IEC 62741

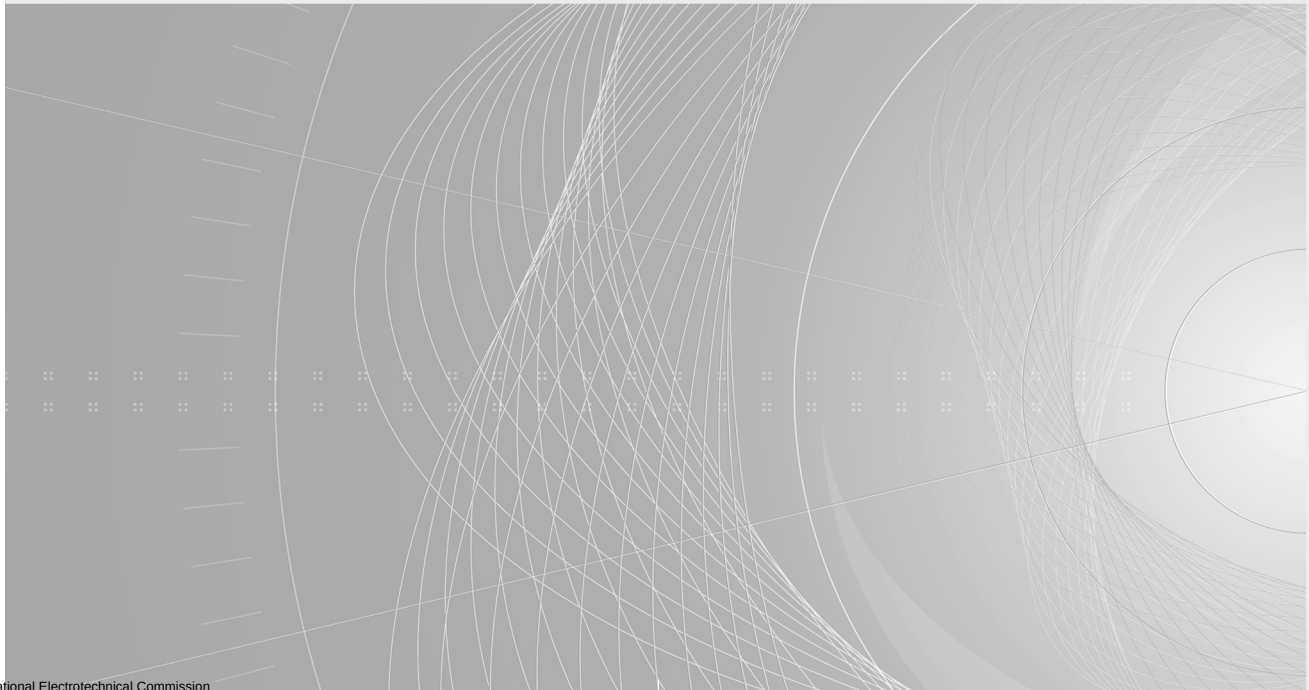
Edition 1.0 2015-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Demonstration of dependability requirements – The dependability case

Démonstration des exigences de sûreté de fonctionnement – Argumentaire dans le cadre de la sûreté de fonctionnement



IEC 62741:2015-02(en-fr)

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

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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

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

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

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

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

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

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
Plus de 60 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

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

IEC 62741

Edition 1.0 2015-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Demonstration of dependability requirements – The dependability case

Démonstration des exigences de sûreté de fonctionnement – Argumentaire dans le cadre de la sûreté de fonctionnement

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.120.01; 21.020

ISBN 978-2-8322-2247-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

DEMONSTRATION OF DEPENDABILITY REQUIREMENTS – THE DEPENDABILITY CASE

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 62741 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1591/FDIS	56/1609/RVD

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

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

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

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

INTRODUCTION

Dependability is the ability to perform as and when required. Acceptable levels of dependability are therefore essential for continued performance and optimized life cycle costs.

In order to achieve dependability of a system, dependability requirements should be established, the risks of not meeting them identified and a suitable set of activities developed to meet and demonstrate the requirements and manage the risks. A dependability case provides a convenient and convincing means of recording the output of these activities in a single location and presenting an argument, supported by evidence, that risks have been treated and that the necessary dependability has been or will be achieved and will continue to be achieved over time. It serves as the main means of communication on dependability among customers, suppliers and other stakeholders and promotes cooperation among them. This is essential for dependability achievement and providing assurance as part of the customer/supplier relationship.

Preparing a dependability case can also improve dependability through the actions taken to prepare and develop the argument within the dependability case. It can improve the cost effectiveness of a dependability programme because if an activity does not provide evidence to support the case, this may indicate that the activity is not necessary.

The activities required for the achievement of dependability depend on the nature and development state of the system and are likely to vary significantly from one project to another.

Throughout this International Standard, the term "dependability" includes all aspects of reliability, availability, maintainability and supportability, as well as other attributes such as usability, testability and durability. In addition, dependability of a system includes all aspects of that system, including components, processes, hardware, software and the interfaces between them.

This standard is intended as guidance: the guidelines are not prescriptive in nature, they are generic, they should be tailored to the specific objectives and are not exhaustive.

This standard does not address safety or the environment.

DEMONSTRATION OF DEPENDABILITY REQUIREMENTS – THE DEPENDABILITY CASE

1 Scope

This International Standard gives guidance on the content and application of a dependability case and establishes general principles for the preparation of a dependability case.

This standard is written in a basic project context where a customer orders a system that meets dependability requirements from a supplier and then manages the system until its retirement. The methods provided in this standard may be modified and adapted to other situations as needed.

The dependability case is normally produced by the customer and supplier but can also be used and updated by other organizations. For example, certification bodies and regulators may examine the submitted case to support their decisions and users of the system may update/expand the case, particularly where they use the system for a different purpose.

2 Normative references

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

IEC 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability* [1]

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

ISO 31000, *Risk management – Principles and guidelines*

3 Terms, definitions and abbreviations

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

3.1 Terms and definitions

3.1.1
dependability case
evidence-based, reasoned, traceable argument created to support the contention that a defined system does and/or will satisfy the dependability requirements

3.1.2
evidence framework
structure identifying what evidence will be/has been produced and when

[1] To be published.

3.1.3
off-the-shelf
OTS
non-developmental item of supply that is both commercial and sold in substantial quantities in the commercial marketplace

Note 1 to entry: Sometimes referred to as COTS (commercial off-the-shelf) or MOTS (modified off-the-shelf).

3.1.4
customer
party which orders or specifies the item, including the dependability requirements

Note 1 to entry: This could be an organization, sponsor, department, company or an individual and can change through the life cycle.

3.1.5
subsystem
part of a system, which is itself a system

3.1.6
supplier
party which supplies the item, which meets its dependability requirement

Note 1 to entry: This could be an organization, department, company or an individual and can change through the life cycle.

3.1.7
system <in dependability>
defined set of items that collectively fulfil a requirement

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

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

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

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

3.2 Abbreviations

COTS	Commercial off-the-shelf
FEM	Finite element modelling
FMECA	Failure mode, effects and criticality analysis
FTA	Fault tree analysis
MOTS	Modified off-the-shelf
OTS	Off-the-shelf

4 Background to the dependability case

4.1 Principles and purpose

A dependability case provides a reasoned and traceable argument based on evidence that a system satisfies the requirements and will continue to do so over time. It demonstrates why certain activities have been undertaken and how they can be judged to be successful. For maximum effectiveness it should be initiated at the concept stage, revised progressively during a system life cycle and is typically summarized in dependability case reports at predefined milestones. It records progress in obtaining evidence that dependability requirements are met and remains with the system throughout its life cycle until retirement.

The dependability case is of the greatest benefit for high value, low quantity systems where direct evidence of dependability may be difficult or expensive to obtain. Since these systems are often highly complex, involve novel technologies and have wide-ranging stakeholders, an explicit argument is necessary in order to demonstrate their detailed dependability claims with suitable evidence.

4.2 Relationship between the dependability case and dependability plans

Effective management of dependability requires organizational arrangements to implement policy, activities implemented in dependability programmes and plans and processes for performance evaluation, assurance and review.

A dependability programme involves

a) dependability plans, that define the activities, techniques and resources required to achieve dependability,

b) methods for measurement and assessment,

c) assurance and review.

The objectives of a dependability plan include ensuring that

1) the dependability requirements of the customer are determined and demonstrated to be understood by both the customer and supplier,

2) activities are planned, agreed and implemented to satisfy and demonstrate the requirements and treat the risks of failure,

3) the customer is provided with assurance that the dependability requirements are being, or will be, satisfied and that uncertainty in the dependability decreases over the course of the plan.

The dependability case provides progressive assurance that dependability requirements are being or will be satisfied and that uncertainty in the dependability is decreasing. In addition, the case demonstrates that the activities in the plan achieve the requirements and treat the risks. This forms part of the argument and evidence for why the system is, or will be, dependable. The plan is usually based on standards and the organization’s experience in managing dependability and is tailored, taking into account factors such as the relevant life cycle stages, the organization’s context, resources available and the risks that need to be managed.

The dependability plan and dependability case are often developed concurrently as both include consideration of the risks of not meeting the requirements. However, the system might meet the dependability requirements but it might not be possible to demonstrate that these requirements have been met. This might be because there is no appropriate activity which can demonstrate that the requirements have been met, or the cost or time required to do so might be excessive. Therefore the dependability plan may also include activities specifically intended to treat the risks of not being able to demonstrate that the requirements have been met and these activities also provide evidence in the dependability case.

A register of risks produced as part of a dependability case should be coordinated with the risks identified as part of planning the dependability programme and with the project risk register. Activities proposed to treat the risks are included in the dependability plan and examined as sources of evidence that risks have been treated. As the dependability plan is implemented, the dependability case is populated with evidence of the successful implementation of the plan. This provides progressive assurance that requirements are being met. If sufficient evidence is not able to be obtained, then the dependability plan should be modified accordingly.

In a well managed project, the dependability plan and dependability case are fully integrated with overall project management. In such a project, the use of the dependability case does not incur an increase in overall workload, since the cost of constructing the case is recouped by

the saving from avoided miscommunication, avoided reworking caused by late discovery of faults, avoided activities without demonstrable benefits and so forth.

In addition, preparing a dependability case assists the development of a cost-effective dependability plan because evidence sought in support of the argument in the dependability case can suggest activities which will improve the dependability plan. In addition, if an activity in the plan is not part of an argument in the dependability case, it should be reviewed to check that it performs a useful function in the plan. (Note that some activities in the dependability plan are included to support other disciplines such as safety which do not normally form part of the dependability case.)

The dependability plan and dependability case should be reviewed and updated in the event of significant changes to the following:

– customer requirements or expectations;
– environment or interfacing systems;
– conditions of use or design intent;
– design;
– actual performance.

4.3 Progressive assurance of dependability

The dependability case provides an expanding body of evidence which aims to progressively decrease the uncertainty around the achievement of the dependability requirements. However, it is the norm rather than the exception that requirements, environments, etc. change during the system life cycle. Therefore uncertainty might not always decrease. There might be occasions, for example, when a different design option renders a proportion of the evidence obsolete, leading to increased uncertainty. There might also be periods when no evidence is provided, for example during testing prior to the release of test results, when uncertainty remains unchanged. In addition, if new evidence conflicts with the existing evidence, this might increase uncertainty.

Figure 1 illustrates two types of product development: new development and MOTS. The vertical axis represents the level of uncertainty identified at any point in the project. As the quantity of dependability evidence increases, the uncertainty generally reduces and progressive assurance is obtained.

The horizontal axis represents the time into the project, from the start of the concept stage "a", through start of development "b", to the end of the realization stage "c", end of utilization “d”, and "e", possible enhancement, and beyond.

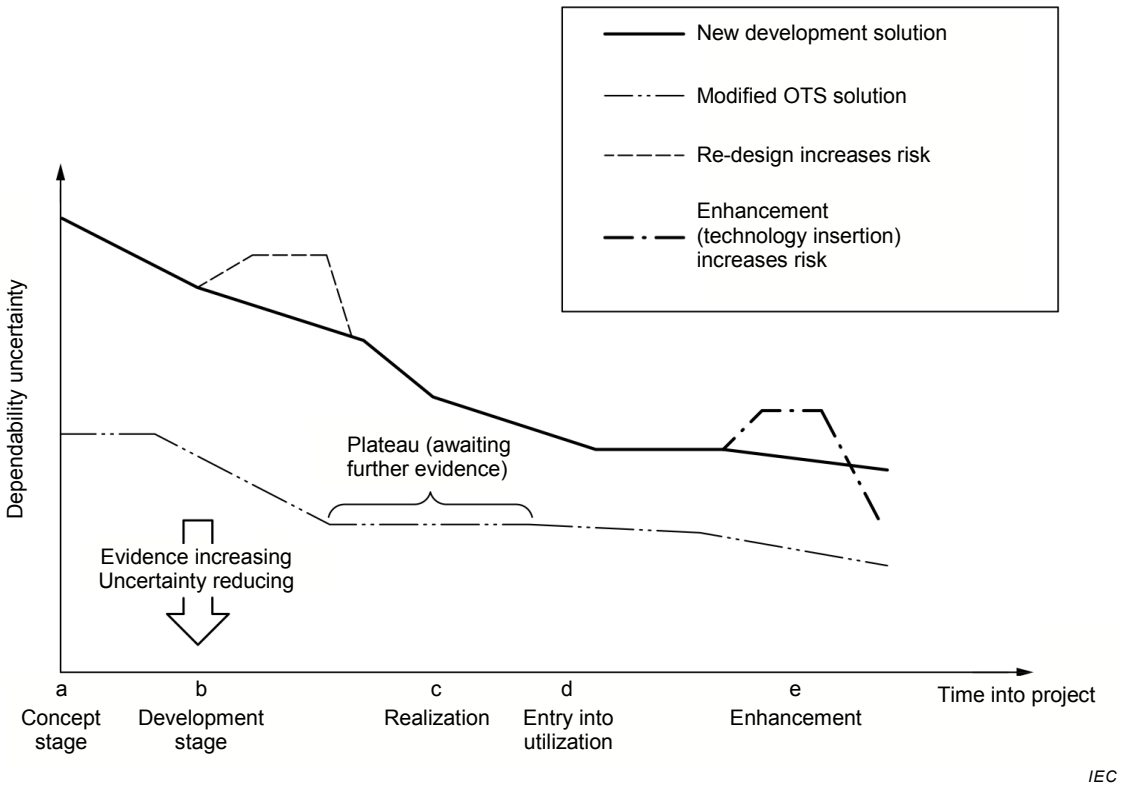


Figure 1 – Illustration of progressive assurance process

At time "a" (start of concept stage) the level of uncertainty is relatively high, but this uncertainty decreases as the project progresses. At time "c", namely at the transition from the realization stage to the utilization stage, the body of evidence is sufficient to assure the dependability to the degree that warrants this transition. The body of evidence (assurance) should continue to build in utilization as successful trials and usage are recorded and the remaining risks can be seen to reduce still further.

Having gone through its own new development period, a MOTS solution is often considered less uncertain than new development as in Figure 1, provided all other things are equal. This is not the case for an OTS solution in new applications or in a new environment and a careful re-assessment is required.

Finally, many changes to uncertainty will be step-changes rather than progressive changes.

5 Principles of the dependability case

5.1 Description of the dependability case

The dependability case starts with an initial statement of dependability requirements. These requirements might include customer's and supplier's internal goals, market strategies, regulatory requirements, etc. as well as requirements explicitly stated by the customer.

The dependability case then makes a top level claim explicitly stating the contention that the system meets the requirements (see 5.2). The dependability case then provides a multi-level structure of claims, sub-claims and connecting sub-arguments that are ultimately based on evidence (see 5.3) and assumptions.

The evidence is presented in the evidence framework (see 5.4) and summarized and referenced in the argument in the dependability case report (see 5.5).

5.2 Making claims in the dependability case

The dependability case uses evidence in order to create an argument for the claims that the dependability requirements have been or will be met.

Figure 2 illustrates the process of building and arguing the claims in the dependability case using the evidence sources.

