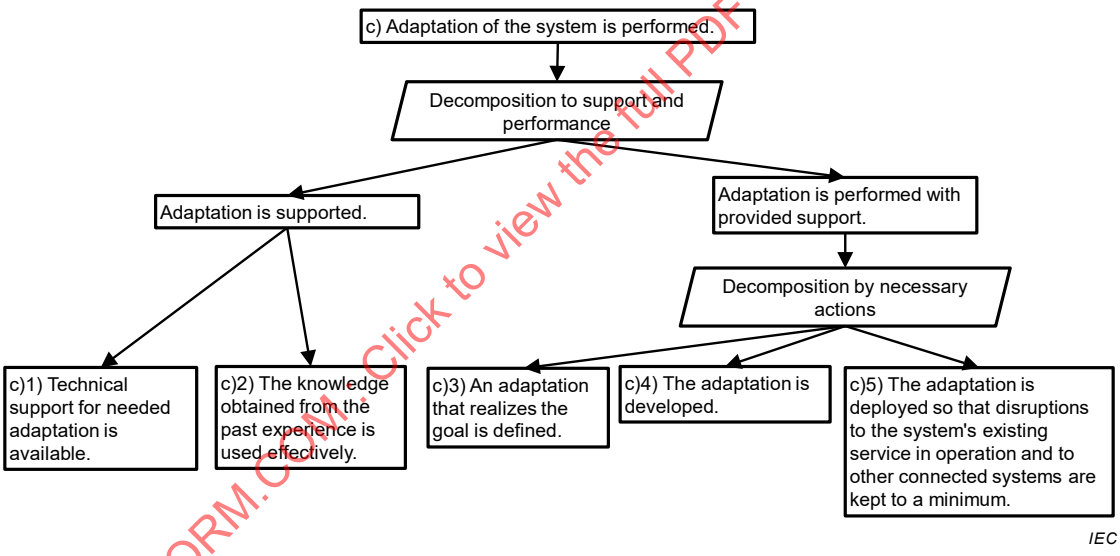


Figure B.18 – Change Accommodation 4

Annex C
(informative)

Smart Grid

C.1 General

Annex C describes a “smart grid” as an example of an open system and illustrates how open systems dependability can be achieved. The DEOS life cycle model given in Clause A.2 is taken as the basis of illustration. Clause C.3 exemplifies construction of a smart grid dependability case to satisfy Clause 5. Clause C.4 describes the Change Accommodation Cycle in the DEOS life cycle of the smart grid, which implements the Change Accommodation process view of 6.5, and Clause C.5 describes the Failure Response Cycle, which implements the Failure Response process view of 6.4. The two cycles also implement the Accountability Achievement process view of 6.3 and the Consensus Building process view of 6.2 regarding adaptations of the smart grid and regarding failure responses, respectively. The example is based on the Danish power grid system.

C.2 Background

A stable and reliable power supply is of vital importance in a modern society. Further, energy saving measures and renewable power sources like wind turbines and solar cells have complicated the operation and administration of a power grid. The most important requirements of a power grid are dependability (availability and its contributing factors of reliability, maintainability and supportability) and safety.

In the European Union the ownership of the power distribution system has been separated from the production and trade of electricity. Distributors pay to use the power grid system to supply electricity that they buy from suppliers. Together with a few large coal fuelled power plants and nuclear power plants, there are now a large number of small power plants producing district heating and selling electricity. The consumers of electricity are also, in many cases, producers of electricity through wind turbines or solar cells. The variation of the supply and demand over day and night has caused the price of electricity to vary from hour to hour. Therefore, the concept of smart grid has been introduced. This includes electric meters for each consumer, which can be read remotely by the operator of the grid. At the same time the consumer may pay a price for the power that depends on the current price on the market, varying from hour to hour. The consumer may also sell surplus electricity to the market.

Electrical power is very difficult to store. This means that the price can be negative in periods of excessive supply, i.e. the supplier has to pay to supply electricity.

The software that controls a smart grid is part of an open system since the system is constantly changing, with new consumers, distributers and producers coming in. Further the software is connected to thousands of consumers, many of whom operate software to control their wind turbines and solar cells. Since these systems will be connected to public consumer networks the whole smart grid is an open system that might be influenced by malware within the network. Therefore, a “firewall” is required towards the consumers, but also towards the power suppliers.

C.3 Construction of a smart grid dependability case

C.3.1 General

For the life cycle of a smart grid to support open systems dependability, a dependability case satisfying Clause 5 should be constructed and maintained. Clause C.3 exemplifies a possible set of steps for this work together with specific issues to be considered in each step in the case of a smart grid. The nine steps below are adopted from a dependability case description guideline in [11].

C.3.2 Steps for construction of a smart grid dependability case

C.3.2.1 Step 1: Clearly define the system's life cycle and identify the input and output documents for each phase

The documents that are input and output throughout the life cycle of a smart grid form the basis of its dependability case. They include the legal text, regulatory rules and company statutes and contracts.

The operator of the grid will have some sort of concession or ownership of the power grid (high power pylons, cables, transformer stations and low voltage distribution networks). The ownership can be based on law or ownership through a public or privately owned company.

The operator of the grid will have contracts with many suppliers and distributors of power. It can be large power plants (coal fuelled, nuclear powered or water power plants) in its own country or in foreign countries. It can also have contracts with grid operators in different countries. Further the grid operator can, through the distributors, buy electricity from privately owned wind turbines and solar cell parks. The supplier can be a consumer or a consortium. All these contracts contain requirements that have to be implemented in the software. For example, who can supply power, when and at which price. This price might vary over the day and night as well as over the year.

The operator of the grid also has contracts with distributors buying power on the open market (at fixed price or at a varying price) and selling the power to the consumers. Also this has to be implemented in the smart grid software.

The life cycle of the smart grid software is as follows:

– **Consensus Building Stage** takes inputs from consultation with concession granting bodies, regulatory agencies, suppliers and consumers and outputs requirement definition documents and contracts before the intelligent meters are installed at the consumers' addresses. The stage is initiated again after a failure response or detection of environmental changes for improving and adapting the grid.
– **Development Stage** involves the following.
  - Architecture design is made after the requirement definition has been approved. The software is divided into a subsystem that keeps the power grid stable (within specifications), a subsystem that buys and sells power and handles payments, a subsystem that handles the contracts and a subsystem that monitors the safety and security of the system.
  - With the input of requirement definition and architecture design, the subsystems are implemented and tested separately and integrated into the power grid software system by a step-by-step integration and integration test process. The software system is tested with test cases followed by a test with simulated operational data. Finally, safety, security and overload tests (surge tests) are performed on the software. Software codes, development logs, test results, and other artefacts are output.
– **Accountability Achievement Stage** provides assurance before the licence to operate is granted. The assurance arguments and evidence to regulatory agencies, suppliers and consumers assure that the developed smart grid will satisfy requirements and that contracts will continue to be honoured. The life cycle enters this stage again after a failure or an adaptation on the grid to account for responses and improvements, to enact compensational clauses of contracts and to assure the improved grid.
– **Operation Stage** implements the final software first on a small "island" before it is implemented on the "mainland". The grid and environment are monitored for failures and changes that might require rebuilding of consensus.

– **Failure Response Stage** provides immediate responses to detected failures according to the plan that is required and/or specified in the regulations and contracts. The plan specifies interfaces with emergency actions of many services depending on the grid. The plan is not considered perfect and the stage has built-in flexibility to adapt to the situation and to escalate responses requiring unplanned involvement of higher authorities. The stage records the results of responses for use in Accountability Achievement Stage and the next iteration of Consensus Building Stage.

C.3.2.2 Step 2: Categorize the input and output documents

How the documents identified in Step 1 are used in construction of the dependability case is considered next and the documents are categorized accordingly. The following is a possible set of document categories and International Standards that are relevant to documents in those categories.

– **Standards on issues specific to a smart grid** include IEC 61850 (all parts), IEC 61000-4-30 and IEC TR 62351-12.

– **Results from risk analysis** on a smart grid are obtained through application of IEC 60812, IEC 61025 and IEC 62551.

– **Dependability requirements** for a smart grid are formulated on the basis of IEC 60050-192 and IEC 60050-692 for vocabulary, and for contents, IEC 62853 (this document), IEC 60300-1, IEC 60300-3-4, IEC 61907, IEC 62347 and IEC 62673.

– **Life cycle documents** that specify the smart grid life cycle are developed on IEC 62853 (this document), IEC 60300-1, ISO/IEC/IEEE 15288, ISO/IEC TR 24774 and guides in ISO/IEC TS 24748-1, ISO/IEC TR 24748-2, ISO/IEC TR 24748-3, ISO/IEC/IEEE 24748-4, ISO/IEC/IEEE 24748-5 and ISO/IEC TS 24748-6.

– **System architecture models** are formulated on the basis of ISO/IEC/IEEE 42010 [6], IEC 61078 and others.

– **Operation-related information** is communicated following IEC 61850, IEC 61000-4-30, and IEC TR 62351-12.

– **Environmental related information** is classified using IEC 60721 (all parts).

– **Test and verification results** are managed according to IEC 62741.

– **Program code:** Software programs are coded using some specific language. The code is software modules to keep the voltage and frequency constant, control loads and respond to network failures as well as software to operate “firewalls” towards the consumers, distributors and the suppliers, and monitor unusual activities in the network (excessive consumption variations, unusual payments, unusual data traffic and possible malware code).

C.3.2.3 Step 3: Set “Service continuity and accountability in the ever-changing system is achieved” as the top-level claim

After the preparation of Steps 1 and 2, the main body of a dependability case construction starts with the definition of the top-level claim. The wording shown is suggested as a stylized opener signifying that the case is about open systems dependability. To define it is to establish its interpretation for the smart grid through defining terms (such as “the system”, “service continuity”) and making contextual information explicit. The power grid must have the least possible down time, recover quickly after failure and stay within the specified voltage and frequency under all load conditions. These goals are codified through the definition of the top-level claim.

C.3.2.4 Step 4: Attach dependability requirements, environmental information, and term definitions to the top-level claim as explicit context

The details established in Step 3 and its association with the top-level claim are recorded explicitly in the dependability case. When GSN is used as in Annex B, this is achieved by attaching to the claim a context node containing references to the documentation of the details. For the smart grid, the details might be: “the power grid is required to have an availability of 0,999 97”; “98 % of the down time has to be less than 1 h”; “further the voltage, frequency,

transients and disturbances must be within the specifications 99,8 % of the time"; "definitions of terms are according to IEC 60050-192 and IEC 60050-692"; "the geographical area covered by the power grid is Northern Europe with temperature, precipitation, wind and sun radiation as defined in IEC 61721".

C.3.2.5 Step 5: Plan the overall argument structure of the dependability case

Planning of the overall argument structure begins with the template provided in Annex B. Instantiation of the template for the smart grid, i.e. making the template into a concrete structured argument, involves decomposition of goals in the template to detailed subgoals specific to the smart grid and forming and/or refining of argument strategies for the new and old goals. The following lists examples of argument strategies suitable to topics of the goals specific to smart grid.

a) Argument strategies based on life cycle are suitable for goals involving
   1) concession (legal text),
   2) ownership of power grid, deeds and land charges registry certificates, contracts,
   3) transformer stations – specifications and drawings,
   4) voltage distribution networks – maps of cable and power lines, locations, connections and capacity, and
   5) contracts with wind turbine farms and solar cell farms.
b) Argument strategies based on system functionality are suitable for goals involving
   1) capacity of the suppliers, stiffness of grid.
c) Argument strategies based on workflow are suitable for goals involving
   1) variations in load and supplies, and
   2) variations in prices.
d) Argument strategies based on failure and risk reduction are suitable for goals involving
   1) prognosis on load and supply,
   2) reserve capacity and redundancy,
   3) procedure for uncoupling to reduce load,
   4) procedure for re-connection after uncoupling,
   5) procedure for "island" operation,
   6) procedure against malware in control system, and
   7) procedure against malware in price negotiation and accounting system.

NOTE Prognosis of consumption can be based on historical data for the load variation over day and night, working days and holidays, summer and winter. Prognosis on supply can be based on the time of the day (solar cells do not produce at night). Weather forecasts can predict cloud cover for solar cells and wind speed for wind turbines. For example, in a major storm the Danish wind turbines were producing electricity to cover the consumption of the whole country. But after a short time the wind turbines dropped out one by one because of too high wind speed.

C.3.2.6 Step 6: Attach the necessary documents as contexts and evidence

After the overall structure of the arguments has been determined, the documents required for each argument should be attached as contexts and evidence. Categorization of the documents input and output throughout the smart grid's life cycle guides this step.

C.3.2.7 Step 7: Develop those dependability subcases derivable from the documents

The arguments should now be developed in the context of the documents attached using the context in Step 6. Argument strategies often involve routine procedural examinations of the complicated context and evidence. Indicating what strategy is used is often not sufficient for readers of the case to fill the gap between the goal of the strategy and its subgoals and/or evidence. If so, the argument strategy is expanded to a dependability subcase that explains the execution result of the procedure in the given context and evidence based on the contents of the

documents. These subcases are often derivable (semi-)automatically, provided the documents are well-structured.

C.3.2.8 Step 8: Use established argument structures for non-derivable dependability subcases and complete the dependability case

The remaining parts of the planned overall argument structure not realized as derived subcases communicate arguments for, or supported by, expert judgments, accepted norms, agreed assumptions and opinions, unavoidable influences, etc. These subcases are developed manually on a case by case basis. However, it is good practice to seek and adopt argument structures for those that have been applied successfully in situations similar to the one at hand. Rationales behind relevant standards and regulations might be turned into successful argument structures. Use of established argument structures avoids difficulties in evaluating too diverse ad hoc arguments.

C.3.2.9 Step 9: Repeat the above steps as many times as necessary

The dependability case needs to be updated frequently since the system is an open system.

The configuration of the grid will change as new cables are laid, new power lines and transformer stations are built, modified or decommissioned.

Changes will occur in the number and capacity of the suppliers, especially wind turbine farms and solar panels. The consumers (factories, offices and households) will change frequently, as well as the distributors that they choose for their supply. The operator of the grid will usually have a concession which requires them to deliver to any customer within a geographical area.

Supply and price agreement will change, often from hour to hour, day and night over the year.

In the following the Change Accommodation Cycle and Failure Response cycle as shown in Figure A.1 are discussed.

These nine steps are introduced and further discussed in [11].

C.4 The Change Accommodation cycle

The Change Accommodation Cycle in the DEOS life cycle of the smart grid as a whole implements the Change Accommodation process view specified in 6.5 and, with respect to adaptations made to the smart grid, the Accountability Achievement process view in 6.3 and the Consensus Building process view in 6.2 (See Clause A.2). After Requirement elicitation and risk analysis the stakeholder's agreements are obtained according to Figure A.1. After that the initial version of the open system software is developed, compiled, verified and tested according to C.3.2.1. After a laboratory test and a test on a limited geographical area (an island), the software is put into use. The achievements and accountability are made explicit in the dependability case that accompanies the application for the licence to operate the smart grid. During ordinary operation, results and problems are monitored. Problems and events are divided into anomalies and failures that are treated through the Failure Response Cycle (Clause C.5), and changes in objectives and/or environments that are treated through the Change Accommodation Cycle. Changes in objectives can for example be a higher emphasis on renewable energy, a lowered target for CO_2 emission, more transparency in concessions and subvention price policy. Changes in environment can be caused by changes in supply structure like for example decommissioning of nuclear power plants, introduction of new international connections (cables), energy storage facilities (water reservoirs or air pressure caves) or conversion of surplus electricity to liquid fuel. Change in environment can also be drought and less snowfall in regions with major water power stations. The Change Accommodation Cycle is closed by new requirement elicitations and updated risk analysis leading to updated stakeholder agreements that together start a new design, implementation, verification and test process. In this respect open systems dependability is similar to the spiral model for software development with the

difference that for open systems the spiral processes continue for the whole operational life of the open system and not just during the initial software development.

C.5 The Failure Response Cycle

The Failure Response Cycle in the DEOS life cycle of the smart grid as a whole implements the Failure Response process view specified in 6.4 and, with respect to failure response, the Accountability Achievement process view in 6.3 and the Consensus Building process view in 6.2 (See Clause A.2). The Failure Response Cycle is initiated by a failure or an anomaly detection. A failure can, for example, be loss of power in an area due to a short circuit, for example, in the power network or a transformer station. The cause can be lightning strikes, overload of high tension wires from wind or ice damage to cables through excavation work or damage to undersea cables from the anchor of a ship. Failures like these tend to happen at random times, even though it is possible to predict the failure probability of a transformer based on age and condition.

For a power outage the first activity is to isolate the problem so that it does not propagate in the system. It might be necessary to uncouple part of the system to reduce the load. In extreme cases it might be necessary to change to “island operation”, i.e. operate the system as a conventional system with no supply from or delivery outside a closed area. The purpose of the failure response is to re-establish the power supply to all consumers in the shortest possible time.

This requires a controlled re-connection of suppliers and consumers. A major part of these activities is handled automatically or semi-automatically by the operation control software modules. Failure detection (or failure prediction) triggers the Failure Response Stage that consists of failure prevention, failure response and cause analysis. Failure response has been described above. Cause analysis is the activity to determine the cause of the outage; see IEC 62740 [19]. Some typical causes were described above. Failure prevention comprises, for example, changing from power lines on masts to cables and preventive maintenance of transformer stations. Activities like maps of cable locations for excavation activities and prohibition of anchoring near undersea cables will also assist failure prevention.

For an open system, anomaly detection is a very important activity. The software surveillance module should continuously watch for abnormal activities. This is primarily to detect attempts to infiltrate and control software with malware. This might happen through consumers which have network connections to the Internet, to the domestic power consuming and power producing devices as well as connection to the price supply and delivery negotiation and accounting subsystem. Anomaly detection also has to look for abnormal accounting like excessive money transfer and sudden changes in consumption or supply from a consumer. This continuous anomaly detection is also very important for open systems while it is less important for non-open systems like embedded software.

The operators of the open system have to maintain an around the clock preparedness to isolate potential malware and analyse and remove the threat. This can include placing some addresses, for example consumer addresses, in quarantine until the problem has been analysed and solved. The solution can include connection to the Change Accommodation Cycles through the requirement elicitation, risk analysis, stakeholder agreement and software development boxes (design, implementation, verification and test).

Bibliography

[1] ISO 26000:2010, *Guidance on social responsibility*

[2] ISO 15489-1:2001, *Information and documentation – Records management – Part 1: General* [1]

[3] ISO/IEC 15026-1, *Systems and software engineering – Systems and software assurance – Part 1: Concepts and vocabulary*

[4] ISO/IEC Guide 2:2004, *Standardization and related activities – General vocabulary*

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

[6] ISO/IEC/IEEE 42010:2011, *Systems and software engineering – Architecture description*

[7] ISO 22301:2012, *Societal security – Business continuity management systems – Requirements*

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

[9] United Nations International Strategy for Disaster Reduction (UNISDR). *Terminology on Disaster Risk Reduction*, 2009

[10] Laprie, Jean-Claude. "From dependability to resilience." *38th IEEE/IFIP Int. Conf. On Dependable Systems and Networks*, 2008

[11] Tokoro, Mario, ed. *Open Systems Dependability – Dependability Engineering for Ever-Changing Systems*. Second edition, CRC Press, 2015

[12] Bloomfield, Robin and Gashi, Ilir. *Evaluating the resilience and security of boundaryless, evolving socio-technical systems of systems*. Research report to DSTL, Centre for Software Reliability, City University, London, 2008

[13] Jamshidi, Mohammad, ed. *System of systems engineering: innovations for the twenty-first century*. John Wiley & Sons, 2011

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

[15] IEC 62741, *Demonstration of dependability requirements – The dependability case*

[16] ISO 31000, *Risk management – Principles and guidelines*

[17] IEC 31010, *Risk management – Risk assessment techniques* [2]

[1] ISO 15489-1:2001 has been cancelled and replaced by ISO 15489-1:2016.

[2] Under preparation. Stage at time of publication: IEC CDV 31010:2017.

[18] Origin Consulting LLC. *GSN Community Standard Version* 1. November 2011 [viewed 2016-01-14]. Available as <http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf>

[19] IEC 62740, *Root cause analysis (RCA)*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÛRETÉ DE FONCTIONNEMENT DES SYSTÈMES OUVERTS

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 62853 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	Rapport de vote
56/1772/FDIS	56/1776/RVD

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

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

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

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

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

INTRODUCTION

Les systèmes ouverts sont des systèmes dont les frontières, les fonctions et la structure changent avec le temps et qui sont envisagés et décrits différemment selon le point de vue. La sûreté de fonctionnement des systèmes ouverts est un attribut clé du cycle de vie d'un système qui fonctionne pendant une période prolongée dans un environnement réel. La sûreté de fonctionnement des systèmes ouverts est la capacité des systèmes ouverts à s'adapter aux changements apportés à leur objet, leurs objectifs, leur environnement et leurs performances réelles et à maintenir la redevabilité continue des parties prenantes de manière à fournir les services attendus au moment requis et lorsque cela est exigé. Les attributs de la sûreté de fonctionnement, tels que la disponibilité, la fiabilité, la maintenabilité et la supportabilité, sont les mêmes pour les systèmes ouverts que pour les systèmes conventionnels, mais ils doivent être envisagés dans un contexte où aucune partie prenante ne comprend pleinement le système et ses risques.