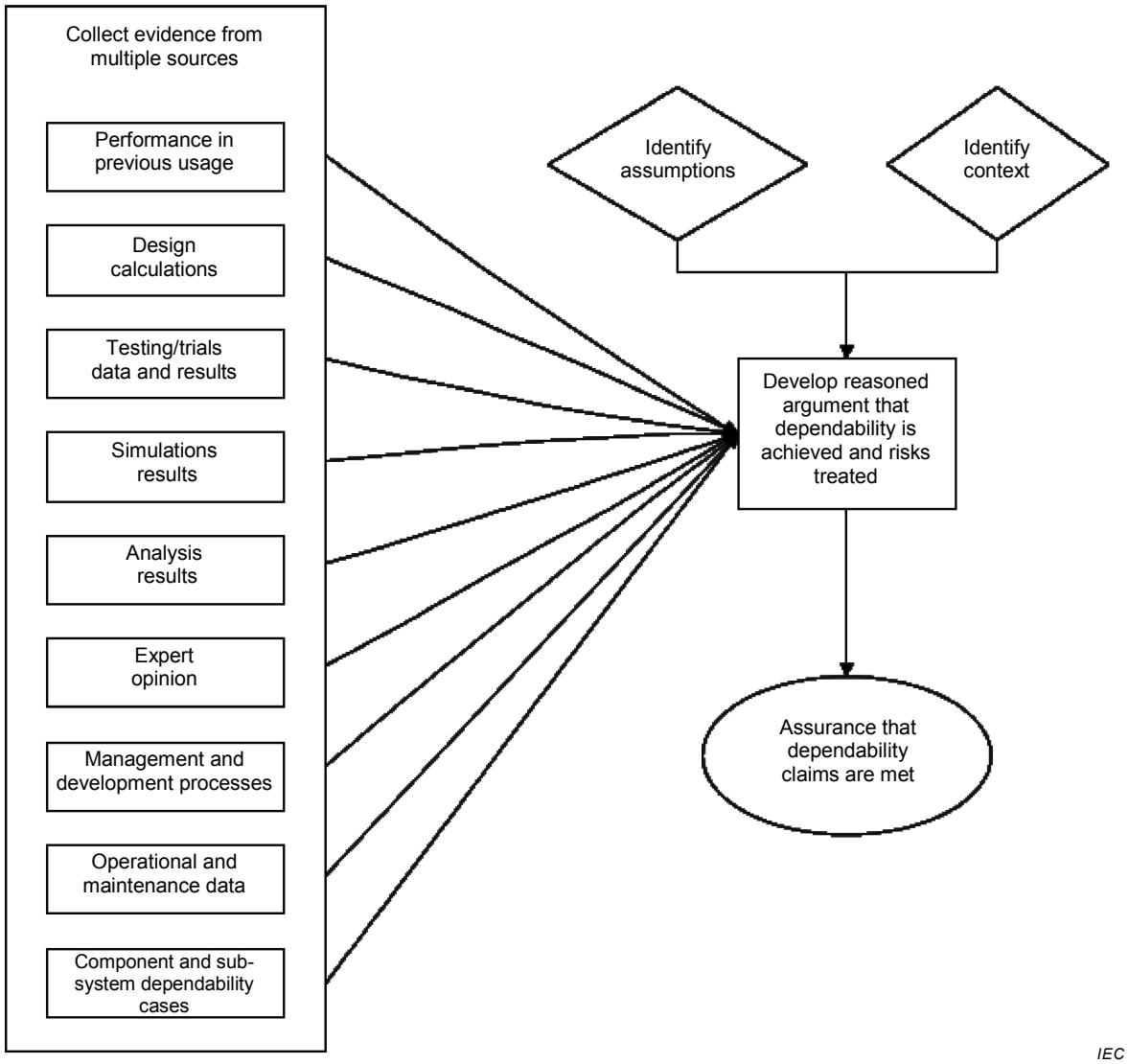


Figure 2 – The development of claims

Any assumptions necessary to make the argument should be identified and explicitly stated, along with the activities planned to validate them. These might include assumptions regarding the conditions of use, the environment in which the system is used or the nature and type of maintenance.

Arguments can fall into one of two categories:

a) arguments that all identified risks to the claim are eliminated or sufficiently treated, supported by evidence of successful treatments and by evidence that risk identification is comprehensive;

b) arguments that there are sufficient grounds for the claim, supported by evidence of truth of each and by evidence of adequacy.

The former requires that consideration is given to all significant sources of risks, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The latter requires that the aspects covered by the evidence are sufficient to provide assurance of the claim.

It is also necessary to identify the context and background for which the argument is made as this identifies the limitations of the dependability case. The context includes the stakeholders who might be interested in the system, the objectives and performance requirements, the system being considered and any proposed limitations on the system's use.

Should any of the assumptions or context change, then the argument and claims in the dependability case will need to be reviewed.

During the implementation of the dependability plan, the key assumptions should be validated, where possible, effectively replacing each with substantiated evidence. Similarly, the contexts in which the argument is made should be validated to match the actual or intended application of the system and the dependability case.

From these sources of evidence and explicitly stated assumptions, a reasoned argument demonstrates how the dependability claims are substantiated. Documents and data relating to all of these make up the dependability case.

5.3 Using evidence in the dependability case

Evidence in the dependability case can be of two sorts. The first is direct evidence that the dependability requirements have been demonstrated. The second is evidence that activities designed to treat the risks that the dependability requirements are not met or demonstrated have been successful.

A wide range of sources of evidence should be used. These can include

a) performance in previous usage/operation,
b) design or other calculations,
c) test and trial data results,
d) simulation results (e.g. FEM or Monte Carlo),
e) results from analysis (e.g. FMECA and FTA) including predictions and modelling,
f) expert opinion, including previously recorded success of the supplier,
g) management and development processes including
   – correct implementation of best practice,
   – the management activities and systems processes followed,
h) operational and maintenance data,
i) dependability cases of components/subsystems provided by their suppliers.

It can also include evidence from activities and tasks carried out for purposes other than the implementation of the dependability plan, such as safety or logistic support analysis.

Before undertaking a dependability activity, its objectives should be fully understood, i.e. how does the activity help achieve dependability, how does it provide evidence for the dependability case, and what are the success criteria for the activity. The success criteria are applied to the records and outputs of the activity to judge if it has achieved its objectives. Evidence that the criteria are met (including the records and outputs) substantiates the claims that the objectives are achieved. Where applicable, the success criteria include that the risks have been adequately treated.

Quantified success criteria are preferred as determining success is simpler and less open to interpretation.

However, quantified success criteria cannot be produced for all activities. In such cases qualitative criteria based on the objectives of the activity should be defined and should include evidence that the activity, as well as the ouput of the activity, are appropriate and correct. For example, the success criteria for modelling are not simply that the predictions and modelling demonstrate compliance with requirements, but that the model itself is an adequate representation of the system, and that all system or system elements (e.g. software) have been included in the modelling. The model should also address the robustness of the design against variations in usage conditions and manufacturing conditions and manufacturing tolerances.

Assurance and evidence does not just result from the outputs of a dependability activity, but also from the timeliness of the activity and any actions which arise. Undertaking the activity at the appropriate time so that it influences the design of the system is very important and activities should be carried out in parallel with the design process. Therefore, the evidence from an analysis activity should include the documentation showing that the activities and actions have been implemented in a timely manner.

5.4 Evidence framework

The evidence framework presents the evidence used to demonstrate the claims and support the argument and is generally presented as a table. The evidence framework captures the current set of compliance and assurance activities (and their success or acceptance criteria) which demonstrate that dependability is achieved and that risks to dependability have been treated.

Figure 3 illustrates the steps to establish and develop the evidence framework. Each dependability case report should base its claims and argument for them on the latest status of the evidence framework.

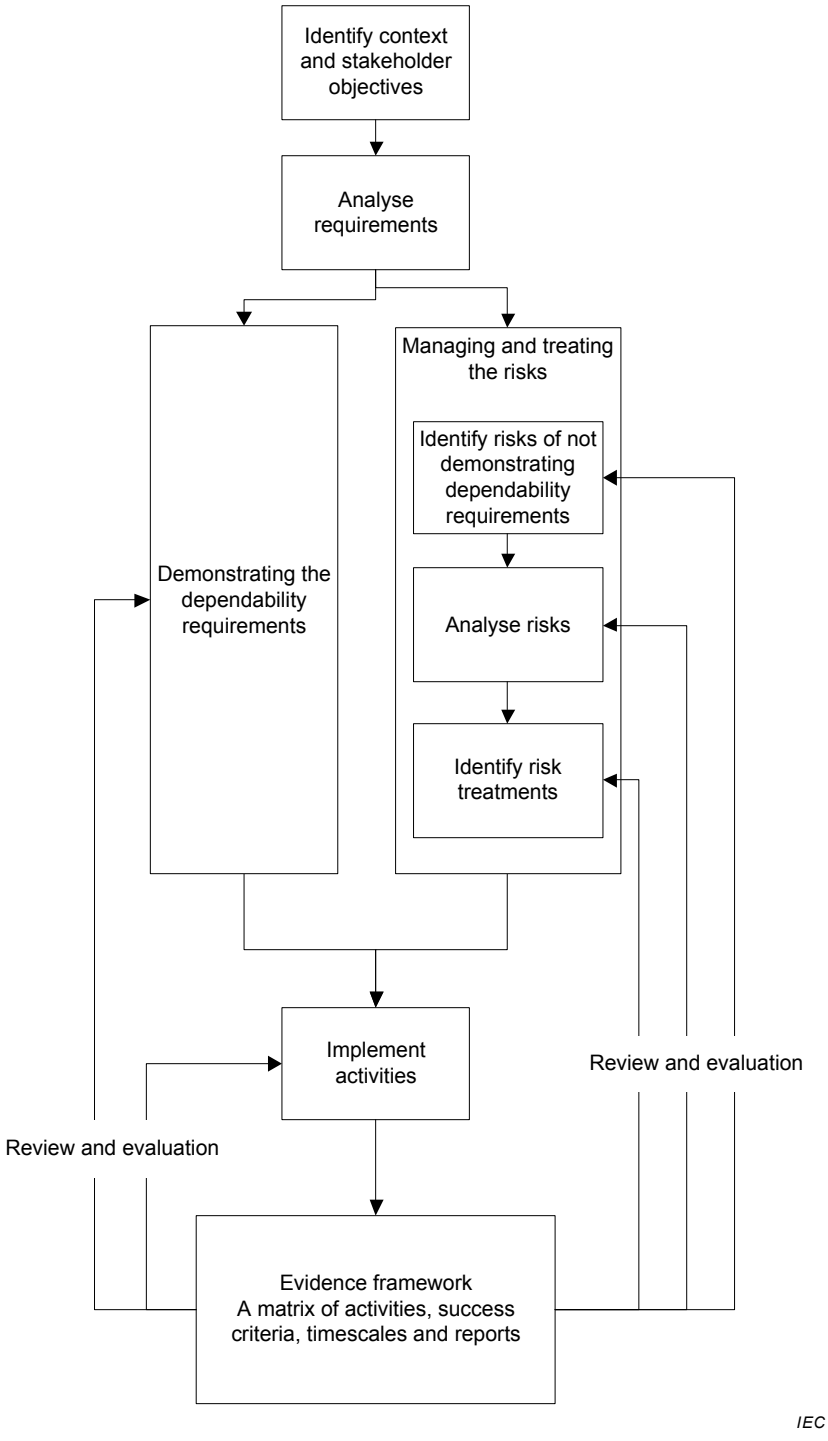


Figure 3 – Establishment and development of the evidence framework

The evidence framework should be tailored to the project. It will vary through the life cycle but should identify or contain

a) the dependability activities, including measurements and tests, which provide evidence for the dependability case,

b) the success or acceptance criteria for the evidence,

c) links to the risks that the activity is intended to treat or the claim which the activity supports (as applicable),

d) the dates/milestones when the activity should be complete and the evidence available,

e) references or links to the evidence actually provided,

f) confirmation of its acceptance (or rejection) (when applicable).

Annex A contains examples of evidence frameworks.

5.5 Dependability case report

In practice, the collation of all documentation into a single document is unmanageable, particularly where there are many and diverse sources of evidence. An acceptable solution is to present periodic updates to the dependability case as dependability case reports. The dependability case is then the body of accumulated dependability case reports which, in turn, refer to source evidence.

Dependability case reports are usually issued at pre-agreed points. They report on the evidence and conclusions drawn from work done so far (referring to papers and data sources where necessary), provide an assessment of overall dependability achievement/progress and a review and evaluation of the dependability activities. At the beginning of each stage, the supplier and customer should agree on the requirements to be satisfied at the end of that stage, i.e. the gate the project must pass before proceeding to the next stage. The agreement may include trade-offs between different competing requirements. The risks arising from this trade-off should be included in the evidence framework. Standards describing processes that could be used to reach robust agreements between customer and supplier are listed in the Bibliography.

When required by a contract, they can be used to provide sufficient detail for stakeholders or the customer to make a decision of whether to proceed from one stage of a project life cycle to the next. Annex B contains a description of the possible contents of a dependability case report.

The dependability case report can be presented as a narrative document but, if a more formal presentation of the argument is required, there are several techniques available which can be used to structure the argument and claims made from the evidence collected. The Bibliography provides informative references to some techniques.

6 Development of the dependability case

6.1 General

This standard primarily describes a project which follows the V-model life cycle where the supplier develops or proposes a system to meet the customer's requirements and the customer manages it according to the changing needs until its retirement.

In projects using other project management processes, such as spiral models or SCRUM models, the requirements are defined as the project progresses and the guidance in this standard should be tailored to each project. However it is still important to agree on the requirements for the next stage and what is required by the end of that stage (e.g. a stable and functional product release).

The dependability case does not belong solely to the customer or supplier but is a joint body of evidence which is developed and added to by different parties at different life cycle stages.

Developing the dependability case enhances communication between the customer and the supplier. For example, a possible cause of failure to meet customer requirements is lack of understanding by the supplier of customer needs. Treating this risk requires the customer and supplier to communicate to reach a common understanding of requirements. Treating this risk early also minimizes costs.

6.2 Preparation of the dependability case

While the dependability case is most effective if started at the concept stage, it may be started at any life cycle stage. This subclause describes the activities which are required at whichever life cycle stage the dependability case is first developed. Subsequent subclauses describe how the dependability case might be developed throughout the project life cycle. For simplicity, it is written in the context of the project starting at the concept stage, where the supplier(s) might develop multiple solutions, one of which is selected by the customer and taken forward through to enhancement and retirement.

The development of the dependability case begins with the customer's activities to determine the dependability requirements and their measurement base. Normally, the way these requirements have to be measured is documented as part of the concept stage of a project. IEC 62347 and IEC 60300-3-4 give guidance on the specification of dependability.

The customer should include the dependability requirements, including availability, reliability, maintainability and supportability requirements, as part of the system specification that will also include performance and usage. Other requirements such as cost and risk profiles may also be specified.

Where necessary, references to other documents or evidence (such as the documents that detail the proposed arrangements for the management of risk, safety, supportability and environment) are also included. The customer should also supply the context for these requirements, from their operating profiles, the role of the project, etc., down to the terminology they employ. Similarly, the customer should clarify all assumptions they made in developing the requirements and expect those which are relevant or appropriate to dependability to be shared with the suppliers.

The customer may present these requirements, together with the context and the assumptions, in an initial dependability case report, with references to any pre-existing evidence, such as dependability performance of similar systems or subsystems. The customer might also identify risks to dependability and how they should be treated by either the supplier or customer. This should include information on how the customer will determine that the risks have been adequately treated.

On receipt of the dependability requirements or initial dependability case report from the customer, the supplier should analyse these dependability requirements and plan the activities to satisfy them. This analysis and planning will involve

a) gaining a full understanding of the requirements,
b) analysing requirements to define system dependability targets,
c) considering any existing evidence,
d) identifying risks (and transferring to the overall project-level risk register) and how they are to be treated.

The requirements that affect system dependability should be analysed to determine their impact at system and subsystem level as the results of these analyses form part of the dependability case. This analysis should include other aspects such as system operation, its environment and the human–machine interfaces, all of which have an impact on system dependability. To gain this understanding, the supplier should be involved in dialogue with the customer to ensure mutual understanding of all aspects. This dialogue results in a definitive statement of the customer’s requirement and all the operational and environmental conditions thereof. This statement gives confidence that the dependability requirements of the customer have been agreed and understood by both the customer and supplier (see 4.2). The customer and supplier should also agree how the risks are to be treated and how the customer will judge that the risks have been adequately treated.

From this, the supplier's dependability design targets and a measurement base are determined. These are design aims, possibly with a margin over the dependability requirement in order to reduce the risk that the requirement will not be met.

The dependability activities lead to an evidence framework and a dependability case. The planning of the dependability activities (to be included in the response to the customer) is based on the work required to demonstrate the achievement of dependability requirements. The objective of planning the activities is to provide confidence to the customer and supplier that the risk of failing to meet or demonstrate the achievement of dependability requirements is minimized, before committing resources.

However, different types of purchase or project can involve different combinations of life cycle stages and, depending upon the contractual arrangements, the dependability case may be started or completed at the end of any stage. For example, if a customer is buying an OTS system, the development might have been completed sometime earlier and the customer may prepare the dependability case that includes only the realization and utilization stages. Alternatively, the OTS system might provide its own dependability case, which includes the concept and development stages, which can be incorporated or referred to by many customers.

However, whichever stage the project begins at, the first dependability case report should include a full assessment of the requirements and the tasks and activities which will be undertaken.

6.3 Concept stage

At the concept stage, the customer should develop an outline set of requirements and may issue an outline dependability case report to the supplier. The customer should also identify risks to be included in the overall project risk register. Where there is a lengthy project, including a significant competitive development stage, then the customer might need to examine the outline requirements to ensure that the proposals from competing suppliers can be assessed for dependability using a common assessment methodology.

It is essential that all the dependability stakeholders are consulted at the concept stage to ensure that their requirements are fully captured. Expert advice and the use of dependability modelling techniques are probably necessary to validate that the requirements are suitable and sufficient.

It is likely that there will be considerable trade-off between different requirements. For this trade-off, the risks of not demonstrating compliance with the requirements may form a key part of the decision-making process, i.e. if compliance with the dependability requirements cannot be demonstrated, this might be a reason for the option's rejection. As part of the concept stage, the supplier or customer may move to a single preferred solution, or this might not occur until the development stage.

The supplier should analyse the requirements and develop one or more solutions. Risks might be identified at this stage that are common to any potential solution and that require specific and timely treatment. These risks might lead to an initial evidence framework that identifies required minimum assurance activities and these activities might, in turn, form part of the contractual requirements or scope of supply. However, in developing these solutions, the supplier may identify different risks to compliance with the dependability requirements for the different solutions. These should also be presented in the initial evidence framework.

The supplier should develop a preliminary set of dependability activities that will demonstrate the satisfaction of the dependability requirements and will treat the risks, based upon the initial evidence framework. This should be presented to the customer in the dependability plan which should outline the design philosophy and principal design features and then identify the differing risks for the proposed designs. In some instances, the risks could be determined using a checklist, but engineering judgement should be a significant input. These risks should

be included with other project risks into the overall project risk management plan. The risks and the plan for their management form part of the dependability case (see IEC 62198).

A dependability case report should be compiled at the end of this stage. It should discuss the development of the plan for providing assurance of dependability and document the justification for the proposed activities as well as outlining the proposed evidence to be collected. The objective of providing the customer with an early dependability case report is to demonstrate to the customer that dependability requirements will be met before resources are committed.

6.4 Development stage

At the development stage, the customer will generally provide a dependability case for a single preferred solution. It is possible that the dependability requirements will be different to those at the concept stage, due to the trade-off between different requirements, which will require the dependability case to be updated.

Through continued analysis of the dependability requirements, the supplier should decide upon a robust design philosophy for the preferred solution. The supplier develops, and places in the evidence framework, the detailed design of the preferred solution, explicit claims that the specific design will meet the requirements and an argument demonstrating how the claims will be substantiated. This should include ensuring that new risks identified while carrying out the activities are fed back to analysis and design at this stage in a timely manner and followed through.

If not completed in the concept stage, or if an update is required, the onus is on the supplier to take the initiative and propose dependability design targets and a measurement base. For example, the customer may specify an availability requirement but the supplier needs separate reliability and maintainability targets to develop the system.

At the development stage, the supplier should update the evidence framework as development progresses and activities are planned and implemented. The dependability case report compiled at the end of this stage should include a partially completed evidence framework consisting of the current and future dependability activities, their success criteria and the project milestone at which the evidence from these activities will be produced in order to be effective.

6.5 Realization stage

The dependability case in the realization stage is primarily concerned with developing and populating the dependability case as activities are completed and evidence becomes available. If the dependability case has been properly managed during the concept and development stages, significant changes would not be expected to the dependability requirements or risks which have previously been identified. However, new risks might be identified or updated treatments proposed as a result of the completed activities and the evidence produced.

The supplier should issue dependability case reports at agreed milestones throughout the realization stage, which should describe how the risks are being treated and provide the customer with increasing confidence that the requirements will be met. The customer's acceptance of the dependability case reports will generally be one of the necessary conditions for interim payments to the supplier.

The customer should study the dependability case reports produced by the supplier. They should review the argument and the nature of evidence provided, including the activities undertaken to treat risks, and monitor the progressive achievement of dependability.

However if the customer finds the supplier's progress unsatisfactory, this should be managed by the normal project procedures. The customer should also consider whether there are any

additional risks relevant to their particular context and update the dependability case accordingly.

At the end of the realization stage, if the customer is satisfied with the dependability case, this will indicate that the system is ready to be utilized.

6.6 Utilization stage

Once the system enters the utilization stage it is important that the dependability of the system be monitored and sustained. The dependability case should be updated to reflect the consequences of issues such as differences in the maintenance regime from that assumed, the way users interact with the system in practice or more detailed understanding of the operating environment.

The manager of the system when it is in use (whether supplier or customer) should review the argument, assumptions and contextual information on which the dependability case was based and check that all are still valid. This review may be held periodically or may be triggered by pre-defined events. The manager should review the register of risks and add new risks that could arise in use that may not have been considered by the supplier. Evidence from operational usage and/or testing and maintenance should be added to the dependability case. It is possible that more than one organization could use the system in different contexts and develop the dependability cases independently.

If the measured or achieved dependability differs significantly from that which was predicted, the possible reasons for this difference should be identified and corrective action undertaken to restore the levels of dependability identified in the requirement(s). If this is not feasible or justifiable, e.g. due to cost, the customer and supplier could agree to revise the requirements. If the change in requirements is significant, the customer and original supplier may then return to the concept stage to agree on revised requirements. Alternatively, the customer may initiate the enhancement stage to adapt the system to the changes. The customer and/or supplier should consider whether there are any additional risks relevant to the changes and update the dependability case accordingly.

At the end of the utilization stage the expectation is that the dependability case and evidence framework demonstrate that the dependability requirements have been met.

6.7 Enhancement stage

It is often the case that the system requires enhancement during the utilization stage. This might be by the customer, in which case the customer should develop the dependability case. Alternatively, it might involve contract action on a supplier. If this happens, the supplier should treat the enhancement as a new project, effectively restarting the dependability case from the concept or development stages, but using the previous dependability case as a baseline. The customer's monitoring actions (see 6.5) and the results should also be captured in the dependability case and the dependability case managed accordingly.

6.8 Retirement stage

For some systems, the retirement stage may also require the dependability case to be updated if, for example, there are specific requirements for disposal and dismantling of the system. The same processes for managing the dependability case should be followed as for previous project stages.

It is also at this stage that the achieved dependability of the system can be measured. It is good practice to review the claims and evidence contained within the dependability case to determine whether these have been achieved. This may also provide lessons learnt for future projects.

The evidence frameworks and the dependability cases accumulated across successful projects may serve as a library of reusable elements for the organization so should be stored within the organization's knowledge management system.

7 Assessing the adequacy of evidence

The robustness of the dependability case in making dependability claims is dependent upon the adequacy of the evidence used. The customer should therefore review not only the argument and claims made in the dependability case but also consider the adequacy of the evidence upon which it is based.

The adequacy of evidence is primarily a function of its practical impact on the demonstration of dependability, the reduction of uncertainty and the treatment of the risks. Whilst it is not necessary to assess the adequacy of specific, detailed dependability activities in their own right, the visibility, traceability and quality of evidence produced are crucial factors. It is therefore necessary to confirm that the evidence is generated, managed, validated and used within an effective dependability management system.

All relevant, available information on the dependability achievements and lessons learnt from a particular design should be used to provide assurance of dependability within the dependability case. It is not acceptable to ignore evidence which counters the argument being made.

The principal criteria for assessing the adequacy of evidence are as follows:

a) the evidence as a whole is clearly derived from a properly planned dependability programme;
b) the links between any specific item of evidence, a dependability requirement, an activity in the dependability plan and identified risks are clear;
c) the evidence is derived from dependability activities carried out by competent people with adequate resources;
d) the status of each item of evidence, in terms of its relevance, completeness, accuracy and how it has been used to influence the system and reduce risk, can be readily identified in the evidence framework.

In order to assess the adequacy of evidence, it is important to seek traceable methods/techniques, assumptions and detailed results. Consequently, an open, honest dialogue between customer and supplier is important. Judgement is required to assess the evidence presented, including its visibility, traceability and quality in accordance with the criteria listed in this clause. Annex C provides a checklist of generic points which are not prescriptive, but which provide additional guidance on assessing the adequacy of evidence in appropriate circumstances.

Annex A
(informative)

Evidence framework

A.1 General

The evidence framework is defined in 5.4. Example column headings and contents are described as follows:

Column no.	Heading	Contents
1	Life cycle stage	Relevant stage in the project life cycle
2	Reference	Reference to the claim Cross-referenced to the project requirements specification or risk register
3	Claim description	Description of the claim supported Coordinated with the project requirements specification or risk register
4	Subclaim	A description of the subclaim Coordinated with the project requirements specification or risk register
5	Evidence required	Evidence needed to support the demonstration of the claim or treat the risks of not meeting the requirements (information, not deliverable reports)
6	Dependability activity	Activity required to generate the necessary evidence (usually a combination of traditional dependability and other activities, i.e. not necessarily an individual dependability activity or technique)
Acceptance criteria		
7	Evidence	Deliverable document/contents
8	Time due	Time the evidence is due in order to be effective
Acceptance status		
9	Evidence	References to the latest evidence, including issue no. and date delivered

Column no.	Heading	Contents
10	Approval status	Whether approved or not. If rejected, include reasons and corrective action. If accepted, signature of approving authority and date of acceptance

Two examples of partial evidence frameworks are illustrated in Table A.1 and Table A.2. Each covers examples of claims and risks at various stages in the project life cycle, assuming the system involves substantial development activity and at different levels of detail.

While each row of the table is complete, neither example evidence framework examines all the expected claims or risks to be treated.

Therefore, when creating an evidence framework, the system should be considered in its own right and it is expected that the evidence framework will be substantially longer than the examples given here. However, the layout of the table may be used as a template.

A.2 Abbreviations used only in this annex

BIT	Built-in test
DRACAS	Data recording and corrective action system
HUMS	Health and usage monitoring system
ITEAP	Integrated test, evaluation and acceptance plan
PRAT	Production reliability acceptance test
OMD	Operational and maintenance demonstration
SMART	Specific, measurable, achievable, realistic, time-bound
TDP	Technology development plan

Table A.1 – Evidence framework for system “X”

“Evidence framework for system "X"						Issue:	Date:	Signature:	
Life cycle stage	**Ref**	**Claim**	**Subclaim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due/required**	**Ref, issue, date**	**Approval status**
Tender (for development)		The system achieves its specified reliability: 99,9 % over a 24 h duty cycle (requirement ref AAA)	Intrinsic reliability of solution components meets the requirements	Demonstration of intrinsic reliability by parts count prediction using part failure rates	Parts count reliability prediction using in-service experience of similar parts, defaulting to industry standard data sources, e.g. data from component or OTS suppliers	Parts count reliability prediction independently reviewed.	2 weeks prior to preliminary design review, update prior to critical design review	Report aa issue 01 dated zzz	Accepted
			Failure modes and criticality of solution(s) are fully understood and treated	Risk that critical failure modes and failure rates for single and double faults are missed so reliability does not meet the target (Risk ref BBB)	FMECA: this information will be provided by the design FMECA, conducted as design practice	FMECA independently reviewed	As parts count reliability prediction	Report bb Issue 02 dated yyy	Rejected. Critical failure modes not all managed. Redesign being undertaken
					Development tests and DRACAS a) to support previous assumptions on failure modes and failure rates; b) to trigger further development and testing of unsatisfactory items and, c) to initiate selection of alternative parts	Test results demonstrate requirements	2 weeks prior to critical design review	Not yet due	

"Evidence framework for system "X"						Issue:	Date:	Signature:	
Life cycle stage	**Ref**	**Claim**	**Subclaim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due/required**	**Ref, issue, date**	**Approval status**
Tender (for development) (cont.)			Solution performs as predicted in use	Demonstration of dependability during utilization	Develop proposals for monitoring and reporting of operational defects and maintenance performance through defect reporting via analysis of DRACAS database	Draft operational and maintenance demonstration plan available including acceptance criteria with regard to the 24 h duty cycle requirement	2 weeks prior to final design review.	Not yet due	
						Test results demonstrate requirements	1 year after entry into use	Not yet due	
		System BIT requirements are achieved (requirement ref CCC)	Testability design strategy tests all required functions	Risk that testability requirements are not verified resulting in either poor performance and/or customer not accepting item (risk ref DDD)	Review BIT design strategy in the light of the functional hierarchy developed in the FMECA (see Claim 1.1.1)	Internal document providing results of the review and showing that the testability design strategy is consistent with the functional hierarchy and the BIT requirements for: Start-up. Continuous checks. Diagnostics. Location	6 weeks prior to critical design review	Not yet due	
			Testability identifies critical failure modes	Risk that testability design strategy misses critical functions resulting in requirement not being achieved (risk ref EEE)	Extension of the FMECA to provide an evaluation of BIT coverage	BIT evaluation report shows that the system testability is consistent with BIT requirements for; Start-up. Continuous checks. Diagnostics. Location	6 weeks prior to final design review	Not yet due	

"Evidence framework for system "X"						Issue:	Date:	Signature:	
Life cycle stage	**Ref**	**Claim**	**Subclaim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due/required**	**Ref, issue, date**	**Approval status**
Tender (for development) (cont.)		The integration of latest technology and communications equipment into the design does not compromise the dependability of the complete system (requirement ref FFF)	Installation of new equipment does not restrict maintenance access to remainder of system	Risk that maintenance access is restricted is treated by technology demonstration plan (TDP) including dependability assessments (risk ref GGG)	Dependability predictions conducted to support the TDP	TDP dependability prediction report demonstrates that design is not compromised by new technology	6 weeks prior to critical design review	Not yet due	
			New technology systems do not produce excessive heat which impacts on performance of existing system	Risk that excessive heat is produced is treated by Technology demonstration plan (TDP) including assessment of heat loads and impact on existing system (risk ref HHH)	Dependability predictions conducted to support the TDP	TDP dependability prediction report demonstrates that design is not compromised by new technology	6 weeks prior to critical design review	Not yet due	
Development		Subsystem z possesses durability for required life (requirement III)	Wear out mechanisms are fully understood and managed	Risk that wear out is not understood by evaluation of expected life and determination of any changes necessary to achieve the requirement (risk ref JJJ)	Review of life data on similar items and environmental evaluation /stress calculations, to determine ageing factors and critical components	Stress calculations, justification of (any) necessary design changes and accelerated life test plan	3 months after contract award	Report dd issue 01 dated www	Accepted
					Accelerated life testing using the highly accelerated life test methodology	Accelerated life test report providing assurance for the final design meets the life requirement	6 months after receipt of test model(s)	Not yet due	

"Evidence framework for system "X"						Issue:	Date:	Signature:	
Life cycle stage	**Ref**	**Claim**	**Subclaim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due/required**	**Ref, issue, date**	**Approval status**
Realization		The chassis suffers no reduction in life during system assembly (as assembly activities include loading that is very different from when system is complete) (requirement ref KKK)	Stresses/fatigue during assembly do not reduce chassis life	Risk of excessive stress / fatigue is treated by analysis of loads on the chassis when suspended; determination of changes to the chassis design and/or the manufacturing fixture(s) to ensure that the expected life of the chassis is not compromised. (risk ref LLL)	Evaluation of the load case	Report, including analysis and calculation records, showing acceptable stress margins. The report will highlight (any) areas of potential overstress and justify changes, if needed, to ensure adequate margins	3 months prior to completion of realization stage	Not yet due	
				Demonstration of manufacturing processes	Production reliability acceptance test (PRAT)	1) PRAT test plan. 2) PRAT test results assuring the integrity of the chassis for manufacture	1) PRAT plan required before start of production. 2) PRAT test results following completion of PRAT	Not yet due	
					Final quality inspection of deliverables	Quality inspection records demonstrating adequate quality	During production	Not yet due	

Table A.2 – Evidence framework for system Y

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
Concept		Reliability of item satisfies customer needs	Dependability requirements are correctly identified by customer and/or are complete	Risk that critical dependability system attributes have not been identified leading to missed requirements	Capability gap analysis. Operational analysis	Requirements document has been signed off by key stakeholders., agreeing completeness and appropriateness	Early in the concept stage, prior to initial business case submission	Report ee Issue 03 dated vvv	Accepted
			Dependability aspects are addressed within systems engineering, so that impact of dependability on capability is fully understood. Dependability requirements are SMART	Risk that sub-claim is not met is treated by: 1) development of utilization stage availability targets. 2) Adequate system numbers. 3) Initial dependability targets linked to utilization stage availability. 4) Assessment of the impact of dependability on operational effectiveness showing no adverse effects	Needs and numbers studies (with dependability input). Availability modelling	Document includes operation availability targets within the sustainability section and first cut dependability targets			

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
Concept (cont.)		Customer has properly managed dependability to achieve good dependability characteristics. Adequate and effective resources are in place	Downstream costs are optimized/ minimized due to effective dependability management	Risk that customer fails to realize the link between dependability and cost of ownership resulting in greater down stream costs	Dependability input into investment decision-making and life cycle cost modelling including the cost(including time) of delivering the required level of dependability	Plans clearly align with outturn of previous projects. Realistic estimates of funding and equipment numbers have been prepared and included in project execution plan by ensuring availability and reliability are included in these early studies as cost drivers. Team in place	Early in the concept stage, prior to initial business case submission	Project execution plan ref ff Issue 02 dated uuu	Accepted
			Programme meets timescale requirements of sponsor	Risk that the customer fails to consider the impact of the requirements on the need for complex or novel technology resulting in programme delays	Assessment of the technology risks including feasibility studies examining the maturity of the technology likely to be used in the solution options	1) Reports showing pull through from research. Formulation of technology demonstrator plans. 2) Input from industry through partnering teams		1) Report gg Issue 01 dated ttt .Report hh Issue 01 dated sss.2) Team mobilized	Report gg accepted. Report hh rejected and being rewritten
			Timescale risks are properly managed and minimized	Risk that customer fails to understand the key timescale risks resulting in low reliability and/or programme delays	Assessment of the timescale risks by Comparison with similar, related or historical projects	Analyses to show the timescales have been planned in accordance with the technology and technical risks. Accepted and agreed schedule		Schedule ii Issue 07 dated rrr	Accepted