La sécurité des systèmes ouverts est particulièrement importante, car ces systèmes sont fortement exposés aux attaques des logiciels malveillants. Etant donné qu'un système ouvert évolue continuellement au cours de sa vie, le processus de conception (éventuellement modélisé par le modèle en spirale de développement de produits) se poursuivra, dans une certaine mesure, pendant toute sa durée de vie.

Le présent document précise l'IEC 60300-1 en fournissant des recommandations supplémentaires sur la gestion de la sûreté de fonctionnement des systèmes ouverts.

Le présent document contient des recommandations sur la sûreté de fonctionnement des systèmes ouverts qui s'appuient sur les quatre vues de processus, dont chacune sélectionne et combine des processus, activités et tâches du cycle de vie du système décrits dans l'ISO/IEC/IEEE 15288: 2015.

- vue de processus d'adaptation aux changements;
- vue de processus d'établissement de la redevabilité;
- vue de processus de réponse aux défaillances;
- vue de processus de recherche d'un consensus.

Il est crucial de réaliser une étude de sûreté de fonctionnement à l'appui de ces vues de processus pour que les parties prenantes comprennent et s'accordent sur les limites de leurs responsabilités, attribuent la redevabilité relative à la mise en œuvre et gèrent dûment les changements nécessaires à l'assurance de la sûreté de fonctionnement des systèmes ouverts.

Le présent document s'adresse aux utilisateurs, aux propriétaires, aux clients et aux organismes impliqués dans la conformité aux exigences de sûreté de fonctionnement des systèmes ouverts, et chargés de la garantir. On entend par "organismes" les entreprises, et institutions publiques ou privées de tous types et de toutes tailles, telles que les administrations publiques, les entreprises commerciales et les associations à but non lucratif.

SÛRETÉ DE FONCTIONNEMENT DES SYSTÈMES OUVERTS

1 Domaine d'application

Le présent document fournit des recommandations relatives à un ensemble d'exigences portant sur les cycles de vie des systèmes et visant à assurer la sûreté de fonctionnement des systèmes ouverts.

Le présent document précise l'IEC 60300-1 en fournissant des détails sur les changements nécessaires pour s'adapter aux caractéristiques des systèmes ouverts. Il définit les vues de processus basées sur l'ISO/IEC/IEEE 15288:2015, qui identifie l'ensemble des processus du cycle de vie du système.

Le présent document est applicable au cycle de vie des produits, des systèmes, des processus ou des services impliquant des aspects matériels, logiciels et humains ou toute combinaison intégrant ces éléments.

La sécurité des systèmes ouverts est particulièrement importante, car ces systèmes sont fortement exposés aux attaques des logiciels malveillants.

Le présent document peut être utilisé pour améliorer la sûreté de fonctionnement des systèmes ouverts et pour garantir que les vues de processus spécifiques aux systèmes ouverts donnent les résultats escomptés. Il aide les organismes à définir les activités et les tâches qui doivent être entreprises pour atteindre les objectifs de sûreté de fonctionnement dans un système ouvert, y compris en matière de communication relative à la sûreté de fonctionnement, ainsi que d'appréciation et d'évaluation de la sûreté de fonctionnement tout au long du cycle de vie du système.

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/)

IEC 60300-1, *Gestion de la sûreté de fonctionnement – Partie 1: Lignes directrices pour la gestion et l'application*

ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes* (disponible en anglais seulement)

3 Termes et définitions

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

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

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/

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

3.1
redevabilité
état consistant, pour une organisation, à être en mesure de répondre de ses décisions et activités à ses organes directeurs, ses autorités constituées et, plus largement, à ses parties prenantes

Note 1 à l'article: La redevabilité inclut l'obligation de rendre des comptes à la société en général.

Note 2 à l'article: Description dans l'ISO 26000:2010 [1]: La redevabilité implique une obligation de la direction à rendre des comptes aux détenteurs de participations de contrôle de l'organisme et une obligation de l'organisme à rendre des comptes aux autorités judiciaires aux niveaux législatif et réglementaire. La redevabilité vis-à-vis de l'impact global des décisions et activités de l'organisme sur la société et l'environnement implique également que son obligation de rendre des comptes aux personnes affectées ainsi qu'à la société en général varie selon la nature de l'impact et des circonstances.

Note 3 à l'article: Définition de l'ISO 15489-1:2001 [2]: principe selon lequel les personnes physiques et morales, ainsi que la collectivité, sont responsables de leurs actions et peuvent être tenus d'en rendre compte.

[SOURCE: ISO 26000:2010, 2.1, modifiée – Les notes à l'article ont été ajoutées.]

3.2
argumentaire
artefact raisonné et auditable créé à l'appui d'une affirmation générale (ou d'un ensemble d'affirmations), et qui comprend une argumentation systématique, les preuves et les hypothèses explicites qui l'étayent (ou qui les étayent)

Note 1 à l'article: Un argumentaire contient les éléments suivants et les liens entre ceux-ci:

– une ou plusieurs affirmations sur les propriétés;
– les arguments qui lient logiquement les preuves et toute hypothèse relative à la/aux affirmations;
– un ensemble de preuves et, potentiellement, les hypothèses étayant les arguments à l'appui de la/des affirmations;
– la justification du choix de l'affirmation générale et la méthode de raisonnement.

Note 2 à l'article: Un argumentaire peut être compris comme une argumentation raisonnée et concluante, étayée par un ensemble de preuves, selon laquelle un système, un service ou un organisme fonctionnera comme prévu pour une application définie, dans un environnement défini et sur une durée de vie définie.

[SOURCE: In English, ISO/IEC 15026-1:2013 [3], 3.1.3, modifiée – La Note 2 à l'article a été ajoutée.]

3.3
adaptation aux changements
ensemble d'activités qui modifient et adaptent un système aux changements apportés à son objet, ses objectifs, son environnement ou ses performances réelles et qui requiert le rétablissement du consensus entre les parties prenantes sur le système

3.4
consensus
accord général caractérisé par l'absence d'opposition ferme à l'encontre de l'essentiel du sujet émanant d'une partie importante des intérêts en jeu et par un processus de recherche de prise en considération des vues de toutes les parties concernées et de rapprochement des positions divergentes éventuelles

Note 1 à l'article: Le consensus n'implique pas nécessairement l'unanimité.

[SOURCE: Guide ISO/IEC 2:2004 [4], 1.7]

3.5
étude de sûreté de fonctionnement
argument basé sur des preuves, raisonné et traçable créé pour soutenir l'affirmation selon laquelle un système défini satisfait et/ou satisfera aux exigences de sûreté de fonctionnement

Note 1 à l'article: Une étude de sûreté de fonctionnement est un argumentaire dont l'affirmation générale porte sur la sûreté de fonctionnement.

[SOURCE: IEC 62741:2015, 3.1.1, modifiée – La Note 1 à l'article a été ajoutée.]

3.6
communication relative à la sûreté de fonctionnement
processus continu et itératif mené par une partie prenante afin de fournir, de partager ou d'obtenir des informations, et d'engager un dialogue avec les autres parties prenantes sur la gestion de la sûreté de fonctionnement

Note 1 à l'article: Le rôle de la communication relative à la sûreté de fonctionnement dans le cadre de la gestion de la sûreté de fonctionnement des systèmes ouverts n'est pas différent de celui de la communication relative au risque dans le cadre de la gestion des risques.

Note 2 à l'article: Voir la définition des termes "communication et concertation" dans le Guide ISO 73:2009 [5], 3.2.1.

3.7
environnement
<système> contexte déterminant le cadre et les circonstances de tous les facteurs d'influence sur un système

[SOURCE: ISO/IEC/IEEE 42010:2011 [6], 3.8]

3.8
réponse aux défaillances
ensemble d'activités initiées immédiatement après qu'une défaillance a été prédite ou détectée afin de prévenir la défaillance ou d'en réduire le plus possible les effets, d'en analyser les causes, d'en prévenir la récurrence et de répondre aux exigences de redevabilité

3.9
cadre de référence
ensemble de conventions applicables à l'élaboration, à l'interprétation et à l'utilisation de documents décrivant une compréhension commune d'un système, de son objet, de ses objectifs, de son environnement, de ses performances réelles, de son cycle de vie et des changements afférents, ainsi que des accords explicites sur ces questions

3.10
erreur d'interaction
erreur qui se produit en raison des interactions entre les éléments, et ce bien que chaque élément satisfasse aux spécifications de performances

3.11
supervision
détermination de l'état d'un système, d'un processus ou d'une activité

Note 1 à l'article: Pour déterminer cet état, il peut être nécessaire de vérifier, surveiller ou observer avec une vision critique.

[SOURCE: ISO 22301:2012 [7], 3.29]

3.12
système ouvert
système dont les frontières, les fonctions et la structure changent avec le temps et qui est envisagé et décrit différemment selon le point de vue

Note 1 à l'article: Par "changement", on entend non seulement l'adaptation à un objet spécifique, mais aussi toute évolution spontanée. Les changements spontanés et non coordonnés au sein d'un système qui couvre plusieurs domaines relevant d'autorités différentes sont par exemple inclus.

Note 2 à l'article: Non seulement les frontières, les fonctions et la structure d'un système ouvert varient dans le temps, mais elles peuvent également être imprécises à tout instant t et être envisagées différemment par les différentes parties prenantes. Ces éléments précisent la définition du système proposée dans l'IEC 60050-192 pour un niveau d'abstraction et un point de vue donnés. Une frontière peut avoir une définition claire à un certain niveau d'abstraction, et perdre en précision à un niveau plus détaillé. Il n'est pas nécessaire de prédéterminer le niveau de détail nécessaire pour un objet ou une partie prenante ni de garantir qu'il peut être atteint.

Note 3 à l'article: Un système ouvert échange les ressources au-delà de ses frontières, avec d'autres systèmes ou avec l'environnement, ce qui modifie potentiellement la frontière elle-même.

Note 4 à l'article: Chaque système substantiel combine des aspects d'un système ouvert et d'un système conventionnel. L'expression "système ouvert" n'est pas utilisée pour la classification des systèmes. Elle s'applique à un système lorsque ses aspects ouverts sont importants dans la discussion relative au système.

Note 5 à l'article: Le fait qu'un système logiciel puisse être "open source" n'a aucun rapport avec le fait qu'il s'agisse d'un système ouvert, en dehors du fait qu'être un logiciel open source lui confère nécessairement certains aspects propres aux systèmes ouverts, tels que l'absence d'autorité centralisée.

3.13
sûreté de fonctionnement des systèmes ouverts
capacité à s'adapter aux changements d'objet, d'objectifs, d'environnement et de performances réelles et à assurer une redevabilité continue, de manière à fournir les services attendus au moment requis et de la manière requise

3.14
processus
ensemble d'activités corrélées ou en interaction qui utilise des éléments d'entrée pour produire un résultat escompté

Note 1 à l'article: La désignation du "résultat escompté" d'un processus par élément de sortie, produit ou service dépend du contexte de la référence.

Note 2 à l'article: Les éléments d'entrée d'un processus sont généralement les éléments de sortie d'autres processus et les éléments de sortie d'un processus sont généralement les éléments d'entrée d'autres processus.

Note 3 à l'article: Deux processus, ou plus, corrélés et en interaction en série peuvent également être qualifiés de processus.

Note 4 à l'article: Les processus d'un organisme sont généralement planifiés et mis en œuvre dans des conditions maîtrisées afin d'apporter une valeur ajoutée.

Note 5 à l'article: Lorsque la conformité de l'élément de sortie résultant ne peut pas être immédiatement ou économiquement validée, le processus est souvent qualifié de "procédé spécial".

Note 6 à l'article: Il s'agit de l'un des termes communs et définitions de base pour les normes de systèmes de management de l'ISO, donnés dans l'Annexe SL du Supplément ISO consolidé aux Directives ISO/IEC, Partie 1. La définition originale a été modifiée afin d'éviter toute circularité entre processus et élément de sortie, et les Notes 1 à 5 à l'article ont été ajoutées.

[SOURCE: ISO 9000:2015 [8], 3.4.1]

3.15
vue de processus
ensemble de processus, d'activités et de tâches qui met l'accent sur une préoccupation particulière d'une partie prenante quant à un système, d'une manière transversale sur l'ensemble du cycle de vie ou sur des parties de celui-ci

3.16
résilience
capacité d'adaptation dans un environnement complexe et changeant

Note 1 à l'article: Définition de la résilience dans la Terminologie de l'UNISDR sur la Réduction des risques de catastrophe [9]: capacité d'un système, d'une communauté ou d'une société exposée à des dangers à résister, à absorber, à s'adapter et à se remettre des effets d'un danger de manière rapide et efficace, y compris à travers la préservation et le rétablissement de ses structures et fonctions de base essentielles.

Note 2 à l'article: Définition de [10]: persistance de l'aptitude à délivrer un service de confiance justifiée en cas de changements.

[SOURCE: Guide ISO 73:2009, 3.8.1.7, modifiée – La définition a été révisée pour ne pas s'appliquer qu'aux organismes, et les notes à l'article ont été ajoutées.]

3.17
partie prenante
personne ou organisme ayant un droit, une participation, une revendication ou un intérêt à l'égard d'un système ou du fait qu'il présente des caractéristiques répondant à ses besoins et à ses attentes

EXEMPLE Utilisateurs finaux, organismes utilisateurs finaux, logisticiens, développeurs, producteurs, formateurs, agents de maintenance, agents chargés de la mise au rebut, acquéreurs, organismes fournisseurs et organismes de réglementation.

Note 1 à l'article: Certaines parties prenantes peuvent avoir des intérêts contraires entre elles ou contraires à ceux du système.

Note 2 à l'article: Le terme "partie intéressée" fait partie des termes et définitions de base communs applicables aux systèmes de management normalisés par l'ISO, définis dans l'Annexe SL du Supplément ISO consolidé aux Directives ISO/IEC, Partie 1. Le présent document utilise le terme admis de "partie prenante", conformément à l'ISO/IEC/IEEE 15288:2015.

[SOURCE: In English, ISO/IEC/IEEE 15288:2015, 4.1.44, modifiée – La Note 2 à l'article a été ajoutée.]

4 Sûreté de fonctionnement des systèmes ouverts

4.1 Systèmes ouverts

Les systèmes ouverts présentent les caractéristiques suivantes (voir [11]).

– Ils sont larges, complexes et interconnectés.
– Ils peuvent inclure des composants de boîte noire.

NOTE 1 Un composant de boîte noire est un composant dont les utilisateurs ne connaissent pas les détails de mise en œuvre et ne peuvent pas contrôler la fonctionnalité et l'interface.

– Leur objet, leurs objectifs, leur environnement et leurs performances réelles ne sont pas déterminés et ils varient au cours de leur vie. Les changements imprévisibles des exigences des utilisateurs, des objectifs de service, des services reçus via le réseau, des composants de boîte noire, des bases technologiques, etc., sont fréquents.
– Leurs frontières, leurs fonctions et leur structure ne cessent d'évoluer et sont perçues différemment par les différentes parties prenantes. Les empêcher de devenir trop imprécises requiert un effort particulier.
– La redevabilité est vitale dans leur cycle de vie et pour assurer la maîtrise des risques, mais son établissement nécessite un effort particulier en raison de l'absence de contrôle central efficace.
– La compréhension des systèmes et de leurs risques par les parties prenantes n'est ni complète ni certaine, à aucun moment donné.
– Les défaillances potentielles dues à une compréhension incomplète des systèmes, à des changements et à des événements non anticipés ne peuvent pas être éliminées ni prévues. Les systèmes doivent être résilients, comporter des dispositifs de maîtrise des risques (notamment des dispositifs antierreur) et de récupération après ces défaillances, et s'adapter afin d'empêcher qu'elles ne se reproduisent.
– Garantir la sûreté de fonctionnement requiert une approche itérative et dépend de l'intégration du fonctionnement et du développement du système. La réalisation des activités de sûreté de fonctionnement tout au long du cycle de vie du système et leur itération aussi souvent que nécessaire revêt une importance particulière pour les systèmes ouverts.

NOTE 2 Certaines de ces fonctionnalités sont partagées avec ce que l'on appelle les "systèmes de systèmes" [12], [13] et les "systèmes non limités ou faiblement limités".

NOTE 3 Selon le point de vue, la plupart des systèmes disposent de ces fonctionnalités à un certain degré, même négligeable. Un système est appelé ouvert lorsque ces fonctionnalités du système sont importantes dans la discussion en cours, qu'il s'agisse d'un système de systèmes ou non.

Un système échange nécessairement des services avec de nombreux autres systèmes interconnectés et gérés indépendamment. Ces systèmes environnants sont gérés selon leurs propres principes et parties prenantes, et leurs interfaces sont susceptibles d'être modifiées pour diverses raisons. Le système doit servir à diverses parties prenantes. Chaque partie prenante a des objectifs différents, et il se peut que le système ne relève pas d'une seule autorité; par ailleurs, les objectifs du système et les systèmes environnants changent avec le temps. Les conditions applicables au système, telles que les exigences et contraintes, changent fréquemment et de manière imprévisible. Ces conditions sont par conséquent incertaines et incomplètes et elles ne peuvent pas être comprises complètement à tout moment donné.

Etant donné qu'un système ouvert évolue continuellement au cours de sa vie, le processus de conception (modélisé par le modèle en spirale de développement de produits) se poursuivra, dans une certaine mesure, pendant toute sa durée de vie.

En outre, il existe des incertitudes et des lacunes au niveau du système lui-même, par exemple en ce qui concerne ses fonctions, sa structure interne et ses frontières. Ses sous-systèmes sont souvent gérés par des parties différentes et les personnes participant à l'intégration et à la coordination des frontières du système peuvent ne pas en avoir une connaissance et une maîtrise complètes. Les services et les composants peuvent être ajoutés ou retirés du système pendant son fonctionnement par et pour différentes parties prenantes. Cette nature dynamique rend les frontières, les fonctions et la structure du système ambiguës dans la pratique, même s'il n'y a en théorie aucune ambiguïté, à aucun moment, d'aucun point de vue.

Pour ces motifs, et en raison de la complexité et de la taille du système, il est très difficile pour toute partie prenante de spécifier, d'appréhender ou de maîtriser le système et sa gestion de manière suffisamment complète et certaine. Les changements et défaillances non anticipés de différents degrés font partie de la nature du système. L'utilisation du terme "systèmes ouverts" met en lumière cet aspect.

Les véritables attentes implicites vis-à-vis du système dépendent toujours du contexte, c'est-à-dire des systèmes environnants et des parties prenantes. Il convient que les objectifs des divers niveaux de systèmes qui entourent le système cible soient pris en compte. A mesure que le contexte change et que les lacunes et incertitudes sont résolues d'une manière ou d'une autre, il convient que le système s'adapte aux changements correspondants des exigences et des hypothèses. Ces changements ne peuvent être totalement anticipés ou spécifiés par avance.

4.2 Problèmes de sûreté de fonctionnement spécifiques aux systèmes ouverts

La sûreté de fonctionnement des systèmes ouverts vise à assurer la continuité du service sur des périodes prolongées en dépit des changements et défaillances. Le maintien de la continuité de service impose des exigences tout au long du cycle de vie du système et de ses itérations, avec le soutien des activités d'amélioration.

La gestion de la sûreté de fonctionnement décrite dans l'IEC 60300-1 s'applique généralement aux systèmes ouverts et le présent document doit être utilisé comme un complément à l'IEC 60300-1. L'IEC 60300-1 requiert que l'amélioration continue soit assurée au moyen de la planification et du contrôle des activités d'amélioration ainsi que des revues d'avancement appropriées. La sûreté de fonctionnement des systèmes ouverts s'appuie sur cette base, car elle dépend directement des améliorations liées aux changements imprévisibles fréquents. Une approche itérative du cycle de vie peut être appliquée pour permettre l'adaptation à ces changements (voir l'Annexe A).

Le domaine d'application de la gestion de la sûreté de fonctionnement d'un système ouvert n'est pas trivial en raison des caractéristiques expliquées en 4.1. Le simple respect d'accords explicites ne suffit pas, car aucun accord ne peut couvrir de manière adéquate tous les aspects du système considéré, et aucun système ouvert ne peut être complètement défini. Les parties prenantes doivent être préparées à agir au-delà des accords, dans une compréhension commune du système et de son environnement. En principe, la sûreté de fonctionnement des systèmes ouverts vise à renforcer la confiance dans le système même en cas d'hypothèses infirmées, d'exigences invalidées par des changements et d'éventuelles défaillances du système.

L'argument ci-dessus met en lumière l'importance des processus qui revoient et révisent en continu le domaine d'application de la gestion de la sûreté de fonctionnement et qui fournissent une documentation explicite et un accord relatif audit domaine d'application. L'accord relatif au domaine d'application conclu par les parties prenantes doit reposer sur des accords relatifs à la redevabilité.

Les causes non anticipées ne peuvent pas être prévenues. Il est néanmoins possible d'identifier les fonctions principales, d'anticiper les possibles conséquences de la perte de ces fonctions principales et de protéger ces fonctions principales afin qu'elles puissent être rétablies rapidement ou couvertes par la redondance.

4.3 Objectif

La sûreté de fonctionnement des systèmes ouverts a pour objectif de maintenir un certain niveau de continuité de service pour un système dans le contexte des systèmes environnants, des parties prenantes et de l'environnement, dans la mesure du possible, en cas d'événements non anticipés et de changements dus à la nature incomplète et incertaine des connaissances des parties prenantes.

Les systèmes ne sont plus considérés comme définitifs, mais comme des systèmes ouverts, impossibles à connaître de manière complète ou certaine. Il convient qu'un système intégrant la sûreté de fonctionnement des systèmes ouverts ait la capacité:

– d'éliminer de manière continue les facteurs susceptibles de provoquer des défaillances, et donc de s'améliorer lui-même;
– de prendre des mesures rapides et appropriées en cas de défaillance;
– de prévenir, de réduire et d'atténuer les dommages;
– de fournir de manière continue les services anticipés par les parties prenantes dans la mesure du possible (dégradation progressive);
– de maintenir les activités et les tâches de manière à assurer une redevabilité quant aux opérations et processus du système;
– d'aider à comprendre et à communiquer les hypothèses formulées lors de la description du système, à documenter explicitement ces hypothèses et à déterminer le niveau de sûreté de fonctionnement du système à travers la documentation et l'autorité chargée de l'accepter.

Ces capacités sont attendues de la part de tout système qualifié de sûr au sens de la sûreté de fonctionnement, bien qu'elles aient une importance particulière pour les systèmes ouverts, plus susceptibles d'être affectés par des changements observés dans d'autres systèmes qui lui sont reliés. Le niveau de sûreté de fonctionnement spécifique des systèmes ouverts tient aux lacunes et aux incertitudes en dépit desquelles ces capacités doivent être établies. Elle ne diffère donc pas de la sûreté de fonctionnement conventionnelle, mais elle se définit comme un processus permettant d'atteindre la capacité en question.

4.4 Garantie de la sûreté de fonctionnement des systèmes ouverts

Pour qu'un système ouvert soit sûr, il convient que son cycle de vie permette aux parties prenantes:

a) d'établir un cadre de référence compris par toutes les parties prenantes et traitant du système, de son objet, de son fonctionnement, de son environnement et des changements afférents, puis d'établir une compréhension commune et des accords explicites sur ces questions dans ce cadre de référence;

b) de rendre transparente la relation entre une incapacité à exécuter une partie de l'accord entre les parties prenantes et ses implications pour les parties prenantes et la société en général, y compris l'obligation, pour les parties prenantes redevables, de trouver des solutions, afin que les efforts nécessaires soient déployés pour honorer l'accord et garantir l'existence de solutions en cas de dommages potentiels;

c) de planifier et d'appliquer des mesures immédiates contre les défaillances afin de fournir les services attendus, dans la mesure du possible, avec le moins de perturbations et de dommages possible, de la manière la plus opportune dans le contexte;

d) d'organiser les activités découlant de l'adaptation du système aux changements de son environnement, de son objet, de l'accord, etc., et de tirer profit de l'expérience des défaillances précédentes afin d'améliorer la sûreté de fonctionnement en continu.

Ces quatre pratiques sont applicables concomitamment et chacune dépend des autres. Le point a) établit les bases de b), c) et d). Le point b) contribue à appliquer les accords mentionnés en a) et promeut la confiance du public dans le système en communiquant les plans et les activités exécutés conformément à c) et d). Le point c) donne les informations nécessaires à b) et déclenche le point d) pour prévenir la récurrence des défaillances. Le point d) relance le processus a) afin de refléter les changements dépendants du temps dans la compréhension commune et les accords explicites de a), qui est toujours un instantané provisoire nécessitant une mise à jour continue.

La manière dont ces quatre pratiques sont combinées et se complètent peut être représentée sous forme de modèles de cycle de vie. L'Annexe A en donne des exemples. Un exemple d'application de la sûreté de fonctionnement des systèmes ouverts à un système ouvert concret est donné à l'Annexe C.

4.5 Relation avec la résilience et la tolérance aux pannes

Le concept de résilience pour les systèmes ouverts est très similaire à celui qui s'applique aux systèmes conventionnels. La résilience traditionnelle (voir 3.16 et Note 1 à l'article) souligne la capacité d'un système à reprendre un fonctionnement normal après des perturbations, tandis que la sûreté de fonctionnement des systèmes ouverts tient compte du fait que même la définition du "fonctionnement normal" varie dans le temps ou suivant le point de vue. Un concept plus récent de résilience (voir 3.16, Note 2 à l'article) tient compte d'une gamme plus large de changements et d'adaptations et partage l'objectif de la sûreté de fonctionnement des systèmes ouverts. La seule différence est la suivante: la sûreté de fonctionnement des systèmes ouverts se concentre sur les cas où les changements et les adaptations nécessaires découlent de l'ouverture des systèmes, et donc sur les notions de consensus et de redevabilité dans une approche axée sur le cycle de vie du système.

L'idée de tolérance aux pannes, en revanche, diffère entre les systèmes conventionnels et les systèmes ouverts. Dans un système conventionnel, il est présumé possible, au moins en principe, d'énumérer toutes les pannes importantes potentielles. Une procédure fixe et concrète visant à réduire l'écart par rapport au fonctionnement normal est donnée pour obtenir la tolérance aux pannes; les notions d'écart et de fonctionnement normal y sont définies de manière explicite. La sûreté de fonctionnement des systèmes ouverts, quant à elle, concerne une situation où ces notions ne peuvent pas être définies de manière explicite.

5 Conformité

Pour que le cycle de vie d'un système prenne en charge la sûreté de fonctionnement des systèmes ouverts, il convient de fournir une étude de sûreté de fonctionnement [14], [15] démontrant ce qui suit:

a) le cycle de vie du système satisfait aux exigences de toutes les vues de processus spécifiées à l'Article 6;

b) l'adéquation de ces exigences à garantir la sûreté de fonctionnement des systèmes ouverts pour le système cible a été prise en compte.

NOTE 1 L'étude de sûreté de fonctionnement est nécessaire pour s'assurer que les parties prenantes comprennent et s'accordent sur les limites de leurs responsabilités, et attribuent la redevabilité relative à la mise en œuvre et à la gestion des changements de manière appropriée.

NOTE 2 De par sa nature, la sûreté de fonctionnement des systèmes ouverts n'est pas démontrée par un ensemble de conditions suffisantes fixes. La conformité de chaque application du présent document est évaluée au regard des considérations supplémentaires mentionnées en b) et compte tenu des spécificités de l'objectif.

Un modèle d'étude de sûreté de fonctionnement qui démontre les affirmations ci-dessus est donné en Annexe B à titre d'information.

6 Vues de processus visant à assurer la sûreté de fonctionnement des systèmes ouverts

6.1 Généralités

L'Article 6 décrit les quatre vues de processus qui traitent des quatre pratiques de sûreté de fonctionnement des systèmes ouverts exposées en 4.4 a) à d). Certaines des activités et tâches requises pour mettre en œuvre ces processus sont tirées de l'ISO/IEC/IEEE 15288:2015.

Chaque pratique de sûreté de fonctionnement des systèmes ouverts nécessite un ensemble d'activités et de tâches recoupant de nombreux processus de cycle de vie. Le concept de vue de processus est introduit afin de regrouper au même endroit un ensemble d'activités associées décrit dans l'ISO/IEC/IEEE 15288:2015, Annexe E.

L'Article 6 spécifie les quatre vues de processus qui sont conformes au point de vue de processus décrit dans l'ISO/IEC/IEEE 15288. Une vue de processus est définie à partir des informations suivantes:

a) nom de la vue de processus;

b) objet de la vue de processus;

c) résultats de la vue de processus;

d) identification et description du processus, des activités et des tâches qui mettent en œuvre la vue de processus et les références aux sources pour ces processus, activités et tâches dans d'autres normes.

L'Article 6 spécifie chacune des quatre vues de processus en donnant les éléments a) à d) ci-dessus.

Les quatre vues de processus fonctionnent ensemble pour atteindre l'objectif de sûreté de fonctionnement des systèmes ouverts. Avec les autres processus de cycle de vie du système et vues de processus, elles forment un modèle de cycle de vie du système conforme aux exigences pour chaque application de l'ISO/IEC/IEEE 15288:2015 comme indiqué en Annexe A.

NOTE 1 L'ISO/IEC/IEEE 15288 décrit les processus, ainsi que les activités et les tâches correspondantes. Des ensembles sélectionnés de ces processus peuvent être appliqués tout au long du cycle de vie pour gérer et réaliser les phases du cycle de vie d'un système.

NOTE 2 L'avant-dernier alinéa du Paragraphe 4.4 souligne les relations entre les quatre vues de processus. L'Article A.2 décrit ces relations à travers un exemple de modèle de cycle de vie.

Dans le reste de l'Article 6, chaque paragraphe (par exemple le Paragraphe 6.i) décrit une vue de processus et est organisé comme suit.

Le titre de 6.*i* est le nom de la vue de processus (a).

Le Paragraphe 6.*i*.1, "Objet", précise l'objet de la vue de processus (b). Le premier paragraphe correspond au message clé de l'objet; les paragraphes suivants ajoutent quelques explications.

Le Paragraphe 6.*i*.2, "Résultats", établit la liste des résultats du processus (c). Dans certains cas, les résultats sont triés hiérarchiquement. L'Annexe B contient une structure de modèle d'argumentation pour les études de sûreté de fonctionnement utilisant les résultats, qui permet d'apporter des éléments de justification pour la sélection des résultats.

Le Paragraphe 6.*i*.3 "Processus, activités et tâches" constitue la partie principale du présent document. Il établit la liste des processus, activités et tâches (d) de l'ISO/IEC/IEEE 15288 qui mettent en œuvre la vue de processus, avec des conseils spécifiques à la réalisation de la sûreté de fonctionnement des systèmes ouverts. Pour chaque processus conforme à l'ISO/IEC/IEEE 15288, un paragraphe facultatif décrit sa pertinence vis-à-vis de la vue de processus; il est suivi d'une liste de descriptions détaillées des activités et tâches associées, avec des indications du résultat de la vue de processus. Les descriptions au 6.*i*.3 doivent être utilisées comme des compléments à celles de l'ISO/IEC/IEEE 15288:2015, qui contient les définitions et les contextes des processus, activités et tâches associés.

Le Paragraphe 6.*i*.3 contient des références à des articles de l'ISO/IEC/IEEE 15288:2015 et à des articles du présent document. Elles se distinguent de la manière suivante. Des crochets en chevron (<>) sont utilisés pour faire référence au numéro de paragraphe d'un processus dans l'ISO/IEC/IEEE 15288:2015 et à l'étiquette d'élément de liste d'une activité ou d'une tâche dans le cadre de ce processus. Par exemple, "<6.4.2> Processus de définition des besoins et exigences des parties prenantes" fait référence au Paragraphe 6.4.2 de l'ISO/IEC/IEEE 15288:2015 et, dans le contexte de <6.4.2>, "<a)1)>" fait référence à la tâche "1) Identifier les parties prenantes qui ont un intérêt dans le système tout au long de son cycle de vie" dans le cadre de l'activité "a) Préparer la définition des besoins et exigences des parties prenantes". Pour une liste à deux niveaux, une référence à un élément de liste de niveau 1, par exemple "<a)>", fait référence à l'ensemble des éléments de niveau 2 <a)1)>, <a)2)>, …, <a)n)> qui constituent l'élément de niveau 1 <a)>. Les crochets droits ([]) sont utilisés pour faire référence à l'étiquette d'élément de liste du résultat d'une vue de processus au Paragraphe 6.*i*.2 du présent document.

6.2 Vue de processus de recherche d'un consensus

6.2.1 Objet

La vue de processus de recherche d'un consensus a pour objet d'établir et de maintenir une compréhension commune et des accords explicites sur le système, son objet, ses objectifs, son environnement, ses performances réelles, son cycle de vie et les changements afférents.

NOTE 1 Contrairement aux accords explicites, la compréhension commune du système n'est pas nécessairement documentée de manière explicite et inclut l'attitude, les croyances, les perceptions et les valeurs partagées par les parties prenantes.

Il convient de parvenir à cette fin (l'objet) en tenant compte des points suivants.

Il convient de s'assurer que la même compréhension est partagée par l'ensemble des parties prenantes de manière à ce que l'écart inévitable qui demeure entre les interprétations soit acceptable. Les accords explicites incluent les accords couvrant les avantages et responsabilités des parties prenantes en matière de développement et d'exploitation du système, ainsi que les accords qui portent sur les hypothèses formulées.

L'établissement de la compréhension commune et des accords explicites constitue une mesure préventive générique contre les événements non anticipés.

NOTE 2 Certaines parties prenantes peuvent se contenter de comprendre que les autres parties prenantes garantissent les résultats souhaités, sans exprimer le besoin de comprendre tous les détails que cela implique.

La réalisation de la finalité de cette vue de processus passe par:

– l'établissement d'une compréhension commune et d'un accord explicite entre les parties prenantes [6.2.2 résultats a)1) à a)7)];
– la maintenance de la compréhension et de l'accord [b)1) à b)5)].

La relation entre l'objectif et les résultats est décrite à l'Article B.2.

6.2.2 Résultats

a) Une compréhension commune et des accords explicites sont établis entre les parties prenantes.

1) Les parties prenantes du système sont identifiées.

NOTE 1 La liste des parties prenantes évolue avec le temps et selon le point de vue.

2) Un cadre de référence compris par toutes les parties prenantes est établi. Ce cadre comprend le vocabulaire et les hypothèses de base sur l'environnement du système.

3) L'objet, les objectifs, l'environnement, les performances réelles, le cycle de vie du système et les changements afférents sont compris de la même manière dans le cadre de référence par chaque partie prenante. Il en va de même des hypothèses relatives au système et aux responsabilités des parties prenantes.

4) Un processus d'arbitrage est préconvenu pour les situations dans lesquelles aucun consensus ne peut être atteint, afin que les conflits d'intérêts puissent être résolus.

NOTE 2 Les conflits d'intérêts peuvent inclure les conflits qui ont trait aux droits de propriété intellectuelle.

5) Des accords explicites sont développés à partir de la compréhension visée en 3), puis sont consignés. Les enregistrements comprennent des comptes-rendus de leur développement et le raisonnement qui explique pourquoi les différentes parties des accords sont considérées comme appropriées et réalisables.

6) Les différences d'interprétation des documents de l'accord restent dans des limites acceptables.

7) Les résultats ci-dessus sont atteints de manière juste et équitable pour toutes les parties prenantes.

NOTE 3 L'équité et la bonne foi contribuent à la résilience face aux événements non anticipés. L'absence d'équité et de bonne foi entraînent à long terme des problèmes qui affectent toutes les parties prenantes.

NOTE 4 L'extorsion d'opinions et d'exigences, par exemple, n'est pas un acte équitable ni de bonne foi, et aura à long terme un impact disproportionné, provoquant l'incapacité des grands systèmes ouverts à atteindre leurs objectifs.

b) La compréhension commune et l'accord explicite entre les parties prenantes sont maintenus.

1) La politique de gestion des changements relatifs aux accords est établie.

NOTE 5 Cette politique s'applique à toutes les phases, y compris à l'identification initiale des exigences du service et à leur révision.

2) Le consensus entre les parties prenantes est maintenu lorsque les objectifs commerciaux, les besoins des parties prenantes, le système ou l'environnement changent.

NOTE 6 Ces changements peuvent être rendus nécessaires par un traitement post-défaillance.

NOTE 7 Le maintien du consensus entre les parties prenantes implique qu'il soit révisé, validé et renouvelé de manière à refléter les nouveaux objectifs, besoins, système et environnement après un changement.

3) Les processus d'établissement d'un consensus sont examinés lorsque les objectifs commerciaux, les besoins des parties prenantes, le système ou l'environnement changent.

NOTE 8 Le consensus peut être limité à une partie des activités ou à certaines parties prenantes, et n'avoir aucune influence sur le reste des activités ou les autres parties prenantes. Les parties prenantes peuvent également, par acceptation passive, choisir de ne pas s'impliquer dans des questions qui n'ont pour elles aucune

importance ou qu'une importance limitée. Souvent, une activité est contrôlée par un petit groupe de parties prenantes spécialisées, ce que le reste des parties prenantes acceptent tant que les performances sont acceptables et que leurs intérêts vitaux ne sont pas affectés.

NOTE 9 Les mesures visant à impliquer les parties prenantes sont décrites au Paragraphe 5.3 de l'IEC 60300-1:2015 (troisième élément de la liste détaillée).

4) La responsabilité de la production et de l'approbation de l'étude de sûreté de fonctionnement est définie.

5) La réalisation du consensus, un compte-rendu de son développement et l'explication des raisons pour lesquelles le consensus est considéré comme approprié et réalisable sont consignés dans l'étude de sûreté de fonctionnement (voir IEC 62741 [15]).

6.2.3 Processus, activités et tâches

Il convient que la vue de processus de recherche d'un consensus soit mise en œuvre sur la base des activités et des tâches du processus suivant tiré de l'ISO/IEC/IEEE 15288.

NOTE 1 Dans ce qui suit, des chevrons simples (<>) sont utilisés pour faire référence aux numéros de paragraphes et aux étiquettes d'éléments de liste dans l'ISO/IEC/IEEE 15288:2015. Les crochets droits ([]) sont utilisés pour faire référence à l'étiquette d'élément de liste correspondant au résultat d'une vue de processus du présent document. Voir le dernier paragraphe de 6.1 pour de plus amples informations.

<6.1.1> Le Processus d'acquisition établit et maintient, entre un acquéreur et un fournisseur, un accord qui fait partie des accords explicites visés en [a), b)]. Il convient que les acquéreurs tiennent compte des préoccupations des parties autres que les acquéreurs et fournisseurs, telles que les utilisateurs finaux, la communauté locale et les organismes de réglementation [a)].

– <a)1)>: Il convient que la stratégie d'acquisition clarifie les tactiques destinées à parvenir à une compréhension commune et à des accords explicites dans [a)].
– <c)1), c)4)>: Il convient que le développement et les négociations relatives aux modifications de l'accord entre l'acquéreur et le fournisseur soient menés de manière équitable et de bonne foi [a)7)].
– <d)>: La supervision de l'accord fait partie de la politique et vise à maintenir l'accord explicite [b)1), b)2), b)3)].
– <d)1)>: Il convient d'inclure l'évaluation de l'équité et de la bonne foi à l'évaluation de l'exécution de l'accord [a)7)].

<6.1.2> Le Processus de fourniture établit et maintient, entre l'acquéreur et le fournisseur, un accord qui fait partie des accords explicites visés en [a), b)]. Il convient que les fournisseurs tiennent compte des préoccupations des parties autres que les acquéreurs et fournisseurs, telles que les utilisateurs finaux, la communauté locale et les organismes de réglementation [a)].

– <a)1)>: L'identification des acquéreurs fait partie de l'identification des parties prenantes [a)1)].
– <a)2)>: Il convient que la stratégie de fourniture clarifie les tactiques pour réaliser [a)].
– <c)1), c)4), d)1)>: Il convient de mener les négociations et l'exécution d'un accord de manière équitable et de bonne foi [a)7)].
– <d)2)>: Il convient d'inclure l'évaluation de l'équité et de la bonne foi à l'évaluation de l'exécution de l'accord [a)7)].

<6.2.1> Il convient que le Processus de gestion du modèle de cycle de vie spécifie les liens entre les processus du cycle de vie qui permettent la réalisation de tous les résultats de cette vue de processus [a), b)].

<6.2.5> Le Processus de gestion de la qualité formule les aspects de la compréhension commune et des accords explicites en tant que qualités gérées. Il gère également la qualité de la compréhension commune et des accords explicites [a), b)].