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
Concept (cont.)			Assurance of dependability by supplier meets standards	Risk that customer fails to outline the strategy for assurance resulting in adequate evidence not being produced and customer dissatisfaction	An agreed dependability plan	A draft dependability plan outlining the elements, work and the strategy to treat the key risks. Statements of work for concept stage studies in initial business case. Plan includes customer's acceptance criteria	Early in the concept stage, prior to initial business case submission	Report jj draft C dated qqq	Accepted
Tender (for development)		Dependability supporting evidence is adequate and correct and meets the customer needs/expectation	Customer and supplier have communicated and agreed requirements and objectives	Risk that supplier does not understand customer's requirements leading to dependability supporting evidence being developed in an adhoc manner and failing to address the customer needs/expectation	Reliability predictions based on similar equipment failure rates, and any factors applied due to differences in duty cycle, usage, complexity, etc. leading to dependability requirements	Clear dependability requirements with the requisite evidence contained in the dependability case issued to the supplier.	Early in the development stage, prior to final business case submission	Not yet due	
					Details of utilization stage analysis and operational availability studies	Initial risk register			
Tender (for development) (cont.)		Customer selects the optimal solution from a dependability perspective so that dependability goals are	Selection mechanism includes dependability and has been rigorously and effectively	Risk that selection mechanism fails to rigorously address dependability so that dependability	Reliability estimates of concept options. Assessment studies allowing dependability estimates to be	Option selection reports showing evidence that the dependability has been factored into the selection process	In the development stage, prior to final business case submission	Not yet due	

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
		achieved	used	is not achieved	input along with other attributes into a structured option selection system				
Tender (for development) (cont.)				Risk that inadequate weighting is given to dependability in dependability assessment method so that other attributes are given undue weighting over dependability	Draft dependability assessment questions for tender marking scheme, ensuring dependability is given equal weighting to performance, time and cost	Final scores from the bid assessment, plus key risks and dependability achievement milestones necessary to contract for the production of dependability evidence are contained within the dependability case	In the development stage, prior to final business case submission		
				Risk that the technological risks associated with each option are not adequately assessed so that requirements are not met	Assessment of likely software complexity through measurements of the size and complexity of the software	Option selection reports include assessment of software dependability through life	In the development stage, prior to final business case submission	Not yet due	
					Project dependability design guidelines and definition of how these guidelines are to be contracted against	Stakeholder acceptance for the project dependability design guidelines has been obtained	In the development stage, prior to final business case submission	Not yet due	
Development		Supplier fully understands the intent of the	Supplier and customer have communicated	Risk that the supplier has not formally	Analysis of duty cycle, loads, temperature	Supplier's dependability case report demonstrates that the	Provided with the tender or early in the		

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
		requirements so that objectives are aligned with customer	and agreed the intent of the requirements, in particular with respect to the environmental constraints	addressed the impact of environmental constraints on dependability so that requirements are not met	levels, vibration levels. Analysis of the operational environment and required modes of operation Analysis of damage accumulation effects, dust, dirt ingress, moisture, etc.	environmental factors and duty cycle loads have been understood and will influence the design	realization stage		
		Supplier has recognized and treated the risks associated with dependability so that dependability requirements are met	Adequate risk management has taken place and has included dependability with project risks	Risk that supplier fails to involve dependability staff with formal risk identification resulting in risks not being identified and treated.	Identification of risks associated with dependability. Analysis of the strength of design of critical components against duty cycle loads	Customer review of supplier risk matrix supported by dependability case reports showing: - modelling using the measured inputs (loads), to ensure that the strength of design of mission critical sub-systems and components is adequate to meet the needs of the mission, and have the durability to continue to function for the design life of the equipment; - a structured analysis of potential failure modes to ensure that all	Early in the design process to influence the design of prototype equipment	Not yet due	
				Risk that risk registers are not integrated leading to misalignment between dependability and project risks	Predictions and modelling to identify critical systems.				
Development (cont.)					Analysis of interface and integration issues				

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	Ref.	Claim	Sub-claim	Evidence required	Dependability activity	Success/acceptance criteria		Acceptance status	
						Evidence	Time due	Ref, Issue, date:	Approval status
						interface and integration issues are addressed and are not overlooked as causes of unreliability; - reliability modelling, predictions and allocations to determine criticality			
		OTS components perform as expected during development stage	Suitable OTS components used within the design	Demonstration of dependability predictions supported by in-service data for OTS sub-systems	Assessment studies where dependability estimates for OTS sub-systems consider existing data and the impact of differences between the new application and that of applicable to the source data	Independently reviewed report.	Provided with the tender or early in the development stage	Not yet due	
						Option selection reports include realistic predictions for OTS sub-systems dependability			
		Testing is effective as test results can be properly sentenced	Design makes use of automated usage and fault reporting to record system condition and usage	Risk that events cannot be sentenced during testing, as all input parameters are not known, and hence dependability cannot be measured	HUMS to be implemented effectively and efficiently as part of the design process	Maintainability analysis report identifying functions covered by HUMS	Provided with the tender or early in the development stage	Not yet due	

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	Ref.	Claim	Sub-claim	Evidence required	Dependability activity	Success/acceptance criteria		Acceptance status	
						Evidence	Time due	Ref, Issue, date:	Approval status
Development (cont.)		The system achieves required dependability levels after the transition from development to utilization	The transition from development to utilization is properly managed and the required activities are undertaken	Risk that supplier expects that dependability issues will be addressed by the customer in utilization resulting in poor dependability and customer dissatisfaction	Identification of the risks and the planned dependability activities to treat those risks, along with the technical capability, resources and controls/success criteria to ensure it will happen	Supplier's dependability plan including: – clear dependability management and organizational structure; – systematic plan of activities for satisfying the dependability requirements set against the identified risks; – dependability activities with clear objectives and success criteria; – planned dependability activities in time to influence design; – dependability target allocations to subcontractors; – subcontractors' dependability plans and case; – a clear test and evaluation plan; – planned dependability milestones for dependability achievement with periodic reviews	During proposals for project and during early development stage	Not yet due	
Development (continued)		Supplier carries out adequate	Test and evaluation	Demonstration of dependability by	Execute, monitor and review	Customer's acceptance of supplier's	During development	Not yet due	

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
		testing to provide sufficient evidence to demonstrate requirements to the satisfaction of the customer	criteria have been formally agreed between the supplier and the customer	design and test and evaluation data which provides engineering and statistical confidence that the pre-production prototype design has met the dependability requirements	dependability plan activities, amending where appropriate	dependability case reports showing: – design changes resulting from the outputs of design studies (stress analysis, FMECAs, etc.); Detailed and effective DRACAS; – component test results; – sub-system test results; – other test results; – reliability growth test results; – reliability demonstration trials; – operational and maintenance trial results; – performance trial results; – information on design review action; – field data from other users	prior to system acceptance and realization		
Development (cont.)		Reliability of OTS software packages is not affected when	The OTS interfaces are compatible with the	Demonstration that integration testing within the software	DRACAS report from the testing and development	DRACAS report shows evidence of: – design modifications leading to satisfactory	During development prior to system acceptance	Not yet due	

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
		integrated into the system	system software architecture	integration laboratory does not affect dependability results. Includes test analyse and fix process reported by formal DRACAS	activities	reliability growth; – input to dependability prediction reports to cover likely software failure rates cycles	and realization stage		
Realization		The system achieves required dependability levels after the transition from development to utilization	Supplier has accounted for and managed the scale of change between prototype and production system	Risk that the transition from development to utilization is badly managed by the supplier and activities are not undertaken due to lack of time resulting in poor initial dependability	Evidence that lessons learned from pre production prototype builds have influenced the production process	Supplier's dependability case reports showing:- production confirmatory/qualification trials results;- production reliability acceptance testing (PRAT) first batch results;- evidence of changes in production and quality procedures to capture defects;- capability indicators from Six Sigma processes	Preceding and during first off realization stage	Not yet due	
					Sufficient test and evaluation data to provide engineering and statistical confidence that the production build standard will meet the dependability requirements and show the reliability has not been degraded by the production process				
Realization (continued)					Mature production and quality processes alongside				

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	Ref.	Claim	Sub-claim	Evidence required	Dependability activity	Success/acceptance criteria		Acceptance status	
						Evidence	Time due	Ref, Issue, date:	Approval status
					pre-production prototype design				
					Procedures for the investigation and rectification of faults, failures and defects				
		Produced items are of acceptable quality.	Supplier has mature production facility and processes	Demonstration of consistent quality of manufacture (PRAT test plan)		PRAT batch test results.	At agreed points during realization stage	Not yet due	
			Supplier carries out suitable and sufficient monitoring	Demonstration of the implementation of effective quality procedures		Quality inspection records			
		OTS components perform as expected during realization	Assembly information for OTS equipment is suitable for application	Demonstration of consistent quality of assembly/ integration of OTS components through PRAT test plan		PRAT batch test results. Quality inspection records	At agreed points during realization stage	Not yet due	
				Demonstration of the implementation of effective quality procedures for assembly and integration					
Utilization		Change in use, environment and support is identified and well managed	Customer has specified system support requirements	Risk that dependability is degraded due to inadequate consideration of change in use,	Equipment usage and failure data along with the appropriate analysis to	Operational and maintenance demonstration (OMD) trial results. OMD dependability study results.	At the start and throughout utilization stage	Not yet due	

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
				support and environment	provide reliability estimates and failure trends. Identification of systematic failure modes and the introduction of modifications through post design services Data on repair costs and resources	OMD data collection and analysis			
Utilization/ retirement		Lessons are learnt from the project to prevent issues on future projects	System ownership and reporting responsibilities are defined by the customer	Risk that lessons learnt are not passed to future projects as they are not captured or disseminated by the customer resulting in problems repeating themselves	Full dossier of all elements of dependability work from concept through to utilization or retirement from regular lessons learnt activities	Early studies results.	On-going through to utilization and retirement	Not yet due	
			Customer's team is only demobilized once assurance and lessons learnt have been completed		Collation of all requirements documents, dependability data and reports into a corporate data repository	Mature dependability requirements			
Utilization/ retirement (cont.)					Production of a final lessons learnt report Providing insight into effective-ness of the plan	Extracts from through life management plan			

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	Ref.	Claim	Sub-claim	Evidence required	Dependability activity	Success/acceptance criteria		Acceptance status	
						Evidence	Time due	Ref, Issue, date:	Approval status
					and the final dependability estimates achieved				
						Outputs from dependability meetings (dependability plan, etc.).			
						ITEAP and acceptance reports			
						Fully populated dependability case with all dependability evidence reports (including operational and maintenance usage)			
						Analysis of lessons learned			

Annex B
(informative)

General requirements for the dependability case report

B.1 General

This annex provides the headings and describes the content for sections within the dependability case report. It is not envisaged that this structure will be suitable for every project, but it is intended to provide guidance on the information that should be contained within the reports.

The dependability case report provides dependability evidence at a specific agreed milestone within the life cycle. The reports present an argument based on claims, which in turn is based on evidence and assumptions that the system will satisfy the dependability requirements. The report is not expected to contain all the evidence produced up to that milestone, but to summarize and act as a "signpost", indicating where the detailed evidence can be found.

This standard refers to dependability, which might be taken to imply that documentary evidence for reliability and maintainability will be summarized in a single report. If the evidence framework requires separate reports, or the customer or supplier considers that having separate reports presents a clearer picture, or provide a more focused approach, separate reliability and maintainability case reports are considered perfectly acceptable.

Where appropriate, to improve readability and the transfer of information, dependability case reports associated with a given project should attempt to adopt a common format.

B.2 Elements required for the dependability case report

Each dependability case report should list and cross reference the requirements in the evidence framework, against which the evidence shall be judged, and be traceable to the original customer's requirements.

The dependability case report should also outline the background, purpose and scope of the report detailing, for example:

a) an outline of the circumstances which led to the need for, and development of, the dependability case report;
b) the purpose of the dependability case report, i.e. why and for whom it has been produced;
c) the scope and boundary of the dependability case report;
d) what the report covers (and does not cover);
e) boundaries of responsibility with respect to managerial control and other stakeholders;
f) relationship with other reports, if applicable;
g) applicability and compliance with relevant regulations and standards.

B.3 Context and assumptions

B.3.1 Stakeholders

This clause describes the stakeholders interested in the system, their expectations and any requirements which are derived from them.

B.3.2 System description

The system description should contain the following items:

a) Physical description – this should briefly describe the system's physical or functional characteristics.

b) System boundary – this should describe the system's physical or functional boundary. Block diagrams can provide a good method of illustrating the boundary of the system considered in the dependability case (see IEC 61078).

c) Operation – this should describe the system's primary role or function and any secondary roles. It should include its typical anticipated duty cycle.

d) Environment – this should describe the system's operating environments.

e) Interfaces with other equipment/systems – this should define equipment associated with the inputs, outputs and services to the subject system. Where appropriate, it should also describe such equipment physically near to the installed system.

f) Users and required human machine interfaces – this should describe the people who will use the system and the interfaces they will have with the system.

g) Build standard/software version – this should relate to a specific build standard of the system, including software version(s) where appropriate.

h) Configuration control – to ensure the report reflects the latest build standard/version, the description should indicate where the latest build standard/version is defined, for example, the master record index.

i) Personnel skill levels and training – the skill level and the training required to operate and maintain the system should be described.

j) Maintenance policy – this should describe the support regimes for each of the system's role or anticipated duty cycle profiles.

B.3.3 Dependability requirements

This should reflect the customer's requirements and the supplier's understanding of those requirements and how they are to be measured. The requirements should be considered in their widest context in that they should include the environment and usage requirements, as well as the explicitly defined dependability requirements. The supplier should describe how the requirements have been interpreted for the proposed design solution and developed into project target dependability.

B.3.4 Limitations on use

This section should define the boundaries on system use or the context in which the arguments are made which, if exceeded, mean that the dependability claims might not be valid. These limitations include the system's operating envelope, the environment and important maintenance activities.

B.3.5 Assumptions

All assumptions should be explicitly identified, either in the dependability case report or in a separate assumptions register. Where possible, activities to validate the assumptions should be identified and included in the evidence framework.

B.4 Risks

Through analysis of the dependability requirements, the supplier should identify the risks associated with the system not satisfying the dependability requirements, and how these risks will be, or have been, treated during the project. This information would normally be found in the evidence framework.

B.5 Dependability plan

The supplier should determine how they intend to meet and demonstrate the requirements and provide the necessary assurance. This section justifies the activities in the supplier's dependability plan and identifies the success criteria for these activities.

B.6 The evidence framework

This section should provide a complete overview of the evidence, whether during the development and realization stages or during system utilization. It should also show when and by whom dependability case reports are to be issued. Specific entries in the evidence framework can be selected by the customer and might be matched to payment milestones for control purposes.

B.7 Body of evidence

This should index the existing evidence. See 5.3 for examples of the types of evidence which might be included. Every item of evidence should be cross-referenced to the evidence framework and to the claims it demonstrates or the risks which it treats.

The body of evidence should also trace the history of reviews and updates of the dependability design philosophy, targets and plan, which keep these in line with the changing status of the original risks, as well as any new/emerging risks. The body of evidence should distinguish between the factual evidence and the arguments or inference drawn from the facts.

B.8 Review of evidence to date

This section should provide a balanced review of the body of evidence in terms of its completeness, timeliness and acceptability with regard to the criteria contained in the evidence framework.

B.9 Dependability claims and argument

This section contains the argument which supports the claims that the system satisfies each of the dependability requirements. This section should provide the reasoning why each of the requirements will be, or is being, met in utilization, based on the context, evidence and any assumptions.

All assumptions should be listed explicitly or an assumptions list referenced. At the start of the utilization stage, any remaining significant assumptions should be explicitly highlighted, along with any limitations on use which these may cause.

B.10 Conclusions and recommendations

This section should contain a diary of the conclusions drawn from the dependability evidence accumulated to date, including whether the system is likely to satisfy its dependability requirements. This includes referring back to the conclusions of the previous issues of the dependability case report and describing how the arguments have changed.

In interim issues, it should recommend whether the project should proceed to its next milestone, or what further work is required to enable the project to progress. In addition, it should recommend what activities should be conducted in the future in order to generate the necessary assurance that the dependability requirements will be satisfied.

The status of the dependability assumptions, evidence, argument, claims and residual risks should be summarized and discussed. Conclusions should be drawn with regard to the status of the progressive assurance and the activities necessary to treat the residual risks.

The recommendations should be based on current shortfalls in the evidence available and should propose changes, as appropriate, to the dependability design philosophy, targets and activities in order to maximize the progress towards providing assurance that the system satisfies each of the dependability requirements.

Annex C
(informative)

Checklist of points for assessing the adequacy of evidence

This annex provides a checklist, which should be considered as a prompt to initiate action where the checklist points have relevance and does not imply a "Yes" and "No" answer. Judgement is required to evaluate the evidence presented. The checklist should not be considered as being prescriptive or exhaustive: it is generic and provides guidance to supplement the general guidance provided in Clause 7 of this standard.

Checklist:

1) Are the objectives of the activity clearly defined?
2) Has the activity been undertaken in a systematic manner and is it complete?
3) Has the activity been undertaken at a time that allows influence on the design?
4) Does the activity properly reflect the usage and environment of the system and has this been documented?
5) Has the activity been undertaken to reflect the physical and functional boundaries of the system?
6) Are any assumptions recorded (e.g. inputs from other systems or services), and are they realistic and reasonable?
7) Is justification given for the activity method/technique used, and is it reasonable?
8) Who was consulted during the activity (e.g. user, maintainer, designer)? Was this level of consultation reasonable?
9) Are the activity recommendations clearly defined, and are they reasonable?
10) Does documentary evidence indicate that the recommendations have been implemented?
11) Have the activity results been progressively updated to reflect the latest design, and are these being used as an input to design reviews?

Bibliography

Documents for structuring arguments

Toulmin method – Toulmin, S., The Uses of Argument, 1958, 2nd edition, 2003

Goal Structuring Notation – GSN Community Standard

http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf

Documents for reaching formal agreements

ISO/IEC 12207, *Systems and software engineering – Software life cycle processes*

ISO/IEC 15026, *Systems and software engineering – Systems and software assurance*

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

Documents for dependability

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

IEC 60300-3-4, *Dependability management – Part 3-4: Application guide – Guide to the specification of dependability requirements*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and Boolean methods*

IEC 62347, *Guidance on system dependability specifications*

Documents for managing risks

IEC/ISO 31010, *Risk management – Risk assessment techniques*

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

———————

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

____

DÉMONSTRATION DES EXIGENCES DE SÛRETÉ DE FONCTIONNEMENT – ARGUMENTAIRE DANS LE CADRE DE LA SÛRETÉ DE FONCTIONNEMENT

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 62741 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1591/FDIS	56/1609/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.

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

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

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

INTRODUCTION

La sûreté de fonctionnement est la capacité d'exécuter comme exigé et lorsque cela est exigé. Les niveaux acceptables de sûreté de fonctionnement sont ainsi essentiels pour une performance continue et des coûts du cycle de vie optimisés.

Afin d'atteindre la sûreté de fonctionnement d'un système, il convient d'établir les exigences en la matière, d'identifier les risques de non-satisfaction, et de développer un ensemble adapté d'activités pour satisfaire aux exigences, démontrer les exigences et gérer les risques. Une étude de sûreté de fonctionnement fournit un moyen pratique et convaincant d'enregistrer le résultat de ces activités dans un seul endroit et de présenter un argument, étayé par des preuves, que les risques ont été traités et que la sûreté de fonctionnement nécessaire a été ou sera atteinte ou continuera d'être atteinte dans le temps. Elle sert de moyen principal de communication sur la sûreté de fonctionnement entre clients, fournisseurs et autres acteurs et favorise la coopération entre eux. Cela est essentiel pour assurer la sûreté de fonctionnement et fournir l'assurance dans le cadre de la relation client/fournisseur.

La préparation d'une étude de sûreté de fonctionnement peut améliorer la sûreté de fonctionnement par le biais des actions prises pour préparer et développer l'argument dans l'étude de sûreté de fonctionnement. Elle peut améliorer le rapport coût-efficacité d'un programme de sûreté de fonctionnement car si une activité ne fournit pas la preuve qu'elle étaie l'étude, ceci peut indiquer que l'activité n'est pas nécessaire.

Les activités exigées pour la réalisation de la sûreté de fonctionnement dépendent de la nature et de l'état de développement du système et sont susceptibles de varier fortement d'un projet à l'autre.

Tout au long de la présente Norme internationale, le terme "sûreté de fonctionnement" inclut tous les aspects liés à la fiabilité, la disponibilité, la maintenabilité et l'aptitude au soutien, ainsi que d'autres attributs tels que l'aptitude à l'utilisation, la testabilité et la durabilité. De plus, la sûreté de fonctionnement d'un système inclut tous les aspects de ce système, y compris les composants, processus, matériels, logiciels et les interfaces entre eux.

La présente norme fait office de lignes directrices, lesquelles n'étant pas prescriptives par nature, mais étant génériques. Il convient qu'elles soient adaptées aux objectifs spécifiques et qu'elles ne soient pas exhaustives.

La présente norme n'aborde pas les questions liées à la sécurité ou l'environnement.

DÉMONSTRATION DES EXIGENCES DE SÛRETÉ DE FONCTIONNEMENT – ARGUMENTAIRE DANS LE CADRE DE LA SÛRETÉ DE FONCTIONNEMENT

1 Domaine d'application

La présente Norme internationale fournit des lignes directrices concernant le contenu et l'application d'une étude de sûreté de fonctionnement et établit les principes généraux pour la préparation d'une étude de sûreté de fonctionnement.

La présente norme est rédigée dans le cadre d'un projet de base où un client commande un système qui satisfait aux exigences de sûreté de fonctionnement d'un fournisseur et gère alors le système jusqu'à sa mise hors service. Les méthodes fournies dans cette norme peuvent être modifiées et adaptées aux autres situations, si nécessaire.

L'étude de sûreté de fonctionnement est normalement produite par le client et le fournisseur et peut également être utilisée et mise à jour par d'autres organisations. Par exemple, les organismes de certification et législateurs peuvent examiner l'étude soumise pour étayer leurs décisions et les utilisateurs du système peuvent mettre à jour/développer l'étude, notamment lorsqu'ils utilisent le système à une autre fin.

2 Références normatives

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

IEC 60050-192, *Vocabulaire électrotechnique international – Partie 192: Sûreté de fonctionnement* [1]

IEC 60300-1, *Gestion de la sûreté de fonctionnement – Partie 1: gestion du programme de sûreté de fonctionnement*

ISO 31000, *Management du risque – Principes et lignes directrices*

3 Termes, définitions et abréviations

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

3.1 Termes et définitions

3.1.1
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

1 A publier.

3.1.2
tableau des preuves
structure identifiant quelle preuve sera/a été produite et quand

3.1.3
disponible
OTS
article immédiatement disponible qui est à la fois commercial et vendu en grandes quantités sur le marché

Note 1 à l'article: Parfois appelé COTS (commercial off-the-shelf, *en français:* disponible dans le commerce) ou MOTS (modified off-the-shelf, *en français:* disponible avec modification).

3.1.4
client
partie qui commande ou spécifie l'article, notamment les exigences de sûreté de fonctionnement

Note 1 à l'article: Il peut s'agir d'une organisation, d'un mécène, d'un département, d'une entreprise ou d'un individu et peut changer tout au long du cycle de vie.

3.1.5
sous-système
partie d'un système, qui est lui-même un système

3.1.6
fournisseur
partie qui fournit l'article, qui satisfait à son exigence de sûreté de fonctionnement

Note 1 à l'article: Il peut s'agir d'une organisation, d'un département, d'une entreprise ou d'un individu et peut changer tout au long du cycle de vie.

3.1.7
système <dans la sûreté de fonctionnement>
ensemble défini d'éléments qui satisfont collectivement à une exigence

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

Note 2 à l'article: Les ressources externes (de l'extérieur de la limite du système) peuvent être exigées pour le fonctionnement du système.

Note 3 à l'article: Une structure du système peut être hiérarchique (système, sous-système, composant, etc.).

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

3.2 Abréviations

Terme	Terme en français	Equivalent en anglais
COTS	Disponible dans le commerce	Commercial off-the-shelf
FEM	Modélisation par éléments finis	Finite element modelling
AMPEC	Analyse des modes de panne, de leurs effects et de leur criticité	Failure mode, effects and criticality analysis (FMECA)
FTA	Analyse par arbre de panne	Fault tree analysis
MOTS	Disponible avec modification	Modified off-the-shelf
OTS	Off-the-shelf	Prêt à être utilisé

4 Contexte de l'étude de sûreté de fonctionnement

4.1 Principes et objet

Une étude de sûreté de fonctionnement fournit un argument raisonné et traçable fondé sur le fait qu'un système satisfait aux exigences et continue ainsi dans le temps. Elle démontre pourquoi certaines activités ont été entreprises et comment elles peuvent être jugées comme réussies. Pour une efficacité maximale, il convient que l'étude de sûreté de fonctionnement soit initiée dans la phase de conception, révisée progressivement au cours du cycle de vie d'un système et qu'elle soit généralement résumée dans les rapports d'étude de sûreté de fonctionnement aux étapes prédéfinies. Elle enregistre l'avancement relatif à l'obtention de la preuve que les exigences de sûreté de fonctionnement sont satisfaites et accompagne le système tout au long de son cycle de vie jusqu'à sa mise hors service.

L'étude de sûreté de fonctionnement est très avantageuse pour les systèmes de grande qualité, et en faible quantité où la preuve directe de la sûreté de fonctionnement peut être difficile ou chère à obtenir. Comme ces systèmes sont souvent très complexes, impliquent des nouvelles technologies et ont des acteurs très variés, un argument explicite est nécessaire pour formuler des affirmations de sûreté de fonctionnement détaillées avec des preuves appropriées.

4.2 Relation entre l'étude de sûreté de fonctionnement et les plans de sûreté de fonctionnement

La gestion efficace de la sûreté de fonctionnement exige des dispositions organisationnelles pour mettre en application la politique, les activités mises en application dans les programmes et plans de sûreté de fonctionnement et les processus d'évaluation, de garantie et d'étude de performances.

Un programme de sûreté de fonctionnement implique

a) les plans de sûreté de fonctionnement qui définissent les activités, techniques et ressources exigées pour atteindre la sûreté de fonctionnement,

b) les méthodes de mesure et d'évaluation,

c) l'assurance et la revue.

Les objectifs d'un plan de sûreté de fonctionnement incluent de garantir que

1) les exigences du client en matière de sûreté de fonctionnement sont déterminées et réputées être comprises à la fois par le client et par le fournisseur,

2) les activités sont planifiées, approuvées et mises en application pour satisfaire aux exigences, démontrer les exigences et traiter les risques de défaillance,

3) le client dispose de l'assurance que les exigences de sûreté de fonctionnement sont, ou seront, satisfaites et que l'incertitude de la sûreté de fonctionnement diminue au cours du plan.

L'étude de sûreté de fonctionnement offre l'assurance progressive que les exigences de sûreté de fonctionnement sont, ou seront, satisfaites et que l'incertitude de la sûreté de fonctionnement diminue. De plus, l'étude montre que les activités dans le plan satisfont aux exigences et traitent les risques. Cela fait partie de l'argument et preuve que le système est ou sera soumis à la sûreté de fonctionnement. Le plan repose habituellement sur les normes et l'expérience de l'organisation à gérer la sûreté de fonctionnement et est adapté, en tenant compte des facteurs comme les stades du cycle de vie respectifs, le contexte de l'organisation, les ressources disponibles et les risques qu'il est nécessaire de gérer.

Le plan de sûreté de fonctionnement et l'étude de sûreté de fonctionnement sont souvent développés conjointement car les deux incluent la considération des risques liés à la non-satisfaction des exigences. Toutefois, le système pourrait satisfaire aux exigences de sûreté de fonctionnement, mais il pourrait ne pas être possible de démontrer que ces exigences ont

bien été satisfaites. En effet, il se peut qu'aucune activité appropriée ne peut démontrer que les exigences ont été satisfaites, les coûts ou la durée exigés pour ce faire pouvant être trop importants. Par conséquent, le plan de sûreté de fonctionnement peut également inclure les activités spécialement destinées à traiter les risques liés à l'impossibilité de démontrer que les exigences ont été satisfaites et que ces activités apportent également la preuve dans l'étude de sûreté de fonctionnement.

Il convient qu'un registre des risques produit dans le cadre de l'étude de sûreté de fonctionnement soit coordonné avec les risques identifiés dans le cadre de la planification du programme de sûreté de fonctionnement et avec le registre des risques liés à un projet. Les activités proposées pour traiter les risques sont incluses dans le plan de sûreté de fonctionnement et examinées comme sources de preuve selon laquelle ces risques ont été traités. Comme le plan de sûreté de fonctionnement est mis en application, l'étude de sûreté de fonctionnement est renseignée avec la preuve de la mise en application réussie du plan. Ceci fournit une assurance progressive que les exigences ont été satisfaites. Si aucune preuve suffisante ne peut être obtenue, il convient alors que le plan de sûreté de fonctionnement soit modifié en conséquence.

Dans un projet bien géré, le plan de sûreté de fonctionnement et l'étude de sûreté de fonctionnement sont entièrement intégrés avec la gestion du projet général. Dans un tel projet, l'utilisation de l'étude de sûreté de fonctionnement n'induit pas une augmentation de la charge de travail générale, car le coût d'élaboration de l'étude est recoupé par l'économie liée à une mauvaise communication évitée, à une révision évitée due à la découverte tardive des défauts, aux activités évitées sans avantages démontrables, etc.

De plus, la préparation d'une étude de sûreté de fonctionnement facilite le développement d'un plan de sûreté de fonctionnement économique car la preuve recherchée à l'appui de l'argument dans l'étude de sûreté de fonctionnement peut suggérer les activités qui améliorent le plan de sûreté de fonctionnement. De plus, si une activité dans le plan ne fait pas partie d'un argument dans l'étude de sûreté de fonctionnement, il convient de l'étudier pour vérifier qu'elle exécute une fonction utile dans le plan. (Noter que certaines activités du plan de sûreté de fonctionnement sont incluses à l'appui d'autres disciplines, comme la sécurité, qui ne font en principe pas partie de l'étude de sûreté de fonctionnement.)

Il convient d'examiner et de mettre à jour le plan de sûreté de fonctionnement et l'étude de sûreté de fonctionnement en cas de changements significatifs de ce qui suit:

– exigences ou attentes du client;
– environnement ou systèmes d'interface;
– conditions d'utilisation ou usage prévu;
– conception;
– performance réelle.

4.3 Assurance progressive de la sûreté de fonctionnement

L'étude de sûreté de fonctionnement fournit un plus grand élément de preuve qui vise à réduire progressivement l'incertitude liée à la satisfaction des exigences de sûreté de fonctionnement. Toutefois, les exigences, les environnements, etc. changent la norme plutôt que l'exception pendant le cycle de vie du système. L'incertitude pourrait donc ne pas toujours diminuer. Il pourrait y avoir des occasions, par exemple, lorsqu'une option de conception différente rend une partie de la preuve obsolète, qui entraînant une incertitude accrue. Il pourrait également y avoir des périodes où aucune preuve n'est fournie, par exemple, pendant les essais avant la publication des résultats d'essai, lorsque l'incertitude reste inchangée. De plus, si une nouvelle preuve entre en conflit avec la preuve existante, ceci pourrait augmenter l'incertitude.

La Figure 1 montre deux types de développement de produit: nouveau développement et MOTS (disponible avec modification). L'axe vertical représente le niveau d'incertitude identifié

à tout moment du projet. Lorsque la quantité de la preuve de la sûreté de fonctionnement augmente, l'incertitude diminue généralement et une assurance progressive est obtenue.

L'axe horizontal représente le temps dans le projet, du début de la phase de conception "a", en passant par le début du développement "b", à la fin de la phase de réalisation "c", à la fin de l'utilisation "d" et "e", l'amélioration possible, et au-delà.

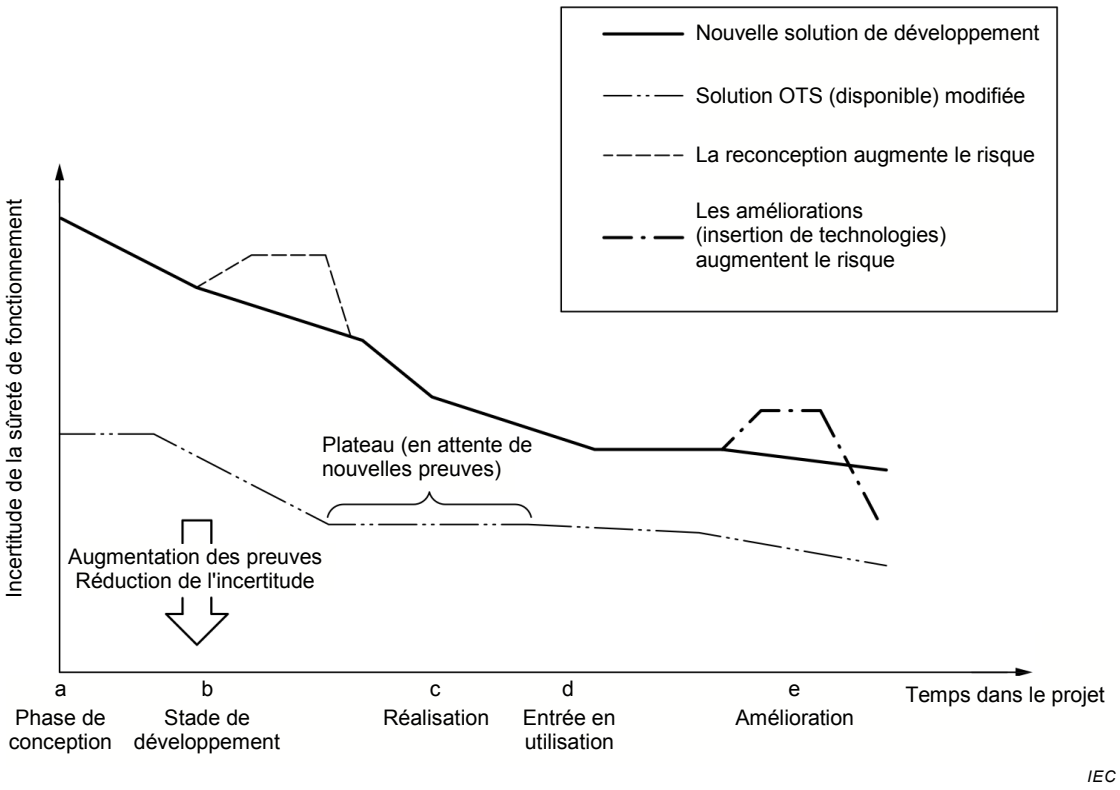


Figure 1 – Illustration du processus d'assurance progressive

Au moment "a" (début de la phase de conception), le niveau d'incertitude est relativement élevé, mais cette incertitude diminue lorsque le projet progresse. Au moment "c", en effet à la transition de la phase de réalisation à la phase d'utilisation, l'élément de preuve est suffisant pour garantir la sûreté de fonctionnement selon l'étendue qui garantit cette transition. Il convient que l'élément de preuve (assurance) continue d'intégrer l'utilisation au fur et à mesure que les essais et l'utilisation réussis sont enregistrés et la diminution continue des risques résiduels peut être considérée.