– <a)1)>: Il convient que les politiques, objectifs et procédures de gestion de la qualité traitent du niveau de compréhension commune et du niveau de consentement aux accords explicites [a) et b)]. Il convient que les parties prenantes développent une compréhension

commune et des accords explicites sur la gestion de la qualité en tenant compte du fait que, en général, aucune organisation centrale ne gère la qualité du système dans son ensemble [a), b)].

– <a)2), a)3)>: Il convient que la compréhension commune de la gestion de la qualité tienne compte du fait que les définitions des responsabilités et des critères d'évaluation ne sont pas parfaites et sont susceptibles d'être modifiées; il convient aussi que les parties prenantes soient préparées à agir, si nécessaire, au-delà de leur responsabilité définie dans l'intérêt de la qualité globale [b)].

– <a)3)>: Il convient de développer les critères d'évaluation de manière équitable et de bonne foi [a)7)].

<6.2.6> Le Processus de gestion des connaissances constitue une source de la compréhension commune.

– <a)1), b)1), c)1)>: Il convient que la stratégie de gestion des connaissances, la classification pour le partage des connaissances et une taxonomie visant à organiser les connaissances fournissent un cadre de référence compris par toutes les parties prenantes [a)2)].

– <d)>: Il convient d'intégrer la maintenance des connaissances à la maintenance de la compréhension commune et des accords explicites [b)].

<6.3.1> Le Processus de planification de projet englobe la compréhension commune et les accords explicites sous forme de plans [a), b)].

– <a), b)1) à b)6)>: Il convient que la définition et la planification du projet (objectifs, contraintes, domaine d'application, modèle de cycle de vie, organigramme technique du projet, échéancier, critères de réalisation des phases du cycle de vie, coûts et budget, rôles, responsabilités, redevabilités, etc.) reflètent la compréhension commune et les accords explicites et contribuent à les approfondir et à les clarifier, formant ainsi la base de leur maintenance [a)2), a)3), a)5), a)6), b)1), b)2), b)3)].

– <b)4)>: Il convient que la responsabilité de l'étude de sûreté de fonctionnement soit définie dans les plans de projet [b)4)].

– <b)7)>: Il convient que la communication et l'examen des plans fassent partie du développement et du maintien des accords explicites et que l'examen fournisse et consigne les justifications des accords [a)5), b)2), b)5)].

<6.3.2> Le Processus d'évaluation et de contrôle du projet régit la maintenance de la compréhension commune et des accords explicites lorsque des changements surviennent.

– <b), c)>: L'évaluation et le contrôle du projet incluent l'évaluation et le contrôle (i) du consensus entre les parties prenantes concernant l'évolution du contexte et (ii) des performances des processus pertinents quant aux résultats exigés de cette vue de processus [b)1), b)2), b)3)].

<6.3.3> Le Processus de gestion des décisions résout les conflits qui découlent de l'établissement et du maintien de la compréhension commune et des accords explicites, et gère les décisions d'acceptation des avis sans opposition [a), b)].

– <a)1)>: Il convient d'inclure à la stratégie de gestion des décisions un processus d'arbitrage préconvenu [a)4)].

– <a)3)>: Outre les parties prenantes pour lesquelles des conflits d'intérêts existent, il convient d'identifier et d'impliquer celles qui sont affectées par la décision [a)1), a)7)].

– <b)2)>: Il convient de déterminer de manière équitable et de bonne foi le résultat souhaité et les critères de sélection par l'application récursive de la vue de processus de recherche d'un consensus [a)6), a)7)].

– <c)2), c)3)>: Il convient qu'un rapport consignant les résolutions, la justification des décisions, les hypothèses associées, ainsi que les actions de suivi et d'évaluation rende compte de la recherche d'un consensus et prouve son équité et sa bonne foi [a)7), b)5)].

NOTE 2 Les renvois à la vue de Processus de recherche d'un consensus et au Processus de gestion des décisions sont mutuellement récursifs. La recherche d'un consensus requiert que des décisions soient prises, et chaque décision requiert un consensus sur les résultats souhaités et les critères de sélection.

<6.3.6> Le Processus de gestion des informations génère, reçoit, confirme, transforme, conserve, récupère, diffuse et supprime les informations relatives à la compréhension commune, aux accords explicites et à leur gestion.

– <a)1), a)5)>: Il convient que la stratégie relative aux actions de gestion et de maintien des informations inclue la politique concernant la gestion des changements apportés aux accords [b)1)], le maintien du consensus entre les parties prenantes [b)2)] et la révision des processus en vue de l'établissement de ce consensus [b)3)]. Il convient que ces actions permettent de réduire les différences d'interprétation [a)6)] et qu'elles garantissent l'équité et l'équitabilité pour toutes les parties prenantes [a)7)].
– <a)2)>: Il convient que les éléments d'information à gérer incluent la liste des parties prenantes identifiées [a)1)], le cadre de référence [a)2)], la compréhension de l'objet du système, etc. [a)3)], le processus d'arbitrage convenu [a)4)], les accords explicites [a)5)], l'étude de sûreté de fonctionnement [b)4)] et le compte-rendu du développement du consensus et le raisonnement ayant conduit à celui-ci [b)5)].
– <a)3)>: La désignation des autorités et des responsabilités en matière de gestion des informations contient celle de l'étude de sûreté de fonctionnement [b)4)].
– <a)4)>: Les formes et la structure des éléments d'information font partie du cadre de référence [a)2)] et il convient que leur contenu reflète la compréhension commune [a)3),a)5)].
– <b)1)>: Il convient que le développement des informations sur les accords explicites suive le processus d'arbitrage convenu pour résoudre les conflits d'intérêts [a)4)]. Il convient que le cadre de référence établi en [a)2)] soit utilisé pour transformer les informations en informations utilisables par les parties prenantes.
– <b)5)>: Il convient que les informations, notamment le compte-rendu de l'élaboration des accords explicites et du raisonnement ayant conduit à ceux-ci [b)5)], soient éliminées seulement après une étude approfondie de leur valeur quant à l'adaptation aux changements et à l'établissement de la redevabilité à une date ultérieure, y compris lorsque ces derniers sont liés à une réponse à une défaillance.

<6.3.8> Le Processus d'assurance qualité garantit l'établissement et le maintien de la compréhension commune et des accords explicites d'une qualité suffisante, ainsi que le respect de leurs contenus représentés comme des exigences de qualité.

– <b), c)>: Il convient que le processus d'évaluation du produit ou service fasse partie de la maintenance de la compréhension commune et des accords explicites [b)1), b)2)].
– <d)>: Il convient qu'un rapport consignant les activités d'assurance qualité rende compte de la recherche d'un consensus [b)5)].
– <e)>: Il convient que le traitement des problèmes réponde à la question de savoir si leurs causes exigent une mise à jour de la compréhension commune, des accords explicites et des processus [b)1), b)2), b)3)].

<6.4.1> Le Processus d'analyse opérationnelle ou de mission fournit le cadre de référence et commence à générer la compréhension commune des environnements, etc., au sein de ce cadre. Il convient que l'application du processus tienne compte du fait que le système risque de ne pas disposer d'une organisation englobant toutes les parties prenantes.

– <a)2), b)2)>: Il convient que la stratégie d'analyse et la définition de l'espace de problème clarifient le cadre de référence et la compréhension commune dans ce cadre à partager; il convient également qu'elles fassent preuve d'équité et de bonne foi [a)2), a)3), a)7)].
– <b)1)>: Il convient, après l'analyse du problème, de confirmer que toutes les parties prenantes partagent la même compréhension du domaine d'application, de la base ou des moteurs des problèmes ou opportunités traités dans <b)1) NOTE 1> [a)2), a)3), a)6)].
– <c)1)>: Il convient que l'identification des principaux groupes de parties prenantes tienne compte du fait que les parties prenantes peuvent évoluer dans le temps et que chacune

d'entre elles puisse identifier des entités différentes en tant que principaux groupes de parties prenantes au sein du système; il convient d'identifier chaque partie prenante et son ou ses rôles [a)1)]; il convient d'inclure aux concepts opérationnels préliminaires des politiques de services qui reflètent la compréhension commune [a)2)].

– <c)2)>: Il convient que les catégories de solutions identifiées soient partagées entre toutes les parties prenantes et que chaque partie prenante soit en mesure d'examiner les solutions en fonction de son propre point de vue en matière d'équité et de bonne foi [a)3), a)7)].

– <d)>: Il convient que les parties prenantes identifient et conviennent entre elles de l'identité de l'évaluateur et de la méthode d'évaluation [a)7)].

– <e)1)>: Outre la traçabilité entre les résultats de l'analyse et d'autres artefacts dans une itération d'un cycle de vie, il convient de maintenir la traçabilité entre les résultats de l'analyse avant et après les changements [b)2), b)5)] (voir <6.4.1.1 NOTE 2>).

<6.4.2> Le Processus de définition des besoins et exigences des parties prenantes développe la compréhension commune et les accords explicites sur la finalité du système, etc., en tant que définitions des besoins et exigences des parties prenantes [a)3), a)5)].

– <a)1)>: Il convient que l'identification des parties prenantes tienne compte du fait que les parties prenantes peuvent évoluer dans le temps et que chacune d'entre elles puisse identifier des entités différentes en tant que parties prenantes au sein du système; il convient d'identifier chaque partie prenante et son ou ses rôles [a)1)].

– <a)2)>: Il convient que la stratégie de définition des besoins et exigences des parties prenantes assure une résolution équitable et de bonne foi des différents avis et conflits, qui contribue à garantir le système et son intégrité [a)4), a)7)] (voir <6.4.2.3 a)2) NOTE>); il convient que la stratégie prévoit la manière d'établir une compréhension commune des politiques du service du système [a)3)].

– <b)1)>: Il convient que la définition du contexte d'utilisation résolve les différences entre les présuppositions des parties prenantes de manière équitable et de bonne foi [a)2), a)3), a)7)].

– <b)2), b)3), b)4)>: Il convient que la détermination des besoins explicites et implicites porte une attention particulière à <b)2) NOTE 1>; il convient que les besoins des parties prenantes soient formulés conjointement avec leurs présuppositions relatives au système et à son environnement; il convient de tenir compte du fait que des différences entre les présuppositions peuvent n'apparaître qu'après une certaine durée de fonctionnement; ces différences entravent la communication relative à la sûreté de fonctionnement entre les parties prenantes, peuvent constituer un obstacle à la recherche d'un consensus et peuvent mener à des décisions inappropriées [a)2), a)3)]; il convient que la détermination, l'identification, la sélection et la définition des besoins des parties prenantes soient équitables et de bonne foi [a)7)].

– <c)>: Il convient d'inclure au concept opérationnel des politiques relatives au service du système qui reflètent la compréhension commune [a)2)].

– <f)>: Il convient de gérer les changements de la définition des besoins et exigences des parties prenantes [b)].

<6.4.3> Le Processus de définition des exigences du système transforme le consensus des parties prenantes en exigences concrètes du système. Cela facilite la maintenance ainsi que l'évaluation des résultats de cette vue de processus [a), b)].

– <b), c)>: Il convient qu'avant de choisir un ensemble particulier d'exigences techniques, les parties prenantes parviennent à un consensus sur les conséquences anticipées et sur les risques liés à ce choix selon leurs propres termes [a)5), a)6), a)7)].

<6.4.4> La définition de l'architecture fournit une partie du cadre de référence et des accords explicites [a)2), a)5)].

– <b)1)>: Il convient que le point de vue de l'architecture forme le cadre de référence visé en [a)2)].

– <f)2)>: Il convient que l'acceptation explicite de l'architecture fasse partie des accords explicites [a)5)].

<6.4.9> Le Processus de vérification fait partie de l'évaluation de l'accord explicite [a)6), b)2)].

– <c)3)>: L'accord des parties prenantes quant au respect des exigences par le système fait partie des accords explicites visés en [a)5)].

<6.4.11> Le Processus de validation fait partie de l'évaluation des accords explicites [a)6), b)2)].

6.3 Vue de processus d'établissement de la redevabilité

6.3.1 Objet

La vue de processus d'établissement de la redevabilité a pour objet d'établir la relation entre la violation d'un accord explicite et ses implications pour les parties prenantes et la société en général. Cela inclut l'obligation, pour les parties prenantes redevables, de trouver des solutions permettant d'améliorer les chances de parvenir à un consensus sur le système, d'entretenir la confiance en celui-ci et de garantir l'existence de solutions en cas de dommages potentiels.

NOTE 1 Les cas où une partie prenante n'est pas en mesure de respecter l'accord en raison d'un événement extraordinaire dommageable sont considérés comme des violations de l'accord.

NOTE 2 Les accords doivent être suffisamment explicites pour clarifier de quoi chaque partie prenante doit être tenue responsable. Si nécessaire, les accords explicites doivent faire référence aux accords implicites, tels que les règles de bon usage du secteur concerné.

Il convient de parvenir à cette fin (l'objet) en tenant compte des points suivants.

La vue de processus d'établissement de la redevabilité assure la redevabilité vis-à-vis de la société en général. La redevabilité correspond à la responsabilité globale des décisions et des mesures prises dans toute partie du cycle de vie d'un système. La redevabilité inclut la responsabilité de la communication d'informations aux utilisateurs et autres parties prenantes, et la responsabilité de la supervision et du maintien des contrôles des risques identifiés. Attendu qu'il n'existe aucun contrôle central des systèmes ouverts, il est difficile d'identifier la partie redevable d'une décision, d'une mesure ou d'un contrôle particulier.

La redevabilité a un impact immédiat sur la confiance des personnes dans le système; or, cette propriété subjective du système est essentielle à la sûreté de fonctionnement. L'absence de redevabilité empêche certains systèmes de rétablir leurs services dans le cadre d'une reprise technique après une défaillance, en raison d'exigences réglementaires, de l'opinion publique et d'autres raisons de nature sociale.

La redevabilité est nécessaire pour garantir la sûreté de fonctionnement du système et elle renforce la sûreté de fonctionnement globale des systèmes interconnectés et gérés indépendamment. L'impact des défaillances d'un système peut être réduit par les systèmes interconnectés environnants qui partagent des informations sur la défaillance.

La réalisation de la finalité de cette vue de processus passe par:

– l'établissement de la relation entre la violation d'un accord et ses implications, y compris l'obligation, pour les parties prenantes redevables, de trouver des solutions avant les événements pour lesquels une redevabilité est requise [résultats de 6.3.2 a) à e)];
– l'exécution de mesures permettant d'anticiper les événements pour lesquels une redevabilité est requise, et d'y répondre [f) à h)];
– la communication des informations adéquates aux parties prenantes et à la société en général [i)1) à i)5)].

La relation entre l'objet et les résultats est décrite à l'Article B.3.

6.3.2 Résultats

a) Les décisions clés qui contrôlent le cycle de vie du système et les risques liés au cycle de vie du système sont identifiées, y compris celles qui contrôlent les résultats des processus et des vues de processus.

NOTE 1 Les décisions clés incluent les décisions prises à l'issue de chaque phase du cycle de vie et les décisions qui ont une grande influence sur les progrès ultérieurs du cycle de vie du système.

b) Une personne ou une entité est identifiée comme redevable pour chaque décision clé contrôlant le cycle de vie du système et les risques liés à ce cycle.

c) Les décisions clés pouvant être à l'origine de la défaillance ou de la violation de chaque élément de chaque accord explicite sont identifiées.

NOTE 2 Les décisions clés susceptibles d'entraîner une violation de l'accord en raison de facteurs extérieurs au système sont notamment l'acceptation des risques et l'acceptation de résultats insuffisants de l'analyse des risques.

NOTE 3 Les parties prenantes redevables d'une violation de l'accord sont celles qui sont redevables des décisions clés identifiées comme potentiellement à l'origine de la violation.

d) Les conséquences de chaque violation de chaque accord explicite sur les parties prenantes non redevables et sur la société en général sont évaluées.

NOTE 4 L'évaluation inclut l'analyse de la contrôlabilité des conséquences par les parties prenantes redevables dotées de l'autorité et des ressources.

NOTE 5 Chaque élément de chaque accord explicite est formulé de manière à permettre un tel examen.

e) Pour chaque violation de chaque accord explicite, les implications pour les parties prenantes redevables, ainsi que les solutions pour les parties prenantes non redevables et pour la société en général, sont convenues.

NOTE 6 Pour les parties prenantes redevables, ces implications incluent l'obligation de fournir les solutions convenues pour les parties prenantes non redevables et pour la société en général. La vue de processus de recherche d'un consensus est employée pour réviser l'accord original afin que le contrôle des parties prenantes redevables suffise pour remplir les obligations.

NOTE 7 L'accord sur les implications d'une violation de l'accord de base et sur les solutions à y apporter tient notamment compte des cas où cette violation est causée par des changements perturbateurs non pris en compte dans les points a) à d).

f) Les résultats anticipés et non anticipés des décisions sur l'ensemble du système sont supervisés et évalués. Cela inclut la supervision des violations des accords.

g) Des boucles de rétroaction sont établies pour informer les décisionnaires et autres parties prenantes des résultats des décisions et des mesures.

NOTE 8 Les boucles de rétroaction repèrent les résultats non souhaités et initient des mesures pour y remédier.

NOTE 9 Les boucles de rétroaction améliorent la compréhension du comportement du système et les interactions entre les décisionnaires responsables des différentes parties du système. La qualité des boucles de rétroaction est cruciale, dans la mesure où les parties qui prennent des décisions n'ont pas une compréhension complète de l'ensemble du système; les décisions peuvent ainsi avoir des conséquences non souhaitées dans d'autres parties du système.

NOTE 10 La gestion des décisions est particulièrement difficile pour les systèmes ouverts. Elle est associée à la fois à la vue de processus de recherche d'un consensus et à la vue de processus d'établissement de la redevabilité. La mise en œuvre d'une décision consensuelle, la transmission des résultats de la décision et le traitement des conséquences non souhaitées dans d'autres parties du système donnent lieu à des problèmes. Les boucles de rétroaction contribuent à résoudre ces problèmes.

h) En cas de violation d'un accord, les parties prenantes redevables fournissent sans délai les solutions destinées aux parties prenantes non redevables et à la société en général.

i) Des informations adéquates et pertinentes sont communiquées sans délai par les parties prenantes redevables aux parties prenantes non redevables et à la société en général.

NOTE 11 Dans certains cas, les informations de plusieurs processus du cycle de vie doivent être intégrées.

NOTE 12 Les informations sont adéquates et pertinentes lorsque (1) elles sont exhaustives; (2) les destinataires les comprennent facilement; (3) elles permettent à chaque destinataire de réduire les dommages liés à la défaillance et (4) les destinataires ont démontré leur confiance en leur adéquation et en leur validité.

1) Des réponses rapides, valides et adéquates sont données aux demandes légitimes d'informations sur le système formulées par une partie prenante.
2) Les parties prenantes ont une confiance justifiée dans les informations fournies sur le système.
3) À la suite d'une défaillance, des informations adéquates et pertinentes sont choisies et communiquées aux parties prenantes du système, aux parties prenantes des systèmes interconnectés et au grand public.

NOTE 13 Les informations sont données par la vue de processus de réponse aux défaillances.

4) Les informations sur les changements apportés aux exigences, aux attentes, aux descriptions et aux performances du système sont choisies et communiquées aux parties prenantes du système, aux parties prenantes des systèmes interconnectés et au grand public.
5) Les informations sur les écarts entre les exigences, les attentes, les descriptions et les performances du système, le cas échéant, sont choisies et communiquées aux parties prenantes du système, aux parties prenantes des systèmes interconnectés et au grand public.

6.3.3 Processus, activités et tâches

Il convient que la vue de processus d'établissement de la redevabilité soit mise en œuvre via les activités et tâches des processus suivants prévus par l'ISO/IEC/IEEE 15288.

<6.1.1> Processus d'acquisition

– <c)>: L'établissement de l'accord entre l'acquéreur et le fournisseur (y compris des critères d'acceptation et des obligations de l'acquéreur) implique des décisions clés contrôlant le cycle de vie du système [a)]; sa non-application constitue une violation de l'accord, et il convient d'identifier les décisions clés qui y ont conduit, etc. [b), c), d), e)].
– <d)>: La supervision de l'accord entre dans le cadre des boucles de rétroaction [f), g)].

<6.1.2> Processus de fourniture

– <c)>: L'établissement de l'accord entre l'acquéreur et le fournisseur, notamment des critères d'acceptation et des obligations de l'acquéreur, implique des décisions clés contrôlant le cycle de vie du système [a)]; sa non-application constitue une violation de l'accord, et il convient d'identifier les décisions clés qui y ont conduit, etc. [b), c), d), e)]. Il convient que la maintenance de l'accord permette également l'obtention de résultats [f), g)].
– <e)4)>: Il convient que la responsabilité du produit ou du service soit transférée d'une manière qui assure la réalisation continue des résultats [f), g), h), i)].