A l'issue de sa propre nouvelle phase de développement, une solution MOTS est souvent considérée comme moins incertaine que le nouveau développement indiqué à la Figure 1, toute chose étant égale par ailleurs. Ce n'est pas le cas pour une solution OTS (disponible) dans les nouvelles applications ou dans un nouvel environnement et une réévaluation prudente est exigée.

Finalement, de nombreuses modifications de l'incertitude sont des changements d'étape plutôt que des changements progressifs.

5 Principes de l'étude de sûreté de fonctionnement

5.1 Description de l'étude de sûreté de fonctionnement

L'étude de sûreté de fonctionnement commence par une déclaration initiale des exigences de sûreté de fonctionnement. Ces exigences pourraient inclure les objectifs internes du client et

du fournisseur, les stratégies de marché, les exigences réglementaires, etc. ainsi que les exigences explicitement définies par le client.

Ainsi, l'étude de sûreté de fonctionnement établit une affirmation de niveau supérieur indiquant le fait que le système satisfait aux exigences (voir 5.2). L'étude de sûreté de fonctionnement fournit ainsi une structure à plusieurs niveaux d'affirmations, sous-affirmations et sous-arguments qui reposent finalement sur les preuves (voir 5.3) et hypothèses.

La preuve est présentée dans le tableau des preuves (voir 5.4) et résumée et référencée dans l'argument dans le rapport d'étude de sûreté de fonctionnement (voir 5.5).

5.2 Formulation des affirmations dans l'étude de sûreté de fonctionnement

L'étude de sûreté de fonctionnement utilise la preuve afin de créer un argument pour les affirmations dont les exigences de sûreté de fonctionnement ont été ou seront satisfaites.

La Figure 2 montre le processus d'établissement et d'argumentation des affirmations dans l'étude de sûreté de fonctionnement à l'aide des sources de preuve.

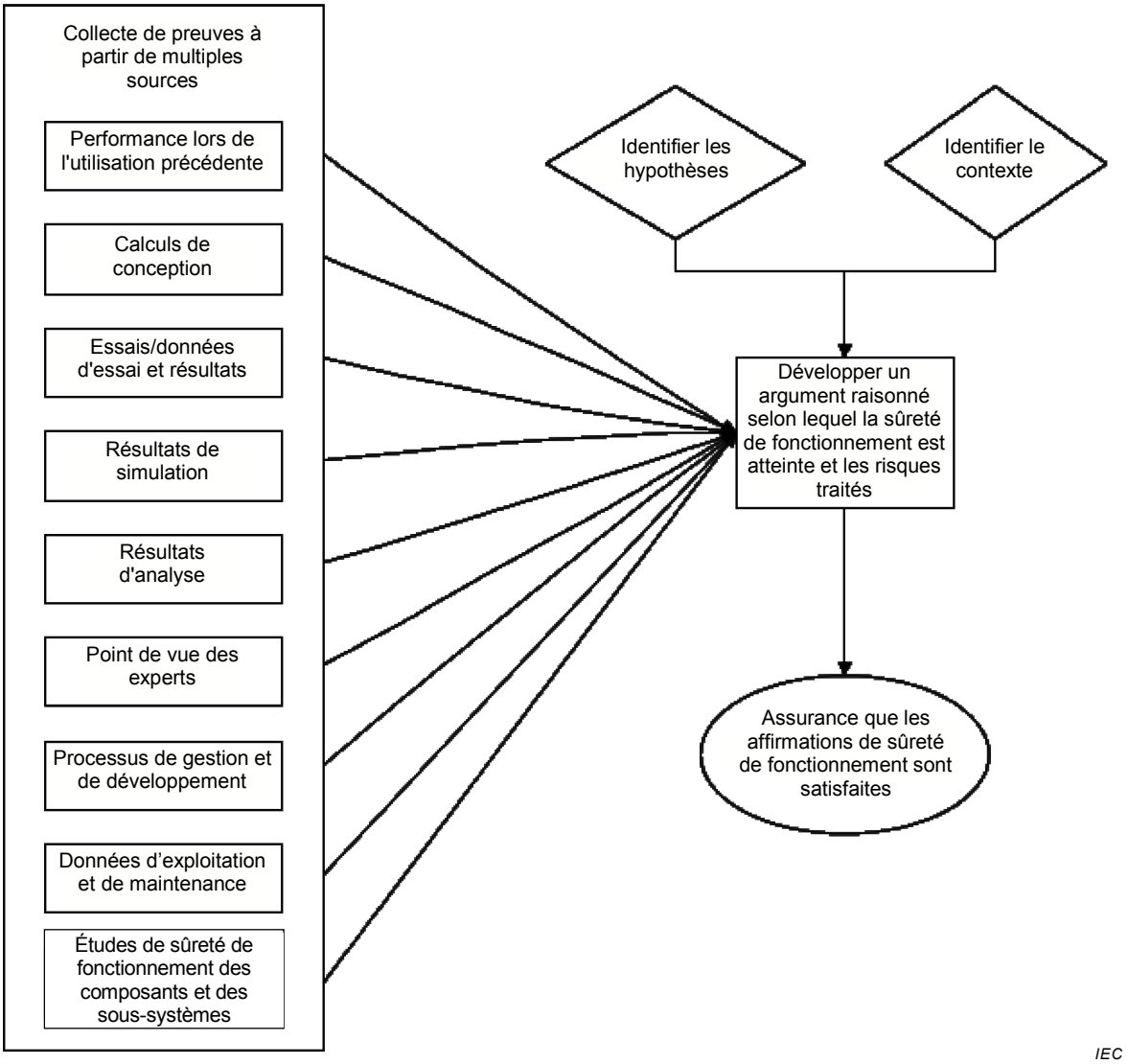


Figure 2 – Le développement des affirmations

Il convient d'identifier et d'indiquer explicitement les hypothèses nécessaires pour soutenir l'argument, avec les activités planifiées pour les valider. Elles pourraient inclure les hypothèses concernant les conditions d'utilisation, l'environnement dans lequel le système est utilisé ou la nature et le type de maintenance.

Les arguments peuvent entrer dans une des deux catégories:

a) les arguments qui ont tous identifié des risques relatifs à l'affirmation sont éliminés ou suffisamment traités, étayés par la preuve de traitements réussis et par la preuve que l'identification des risques est complète;

b) les arguments selon lesquels il existe des raisons suffisantes d'affirmation, étayées par la preuve de la véracité de chacune et par la preuve de l'adéquation.

La première catégorie exige de tenir compte de toutes les sources significatives de risques, des zones d'impacts, des événements (y compris les changements de circonstances), ainsi que de leurs causes et leurs éventuelles conséquences. La deuxième catégorie exige que tous les aspects couverts par la preuve soient suffisants pour assurer l'affirmation.

Le contexte pour lequel l'argument est soutenu doit également être identifié car il identifie les limites de l'étude de sûreté de fonctionnement. Le contexte inclut les acteurs qui pourraient

être intéressés par le système, les objectifs et les exigences de performance, le système étant considéré et les limitations relatives à l'utilisation du système proposées.

Si l'une des hypothèses ou le contexte change, l'argument et les affirmations de l'étude de sûreté de fonctionnement doivent être révisés.

Pendant la mise en application du plan de sûreté de fonctionnement, il convient de valider les principales hypothèses, si possible, en remplaçant chacune d'elle par une preuve étayée. De manière similaire, il convient que les contextes dans lesquels l'argument est soutenu soient validés pour répondre à l'application réelle ou prévue du système et de l'étude de sûreté de fonctionnement.

A partir de ces sources de preuve et des hypothèses explicitement émises, un argument raisonné montre comment les affirmations de sûreté de fonctionnement sont étayées. Les documents et données associés représentent l'étude de sûreté de fonctionnement.

5.3 Utilisation de la preuve dans l'étude de sûreté de fonctionnement

Dans l'étude de sûreté de fonctionnement, la preuve peut se présenter sous deux formes. La première est la preuve directe que les exigences de sûreté de fonctionnement ont été démontrées. La deuxième est la preuve que les activités de traitement des risques de non-satisfaction ou de non-démonstration des exigences de sûreté de fonctionnement ont abouti.

Il convient d'utiliser une grande variété de sources. Elles peuvent inclure

a) les performances lors de l'utilisation/opération précédente,

b) la conception ou d'autres calculs,

c) l'essai et les résultats de données d'essai,

d) les résultats de simulation (FEM ou Monte Carlo, par exemple),

e) les résultats d'analyse (AMPEC et FTA, par exemple) y compris les prévisions et la modélisation,

f) le point de vue des experts, y compris le succès précédemment enregistré du fournisseur,

g) processus de gestion et de développement, notamment
   - la mise en application correcte des pratiques d'excellence,
   - les activités de gestion et les processus de systèmes observés,

h) les données d'exploitation et de maintenance,

i) les études de sûreté de fonctionnement des composants/sous-systèmes fournis par leurs fournisseurs.

Elle peut également inclure la preuve des activités et tâches effectuées à d'autres fins que la mise en application du plan de sûreté de fonctionnement, comme l'analyse de la sécurité ou du support logistique.

Avant d'entreprendre une activité de sûreté de fonctionnement, il convient de comprendre totalement ses objectifs, à savoir comment l'activité aide à atteindre la sûreté de fonctionnement, comment elle fournit la preuve pour l'étude de sûreté de fonctionnement et les critères de réussite pour l'activité. Les critères de réussite sont appliqués aux enregistrements et résultats de l'activité pour évaluer si elle a atteint ses objectifs. La preuve que les critères sont satisfaits (notamment les enregistrements et les résultats) étaie les affirmations selon lesquelles les objectifs sont atteints. Le cas échéant, les critères de réussite incluent que les risques ont été correctement traités.

Les critères de réussite quantifiés sont privilégiés, la détermination du succès étant plus simple et moins ouverte à l'interprétation.

Les critères de réussite quantifiés ne peuvent cependant pas être produits pour toutes les activités. Dans ces cas, il convient de définir les critères qualitatifs reposant sur les objectifs de l'activité et que ceux-ci incluent que l'activité, et son résultat, sont appropriés et corrects. Par exemple, les critères de réussite pour la modélisation ne consistent pas simplement à ce que les prévisions et la modélisation démontrent le respect des exigences mais que le modèle lui-même soit une représentation adéquate du système et que tous les systèmes ou éléments du système (ex.: logiciels) aient été inclus dans la modélisation. Il convient que le modèle traite également la robustesse de la conception par rapport aux variations des conditions d'utilisation et des conditions et tolérances de fabrication.

L'assurance et la preuve ne résultent pas simplement des résultats d'une activité de sûreté de fonctionnement mais également de la ponctualité de l'activité et des actions qui surviennent. L'exécution de l'activité au moment approprié de manière à ce qu'elle influence la conception du système est très importante et il convient que les activités soient effectuées en parallèle avec le processus de conception. Par conséquent, il convient que la preuve d'une activité d'analyse inclue la documentation indiquant que les activités et actions ont été mises en application dans les délais.

5.4 Tableau des preuves

Le tableau des preuves présente la preuve utilisée pour démontrer les affirmations et prendre en charge l'argument. Il se présente en général sous la forme d'un tableau. Le tableau des preuves capture l'ensemble actuel des activités de conformité et d'assurance (et leurs critères de réussite ou d'acceptation) qui montrent que la sûreté de fonctionnement est atteinte et que les risques relatifs à la sûreté de fonctionnement ont été traités.

La Figure 3 montre les étapes permettant d'établir et de développer le tableau des preuves. Il convient que chaque rapport d'étude de sûreté de fonctionnement base ses affirmations et arguments en fonction du dernier statut du tableau des preuves.

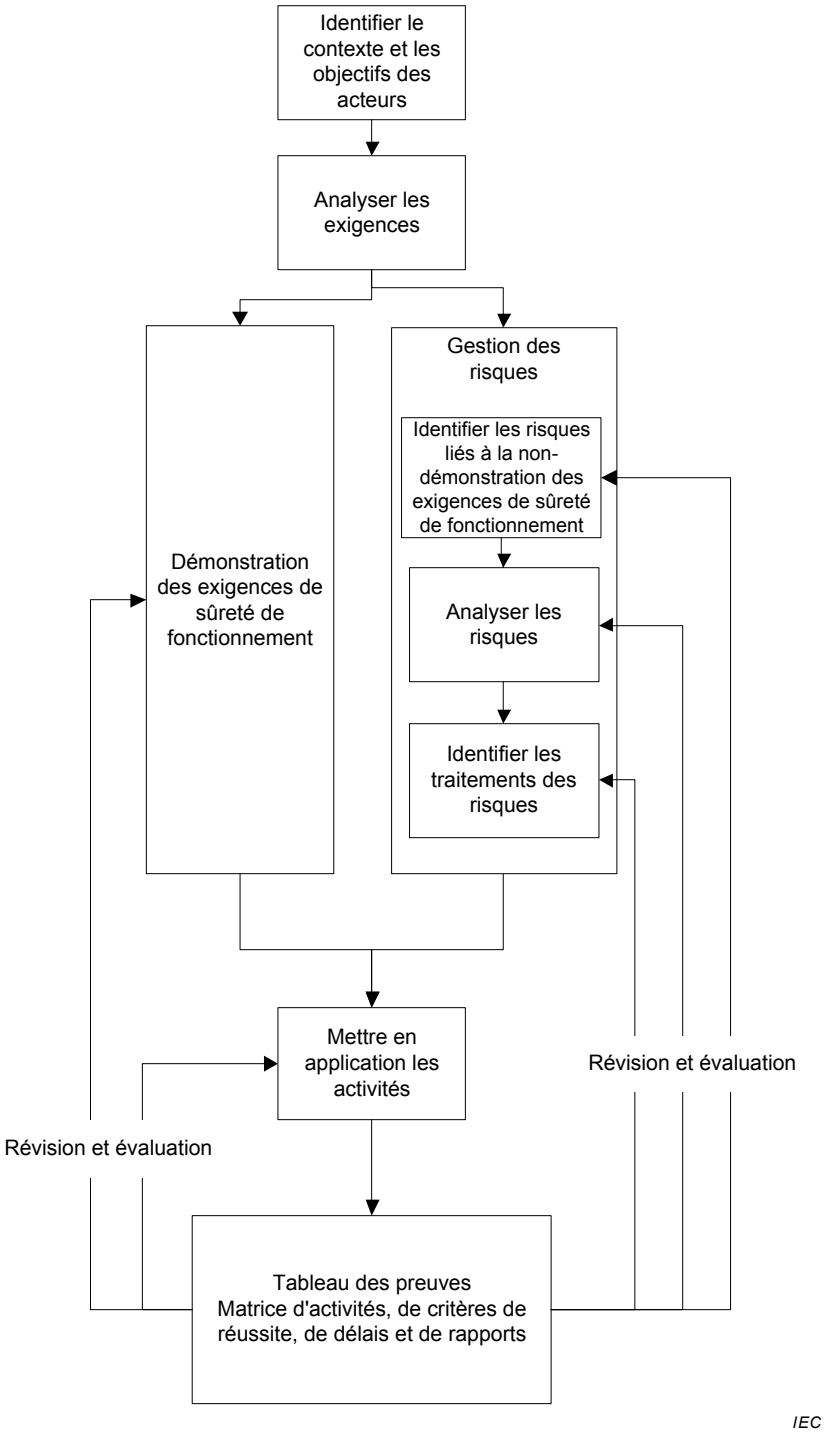


Figure 3 – Établissement et développement du tableau des preuves

Il convient que le tableau des preuves soit adapté au projet. Il varie tout au long du cycle de vie mais il convient qu'il identifie ou contienne

a) les activités de sûreté de fonctionnement, notamment les mesures et essais, qui apportent la preuve pour l'étude de sûreté de fonctionnement,

b) les critères de réussite ou d'acceptation de la preuve,

c) les liens relatifs aux risques que l'activité est censée traiter ou l'affirmation que l'activité étaie (si applicable),

d) les dates/étapes auxquelles il convient que l'activité soit terminée et la preuve disponible,

e) les références ou liens relatifs à la preuve réellement fournis,

f) la confirmation de son acceptation (ou rejet) (si applicable).

L'Annexe A comprend des exemples de tableaux des preuves.

5.5 Rapport d'étude de sûreté de fonctionnement

En pratique, la collation de toute la documentation dans un seul document est ingérable, en particulier lorsque les sources de preuves sont nombreuses et diverses. Une solution acceptable est de présenter les mises à jour périodiques de l'étude de sûreté de fonctionnement comme des rapports d'étude de sûreté de fonctionnement. L'étude de sûreté de fonctionnement est alors l'élément des rapports d'étude de sûreté de fonctionnement accumulés qui, à leur tour, font référence à la preuve source.

Les rapports d'étude de sûreté de fonctionnement sont généralement élaborés aux points prédéfinis. Ils apportent la preuve et les conclusions tirées du travail effectué jusqu'à présent (faisant référence aux documents et sources de données, si nécessaire), fournissent une évaluation de la réalisation/avancement de la sûreté de fonctionnement générale et un examen et une évaluation des activités de sûreté de fonctionnement. Au début de chaque phase, il convient que le fournisseur et le client conviennent des exigences à satisfaire à la fin de cette même phase, c'est-à-dire les étapes que le projet doit traverser avant de passer à la phase suivante. L'accord peut inclure des compromis entre différentes exigences concurrentes. Il convient que le risque résultant de ce compromis soit inclus dans le tableau des preuves. Les normes décrivant les processus qui pourraient être utilisés pour parvenir à des accords solides entre le client et le fournisseur sont énumérées dans la Bibliographie.

Si exigé par un contrat, elles peuvent être utilisées pour fournir des détails suffisants pour les acteurs ou le client pour prendre une décision sur le passage ou non à une phase d'un cycle de vie du projet à l'autre. L'Annexe B comprend une description du contenu possible d'un rapport d'étude de sûreté de fonctionnement.

Le rapport d'étude de sûreté de fonctionnement peut être présenté comme un document narratif mais, si une présentation plus formelle de l'argument est exigée, il existe plusieurs techniques disponibles qui peuvent être utilisées pour structurer l'argument et les affirmations établies à partir des preuves collectées. La Bibliographie fournit des références normatives à certaines techniques.

6 Développement de l'étude de sûreté de fonctionnement

6.1 Généralités

La présente norme décrit principalement un projet qui observe le cycle de vie du modèle V où le fournisseur développe ou propose un système pour satisfaire aux exigences du client et le client le gère selon les besoins variables jusqu'à sa mise hors service.

Dans les projets utilisant d'autres processus de gestion de projets, comme les modèles spiralés ou modèles SCRUM, les exigences sont définies lorsque le projet progresse et il convient que les lignes directrices dans cette norme soient adaptées à chaque projet. Il est toujours important cependant de convenir des exigences pour la phase suivante et de ce qui est exigé par la fin de cette phase (par exemple, une version de produit stable et fonctionnelle).

L'étude de sûreté de fonctionnement n'appartient pas seulement au client ou au fournisseur, mais est un élément de preuve conjoint qui est développé et ajouté par différentes parties aux différentes phases du cycle de vie.

Le développement de l'étude de sûreté de fonctionnement améliore la communication entre le client et le fournisseur. Par exemple, une cause possible de non-satisfaction des exigences du client est le manque de compréhension par le fournisseur des besoins du client. Traiter ce risque nécessite que le client et le fournisseur communiquent pour atteindre une

compréhension commune des exigences. Traiter ce risque de manière anticipée minimise également les coûts.

6.2 Préparation de l'étude de sûreté de fonctionnement

Même si l'étude de sûreté de fonctionnement est plus efficace si elle commence au stade de la conception, elle peut néanmoins être lancée à tous les stades du cycle de vie. Le présent paragraphe décrit les activités exigées quel que soit le stade du cycle de vie auquel l'étude de sûreté de fonctionnement est en premier lieu développée. Les paragraphes suivants décrivent comment l'étude de sûreté de fonctionnement pourrait être développée tout au long du cycle de vie du projet. Pour simplifier, elle est rédigée dans le contexte du lancement du projet à la phase de conception, où le fournisseur peut développer de multiples solutions, dont l'une est sélectionnée par le client et est poursuivie jusqu'à l'amélioration et la mise hors service.

Le développement de l'étude de sûreté de fonctionnement commence par les activités du client pour déterminer les exigences de sûreté de fonctionnement et leur base de mesure. Normalement, la manière dont ces exigences doivent être mesurées est documentée dans le cadre du stade de conception d'un projet. L'IEC 62347 et l'IEC 60300-3-4 fournissent des lignes directrices sur la spécification de la sûreté de fonctionnement.

Il convient que le client inclue les exigences de sûreté de fonctionnement, y compris les exigences de disponibilité, de fiabilité, de maintenabilité et d'aptitude au soutien dans le cadre de la spécification du système qui inclut également la performance et l'utilisation. D'autres exigences comme les profils de coûts et de risques peuvent également être spécifiées.

Si nécessaire, des références à d'autres documents ou preuves (comme les documents qui détaillent les dispositions proposées pour la gestion du risque, la sécurité, l'aptitude au soutien et l'environnement) sont également incluses. Il convient que le client fournisse également le contexte pour ces exigences en partant de leurs profils d'exploitation, du rôle du projet, etc. jusqu'à la terminologie utilisée. De même, il convient que le client clarifie toutes les hypothèses émises lors du développement des exigences et qu'il s'attende à ce que les exigences pertinentes ou appropriées pour la sûreté de fonctionnement soient partagées avec les fournisseurs.

Le client peut présenter ces exigences, avec le contexte et les hypothèses, dans un rapport d'étude de sûreté de fonctionnement initial, avec des références aux preuves déjà existantes (les performances de sûreté de fonctionnement des systèmes ou sous-systèmes similaires, par exemple). Le client pourrait également identifier les risques relatifs à la sûreté de fonctionnement et comment il convient de les traiter par le fournisseur ou le client. Il convient que cela inclue les informations relatives à la manière dont le client détermine que les risques ont été correctement traités.

Lors de la réception des exigences de sûreté de fonctionnement ou du rapport d'étude de sûreté de fonctionnement initial du client, il convient que le fournisseur analyse ces exigences de sûreté de fonctionnement et planifie les activités pour les satisfaire. Cette analyse et cette planification impliquent

a) la compréhension totale des exigences,
b) d'analyser les exigences pour définir les objectifs de sûreté de fonctionnement du système,
c) de tenir compte des preuves existantes,
d) d'identifier les risques (et de les transférer dans le registre des risques au niveau du projet global) et la manière dont ils doivent être traités.

Il convient d'analyser les exigences qui affectent la sûreté de fonctionnement du système afin de déterminer leur impact au niveau du système et du sous-système, et que les résultats de ces analyses représentent l'étude de sûreté de fonctionnement. Il convient que cette analyse inclue tous les autres aspects comme l'exploitation du système, son environnement et les interfaces homme-machine, dont tous ont un impact sur la sûreté de fonctionnement du

système. Pour acquérir cette compréhension, il convient que le fournisseur participe au dialogue avec le client pour garantir la compréhension mutuelle de tous les aspects. Ce dialogue entraîne une déclaration définitive des exigences du client et de toutes les conditions d'exploitation et environnementales. Cette déclaration assure que les exigences de sûreté de fonctionnement du client ont été acceptées et bien comprises par le client et le fournisseur (voir 4.2). Il convient également que le client et le fournisseur conviennent de la manière dont les risques doivent être traités et de la manière dont le client juge que les risques ont été correctement traités.

Dès lors, les objectifs de conception de sûreté de fonctionnement et une base de mesure sont déterminés. Il s'agit des objectifs de conception, éventuellement avec une marge relative à l'exigence de sûreté de fonctionnement pour réduire le risque que l'exigence ne soit pas satisfaite.

Les activités de sûreté de fonctionnement aboutissent à un tableau des preuves et à une étude de sûreté de fonctionnement. La planification des activités de sûreté de fonctionnement (à inclure dans la réponse au client) repose sur le travail exigé pour démontrer que les exigences de sûreté de fonctionnement ont été satisfaites. La planification des activités doit assurer le client et le fournisseur que le risque de non-satisfaction ou de non-démonstration des exigences de sûreté de fonctionnement est minimisé, avant d'engager des ressources.

Différents types d'achat ou de projet peuvent cependant impliquer différentes combinaisons de phases de cycles de vie et, selon les arrangements contractuels, l'étude de sûreté de fonctionnement peut être démarrée ou complétée à la fin de toute/n'importe quelle phase. Par exemple, si un client achète un système OTS, le développement peut avoir terminé un peu plus tôt et le client peut préparer l'étude de sûreté de fonctionnement incluant uniquement les phases de réalisation et d'utilisation. D'autre part, le système OTS peut fournir sa propre étude de sûreté de fonctionnement, incluant les phases de conception et de développement, qui peuvent être intégrées ou mises en référence par de nombreux clients.

Mais, quelle que soit la phase à laquelle commence le projet, il convient que le premier rapport d'étude de sûreté de fonctionnement inclue une évaluation complète des exigences et des tâches et activités qui sont entreprises.

6.3 Phase de conception

A la phase de conception, il convient que le client développe un ensemble détaillé d'exigences et qu'il puisse établir un rapport d'étude de sûreté de fonctionnement détaillé pour le fournisseur. Il convient que le client identifie également les risques à inclure dans le registre de risques de projet général. Lorsqu'il s'agit d'un projet long, incluant une phase de développement compétitive importante, ainsi le client pourrait avoir besoin d'examiner l'ensemble des exigences pour s'assurer que les propositions des fournisseurs concurrents peuvent être évaluées pour la sûreté de fonctionnement en utilisant une méthodologie d'évaluation commune.

Il est essentiel que tous les acteurs de la sûreté de fonctionnement soient consultés lors de la phase de conception pour garantir que leurs exigences sont entièrement intégrées. Le point de vue des experts et l'utilisation de techniques de modélisation de la sûreté de fonctionnement sont probablement nécessaires pour valider que les exigences sont adaptées et suffisantes.

Il est probable qu'il y ait un compromis considérable entre les différentes exigences. Pour ce compromis, les risques de ne pas démontrer la satisfaction aux exigences peuvent former une partie essentielle du processus de prise de décision, c'est-à-dire que si la satisfaction des exigences de sûreté de fonctionnement ne peut pas être démontrée, cela peut être un motif de rejet de l'option. Dans le cadre de la phase de conception, le fournisseur ou le client peut opter pour une seule solution privilégiée, ou ceci peut ne pas se produire jusqu'à la phase de développement.

Il convient que le fournisseur analyse les exigences et qu'il développe une ou plusieurs solutions. Des risques communs à n'importe quelle solution potentielle et exigeant un traitement spécifique et ponctuel pourraient être identifiés à cette phase. Ces risques pourraient conduire à un tableau des preuves initial identifiant les activités d'assurance minimales exigées et ces activités pourraient, à leur tour, faire partie des exigences contractuelles ou de l'étendue de fourniture. Mais, lors du développement de ces solutions, le fournisseur peut identifier différents risques relatifs à la satisfaction des exigences de sûreté de fonctionnement pour les différentes solutions. Il convient également de les présenter dans le tableau des preuves initial.

Il convient que le fournisseur développe un ensemble préalable d'activités de sûreté de fonctionnement pour démontrer la satisfaction aux exigences de sûreté de fonctionnement et traiter les risques, en fonction du tableau des preuves initial. Il convient de le présenter au client dans le plan de sûreté de fonctionnement et que celui-ci décrive la philosophie de conception et les caractéristiques de conception principales et qu'il identifie les différents risques pour les conceptions proposées. Dans certains cas, les risques peuvent être déterminés à l'aide d'une liste de contrôle, mais il convient que l'avis technique ait un poids plus fort. Il convient d'inclure ces risques avec les autres risques du projet dans le plan de gestion des risques du projet général. Les risques et leur plan de gestion font partie de l'étude de sûreté de fonctionnement (voir IEC 62198).

Il convient de compiler un rapport d'étude de sûreté de fonctionnement à la fin de cette phase. Il convient d'aborder le développement du plan pour garantir la sûreté de fonctionnement et documenter la justification des activités proposées ainsi que la définition de la preuve proposée à collecter. Le rapport d'étude de sûreté de fonctionnement vise à démontrer au client que les exigences de sûreté de fonctionnement sont satisfaites avant d'engager les ressources.

6.4 Phase de développement

Lors de la phase de développement, le client fournit généralement une étude de sûreté de fonctionnement pour une seule solution privilégiée. Les exigences de sûreté de fonctionnement peuvent être différentes de celles à la phase de conception, en raison du compromis entre les différentes exigences, qui exige la mise à jour de l'étude de sûreté de fonctionnement.

Grâce à l'analyse continue des exigences de sûreté de fonctionnement, il convient que le fournisseur décide d'une philosophie de conception solide pour la solution privilégiée. Le fournisseur développe et place dans le tableau des preuves la conception détaillée de la solution privilégiée, les affirmations explicites selon lesquelles la conception spécifique satisfait aux exigences et un argument démontrant comment les affirmations sont étayées. Il convient de garantir que les nouveaux risques identifiés lors de l'exécution des activités soient communiqués pour analyse et conception à ce stade de manière ponctuelle et suivie.

En cas de non-exécution lors de la phase de conception, ou si une mise à jour est exigée, il incombe au fournisseur de prendre une initiative et de proposer des objectifs de conception de sûreté de fonctionnement et une base de mesure. Par exemple, le client peut spécifier une exigence de disponibilité mais le fournisseur a besoin d'objectifs de fiabilité et de maintenabilité séparés pour développer le système.

Lors de la phase de développement, il convient que le fournisseur mette à jour le tableau des preuves au fur et à mesure du développement et de la planification et la mise en œuvre des activités. Il convient que le rapport d'étude de sûreté de fonctionnement compilé à la fin de cette phase inclue un tableau des preuves partiellement complété incluant les activités de sûreté de fonctionnement actuelles et futures, leurs critères de réussite et la phase du projet à laquelle la preuve issue de ces activités est produite pour être effective.

6.5 Phase de réalisation

L'étude de sûreté de fonctionnement dans la phase de réalisation a pour principal objet de développer et de remplir l'étude de sûreté de fonctionnement lorsque les activités sont terminées et que la preuve devient disponible. Si l'étude de sûreté de fonctionnement a été correctement gérée pendant les phases de conception et de développement, aucun changement significatif ne devrait affecter les exigences de sûreté de fonctionnement ou les risques qui ont été précédemment identifiés. Néanmoins, de nouveaux risques pourraient être identifiés ou des traitements mis à jour proposés suite aux activités exécutées et à la preuve produite.

Il convient que le fournisseur établisse les rapports d'étude de sûreté de fonctionnement aux délais convenus lors de la phase de réalisation et qu'ils décrivent comment les risques sont traités et qu'ils fournissent au client une confiance accrue que les exigences sont satisfaites. En règle générale, l'acceptation des rapports d'étude de sûreté de fonctionnement par le client est l'une des conditions nécessaires aux paiements provisoires du fournisseur.

Il convient que le client étudie les rapports d'étude de sûreté de fonctionnement produits par le fournisseur. Il convient qu'ils étudient l'argument et la nature de la preuve fournie, notamment les activités entreprises pour traiter les risques, et qu'ils surveillent la réalisation progressive de la sûreté de fonctionnement.

Mais, si le client n'est pas satisfait de la progression du fournisseur, il convient que cela soit géré par les procédures normales du projet. Il convient également que le client considère également s'il existe des risques supplémentaires concernant leur contexte particulier et qu'il mette à jour l'étude de sûreté de fonctionnement en conséquence.

A la fin de la phase de réalisation, si le client est satisfait de l'étude de sûreté de fonctionnement, ceci indique que le système est prêt à être utilisé.

6.6 Phase de l'utilisation

Lorsque le système passe à la phase de l'utilisation, il est important de surveiller et de maintenir la sûreté de fonctionnement du système. Il convient de mettre à jour l'étude de sûreté de fonctionnement afin de refléter les conséquences de problèmes tels que les différences dans le régime d'entretien par rapport à ce qui avait été prévu, la manière dont les utilisateurs interagissent avec le système dans la pratique ou une compréhension plus détaillée de l'environnement d'exploitation.