<6.2.1> Processus de gestion du modèle de cycle de vie

– <a)3)>: Il convient d'inclure l'identification d'une personne ou d'une entité redevable de chaque décision clé à l'établissement des rôles, etc. [b)].
– <a)4)>: La définition des critères commerciaux et la manière dont ils contrôlent les phases du cycle de vie impliquent des décisions clés [a), b)]. Il convient de documenter leur développement [i)].
– <a)5)>: Il convient que les modèles normalisés établis de cycle de vie spécifient les liens entre les processus du cycle de vie qui permettent la réalisation de tous les résultats de la vue de processus d'établissement de la redevabilité [a) à i)].

<6.2.3> Il convient que le Processus de gestion du portefeuille identifie les décisions clés qui contrôlent l'interface entre le cycle de vie d'un système et ceux des autres systèmes [a)].

– <a)3)>: La définition des responsabilités et de l'autorité fait partie de la réalisation de [a), b)] et il convient de considérer conjointement avec [c), d), e)].
– <a)5)>: L'allocation de ressources à une personne ou à une entité qui en est redevable implique des décisions clés [a), b)].

– <c)1)>: Il convient de tenir compte sans délai de l'annulation et de la suspension du projet [i)].

<6.2.5> Processus de gestion de la qualité

– <a)1), a)3)>: L'établissement de politiques de gestion de la qualité, etc., et la définition des critères et méthodes d'évaluation de la qualité impliquent des décisions clés [a)] et il convient de prendre en compte les résultats [b), c), d), e), h)] conjointement. Il convient que chaque identification ou définition soit accompagnée de l'attribution de sa redevabilité.
– <a)2)>: La définition des responsabilités et de l'autorité de mise en œuvre de la gestion de la qualité fait partie de la réalisation de [b)].
– <b)>: L'évaluation de la satisfaction des clients fait partie de la réalisation de [d), f), g)].
– <c)>: La planification de mesures correctives et préventives fait partie des obligations des parties prenantes redevables [e), h)]; elle entre dans le cadre des boucles de rétroaction [g)].

<6.2.6> Il convient d'exécuter le Processus de gestion des connaissances dans un contexte où les connaissances sont vouées à être partagées entre plusieurs organismes [f), g), i)]. Il convient d'inclure aux informations adéquates visées en [i)] les retours d'expérience que les parties prenantes redevables ont utilisés dans le cadre de leurs décisions.

<6.3.1> Processus de planification de projet: Toutes les définitions et identifications établies dans le cadre de ce processus impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)].

– <a)4)>: Il convient que la structure de répartition du travail soit accompagnée d'une attribution des redevabilités et d'une identification des informations pertinentes à diffuser [b), i)].
– <b)4)>: Il convient d'inclure l'identification des informations à diffuser en cas de défaillance du système à la redevabilité définie [i)].
– <b)6)>: La planification de l'acquisition implique des décisions clés [a)] et il convient de la prendre en compte conjointement avec [b), c), d), e), h)].

<6.3.2> Processus d'évaluation et de contrôle du projet

– <a)1)>: La définition de la stratégie d'évaluation et de contrôle du projet implique des décisions clés [a)] et il convient de la prendre en compte conjointement avec [b), c), d), e), h)].
– <b)>: Il convient d'inclure à l'évaluation du projet l'évaluation visée en [d)]. Il convient de fournir le résultat avec les informations sur la redevabilité [i)].
– <c)>: Il convient d'inclure au contrôle du projet les boucles de rétroaction visées en [g)], l'application de mesures correctives [h)] et la communication d'informations [i)].

<6.3.3> Processus de gestion des décisions: La redevabilité quant à la prise et à la gestion des décisions inclut la responsabilité de montrer que les parties prenantes redevables ont tenu compte de toutes les informations pertinentes et bien respecté le Processus de gestion des décisions.

– <a)1), c)3)>: Il convient que la stratégie de gestion des décisions fournisse des boucles de rétroaction de qualité [g)].
– <c)2), c)3)>: Il convient d'inclure au rapport de décisions la preuve que la redevabilité quant à la prise et à la gestion des décisions est établie [i)].

<6.3.4> Processus de gestion des risques: La redevabilité quant à la gestion des risques identifiés, c'est-à-dire leur supervision et le maintien de leur maîtrise, revêt une importance particulière. Elle doit être clairement définie, même pour les risques qui ne sont pas parfaitement compris [b), e), f), h)].

– <a)1), d)>: La définition de la stratégie de gestion des risques et des décisions relatives au traitement des risques impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)].

<6.3.5> Processus de gestion de la configuration

– <b), c)>: L'identification des éléments de configuration et la gestion de leurs changements dans le cadre du Processus de gestion de la configuration impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)].
– <d), e)>: Il convient que le rapport sur l'état de configuration et l'évaluation de la configuration fournissent une partie des informations adéquates selon [i)] qui aident à assurer la confiance des parties prenantes dans les informations communiquées sur le système [i)2)].
– <e)4), e)5)>: Il convient d'évaluer la configuration dans le cadre de la supervision des violations des accords [f)] et des boucles de rétroaction qui informent les décisionnaires [g)].

<6.3.6> Il convient que le Processus de gestion des informations gère et fournisse les informations adéquates visées en [i)]. Il convient en particulier d'obtenir une confiance justifiable de la part des parties prenantes [i)2)]. Il convient que les informations fournies tiennent compte de la coopération de plusieurs processus du cycle de vie.

– <a)1)>: Il convient que la stratégie de gestion des informations soutienne la mise en place de boucles de rétroaction visant à transmettre le résultat des décisions aux décisionnaires [g)].
– <a)2)>: Il convient que tous les processus recourent au Processus de gestion des informations afin de collecter et de gérer les données de journal et autres preuves susceptibles d'établir et de justifier de l'adéquation et de la validité des informations relatives à la redevabilité; il convient de fournir la représentation objective de la justification [i)2)].
– <b)1)>: Il convient de collecter et d'utiliser les éléments d'information avec les preuves de leur authenticité sous une forme vérifiable par les destinataires des informations [i)2)].
– <b)3)>: Il convient de procéder à la publication, à la distribution ou de fournir l'accès aux informations de manière à réaliser [i)].
– <b)5)>: L'élimination d'informations implique des décisions clés. Il convient de ne procéder à cette élimination qu'après une étude approfondie des effets futurs d'une telle opération sur l'établissement de la redevabilité [a) à i)].

<6.3.7> Il convient que le Processus de mesure entre dans le cadre des boucles de rétroaction [g)].

– <a)3)>: Il convient d'envisager l'intégration aux boucles de rétroaction des besoins en informations concernant la surveillance des résultats non anticipés [f), g)].

<6.3.8> Processus d'assurance qualité

– <a)1)>: La définition de la stratégie d'assurance qualité implique des décisions clés [a)] et il convient de la prendre en compte conjointement avec [b), c), d), e), h)].

<6.4.1> Processus d'analyse opérationnelle ou de mission

– <c)>: Il convient d'inclure à la caractérisation de l'espace de solutions la redevabilité de chaque partie prenante majeure identifiée [b)].

<6.4.2> Processus de définition des besoins et exigences des parties prenantes

– <a)1), b), c), d)>: L'identification des parties prenantes, la définition des besoins des parties prenantes, la définition du concept opérationnel et autres concepts relatifs au cycle de vie et

la définition des exigences des parties prenantes impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)].

– <b)2), d)3)>: Il convient d'identifier les besoins des parties prenantes conjointement avec leur redevabilité [b), c), d), e), h)].

– <c)>: Il convient d'inclure la définition de la redevabilité des principaux groupes de parties prenantes identifiés en <6.4.1> au concept opérationnel et aux autres concepts du cycle de vie. Il convient que l'analyse des scénarios identifie les décisions clés prises par les parties prenantes dans le cadre des scénarios et analyse les impacts et conséquences potentiels de ces décisions [a), b), c), d), e), h)].

– <e)>: Accepter le résultat de l'analyse des besoins des parties prenantes de manière appropriée est une décision clé et la personne responsable du processus de définition des besoins et exigences des parties prenantes est redevable de cette décision [a), b), c), d), e), h)].

– <e)3)>: La transmission de l'analyse des exigences aux parties prenantes concernées entre dans le cadre des boucles de rétroaction [g)].

– <f)1)>: Il convient que l'accord explicite sur les exigences des parties prenantes identifie la redevabilité pour chaque élément de l'accord [c), d), e), h)].

– <f)2)>: Il convient d'assurer la traçabilité de l'attribution de la redevabilité [b)]. Il convient que la traçabilité soit maintenue de manière adéquate pour réaliser [c), d), e), i)]. Il convient d'assurer la traçabilité entre les exigences des parties prenantes et les exigences de supervision du système [f), g)].

– <f)3)>: Il convient d'établir un compte-rendu de la sélection des éléments d'information clés pour référence afin de réaliser [i)].

<6.4.3> Processus de définition des exigences du système

– <a)1), b)2), b)4), d)3)>: La définition de la limite fonctionnelle, des contraintes de mise en œuvre, des exigences du système et le choix des éléments d'information clés pour référence impliquent des décisions clés [a)]; il convient de les prendre en compte conjointement avec [b), c), d), e), h)].

– <a)1)>: Il convient de définir la limite fonctionnelle conjointement avec la limite de redevabilité [a), b), c), d), e), h)].

– <b)1)>: Il convient de définir les fonctions conjointement avec la redevabilité quant à leur exécution [a), b), c), d), e), h)].

– <b)3)>: Il convient d'identifier les exigences du système critiques et liées au risque conjointement avec la redevabilité associée [c), d), e)].

– <b)4)>: Il convient que la définition des exigences des parties prenantes et les éléments de justification associés clarifient les décisions clés qui ont influencé la définition et la redevabilité des exigences [a), b), c), d), e), h)].

– <c)>: Accepter le résultat de l'analyse des exigences du système de manière appropriée est une décision clé et la personne responsable du processus de définition des exigences du système est redevable de cette décision [a), b), c), d), e), h)].

– <c)3)>: La transmission de l'analyse des exigences aux parties prenantes concernées entre dans le cadre des boucles de rétroaction [g)].

– <d)2)>: Il convient d'assurer la traçabilité de l'attribution de la redevabilité [b)]. Il convient que la traçabilité soit maintenue de manière adéquate pour réaliser [c), d), e), i)].

<6.4.4> Processus de définition de l'architecture

– <a)1), a)2), a)4), b), d)1), d)2), e)3), f)2)>: Les décisions suivantes impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)]: l'identification des facteurs déterminants, l'identification des préoccupations des parties prenantes, la définition des critères d'évaluation, la définition du point de vue de l'architecture, l'identification des éléments du système, les définitions des interfaces et des interactions entre les éléments du système et avec les entités externes, le choix et l'acceptation de l'architecture.

– <a)4)>: Il convient d'inclure les critères de redevabilité décrits dans les architectures candidates aux critères d'évaluation des architectures.

– <c)>: Il convient de développer des modèles et des vues qui clarifient la manière dont les résultats [a), b), c), d), e), h)] sont obtenus.

– <d)>: Il convient d'inclure l'attribution de la redevabilité à la relation entre architecture et conception.

– <f)6)>: Il convient d'assurer la traçabilité de l'attribution de la redevabilité [b)]. Il convient que la traçabilité soit maintenue de manière adéquate pour réaliser [c), d), e), i)].

– <f)7)>: Il convient d'établir un compte-rendu de la sélection des éléments d'information clés pour référence afin de réaliser [i)].

<6.4.5> Processus de définition de conception

– <b)1), b)2), b)5), c), d)4)>: Les points suivants impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)]:

  - affectation des exigences du système aux éléments du système;
  - transformation des caractéristiques architecturales en caractéristiques de conception;
  - définition de l'interface entre les éléments du système et avec les entités externes;
  - identification des éléments non liés au développement (évaluation des autres solutions permettant d'obtenir des éléments du système);
  - choix des éléments d'information clés pour référence;

– <b)1)>: Il convient que l'affectation des exigences du système aux éléments du système prenne également en compte l'attribution de la redevabilité [b), c), d), e), h)].

– <b)2)>: Lorsque les caractéristiques architecturales sont transformées en caractéristiques de conception, il convient également d'en attribuer la responsabilité. [b), c), d), e), h)].

– <b)5)>: Il convient de définir les interfaces des éléments du système conjointement avec le domaine d'application de la redevabilité associée [b), c), d), e), h)].

– <c)>: Il convient de clarifier la redevabilité quant aux éléments non liés au développement [b), c), d), e), h)].

– <d)3)>: Il convient également de maintenir la traçabilité des redevabilités [b), c), d), e), h), i)].

– <d)4)>: Il convient d'établir un compte-rendu de la sélection des éléments d'information clés pour référence afin de réaliser [i)].

<6.4.6> Processus d'analyse du système: Il convient d'établir un compte-rendu des points suivants, au titre des informations adéquates visées en [i)]:

– <a)1)>: identification du problème requérant une analyse du système;

– <a)2)>: identification des parties prenantes de l'analyse du système;

– <a)3)>: définition du domaine d'application, des objectifs et du niveau de fidélité de l'analyse du système;

– <b)1)>: identification des hypothèses;

– <b)4)>: établissement de la/des conclusion(s) de l'analyse;

– <c)2)>: sélection des éléments d'information clés pour référence.

<6.4.7> Processus de mise en œuvre

– <a)1), a)2)>: La définition de la stratégie de mise en œuvre, l'identification des contraintes et de la technologie de mise en œuvre impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)].

– <c)>: Il convient d'établir un compte-rendu sur l'établissement des critères utilisés pour discerner les anomalies et sur la sélection des éléments d'information clés pour référence afin de réaliser [i)].

– <c)2)>: Il convient également de maintenir la traçabilité de la redevabilité quant aux éléments du système mis en œuvre [b), c), d), e), h), i)].

<6.4.8> Processus d'intégration

– <a)5)>: Il convient d'intégrer les contraintes d'intégration du système aux exigences, à l'architecture ou à la conception du système dans le cadre de la rétroaction [g)].
– <c)1), c)3)>: Il convient d'établir un compte-rendu sur le mode d'établissement des critères utilisés pour discerner les anomalies et sur le choix des éléments d'information clés pour référence afin de réaliser [i)].
– <c)2)>: Il convient également de maintenir la traçabilité de la redevabilité quant aux éléments du système intégrés [b), c), d), e), h), i)].
– <b)1), b)3)>: L'acceptation des éléments du système mis en œuvre et l'évaluation des résultats de la vérification des interfaces, etc., comme étant satisfaisants sont des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)].

<6.4.9> Processus de vérification

– Il convient d'établir un compte-rendu des points suivants, au titre des informations adéquates visées en [i)]:
  - <a)1)>: identification du domaine d'application de la vérification et des mesures de vérification correspondantes;
  - <b)>: exécution de la vérification;
  - <c)1)>: mode d'établissement des critères utilisés pour discerner les anomalies;
  - <c)3)>: obtention de l'accord des parties prenantes quant au fait que le système ou l'élément du système respecte l'exigence spécifiée;
  - <c)5)>: sélection des éléments d'information clés pour référence.
– <a)5)>: Il convient d'intégrer les contraintes de vérification du système aux exigences, à l'architecture ou à la conception du système dans le cadre de la rétroaction [g)].
– <c)3)>: Confirmer que le système ou que l'élément du système respecte les exigences spécifiées est une décision clé [a)] et il convient de la considérer conjointement avec [b), c), d), e), h)].
– <c)4)>: Il convient également de maintenir la traçabilité de la redevabilité quant aux éléments du système vérifiés [b), c), d), e), h), i)].

<6.4.10> Processus de transition

– Les points suivants impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)]:
  - <a)1)>: définition de la stratégie de transition;
  - <a)2)>: identification des changements sur l'infrastructure ou le site;
  - <a)3)>: identification de la formation nécessaire des opérateurs, utilisateurs et autres parties prenantes;
  - <b)10)>: décision de mettre en service le système.
– Il convient d'établir un compte-rendu des points suivants, au titre des informations adéquates visées en [i)]:
  - <b)4)>: confirmation que le système est bien installé;
  - <b)6)>: confirmation que la vérification du système installé valide la satisfaction des exigences des parties prenantes dans l'environnement opérationnel;
  - <b)7)>: confirmation que la capacité du système installé à délivrer les fonctions requises est démontrée;
  - <b)8)>: confirmation que la durabilité du système installé par les systèmes d'activation est démontrée;

- <b)9)>: confirmation que l'état de préparation opérationnelle est démontré par l'examen;
- <c)1), c)2)>: établissement des critères utilisés pour discerner les anomalies, les incidents et les problèmes opérationnels;
- <c)3)>: sélection des éléments d'information clés pour référence.

– <a)1)>: Il convient d'inclure l'attribution de la redevabilité à la stratégie de transition [b), c), d), e), h)].

– <a)3)>: Il convient d'inclure à l'identification des formations nécessaires des opérateurs, etc., l'identification de leur redevabilité [b), c), d), e), h)].

– <a)4)>: Il convient d'intégrer les contraintes de transition du système aux exigences, à l'architecture ou à la conception du système dans le cadre de la rétroaction [g)].

– <b)5)>: Il convient d'inclure à la formation des opérateurs, etc., des informations sur leur redevabilité [b), c), d), e), h)].

– <b)9)>: Il convient que l'examen de l'état de préparation opérationnelle prenne en compte la perspective de l'établissement de la redevabilité dans l'environnement installé [b), c), d), e), h)].

– <c)3)>: Il convient également de maintenir la traçabilité de la redevabilité quant aux éléments du système ayant fait l'objet d'une transition [b), c), d), e), h), i)].

<6.4.11> Processus de validation

– Il convient d'établir un compte-rendu des points suivants, au titre des informations adéquates visées en [i)]:
  - <a)1)>: identification du domaine d'application de la validation et des mesures de validation correspondantes;
  - <b)>: exécution de la validation;
  - <c)1)>: établissement des critères utilisés pour discerner les anomalies;
  - <c)3)>: obtention de l'accord des parties prenantes quant au fait que le système ou l'élément du système répond aux besoins des parties prenantes;
  - <c)5)>: sélection des éléments d'information clés pour référence.

– <b)3), c)3)>: Confirmer que le système ou que l'élément du système répond aux besoins des parties prenantes est une décision clé [a)] et il convient de la considérer conjointement avec [b), c), d), e), h)];

– <b)3)>: Il convient que l'examen des résultats de la validation prenne en compte la perspective de l'établissement de la redevabilité [b), c), d), e), h)].

– <c)4)>: Il convient également de maintenir la traçabilité de la redevabilité quant aux éléments du système ayant fait l'objet d'une transition [b), c), d), e), h), i)].

<6.4.12> Le Processus d'exploitation est au cœur de l'établissement de la redevabilité [f), g), h), i)].

– Les points suivants impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)]:
  - <a)1)>: définition de la stratégie opérationnelle;
  - <a)2)>: identification des contraintes opérationnelles du système à intégrer aux exigences, à l'architecture ou à la conception du système;
  - <a)3)>: identification et planification des systèmes ou services d'activation nécessaires pour prendre en charge le fonctionnement;
  - <a)6)>: affectation de personnel formé et qualifié aux postes d'opérateurs;
  - <b)3)>: définition des éléments d'information supervisés;
  - <b)5)>: décision de réaliser des opérations d'urgence ou non.

– Il convient d'établir un compte-rendu des points suivants, au titre des informations adéquates visées en [i)]:
  - <b)4)>: définition des limites acceptables des paramètres d'exécution des services;
  - <c)1), c)2)>: établissement des critères utilisés pour discerner les anomalies, les incidents et les problèmes opérationnels;
  - <c)4)>: sélection des éléments d'information clés pour référence;
  - <d)3)>: détermination du degré de satisfaction des besoins des clients par les services fournis par le système.
– <a)1)>: Il convient que la stratégie opérationnelle clarifie l'attribution de la redevabilité relative à la supervision et à l'assistance client [b), c), d), e), f), g), h), i)].
– <a)3)>: Il convient d'inclure à l'identification des systèmes d'activation l'identification de la limite de redevabilité entre le système et les systèmes d'activation [b), c), d), e), h)].
– <a)6)>: La formation et la qualification des opérateurs incluent leur sensibilisation à leur redevabilité [h)].
– <b)3)>: Il convient que la supervision du fonctionnement du système couvre les résultats anticipés et non anticipés des décisions sur l'ensemble du système [f)]. Il convient que la supervision fasse partie des boucles de rétroaction [g)]. Il convient que la supervision permette l'identification rapide des parties prenantes redevables et la communication des informations relatives à la redevabilité en cas d'anomalies et de défaillances [h), i)]. Il convient d'établir une traçabilité entre les mesures de supervision et la violation de l'accord indiquée en [6.3.2] par le biais de la chaîne de redevabilité décrite en <6.4.5 d)3), 6.4.7 c)2), 6.4.8 c)2), 6.4.9 c)4), 6.4.10 c)3), 6.4.13 d)4)>.
– <b)4)>: Il convient d'identifier, d'analyser et de consigner les anomalies opérationnelles relatives aux accords, aux exigences des parties prenantes et aux contraintes organisationnelles par le biais du processus d'analyse du système [h), i)].
– <b)5)>: Il convient d'inclure aux opérations d'urgence l'initiation de mesures correctives par les parties prenantes redevables [h)] et la communication rapide des informations relatives à la redevabilité [i)3)].
– <c)2)>: Il convient de lier la résolution des incidents et problèmes opérationnels aux parties prenantes redevables et aux mesures qu'elles ont prises [h), i)].
– <c)3)>: Il convient également de maintenir la traçabilité de la redevabilité quant aux éléments opérationnels [b), c), d), e), h), i)].
– <d)1), d)2)>: Il convient que l'assistance client fournisse rapidement des informations fiables, sur demande [i)1), i)2)], en cas de défaillances [i)3)], de changements [i)4)] et lorsqu'un écart de performances est identifié [i)5)].
– <d)3)>: Il convient de déterminer le degré de satisfaction des clients dans le cadre des boucles de rétroaction. Il convient de superviser la satisfaction des parties prenantes conjointement avec le degré de l'établissement de la redevabilité [f), g)].

<6.4.13> Processus de maintenance

– Les points suivants impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)]:
  - <a)1)>: définition de la stratégie de maintenance;
  - <a)2)>: identification des contraintes de maintenance du système;
  - <b)1)>: identification des futurs besoins de maintenance corrective, adaptative, perfective et préventive;
  - <b)5)>: décision de réaliser des opérations de maintenance préventive ou non;
  - <b)6)>: identification des défaillances;
  - <b)7)>: identification des besoins de maintenance adaptative ou perfective;
  - <c)5)>: confirmation que les mesures logistiques incluent des exigences de supportabilité planifiées, dotées de ressources adéquates et mises en œuvre;

- <d)3)>: identification de l'évolution des incidents, des problèmes et des tâches de maintenance et de logistique.

– Il convient d'établir un compte-rendu des points suivants, au titre des informations adéquates visées en [i)]:

  - <a)3)>: identification des métiers adéquats pour les actions concernant le système, la maintenance et la logistique;
  - <d)1), d)2)>: établissement des critères utilisés pour discerner les anomalies, les incidents et problèmes opérationnels;
  - <d)6)>: détermination du degré de satisfaction des clients vis-à-vis du système et de l'aide à la maintenance;
  - <d)5)>: sélection des éléments d'information clés pour référence.

– <a)2)>: Il convient d'intégrer les contraintes de maintenance du système aux exigences, à l'architecture ou à la conception du système dans le cadre de la rétroaction [g)].

– <b)1)>: Il convient que l'examen des incidents et problèmes d'identification des futurs besoins de maintenance évalue le degré de réalisation de [b), c), d), e), h)].

– <b)2), d)2)>: Il convient de lier la résolution des incidents opérationnels et de maintenance aux parties prenantes redevables et à leurs actions [h), i)].

– <d)4)>: Il convient également de maintenir la traçabilité de la redevabilité quant aux éléments de maintenance [b), c), d), e), h), i)].

– <d)6)>: Il convient de déterminer le degré de satisfaction des clients dans le cadre des boucles de rétroaction; il convient de superviser la satisfaction des parties prenantes conjointement avec le degré d'établissement de leur redevabilité [f), g)].

<6.4.14> Processus de mise au rebut

– Les points suivants impliquent des décisions clés [a)] et il convient de les prendre en compte conjointement avec [b), c), d), e), h)]:

  - <a)1)>: définition de la stratégie de mise au rebut;
  - <a)2)>: identification des contraintes de mise au rebut du système à intégrer aux exigences, à l'architecture ou à la conception du système;
  - <a)5)>: spécification des installations de confinement, lieux de stockage, critères d'inspection et périodes de stockage (si le système doit être stocké);
  - <a)6)>: définition des méthodes préventives visant à exclure les éléments et matériaux mis au rebut qu'il convient de ne pas redéfinir, reprendre ou réutiliser dans la chaîne logistique;
  - <b)1)>: décision de désactiver le système ou un élément du système afin de préparer sa mise au rebut;
  - <b)3)>: sélection, à des fins d'enregistrement, des connaissances opérationnelles pertinentes en matière de normes, directives et lois sur la sûreté, la sécurité, le respect de la vie privée et l'environnement;
  - <c)1)>: confirmation que la mise au rebut n'entraînera aucun facteur nuisible à la santé, à la sûreté, à la sécurité ou à l'environnement.

– <c)3)>: Il convient d'établir un compte-rendu de la sélection d'informations à archiver au titre des informations adéquates visées en [i)].

– <c)>: Il convient que la finalisation de la mise au rebut confirme que tout problème de redevabilité a été éliminé pour le système mis au rebut [i)].

6.4 Vue de processus de réponse aux défaillances

6.4.1 Objet

La vue de processus de réponse aux défaillances a pour objet de poursuivre la prestation de service dans toute la mesure du possible, avec le moins d'interruptions et de dommages possible et de la manière la plus opportune dans le contexte.

Il convient de parvenir à cette fin (l'objet) en tenant compte des points suivants.

Les défaillances peuvent être imprévues, ou prévues, mais jugées trop improbables ou trop coûteuses à prévenir, ou prévues et traitées, mais non prévenues en raison d'événements non anticipés.

Aucune solution spécifique ne peut être préparée en réponse à des événements non anticipés entraînant des défaillances. Des mesures génériques peuvent toutefois être préparées afin d'assurer leur exécution rapide. Ces mesures incluent des procédures visant à mettre rapidement en place des contre-mesures spécifiques à la défaillance dans le contexte, en modifiant le contexte si nécessaire. La prévention des formes de défaillances concevables, quelles qu'en soient les causes, passe également par ce type de mesures génériques.

L'intervention humaine joue un rôle clé dans la mesure où toutes les défaillances ne peuvent pas être prévenues ou réduites par des moyens préprogrammés. Pour une réponse rapide et appropriée, il convient que l'intervention humaine bénéficie du soutien d'ordinateurs dans la prise de décisions et la mise en œuvre des actions.

La vue de processus de réponse aux défaillances prépare *a posteriori* des moyens de gérer les conséquences dommageables des opérations du système. Ces actions post-défaillance incluent des mesures contre les conséquences identifiées pour lesquelles aucune cause ne peut être imaginée au moment de l'identification des conséquences. Il est possible de se préparer à ces conséquences, mais seulement en préparant les mesures à prendre après que ces conséquences se sont manifestées.

La vue de processus de réponse aux défaillances identifie les mesures prises contre les pannes, erreurs, défaillances et leurs précurseurs. La réponse aux défaillances inclut la prévention des défaillances à la suite de la détection des précurseurs, les opérations d'urgence à la suite de la détection des défaillances, la maintenance corrective et la maintenance préventive.

La réalisation de la finalité de cette vue de processus passe par:

– la préparation de la réponse aux défaillances [résultats de 6.4.2 a)1) à a)8)];
– l'exécution de la réponse aux défaillances dès qu'elles se produisent [b)1) à b)8)];
– la garantie de la redevabilité relative aux défaillances et à la réponse aux défaillances [c)1) à c)4)];
– l'amélioration du cycle de vie du système grâce à l'expérience des défaillances [d)1), d)2)].

La relation entre l'objet et les résultats est décrite à l'Article B.4.

6.4.2 Résultats

a) La réponse aux défaillances est préparée.
   1) Les fonctions principales à protéger pour assurer la continuité du service sont identifiées.
   2) Les objectifs de la protection des fonctions principales nécessaires à la prestation continue du service sont identifiés.
   3) Les pannes, erreurs, défaillances et leurs précurseurs qui impactent les fonctions principales sont identifiés.

NOTE 1 Il existe des pannes, erreurs, défaillances non identifiées, ainsi que leurs précurseurs. Il s'agit notamment des pannes, erreurs, défaillances et leurs précurseurs qui n'ont été prévus ni repérés par aucune des parties prenantes.

NOTE 2 Les erreurs d'interaction sont traitées dans le cadre de l'identification et de la détection des pannes, des erreurs, des défaillances et de leurs précurseurs.

4) Une analyse des conséquences et de la probabilité des pannes, erreurs et défaillances identifiées, ainsi que de leurs précurseurs, est réalisée.

NOTE 3 Les hypothèses retenues pour l'analyse au moment de la préparation sont vérifiées avant de répondre aux défaillances réelles, etc. Voir b)2) ci-dessous.

5) Pour les pannes, erreurs, défaillances identifiées et leurs précurseurs, les objectifs du traitement nécessaires à la continuité de la prestation du service sont définis et convenus.

NOTE 4 Ces objectifs incluent la prévention des dommages.

6) La disposition à l'égard du traitement de chaque panne, erreur, défaillance identifiée et ses précurseurs est choisie parmi les catégories suivantes:

   i) à superviser et à prévoir lors de la conception;

   ii) à superviser, mais pas à prévoir lors de la conception;

   iii) pas à superviser et pas à prévoir lors de la conception.

NOTE 5 Par "prévoir lors de la conception", on entend que le système est conçu pour apporter un ensemble de réponses spécifiques assurant la continuité du service.

7) Les réponses spécifiques qui protègent les fonctions principales contre les pannes, erreurs, défaillances et leurs précurseurs de la catégorie a)6)i) et les réponses aux défaillances des catégories a)6)ii) et a)6)iii) sont développées.

NOTE 6 Les réponses spécifiques seront basées sur le résultat de l'analyse des conséquences et de l'analyse de la probabilité. Ces réponses doivent être apportées par le système ainsi que par le personnel impliqué dans le cycle de vie du système.

NOTE 7 Les réponses spécifiques incluent les mesures post-défaillance.

NOTE 8 La défaillance des mesures post-défaillance est prise en compte. Les mesures post-défaillance concernant ces défaillances peuvent être déployées sur plusieurs couches et être appliquées de manière récursive à leurs propres défaillances.

8) Des mesures génériques visant à réduire les dommages liés aux défaillances sans cause identifiée sont développées.

NOTE 9 Les mesures génériques incluent l'identification rapide des parties défaillantes du système, l'isolation des parties qui présentent un dysfonctionnement afin de protéger les autres parties qui fonctionnent normalement, l'entretien des services survivants au niveau convenu par consensus entre les parties prenantes, et la restauration après une défaillance.

b) La réponse aux défaillances est réalisée lorsque nécessaire.

1) Les pannes, erreurs, défaillances et leurs précurseurs sont détectés.

2) Une analyse des causes et des conséquences de la panne, de l'erreur, de la défaillance ou de ses précurseurs est réalisée.

NOTE 10 L'analyse des conséquences après la détection des défaillances, etc., consiste à examiner les hypothèses formulées avant la détection, à les comparer à la situation réelle observée, et à confirmer ou modifier les résultats de l'analyse.

3) L'objectif du traitement des pannes, erreurs, défaillances détectées et de leurs précurseurs est précisé en fonction de la situation.

4) Les réponses spécifiques aux pannes, erreurs, défaillances et leurs précurseurs de la catégorie a)6)i) et les réactions aux défaillances des catégories a)6)ii) et a)6)iii) sont exécutées dès la détection de celles-ci.

5) Les réponses aux pannes, erreurs, défaillances et leurs précurseurs des catégories a)6)ii) et a)6)iii) sont conçues après l'événement.

NOTE 11 La supervision de catégorie a)6)ii) permet de repérer plus rapidement les défaillances, etc., et de disposer de données plus détaillées pour la création de réponses par rapport à la non-supervision de catégorie a)6)iii).

6) Les réponses aux pannes, erreurs, défaillances et leurs précurseurs n'aggravent pas les dommages et n'augmentent pas le risque de plus amples dommages.

NOTE 12 Dans certains cas, les activités d'atténuation entraînent de nouveaux dommages. Il faut que ces activités ne causent pas plus de dommages qu'une absence d'intervention.

7) Les dommages subis par le système en question et par les systèmes qui lui sont reliés sont globalement réduits.

8) Les réponses aux défaillances détectées sont évaluées vis-à-vis de l'objectif précisé en b)3).

c) La vue de processus d'établissement de la redevabilité rend compte de la réponse aux défaillances.

1) Les dommages causés par les défaillances sont compensés conformément à l'accord établi.

2) La confiance dans le système est entretenue.

NOTE 13 Par exemple, cela est possible via la diffusion, après chaque réponse à une défaillance, (1) d'un argumentaire garantissant que la réponse a atteint ou atteindra ses objectifs et (2) de l'argumentaire révisé pour le cycle de vie du système (Article 5) garantissant que des mesures préventives sont prises contre d'éventuelles récurrences futures.

3) Les parties prenantes et la société en général sont informées des réponses aux défaillances. Ces informations comprennent:

i) la justification du domaine d'application de l'ensemble des pannes, erreurs, défaillances identifiées et de leurs précurseurs;

ii) la justification du plan de réaction aux pannes, erreurs, défaillances détectées et leurs précurseurs;

iii) le résultat de l'analyse des conséquences de la panne, des erreurs ou des défaillances détectées, ou de leurs précurseurs;

iv) le résultat de la réponse aux défaillances et son évaluation.

4) Les informations nécessaires sont transmises à la vue de processus d'établissement de la redevabilité.

NOTE 14 Les changements perturbateurs peuvent entraîner des défaillances pour lesquelles il n'existe aucune partie prenante redevable ou auxquelles il est impossible de répondre. La communication des informations nécessaires à la vue de processus d'établissement de la redevabilité permet à ces changements perturbateurs d'être rapidement repérés et transmis à la vue de processus d'adaptation aux changements, qui traite des changements en question.

d) Le cycle de vie du système est amélioré sur la base de l'expérience des défaillances survenues après la réponse aux défaillances par la vue de processus d'adaptation aux changements.

1) L'objectif de l'amélioration est défini et convenu.

NOTE 15 L'objectif inclut la prévention de la récurrence de la défaillance, l'amélioration de la stratégie opérationnelle, la précision de la finalité du système, et l'amélioration des processus d'identification des pannes et de gestion des risques. La définition de l'objectif implique l'identification des conséquences réelles de la défaillance conformément à l'analyse des conséquences, et à l'évaluation des dommages et de la valeur des services fournis par le système.

2) Les informations nécessaires sont transmises à la vue de processus d'adaptation aux changements.

6.4.3 Processus, activités et tâches

Il convient de mettre en œuvre la vue de processus de réponse aux défaillances à l'aide des activités et des tâches des processus suivants prévus par la norme ISO/IEC/IEEE 15288.

<6.1.1> Processus d'acquisition

– <c)1)>: Il convient que l'accord conclu entre l'acheteur et le fournisseur identifie les fonctions principales à protéger contre les défaillances, ainsi que les objectifs de protection [a)1), a)2), a)5)].
– <d)1)>: Il convient que l'évaluation de l'exécution de l'accord confirme que les objectifs de protection de <c)1)> et les résultats [b), c)] sont atteints et assurés.

<6.1.2> Processus de fourniture

– <c)1)>: Il convient que l'accord conclu entre l'acheteur et le fournisseur identifie les fonctions principales à protéger contre les défaillances, ainsi que les objectifs de protection [a)1), a)2), a)5)].
– <d)2)>: Il convient que l'évaluation de l'exécution de l'accord confirme que les objectifs de protection de <c)1)> et les résultats [b), c)] sont atteints et assurés.

<6.2.1> Processus de gestion du modèle de cycle de vie

– <a)5)>: Il convient que les modèles de cycle de vie établis spécifient les liens entre les processus de cycle de vie qui permettent la réalisation de tous les résultats de la vue de processus de réponse aux défaillances [a), b), c), d)].

<6.2.4> Processus de gestion des ressources humaines

– <a)>: Les compétences à identifier sont notamment les compétences nécessaires pour comprendre la finalité du système et les compétences nécessaires pour appliquer cette compréhension à l'élaboration d'une intervention humaine permettant d'atteindre les résultats visés [a)7), a)8), b)].

<6.2.5> Processus de gestion de la qualité

– <b)>: Il convient d'évaluer le système de gestion de la qualité afin de déterminer s'il détecte et traite les pannes, les erreurs, les défaillances et leurs précurseurs identifiés en [a)3)], comme anticipé [b), c)].

<6.3.2> Processus d'évaluation et de contrôle du projet

– <a)>: Il convient que la stratégie d'évaluation et de contrôle de projet reflète la compréhension commune établie en [6.2.2 a)] pour accompagner:
  - l'élaboration de mesures génériques contre les défaillances non prévues à la conception, les défaillances dont les causes ne sont pas identifiées [a)8)];
  - la précision des objectifs de traitement des défaillances [b)3)];
  - la mise au point de réponses à des défaillances non prévues lors de la conception [b)5)].
– <c)>: Il convient que le contrôle du projet passe par l'adoption de la vue de processus d'adaptation aux changements pour adapter le système en vue de prévenir la répétition des défaillances [d)].

<6.3.4> Processus de gestion des risques

– <a)1), a)2), b)2), c), d)1), d)2), d)4), e)>: Les processus et procédures de gestion et d'évaluation des risques sont donnés dans l'ISO 31000 [16] et l'IEC 31010 [17]. De plus, il convient d'identifier ce qui suit [a), b)8)]:
  - moyens de communication et de concertation sur les risques, leur maîtrise et leurs traitements;
  - les moyens de réduire la dangerosité des défaillances ayant des causes non identifiées;
  - les moyens de réduire la dangerosité du système et des autres systèmes qui lui sont reliés;
  - les résultats de l'analyse des conséquences et de la probabilité, sous une forme écrite objective;

- une liste des événements dangereux susceptibles de se produire, une liste des événements dangereux jugés improbables, mais qu'il est décidé de superviser, une liste des événements dangereux jugés improbables et qu'il est décidé de ne pas superviser;
- une justification objective de la pertinence de l'ensemble des mesures de détection des pannes, des erreurs, des défaillances et de leurs précurseurs;
- les moyens d'adapter le système aux changements liés aux défaillances.

<6.4.2> Processus de définition des besoins et exigences des parties prenantes

– <b)2)>: Il convient d'identifier les besoins des parties prenantes en même temps que les besoins de protection contre les défaillances [a)1), a)2)]. Il convient que les besoins des parties prenantes comprennent le besoin de ne pas mettre en danger l'ensemble constitué par le système concerné et les systèmes qui lui sont reliés [a)8), b)7)].

– <c)1)>: Il convient que l'analyse des scénarios représentatifs permette d'identifier les fonctions principales à protéger [a)1)]. Elle comprend l'analyse des risques liés aux défaillances afin de définir les besoins de protection contre celles-ci [a)2)] et d'analyser le danger que le système concerné peut représenter pour les systèmes qui lui sont reliés [b)7)].

– <d)2)>: L'identification des exigences des parties prenantes et des fonctions comprend la désignation des fonctions principales à protéger contre les défaillances [a)1)] et celle de l'objectif de protection [a)2)]. Il convient que les exigences des parties prenantes comprennent des exigences spécifiant que le système concerné ne doit pas se mettre lui-même en danger et ni mettre en danger les systèmes qui lui sont reliés [b)7)].

– <e)1)>: Il convient que l'analyse de l'ensemble complet des exigences des parties prenantes comprenne une analyse des risques liés aux défaillances des fonctions principales afin de définir les objectifs de protection adéquats [a)2)], d'envisager des mesures génériques contre les défaillances dont les causes ne sont pas identifiées [a)8)] et de tenir compte du danger que le système concerné peut représenter vis-à-vis des autres systèmes qui lui sont reliés [b)7)]. Il convient que l'analyse permette d'identifier les pannes, erreurs, défaillances et leurs précurseurs qui ont un impact sur les fonctions principales, ainsi que leurs conséquences [a)4), a)5)].

– <e)2)>: Il convient que les mesures des performances critiques comprennent des mesures des degrés de protection pour les fonctions principales [a)2)] et des mesures de traitement des défaillances, etc. [a)5)].

– <f)1)>: Il convient que l'accord sur les exigences des parties prenantes énumère les fonctions principales à protéger [a)1)], les objectifs de protection des fonctions principales [a)2)] et les objectifs de traitement des défaillances, etc., qui ont un impact sur les fonctions principales [a)5)].

<6.4.3> Processus de définition des exigences du système

– <b)1)>: Il convient que la définition des fonctions principales comprenne notamment:
  - les objectifs de protection contre les défaillances [a)2)];
  - l'identification des pannes, des erreurs, des défaillances et de leurs précurseurs qui ont un impact sur la fonction, y compris les erreurs d'interaction [a)3)];
  - les objectifs de traitement des pannes identifiées, etc. [a)5)];
  - la classification du traitement pour chaque panne identifiée, etc. [a)6)].

– <b)3)>: Il convient que l'identification des exigences du système relatives aux risques, etc., permette d'identifier les fonctions principales à protéger contre les défaillances [a)1)]. Il convient d'identifier ce qui suit:
  - les exigences de protection des fonctions principales [a)2)];
  - les exigences de traitement des défaillances pertinentes, etc. [a)5)];
  - les exigences visant à ce que les réponses aux défaillances n'aggravent pas la dangerosité des défaillances et n'augmentent pas le risque de dommages supplémentaires [b)6)];
  - les exigences de supervision des défaillances, etc., à détecter [b)1)];

  - les exigences visant à réduire le danger que le système concerné peut représenter pour les systèmes qui lui sont reliés [b)7)].
- <b)4)>: Il convient que la définition des exigences du système et des justifications clarifie:
  - les exigences de protection des fonctions principales [a)2)] et les exigences relatives au traitement des défaillances, etc. [a)5)];
  - la traçabilité entre les exigences ci-dessus et les exigences fonctionnelles qui en sont la source [c)].
- <c)1)>: Il convient que l'analyse de l'ensemble complet des exigences du système comprenne une analyse des conséquences des défaillances éventuelles des fonctions principales [a)4)] permettant:
  - de définir des objectifs de protection des fonctions principales [a)2)] et des objectifs de traitement des pannes identifiées, etc. [a)5)];
  - d'élaborer des mesures génériques contre les défaillances dont les causes ne sont pas identifiées [a)8)];
  - d'éviter d'aggraver le danger et d'augmenter les risques de dommages supplémentaires par la mise en place de réponses aux défaillances [b)6)];
  - de réduire le danger que le système concerné peut représenter pour tous les systèmes qui lui sont reliés [b)8)].
- <c)2)>: Il convient que les mesures des performances critiques comprennent des mesures du degré de protection pour les fonctions principales [a)2)] et des mesures de traitement des défaillances, etc. [a)5)].
- <d)1)>: Il convient que l'accord sur les exigences du système énumère les fonctions principales à protéger [a)1)], les objectifs de protection des fonctions principales [a)2)] et les objectifs de traitement des défaillances, etc., qui ont un impact sur les fonctions principales [a)5)].
- <d)2)>: Il convient de maintenir la traçabilité entre les exigences de supervision et les exigences relatives aux fonctions principales afin de permettre d'établir la redevabilité quant à la réponse aux défaillances [b)1), c)].

<6.4.4> Processus de définition de l'architecture

- <a)2)>: Il convient que les préoccupations identifiées des parties prenantes se reflètent sur les objectifs de protection des fonctions principales [a)2)] et sur les objectifs de traitement des pannes, etc. [a)5)] dans des itérations du processus de définition de l'architecture avec le Processus de définition des besoins et des exigences des parties prenantes et avec le Processus de définition des exigences du système. Il convient d'identifier les préoccupations des parties prenantes concernant les dommages subis par le système relié au système concerné [b)7)].
- <c)>: Il convient d'élaborer des modèles et des vues concernant le traitement des défaillances, etc. [a)5), a)6)], leur détection [b)1)], et les réponses spécifiques et génériques aux défaillances [a)7), a)8)]. Il convient de tenir compte des interactions entre les réponses aux défaillances et les autres fonctions du système pour éviter que les réponses aux défaillances n'aggravent les dommages [b)7)].
- <c)2)>: Il convient d'identifier les entités architecturales principales liées aux fonctions principales et à leur protection [a)1), a)7)].
- <d)1)>: Il convient d'identifier les éléments de système principaux liés aux entités architecturales principales pour la protection des fonctions principales [a)1), a)7)].
- <d)2), d)3)>: Il convient de tenir compte des erreurs d'interaction, de leur détection et des réponses spécifiques et génériques lors de la définition d'interfaces entre éléments de système et avec des entités externes, de même qu'en présence d'exigences de ségrégation par rapport à des éléments de système [a)3), b)1), a)7), a)8)]. Il convient de tenir compte des interactions entre les réponses aux défaillances et les autres fonctions du système pour éviter que les réponses aux défaillances n'aggravent les dommages [b)6)].

– <f)2)>: Il convient que l'acceptation de l'architecture par les parties prenantes comprenne l'acceptation de l'architecture de traitement des défaillances, etc. [a)6)], les réponses spécifiques aux défaillances [a)7)], les réponses génériques [a)8)] et la détection [b)1)].

– <f)6)>: Il convient de maintenir la traçabilité entre les objectifs de traitement des défaillances, etc. [a)5)] et l'architecture du traitement des défaillances, etc. [a)6)], les réponses spécifiques aux défaillances [a)7)], les réponses génériques [a)8)] et la détection [b)1)] par rapport aux objectifs de protection [a)2)], afin de rendre compte de la réponse aux défaillances [c)].

<6.4.5> Processus de définition de conception

– <a)2)>: Il convient de déterminer les caractéristiques de conception liées aux mesures génériques contre les défaillances dont les causes ne sont pas identifiées [a)8)].

– <a)3)>: Il convient que les principes d'évolution de la conception donnent des recommandations concernant la vue de processus d'adaptation aux changements après la réponse aux défaillances [d)].

– <b)1)>: Il convient d'attribuer aux éléments du système les exigences de protection des fonctions principales [a)2)] et de traitement des pannes, etc. [a)5)].

– <d)3)>: Il convient de maintenir la traçabilité des caractéristiques de conception pour le traitement des défaillances, etc. [a)6)], les réponses spécifiques aux défaillances [a)7)], les réponses génériques [a)8)] et la détection [b)1)] vis-à-vis des entités architecturales de protection des fonctions principales [a)2)] et les objectifs de traitement des pannes [a)5)], à des fins de compte-rendu [c)].

<6.4.6> Processus d'analyse du système

– <c)1)>: Il convient de maintenir la traçabilité des résultats d'analyse du système de manière à permettre de rendre compte de la réponse aux défaillances en temps utile [c)].

<6.4.7> Processus de mise en œuvre

– <c)2)>: Il convient de maintenir la traçabilité des caractéristiques de conception pour rendre compte de la réponse aux défaillances [c)]:

  - éléments de système mis en œuvre pour le traitement des pannes, des erreurs, des défaillances et de leurs précurseurs [a)6)];
  - réponses spécifiques aux défaillances [a)7)];
  - réponses génériques [a)8)];
  - détection des pannes, des erreurs, des défaillances et de leurs précurseurs [b)1)].

<6.4.8> Processus d'intégration

– <a)1)>: Il convient que les points de contrôle du bon fonctionnement et de l'intégrité des interfaces assemblées et des fonctions système sélectionnées comprennent:

  - les interfaces des fonctions principales identifiées en [a)1)];
  - les interfaces des fonctions visant à protéger les fonctions principales [a)2), a)5), a)7), b)1), b)5)];
  - le contrôle des erreurs d'interaction entre éléments de système [a)2), a)8), b)7)];
  - le contrôle des mesures génériques contre les défaillances, sur l'ensemble du système [a)8), b)6), b)7)];
  - le contrôle du fait que les réponses aux défaillances n'aggravent pas la dangerosité et n'augmentent pas le risque de dommages supplémentaires [b)6)];
  - le contrôle du danger potentiel que le système concerné peut représenter pour tous les systèmes qui lui sont reliés [b)8)].

– <b)3)>: Le contrôle des interfaces, des fonctions sélectionnées et des caractéristiques de qualité critiques comprend:
  - l'identification des erreurs d'interaction potentielles [a)3), a)7), b)7)];
  - le contrôle de l'efficacité des mesures génériques contre les défaillances [a)8)];
  - le contrôle du fait que les réponses aux défaillances n'aggravent pas la dangerosité et n'augmentent pas le risque de dommages supplémentaires [b)6)];
  - le contrôle du danger potentiel que le système concerné peut représenter pour tous les systèmes qui lui sont reliés [b)8)].
– <c)2)>: Il convient de maintenir la traçabilité des éléments de système intégrés de manière à permettre une réponse rapide aux défaillances [b)] et un compte-rendu de la réponse aux défaillances en temps utile [c)].

<6.4.9> Processus de vérification

– <a)1)>: Il convient de vérifier, dans le cadre du domaine d'application de la vérification et des mesures correspondantes, que les objectifs de protection des fonctions principales [a)2)] et de traitement des défaillances, etc. [a)5)], sont atteints.
– <c)2)>: Il convient d'enregistrer les incidents d'exploitation et d'assurer un suivi jusqu'à leur résolution d'une manière permettant de rendre compte de la réponse aux défaillances en temps utile [c)].
– <c)3)>: Il convient que l'accord entre les parties prenantes au sujet du respect des exigences spécifiées comprenne un accord de respect des objectifs de traitement des défaillances, etc. [a)5)].
– <c)4)>: Il convient de maintenir la traçabilité des résultats de vérification de manière à permettre une réponse rapide aux défaillances [b)] et un compte-rendu de la réponse aux défaillances en temps utile [c)].

<6.4.10> Processus de transition

– <b)5)>: Il convient de planifier la formation des opérateurs, etc., dans le cadre des réponses et des mesures génériques contre les défaillances [a)7), a)8)]. Il convient que la formation serve aussi à développer les compétences des parties prenantes pour parvenir au résultat [b)] par une intervention humaine.
– <b)9)>: Il est recommandé qu'un examen de l'aptitude opérationnelle confirme que les objectifs visés en [a)2), a)5), a)8), b)1) à b)7)] ont bien été atteints.
– <c)2)>: Il convient d'enregistrer les incidents d'exploitation et d'assurer un suivi jusqu'à leur résolution d'une manière permettant de rendre compte de la réponse aux défaillances en temps utile [c)].
– <c)3)>: Il convient de maintenir la traçabilité des éléments de système ayant fait l'objet d'une transition de manière à permettre une réponse rapide aux défaillances [b)] et un compte-rendu de la réponse aux défaillances en temps utile [c)].

<6.4.11> Processus de validation

– <a)1)>: Il convient d'inclure les points suivants dans le domaine d'application et les mesures de validation:
  - la validation de la protection des fonctions principales du point de vue de leurs objectifs [a)2)];
  - la validation du traitement des défaillances, etc., du point de vue de leurs objectifs [a)5)];
  - la validation des mesures génériques contre les défaillances dont les causes ne sont pas identifiées [a)8), b)1), b)4) à b)7)].
– <c)2)>: Il convient d'enregistrer les incidents d'exploitation et d'assurer un suivi jusqu'à leur résolution d'une manière permettant de rendre compte de la réponse aux défaillances en temps utile [c)].

– <c)4)>: Il convient de maintenir la traçabilité des éléments de système validés de manière à permettre une réponse rapide aux défaillances [b)] et un compte-rendu de la réponse aux défaillances en temps utile [c)].

<6.4.12> Processus d'exploitation

– <a)1)>: Il convient que la stratégie d'exploitation comprenne les procédures suivantes pour [b)]:
  - des procédures de détection des défaillances, etc. [b)1)] et de prédiction des défaillances à partir de leurs précurseurs;
  - des procédures de supervision des défaillances, etc. dans les catégories i) et ii) de [a)6)];
  - des procédures pour [b)3)] et [b)5)] qui permettent de garantir que tout est prêt pour une intervention humaine rapide en cas de détection de défaillances, etc.
– <a)5)>: Il convient de planifier la formation du personnel dans le cadre des mesures génériques indiquées en [a)8)]; il convient que cette formation développe l'aptitude des parties prenantes à atteindre les objectifs [b)] par une intervention humaine qui reflète la compréhension de la finalité du système. Il convient que les exigences de qualification comprennent les exigences d'aptitude mentionnées ci-dessus.
– <b)3)>: Il convient que la supervision de l'exploitation du système comprenne la surveillance des pannes, des erreurs, des défaillances et de leurs précurseurs des catégories i) et ii) de [a)6)], de manière à permettre leur détection [b)1)]. Lorsque des défaillances, etc., sont détectées, il convient d'exécuter les procédures des stratégies d'exploitation permettant d'atteindre les résultats [b)2) à b)7)] et d'en évaluer le résultat [b)8)].
– <b)4)>: Il convient que l'identification de performances inacceptables comprenne l'évaluation de la réponse aux défaillances [b)8)] et qu'elle fasse appel à la vue de processus d'adaptation aux changements, pour améliorer le système [d)].
– <b)5)>: Il convient d'inclure les objectifs des opérations d'urgence nécessaires à la continuité des services et la condition de déclenchement des opérations d'urgence dans les objectifs de protection des fonctions principales mentionnés en [a)2)], ainsi que dans les objectifs de traitement des défaillances, etc., mentionnés en [a)5)].
– <c)1)>: Il convient d'enregistrer les résultats des opérations et les anomalies d'une manière permettant de rendre compte de la réponse aux défaillances [c)] et de l'amélioration du système [d)].
– <c)2)>: Il convient d'enregistrer les incidents et les problèmes d'exploitation et d'en assurer le suivi d'une manière permettant de rendre compte de la réponse aux défaillances [c)] et de l'amélioration du système [d)].
– <c)3)>: Il convient de maintenir la traçabilité des éléments opérationnels de manière à permettre une réponse rapide aux défaillances [b)] et un compte-rendu de la réponse aux défaillances en temps utile [c)].
– <d)>: Il convient que l'assistance client rende des comptes activement sur la réponse aux défaillances [c)].

<6.4.13> Processus de maintenance

– <a)1)>: Il convient que la stratégie de maintenance reflète les objectifs de protection des fonctions principales [a)2)] et les objectifs de traitement des défaillances, etc. [a)5), b)].
– <b)1)>: Il convient d'intégrer l'identification des besoins de maintenance futurs à l'identification et à la détection des pannes, etc. [a)3), b)1)].
– <b)2)>: Il convient d'enregistrer les incidents et les problèmes de maintenance et d'en assurer le suivi d'une manière permettant de rendre compte de la réponse aux défaillances [c)] et de l'amélioration du système [d)].
– <b)3), b)4)>: Il convient d'intégrer le traitement des pannes aléatoires dans la vue de processus de réponse aux défaillances [a), b), c), d)].
– <b)5)>: Il est admis que la maintenance préventive soit choisie comme moyen d'atteindre l'objectif de traitement des pannes, etc. identifiées [a)5), a)7)].

– <b)6)>: Les actions d'identification des défaillances font partie de la réalisation de [b)1), b)2)].

– <c)>: Il convient d'inclure le soutien logistique dans les réponses spécifiques aux précurseurs de défaillance dans [a)7), b)4)].

– <d)1)>: Il convient d'enregistrer les résultats de maintenance, les résultats logistiques et les anomalies d'une manière permettant de rendre compte de la réponse aux défaillances et l'amélioration du système [c), d)].

– <d)2)>: Il convient d'enregistrer les incidents et les problèmes d'exploitation et d'en assurer le suivi d'une manière permettant de rendre compte de la réponse aux défaillances et l'amélioration du système [c), d)].

– <d)3)>: Il convient d'identifier les tendances des incidents et problèmes afin de promouvoir l'amélioration du cycle de vie du système [d)].

– <d)4)>: Il convient de maintenir la traçabilité des éléments de maintenance de manière à permettre une réponse rapide aux défaillances [b)] et un compte-rendu de la réponse aux défaillances en temps utile [c)].

– <d)6)>: Il convient d'intégrer la supervision de la satisfaction des clients dans l'évaluation de la réponse aux défaillances [b)8)] et dans l'amélioration du cycle de vie du système [d)].

<6.4.14> Processus de mise au rebut

– <a)1)>: Il convient de définir la stratégie de mise au rebut de manière à permettre [b)7)].

6.5 Vue de processus d'adaptation aux changements

6.5.1 Objet

La vue de processus d'adaptation aux changements a pour objet de maintenir l'aptitude à l'emploi du système, malgré les changements d'exigences, d'environnements, d'objectifs et/ou d'objet.

Il convient de parvenir à cette fin (l'objet) en tenant compte des points suivants.

La vue de processus soutient l'aptitude à la continuité des services grâce à de véritables solutions aux problèmes provoqués par les changements et elle met l'accent sur la garantie que des défaillances de même type ne se reproduiront pas.

Un grand nombre de types de changements différents exigent des adaptations. Des changements se produisent dans les autres systèmes reliés au système. Les changements dans les environnements technologiques, sociaux et commerciaux sont désormais plus fréquents avec le rythme rapide des innovations. Toute détection d'événements non anticipés signale un changement dans les hypothèses de départ, toujours incomplètes et incertaines. Les changements peuvent ne pas être évidents à détecter. Ils doivent souvent faire l'objet d'une recherche active, par exemple à travers des revues périodiques. Les adaptations requises peuvent ne pas concerner le système lui-même. L'ensemble des processus du cycle de vie doit être revu et adapté lorsque c'est nécessaire. Même l'influence sur l'environnement et le changement d'environnement peuvent constituer une adaptation.

La vue de processus d'adaptation aux changements organise des activités survenant lors de l'adaptation du système à des changements, y compris: la détection des changements, leur analyse, la définition et l'exécution d'actions dans l'intérêt de la continuité des services subissant éventuellement les changements et, là où ces changements induisent des défaillances, les mesures de prévention des défaillances ou de leur répétition.

Il convient de veiller à ce que les plans ne soient pas rigides au point qu'un organisme perde sa flexibilité en cas de situation imprévue.

La réalisation de la finalité de cette vue de processus passe par:

– l'exécution et l'évaluation de l'adaptation lorsque des changements surviennent [résultats de 6.5.2 a) à d)];
– l'amélioration continue du cycle de vie du système et l'établissement de la redevabilité quant à l'adaptation aux changements [e), f)].

La relation entre l'objet et les résultats est décrite à l'Article B.5.

6.5.2 Résultats

a) Les changements sont repérés et identifiés.

1) Les changements de contexte, d'hypothèses, de risques, etc., susceptibles d'exiger une adaptation du système sont identifiés.

NOTE 1 Les éléments soumis à de tels changements sont: les exigences des parties prenantes, les systèmes interconnectés, l'environnement technologique, social et opérationnel, la perception des services par les parties prenantes et la compréhension du consensus par les parties prenantes.

NOTE 2 Les changements peuvent ne pas être évidents. Ils font souvent l'objet d'une recherche active, par exemple à travers des revues périodiques.

2) Lorsque des événements non anticipés, y compris des défaillances, sont détectés, le changement qui les a provoqués est identifié dans le système et/ou l'environnement. Il est admis que cette identification soit déclenchée par la vue de processus de réponse aux défaillances.

NOTE 3 Toute détection d'événements non anticipés, y compris des défaillances, constitue une détection de changement. Le changement peut concerner des faits ou la compréhension de faits présumés.

3) Les changements perturbateurs sont repérés et gérés.

NOTE 4 Les changements perturbateurs sont les changements pour lesquels une adaptation probante du système par des parties prenantes est impossible ou irréalisable. Cela comprend le cas où le coût de l'adaptation nécessaire dépasse les paramètres économiques pouvant être supportés par les parties prenantes redevables selon l'accord en vigueur. Une gestion ordonnée de ces cas peut être planifiée, en anticipant le plus possible, par exemple en introduisant de nouvelles parties prenantes, en excluant des parties prenantes non performantes, en rétablissant un consensus ou en procédant à une mise au rebut anticipée du système.

b) L'adaptation du système est préparée.

1) Les conséquences des changements sur l'aptitude à l'emploi du système sont évaluées et la relation entre les changements et leurs conséquences est documentée.

NOTE 5 L'évaluation comporte une analyse de causalité.

2) L'objectif de l'adaptation visant à maintenir l'aptitude à l'emploi du système est défini. Cela met en jeu les points suivants:

i) les parties prenantes sont informées des besoins d'adaptation, des choix d'adaptation et de leurs conséquences;

ii) Les parties prenantes reçoivent le soutien nécessaire pour négocier des accords dans les nouvelles circonstances.

iii) L'adaptation déclenchée par la vue de processus de réponse aux défaillances empêche que les défaillances se reproduisent.

iv) L'objectif de l'adaptation est défini.

3) L'objectif de l'adaptation est convenu et il est répercuté dans l'accord entre les parties prenantes à travers une mise à jour via la vue de processus de recherche d'un consensus.

NOTE 6 Ce point inclut le fait de prendre la décision d'adapter le système.

NOTE 7 Un soin particulier est apporté en cas d'adaptation à la suite de changements perturbateurs.

c) L'adaptation du système est effectuée.

NOTE 8 L'adaptation peut être d'ordre technique ou non. L'ensemble des processus du cycle de vie est revu et adapté lorsque c'est nécessaire. L'adaptation peut ne pas concerner le système en lui-même. Même l'influence sur l'environnement et le changement d'environnement peuvent constituer une adaptation.

NOTE 9 Lorsque des adaptations sont envisagées, la prévention des erreurs d'interaction entre les parties du système appelées à changer après les adaptations et les parties devant rester inchangées est prise en compte.

1) Une assistance technique est mise à disposition pour réaliser l'adaptation nécessaire.
2) Les connaissances issues des expériences passées sont mises à profit.
3) Une adaptation répondant à l'objectif poursuivi est définie.
4) L'adaptation est mise au point.
5) L'adaptation est déployée de manière à perturber le moins possible les services existants du système en exploitation et les autres systèmes qui y sont reliés.

d) Le système adapté est évalué au regard de l'objectif de l'adaptation.

e) Le cycle de vie du système est amélioré en permanence.

NOTE 10 Une amélioration continue de la capacité du cycle de vie du système à maintenir son aptitude à l'emploi est attendue. Cet aspect est distinct de la recherche de performances système toujours plus élevées, etc.

f) La vue de processus d'établissement de la redevabilité rend compte de l'adaptation.

1) La traçabilité des changements de contexte, etc., par rapport à l'adaptation est maintenue.
2) Les parties prenantes et la société en général sont informées de l'évolution et du résultat de l'adaptation.

6.5.3 Processus, activités et tâches

Il convient de mettre en œuvre la vue de processus d'adaptation aux changements à l'aide des activités et des tâches des processus suivants prévus par la norme ISO/IEC/IEEE 15288.

<6.1.1> Processus d'acquisition

– <c)1), c)4)>: Il convient d'apporter le soutien nécessaire aux parties prenantes lors de la négociation d'un accord entre l'acheteur et le fournisseur dans le nouveau contexte [b)2)ii)].
– <c)2), c)5)>: Il convient d'identifier, à partir de l'objectif de l'adaptation, les changements nécessaires à apporter à l'accord. Il convient que l'objectif de l'adaptation soit considéré comme une mise à jour de l'accord [b)3)].
– <c)3)>: Il convient que les résultats de l'évaluation de l'impact des changements sur l'accord soient rapprochés de la définition de l'objectif de l'adaptation [b)].
– <d)1)>: Il convient que tout écart important dans l'avancement réel de l'exécution de l'accord par rapport à ce qui était planifié soit identifié comme un changement pouvant exiger une adaptation [a)1)].

<6.1.2> Processus de fourniture

– <c)1), c)4)>: Il convient d'apporter le soutien nécessaire aux parties prenantes lors de la négociation d'un accord entre l'acheteur et le fournisseur dans le nouveau contexte [b)2)ii)].
– <c)2), c)5)>: Il convient d'identifier, à partir de l'objectif de l'adaptation, les changements nécessaires à apporter à l'accord. Il convient que l'objectif de l'adaptation soit considéré comme une mise à jour de l'accord [b)3)].
– <c)3)>: Il convient que les résultats de l'évaluation de l'impact des changements sur l'accord soient rapprochés de la définition de l'objectif de l'adaptation [b)].
– <d)2)>: Il convient que tout écart important dans l'avancement réel de l'exécution de l'accord par rapport à ce qui était planifié soit identifié comme un changement pouvant exiger une adaptation [a)1)].

<6.2.1> Processus de gestion du modèle de cycle de vie

– <a)5)>: Il convient que les modèles de cycle de vie établis spécifient les liens entre les processus de cycle de vie qui permettent la réalisation de tous les résultats de la vue de processus d'adaptation aux changements [a) à f)].
– <c)2)>: Il convient que le retour d'expérience d'une itération d'adaptation aux changements soit incorporé à l'amélioration du processus pour permettre son application aux futurs changements [e)].

<6.2.2> Processus de gestion des infrastructures Il convient d'identifier les changements d'infrastructure du projet et les changements d'exigences en matière d'infrastructure comme des changements pouvant exiger une adaptation du système [a)].

<6.2.3> Processus de gestion du portefeuille

– <a)1)>: Il convient d'assurer l'identification des capacités ou des missions potentiellement nouvelles ou modifiées dans le cadre de l'identification des changements et de l'évaluation de leur impact [a)1), b)1)].
– <a)2)>: Il convient que la hiérarchisation, la sélection et l'établissement de nouvelles opportunités d'affaires, etc., éclairent l'évaluation de l'aptitude à l'emploi du système et la définition des objectifs d'adaptation en lien avec les autres projets du portefeuille de l'organisme [b)1), b)2)].
– <a)3)>: Il convient que la définition du projet concernant le système, les obligations et les autorités soit cohérente avec l'objectif de l'adaptation du système [b)2), b)3)].
– <a)4)>: Il convient que les buts, objectifs et résultats anticipés du projet constituent une base pour l'évaluation de l'aptitude à l'emploi du système et la définition de l'objectif de l'adaptation en lien avec les autres projets du portefeuille [b)1), b)2)].
– <a)8)>: Il convient de donner l'autorisation de commencer l'adaptation du système dans le but défini en tenant compte de ses conséquences sur les autres projets au sein du portefeuille de l'organisation [b)3), c)].
– <b)1)>: Il convient d'évaluer la viabilité du projet dans le cadre de l'identification des changements et de l'évaluation de l'aptitude à l'emploi du système [a)1), b)1)].
– <b)2)>: Les actions visant à poursuivre ou à réorienter le projet en ce qui concerne le système sont notamment la prise de décisions quant à l'opportunité d'adapter le système ou non, ainsi que la définition de l'objectif de l'adaptation [b)3), b)2)].

<6.2.5> Processus de gestion de la qualité

– <a)>: Il convient de planifier la gestion de la qualité en tenant compte du fait que les objectifs de gestion de la qualité changent en même temps que la finalité du système [a) à d)].
– <b)1)>: Il convient de recueillir et d'analyser les résultats d'évaluation de l'assurance qualité dans le cadre du repérage et de l'identification des changements pertinents [a)].
– <b)2)>: Il convient d'utiliser l'évaluation de la satisfaction des clients dans l'évaluation l'aptitude à l'emploi du système [b)1)].
– <b)4)>: Il convient de superviser l'état des améliorations de la qualité dans le cadre du repérage et de l'identification des changements pertinents [a)] ainsi que de l'évaluation du système adapté [d)].
– <c)1), c)2)>: Il convient que la planification des mesures correctives et préventives portant sur la gestion de la qualité soit intégrée à la définition de l'objectif de l'adaptation [b)2)].
– <c)3)>: Il convient de recourir à la supervision des mesures correctives et préventives pour évaluer si l'objectif de l'adaptation est atteint dans le système adapté [d)].

<6.2.6> Il convient que le Processus de gestion des connaissances tienne à jour les informations issues des retours d'expérience provenant d'une itération d'adaptation aux changements afin de permettre leur application aux changements futurs [c)2), e)].

<6.3.1> Processus de planification de projet

– <a)1)>: Il convient que les objectifs du projet soient identifiés conjointement avec leur justification, afin de fournir la base nécessaire pour évaluer l'aptitude à l'emploi du système à la suite des changements [b)1)] et pour définir l'objectif de l'adaptation [b)2)].
– <a)2)>: Il convient que le domaine d'application du projet comprenne les activités nécessaires à l'obtention de tous les résultats de la présente vue de processus [a) à f)]. Il convient que les actions de contrôle du projet (voir <a)2) NOTE>) soient planifiées de manière à tenir compte des cas où les objectifs du projet changent [a)]. Il convient que tout changement des activités menées dans le cadre du domaine d'application soit repéré et identifié [a)].
– <a)3)>: Il convient que le modèle de cycle de vie défini pour le projet spécifie les liens entre les processus du cycle de vie qui permettent la réalisation de tous les résultats de la vue de processus d'adaptation aux changements [a) à f)].
– <b)2)>: Il convient que les critères de réussite pour les décisions prises à l'issue de chaque phase du cycle de vie comprennent des critères pour la décision finale de la phase d'utilisation, qui marque le début de la vue de processus d'adaptation aux changements [a)].
– <b)4)>: Il convient que les rôles, responsabilités, obligations et autorités relatifs à la vue de processus d'adaptation aux changements soient définis de manière permettant de rendre compte de l'adaptation aux changements [f)].
– <b)5)>: Il convient que tout changement de l'infrastructure et des services nécessaire aux fins du projet soit repéré et identifié [a)].
– <b)7)>: Il convient que la soumission du plan d'adaptation permette de mettre en œuvre l'accord relatif à l'objectif de l'adaptation [b)3)] et soit utilisée pour rendre compte de l'adaptation [f)].

<6.3.2> Il convient que la Procédure d'évaluation et de contrôle du projet régisse la vue de processus d'adaptation aux changements et permette d'en obtenir tous les résultats [a) à f)]. En particulier, il convient que le processus tienne compte des changements dans les objectifs techniques, les exigences et les objectifs commerciaux en général. Cela suppose d'assister les développeurs dans la conception des adaptations possibles, d'identifier les changements dans le contexte, les hypothèses, les risques et tout autre changement qui nécessite une adaptation du système, et enfin d'identifier les moyens d'adaptation techniques ou non techniques nécessaires à chaque changement.

– <b)>: Il convient que l'évaluation du projet comprenne le repérage et l'identification des changements [a)]. Il convient de mener une évaluation du projet concernant tout changement potentiel du contexte, des objectifs et des plans, afin d'évaluer l'aptitude à l'emploi du système [b)1)] et de définir l'objectif de l'adaptation [b)2)].
– <b)7)>: Il convient que la gestion du projet, la revue technique, les audits et l'inspection déterminent s'il est nécessaire de procéder à l'adaptation du système et si ce dernier est prêt [a), b)].
– <b)8)>: Il convient de superviser les processus critiques et les nouvelles technologies dans le cadre du repérage et de l'identification des changements [a)].
– <b)9)>: Il convient que l'analyse des résultats des mesures permette d'identifier les changements et de faire des recommandations concernant l'objectif de l'adaptation [a), b)2)].
– <b)11)>: Il convient que tout écart important dans l'avancement réel par rapport au plan initial soit identifié comme un changement pouvant exiger une adaptation [a)1)].
– <c)>: Les contrôles du projet comprennent le déclenchement de l'adaptation du système, si nécessaire [b), c)].
– <c)1)>: Les mesures à initier aux fins du contrôle du projet comprennent la définition du but de l'adaptation [b)2)].
– <c)2)>: Il convient de replanifier le projet en reflétant les buts de l'adaptation convenus et l'accord mis à jour [b)3)].

– <c)4)>: Il convient d'autoriser la réalisation de l'adaptation du système dans le cadre du projet, dans les buts définis [b)3), c)].

<6.3.3> Processus de gestion des décisions

– <a)1), c)>: Il convient que la stratégie de gestion des décisions tienne compte des changements des critères de décision dus aux changements dans le contexte, les hypothèses, les risques, etc. Il convient que la gestion des décisions passe en revue les décisions précédentes lorsque des changements sont repérés et identifiés [b)1), b)2)].

<6.3.4> Processus de gestion des risques: Les procédures et processus de gestion et d'évaluation des risques en général sont donnés dans l'ISO 31000 [16] et l'IEC 31010 [17]. Il convient également de tenir compte des éléments suivants.

– <a)1)>: Il convient que la stratégie de gestion des risques tienne compte de l'évolution du contexte de gestion des risques et comprenne des procédures de révision des dispositifs actuels de maîtrise des risques, lorsque des changements sont repérés et identifiés [a), b)1), b)2)].
– <a)2)>: Il convient que le contexte de gestion des risques et le processus d'identification des risques tiennent compte des risques associés aux changements sur les points suivants [a)]:
  - exigences des parties prenantes,
  - systèmes connectés,
  - environnement technologique, commercial et social,
  - perception des services par les parties prenantes,
  - compréhension du consensus par les parties prenantes.
– <b)1)>: Il convient que les seuils de risque et les critères d'acceptation des risques liés aux changements reflètent l'impact des changements sur l'aptitude à l'emploi du système [b)1)].
– <b)3)>: Il convient que le profil de risque soit transmis aux parties prenantes dans le cadre de la négociation de l'objectif de l'adaptation et pour rendre compte de l'adaptation [b)2), f)2)].
– <c)1)>: Il convient d'identifier les risques associés aux changements dans le cadre du repérage et de l'identification des changements [a)1)].
– <c)2), c)3)>: Il convient d'estimer les conséquences des risques associés aux changements et de les comparer aux seuils de risque dans le cadre de l'évaluation de l'aptitude à l'emploi du système [b)1)].
– <c)4)>: La définition des stratégies de traitement et des mesures recommandées concernant les risques associés aux changements qui ne respectent pas les seuils de risque correspondants fait partie de la définition des objectifs de l'adaptation [b)2)] et de la définition de l'adaptation à réaliser [c)3)].
– <d)1)>: L'identification des alternatives recommandées pour le traitement des risques liés aux changements fait partie de la définition des objectifs de l'adaptation [b)2)].
– <d)2)>: Il convient de consigner, dans la mise à jour de l'accord entre les parties prenantes, le fait que les parties prenantes décident qu'il convient de prendre des mesures concernant les risques associés aux changements [b)3)]. La mise en œuvre du traitement des risques associés aux changements fait partie de l'adaptation à mettre en œuvre [c)3)] et de sa mise en œuvre [c)4)].
– <e)1)>: Il convient de superviser continuellement l'ensemble des risques et le contexte de gestion des risques pour identifier les changements, et de réévaluer les risques le cas échéant dans le cadre du repérage et de l'identification des changements [a)1)] ainsi que de l'évaluation de l'aptitude à l'emploi du système [b)1)].
– <e)2)>: Il convient que les mesures d'évaluation de l'efficacité des traitements des risques permettent l'évaluation du système adapté [d)]. La supervision des mesures fait partie du repérage et de l'identification des changements [a)].

<6.3.5> Processus de gestion de la configuration

– <b)1)>: L'identification des éléments de configuration est essentielle pour le repérage et l'identification des changements au sein du système [a)]. Il convient que les éléments du système pour lesquels un changement peut exiger une adaptation soient identifiés comme des éléments de configuration. Les éléments de configuration peuvent être des composants de la boîte noire.
– <b)2)>: Il convient que l'identification de la structure des informations concernant le système tienne compte de la probabilité que la structure du système elle-même est susceptible de changer involontairement en raison d'une incertitude ou d'une lacune au sein du système, ou volontairement du fait du processus d'adaptation [a), f)].
– <b)3)>: Il convient que la mise en place d'identifiants pour les éléments de configuration permette d'assurer la traçabilité entre les éléments de configuration introduits ou modifiés aux fins de l'adaptation et les changements qui ont rendu l'adaptation nécessaire [f)].
– <b)4)>: Il convient que l'établissement d'une base de référence permette le repérage et l'identification des changements au sein du système pendant tout le cycle de vie du système [a)].
– <b)5)>: Il convient d'utiliser l'accord établissant la base de référence entre l'acquéreur et le fournisseur comme mise à jour de la base de référence pour définir l'objectif de l'adaptation, en vue des changements ultérieurs [b)3)].
– <c)>: Il convient que la gestion des changements de configuration comprenne les éléments suivants:
  - l'analyse de l'impact des changements sur l'aptitude à l'emploi du système [b)1)],
  - la notification des adaptations possibles aux parties prenantes concernées [b)2)i)],
  - le soutien aux parties prenantes pendant les négociations et l'accord sur l'objectif de l'adaptation [b)2)ii), b)3)].
– <c)4)>: Il convient que le suivi et la gestion des changements approuvés aident à rendre compte de l'adaptation [f)]. Il convient que la justification de l'adaptation soit consignée à titre de retour d'expérience à utiliser pour les adaptations ultérieures [c)2)].
– <d)>: Il convient que le rapport sur l'état de configuration comprenne le maintien de la traçabilité des éléments de configuration ainsi que les justifications des changements des éléments [f)].
– <e)2)>: Il convient que la vérification de la configuration du produit aide au repérage et à l'identification des changements involontaires au sein du système dus à une incertitude ou à une lacune au sein de celui-ci [a)].
– <f)1)>: Il convient que l'approbation d'une version du système confirme que la version sera mise en œuvre de manière à perturber le moins possible les services existants du système et d'autres systèmes connectés [c)5)].

<6.3.6> Il convient que le Processus de gestion des informations permette:

– le repérage et l'identification des changements, en mettant à disposition les informations anciennes et actuelles sur les éléments susceptibles d'être modifiés [a)],
– la transmission aux parties prenantes d'informations sur les adaptations possibles [b)2)i)],
– la transmission d'informations sur les expériences précédentes de développement d'adaptations [c)2)],
– la transmission de rapports sur l'adaptation aux parties prenantes [f)].

<6.3.7> Processus de mesure

– <a)3)>: Il convient d'identifier les besoins en information concernant le repérage et l'identification des changements [a)] ainsi que l'évaluation de l'aptitude à l'emploi du système [b)1)].
– <b)4)>: Il convient que les résultats des mesures informent les parties prenantes sur l'ampleur des changements [a), b)].

<6.3.8> Processus d'assurance qualité

– <b)>: Il convient de mener une évaluation des produits et des services dans le cadre de l'évaluation du système adapté au regard de l'objectif de l'adaptation [d)].

– <c)1)>: Il convient que l'évaluation des processus du cycle de vie du projet permette l'amélioration continue du cycle de vie du système [e)].

– <e)>: Pour chaque incident et problème traité, il convient d'examiner si l'un des changements exige une adaptation du système ou non [a)2)].

<6.4.1> Processus d'analyse opérationnelle ou de mission

– <a) à e)>: Il convient d'adopter le Processus d'analyse opérationnelle ou de mission en vue de la réalisation de [a), b)] (voir <6.4.1.1, NOTE 2>). Les conditions d'adoption sont notamment les suivantes:

  • des changements sont repérés dans les processus d'exploitation et de maintenance,

  • la vue de processus de réponse aux défaillances définit l'objectif de l'amélioration du cycle de vie après une réponse à une défaillance,

  • des changements sont identifiés dans les entrées de ce processus.

  NOTE 1 Les entrées du Processus d'analyse opérationnelle ou de mission susceptibles de changer sont la stratégie organisationnelle, les problèmes et les opportunités qui y sont identifiés, les buts et objectifs de l'organisme, la possibilité d'utiliser des systèmes ou des services [a)1), NOTE 1].

  Il convient que le résultat du Processus d'analyse opérationnelle ou de mission comprenne des accords explicites entre les parties prenantes quant au lancement de l'adaptation du système et quant aux objectifs possibles de l'adaptation spécifiés en [b)3), b)2)].

– <a)1)>: Il convient que la stratégie organisationnelle définisse des déclencheurs pour les revues périodiques des problèmes et des opportunités afin de détecter les changements, en particulier à l'occasion des événements pertinents concernant l'organisation [a)].

– <b), c)>: Il convient que la définition de l'espace des problèmes et des opportunités, ainsi que la caractérisation de l'espace de solutions, forment la base de l'analyse de l'impact des changements sur l'aptitude à l'emploi du système, et qu'elles fassent partie des objectifs possibles de l'adaptation [b)1), b)2)].

– <d)>: Il convient que l'évaluation des catégories de solutions alternatives fournisse des informations permettant de décider de commencer l'adaptation ou non [b)3)] et de définir les objectifs possibles de l'adaptation en tant que catégorie(s) de solutions alternative(s) préférentielle(s) [b)2)].

– <e)1)>: Il convient de maintenir la traçabilité entre les résultats de l'analyse opérationnelle ou de mission avant et après les changements, ainsi que la traçabilité entre les résultats de l'analyse opérationnelle ou de mission et les artefacts dans les phases ultérieures du cycle de vie [d), e), f)].

<6.4.2> Processus de définition des besoins et exigences des parties prenantes

– <a) à f)>: Il convient d'adopter le Processus de définition des besoins et des exigences des parties prenantes, si nécessaire. Les conditions d'adoption sont les mêmes que celles du Processus d'analyse opérationnelle ou de mission.

NOTE 2 Les entrées du Processus de définition des besoins et des exigences des parties prenantes susceptibles de changer sont le résultat du Processus d'analyse opérationnelle ou de mission, le groupe de parties prenantes identifiées, les besoins des parties prenantes et l'environnement pris en compte dans la définition des scénarios représentatifs.

– <a)1)>: Il convient que l'identification des parties prenantes soutienne la gestion des changements perturbateurs lorsque la liste des parties prenantes existantes peut être modifiée [a)3)].

– <a)2)>: Il convient que la stratégie de définition des besoins et des exigences des parties prenantes comprenne un programme d'examens qui repère les changements dans les parties prenantes identifiées et dans les besoins et exigences qu'elles ont définis. Il convient que ces revues soient déclenchées périodiquement et lorsqu'elles sont nécessaires [a)].