Il convient que le responsable du système, lorsqu'il est utilisé (qu'il s'agisse du fournisseur ou du client) étudie l'argument, les hypothèses et les informations contextuelles sur lesquels repose l'étude de sûreté de fonctionnement et qu'il vérifie que tout est encore valide. Cet examen peut être réalisé régulièrement ou peut être déclenché par des événements prédéfinis. Il convient que le gestionnaire étudie le registre des risques et qu'il ajoute de nouveaux risques qui peuvent survenir lors de l'utilisation et qui peuvent ne pas avoir été pris en compte par le fournisseur. Il convient d'ajouter la preuve provenant de l'exploitation et/ou des essais et de la maintenance dans l'étude de sûreté de fonctionnement. Il se peut que plusieurs organisations puissent utiliser le système dans différents contextes et développer les études de sûreté de fonctionnement de manière indépendante.

Si la sûreté de fonctionnement mesurée ou atteinte diffère fortement de ce qui a été prédit, il convient d'identifier les raisons possibles de cette différence et de prendre des mesures correctives pour restaurer les niveaux de sûreté de fonctionnement identifiés dans la ou les exigence(s). Si cela n'est pas faisable ou justifiable, par exemple, en raison du coût, le client et le fournisseur pourraient s'accorder pour réviser les exigences. Si la modification des exigences est importante, le client et le fournisseur d'origine peuvent alors retourner à la phase de conception pour s'accorder sur les exigences révisées. En alternative, le client peut initier la phase de l'amélioration pour adapter le système aux modifications. Il convient que le client et/ou le fournisseur considère(nt) également s'il existe des risques supplémentaires eu

égard aux changements, et qu'il(s) mette(nt) à jour l'étude de sûreté de fonctionnement en conséquence.

À la fin de la phase de l'utilisation, il est attendu que l'étude de sûreté de fonctionnement et le tableau des preuves montrent que les exigences de sûreté de fonctionnement ont été satisfaites.

6.7 Phase de l'amélioration

Il arrive souvent que le système exige une amélioration pendant la phase de l'utilisation. Ceci pourrait être effectué par le client, auquel cas il convient que le client développe l'étude de sûreté de fonctionnement. En alternative, cela pourrait impliquer une action du contrat sur le fournisseur. Si tel est le cas, il convient que le fournisseur traite l'amélioration comme un nouveau projet, en redémarrant efficacement l'étude de sûreté de fonctionnement à partir des phases de conception ou de développement, mais en se servant de l'étude de sûreté de fonctionnement précédente comme référence. Il convient que les actions de surveillance du client (voir 6.5) et que les résultats soient également capturés dans l'étude de sûreté de fonctionnement et que l'étude de sûreté de fonctionnement soit gérée en conséquence.

6.8 Phase de la mise hors service

Pour certains systèmes, la phase de la mise hors service peut également nécessiter que l'étude de sûreté de fonctionnement soit mise à jour si, par exemple, il existe des exigences spécifiques pour l'élimination et le démontage du système. Il convient d'observer les mêmes processus de gestion du cas de sûreté de fonctionnement que pour les phases de projet précédentes.

Il arrive également qu'à ce stade la sûreté de fonctionnement du système atteinte puisse être mesurée. Il est recommandé d'étudier les affirmations et preuves contenues dans l'étude de sûreté de fonctionnement pour déterminer si elles ont été atteintes. Ceci peut également fournir les leçons tirées pour les projets futurs.

Les tableaux des preuves et les études de sûreté de fonctionnement accumulées dans les projets réussis peuvent servir de bibliothèque d'éléments réutilisables pour l'organisation, il convient ainsi de les enregistrer dans le système de gestion des connaissances de l'organisation.

7 Évaluation de l'adéquation de la preuve

La robustesse de l'étude de sûreté de fonctionnement à émettre des affirmations de sûreté de fonctionnement dépend de l'adéquation de la preuve utilisée. Il convient que le client étudie par conséquent non seulement l'argument et les affirmations émises dans l'étude de sûreté de fonctionnement mais qu'il considère également l'adéquation de la preuve sur laquelle il est basé.

L'adéquation de la preuve dépend principalement de son impact pratique sur la démonstration de la sûreté de fonctionnement, la réduction de l'incertitude et le traitement des risques. Bien qu'il ne soit pas nécessaire d'évaluer à part entière l'adéquation des activités de sûreté de fonctionnement spécifiques et détaillées, la visibilité, la traçabilité et la qualité de la preuve produite sont des facteurs cruciaux. Il doit ainsi être confirmé que la preuve est générée, gérée, validée et utilisée dans un système de gestion de la sûreté de fonctionnement efficace.

Il convient d'utiliser toutes les informations disponibles pertinentes sur les résultats de la sûreté de fonctionnement et les leçons tirées d'une conception particulière pour garantir la sûreté de fonctionnement dans l'étude de sûreté de fonctionnement. Il n'est pas acceptable d'ignorer la preuve qui réfute l'argument avancé.

Les principaux critères d'évaluation de l'adéquation de la preuve sont les suivants:

a) la preuve dans son ensemble est clairement dérivée d'un programme de sûreté de fonctionnement correctement planifié;

b) les liens entre un élément de preuve spécifique, une exigence de sûreté de fonctionnement, une activité dans le plan de sûreté de fonctionnement et les risques identifiés sont clairs;

c) la preuve est dérivée des activités de sûreté de fonctionnement effectuées par les personnes compétentes avec des ressources adéquates;

d) le statut de chaque élément de preuve, en termes de pertinence, d'intégrité, de précision et de la manière dont il est utilisé pour influencer le système et réduire le risque, peut être facilement identifié dans le tableau des preuves.

Afin d'évaluer l'adéquation de la preuve, il est important de rechercher les méthodes/techniques traçables, les hypothèses et les résultats détaillés. Par conséquent, un dialogue honnête et ouvert entre le client et le fournisseur est important. Un jugement est exigé pour évaluer la preuve présentée, notamment sa visibilité, sa traçabilité et sa qualité conformément aux critères listés dans cet article. L'Annexe C fournit une liste de contrôle de points génériques qui ne sont pas prescriptifs, mais qui fournissent des lignes directrices supplémentaires sur l'évaluation de l'adéquation de la preuve dans des circonstances appropriées.

Annexe A
(informative)

Tableau des preuves

A.1 Généralités

Le tableau des preuves est défini en 5.4. Des exemples d'en-têtes de colonne et de contenu sont décrits ci-après:

Colonne n°	En-tête	Contenu
1	Phase du cycle de vie	Phase correspondante dans le cycle de vie du projet
2	Référence	Référence à l'affirmation
		Référence croisée à la spécification des exigences du projet ou au registre de risques
3	Description de l'affirmation	Description de l'affirmation prise en charge
		Coordination avec la spécification des exigences du projet ou le registre de risques
4	Sous-affirmation	Une description de la sous-affirmation
		Coordination avec la spécification des exigences du projet ou le registre de risques
5	Preuves exigées	Preuve venant à l'appui de la démonstration de l'affirmation ou du traitement des risques de ne pas satisfaire aux exigences (informations, rapports non livrables)
6	Activité de sûreté de fonctionnement	Activité exigée pour générer la preuve nécessaire (toujours une combinaison de sûreté de fonctionnement traditionnelle et d'autres activités, à savoir pas nécessairement une activité ou technique de sûreté de fonctionnement individuelle)
Critères d'acceptation		
7	Preuves	Document/contenu livrable
8	Échéance	Date à laquelle la preuve arrive à échéance pour être effective

Colonne n°	En-tête	Contenu
Statut d'acceptation		
9	Preuves	Références à la dernière preuve, notamment n° de publication et date de livraison
10	Statut d'approbation	Approuvé ou non. En cas de rejet, inclure les motifs et les mesures correctives. En cas d'acceptation, signature de l'autorité d'approbation et date d'acceptation

Deux exemples de tableaux des preuves partiels sont illustrés au Tableau A.1 et au Tableau A.2. Chaque tableau montre des exemples d'affirmations et de risques aux différentes phases du cycle de vie du projet, en partant du principe que le système implique une activité de développement substantielle et à différents niveaux de détail.

Même si chaque ligne du tableau est totalement remplie, les tableaux des preuves n'examinent pas toutes les affirmations prévues ou tous les risques à traiter.

Par conséquent, lors de la création d'un tableau des preuves, il convient de considérer l'ensemble du système, et il est prévu que le tableau des preuves soit beaucoup plus long que les exemples décrits ici. Toutefois, la présentation du tableau peut être utilisée comme modèle.

A.2 Abréviations utilisées uniquement dans la présente annexe

Terme	Terme en français	Equivalent en anglais
BIT	Essai intégré	Built-in test
DRACAS	Système d'enregistrement des données et de mesures correctives	Data recording and corrective action system
HUMS	Système de surveillance de l'intégrité et de l'utilisation	Health and usage monitoring system
ITEAP	Plan d'essai, d'évaluation et d'acceptation intégré	Integrated test, evaluation and acceptance plan
PRAT	Essai d'acceptation de la fiabilité de production	Production reliability acceptance test
OMD	Démonstration d'exploitation et de maintenance	Operational and maintenance demonstration
SMART	Spécifique, mesurable, atteignable, réaliste, temporel	Specific, measurable, achievable, realistic, time-bound
TDP	Plan de développement technologique	Technology development plan

Tableau A.1 – Tableau des preuves pour le système "X"

"Tableau des preuves pour le système X"						Publication:	Date:	Signature:	
Phase du cycle de vie	**Réf**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance/exigée**	**Réf., publication, date**	**Statut d'approbation**
Appel d'offres (pour le développe-ment)		Le système atteint sa fiabilité spécifiée: 99,9 % sur un cycle de service de 24 h (référence d'exigence AAA)	La fiabilité intrinsèque des composants de la solution satisfait aux exigences	Démonstration de la fiabilité intrinsèque par la prévision du nombre de pièces à l'aide des taux de défaillance des pièces	Prévision de la fiabilité du nombre de pièces à l'aide de l'expérience en service de pièces similaires, en utilisant par défaut les sources de données normalisées de l'industrie, par exemple données des fournisseurs de composants ou OTS	Prévision de la fiabilité du nombre de pièces étudiée de manière indépendante.	2 semaines avant la revue de conception préliminaire, mise à jour avant la revue de conception critique	Rapport aa édition 01 en date de zzz	Accepté
			Modes de défaillance et criticité de la/des solution(s) entièrement compris et traités	Risque de manquer les modes de défaillance critiques et les taux de défaillance pour les défauts simples et doubles, la fiabilité ne satisfaisant alors plus à l'objectif (référence de risque BBB)	AMPEC: ces informations sont fournies par l'AMPEC de conception, menée comme pratique de conception	AMPEC étudiée de manière indépendante	Dans le cadre de la prévision de la fiabilité du nombre de pièces	Rapport bb édition 02 en date de yyy	Rejeté. Modes de défaillance critiques pas tous gérés. Reconception effectuée

"Tableau des preuves pour le système X"						Publication:	Date:	Signature:	
Phase du cycle de vie	**Réf**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance/exigée**	**Réf., publication, date**	**Statut d'approbation**
Appel d'offres (pour le développe-ment) (suite)					Essais de développement et DRACAS: a) pour étayer les hypothèses précédentes concernant les modes de défaillance et taux de défaillance; b) pour initier des développements et essais supplémentaires des éléments non satisfaisants et, c) pour initier la sélection de pièces alternatives	Les résultats d'essais démontrent les exigences	2 semaines avant la revue de conception critique	Pas encore arrivé à échéance	
			La solution est conforme à son utilisation prévue	Démonstration de la sûreté de fonctionnement pendant l'utilisation	Développer des propositions de surveillance et de notification des défauts d'exploitation et des performances de maintenance au moyen de la notification des défauts à l'aide de l'analyse de la base de données DRACAS	Projet de plan de démonstration d'exploitation et de maintenance disponible, y compris les critères d'acceptation eu égard à l'exigence relative au cycle de service de 24 h	1) 2 semaines avant la revue de conception finale	Pas encore arrivé à échéance	
						Les résultats d'essais démontrent les	1 an après la mise en service	Pas encore arrivé à	

"Tableau des preuves pour le système X"						Publication:	Date:	Signature:	
Phase du cycle de vie	Réf	Affirmation	Sous-affirmation	Preuves exigées	Activité de sûreté de fonctionnement	Critères de réussite/d'acceptation		Statut d'acceptation	
						Preuves	Échéance/exigée	Réf., publication, date	Statut d'approbation
						exigences		échéance	
Appel d'offres (pour le développe-ment) (suite)		Les exigences BIT du système sont satisfaites (référence d'exigence CCC)	La stratégie d'étude de la testabilité soumet à essai toutes les fonctions exigées	Risque que les exigences de testabilité ne soient pas vérifiées, se traduisant par de faibles performances et/ou un client n'acceptant par l'élément (référence de risque DDD)	Étudier la stratégie d'étude BIT à la lumière de la hiérarchie fonctionnelle développée dans l'AMPEC)	Document interne fournissant les résultats de l'examen et montrant que la stratégie d'étude de testabilité est conforme à la hiérarchie fonctionnelle et aux exigences BIT en matière de: Démarrage. Contrôles continus. Diagnostic. Emplacement	6 semaines avant la revue de conception critique	Pas encore arrivé à échéance	
			La testabilité identifie les modes de défaillance critiques	Risque que la stratégie d'étude de testabilité manque aux fonctions critiques, l'exigence n'étant alors pas satisfaite (référence de risque EEE)	Extension de l'AMPEC pour fournir une évaluation de la couverture BIT	Le rapport d'évaluation BIT montre que la testabilité du système satisfait aux exigences BIT; Démarrage. Contrôles continus. Diagnostic. Emplacement	6 semaines avant la revue de conception finale	Pas encore arrivé à échéance	
		L'intégration des derniers équipements technologiques et de communication dans la conception ne compromet la sûreté de fonctionnement de l'ensemble du système (référence	L'installation d'équipements neufs ne limite pas l'accès au reste du système pour la maintenance	Le risque que l'accès prévu pour la maintenance soit limité est traité par le plan de démonstration technologique (TDP), comprenant les évaluations de la sûreté de fonctionnement	Prévisions de sûreté de fonctionnement effectuées pour soutenir le TDP	Le rapport de prévision de la sûreté de fonctionnement du TDP démontre que la conception n'est pas compromise par la nouvelle technologie	6 semaines avant la revue de conception critique	Pas encore arrivé à échéance	

"Tableau des preuves pour le système X"						Publication:	Date:	Signature:	
Phase du cycle de vie	**Réf**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance/exigée**	**Réf., publication, date**	**Statut d'approbation**
		d'exigence FFF)		(référence de risque GGG)					
			Les nouveaux systèmes technologiques ne produisent pas trop de chaleur ayant un impact sur les performances du système existant	Le risque de production de chaleur en excès est traité par le plan de démonstration technologique (TDP) comprenant l'évaluation des charges calorifiques et leur impact sur le système existant (référence de risque HHH)	Prévisions de sûreté de fonctionnement effectuées pour soutenir le TDP	Le rapport de prévision de la sûreté de fonctionnement du TDP démontre que la conception n'est pas compromise par la nouvelle technologie	6 semaines avant la revue de conception critique	Pas encore arrivé à échéance	
Mise au point		Le sous-système z présente une durabilité pour la durée de vie exigée (exigence III)	Les mécanismes d'usure sont entièrement compris et gérés	Risque que l'usure ne soit pas comprise par l'évaluation de la durée de vie prévue et la détermination des modifications nécessaires à apporter pour satisfaire aux exigences (référence de risque JJJ)	Revue des données de durée de vie sur les articles similaires et évaluation environnementale/calculs de contraintes, pour déterminer les facteurs de vieillissement et les composants critiques	Calculs de contraintes, justification des modifications de conception nécessaires et plan d'essai de durée de vie accélérée	3 mois après l'attribution du contrat	Rapport dd édition 01 en date de www	Accepté
					Essais de durée de vie accélérée à l'aide de la méthodologie d'essai de durée de vie très accélérée	Rapport d'essai de durée de vie accélérée pour garantir que la conception finale satisfait à l'exigence relative à la durée de vie	6 mois après la réception du/des modèle(s) d'essai	Pas encore arrivé à échéance	

"Tableau des preuves pour le système X"						Publication:	Date:	Signature:	
Phase du cycle de vie	**Réf**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance/exigée**	**Réf., publication, date**	**Statut d'approbation**
Réalisation		La durée de vie du châssis n'est pas réduite pendant l'assemblage du système (les activités d'assemblage incluant le chargement, qui est très différent lorsque le système est complet) (référence d'exigence KKK)	Les contraintes/la fatigue pendant l'assemblage ne réduisent pas la durée de vie du châssis	Le risque de contrainte/fatigue excessive est traité par l'analyse des charges sur le châssis lorsqu'il est suspendu; détermination des modifications apportées à la conception du châssis et/ou aux accessoires de fabrication pour garantir que la durée de vie du châssis n'est pas compromise. (référence de risque LLL)	Évaluation du cas de charge	Rapport, y compris les dossiers d'analyse et de calcul, montrant les marges de contraintes acceptables. Le rapport souligne les zones de surcontrainte potentielle et justifie les modifications, si nécessaire, pour garantir des marges adéquates.	3 mois avant l'achèvement de la phase de réalisation	Pas encore arrivé à échéance	
				Démonstration des processus de fabrication	Essai d'acceptation de la fiabilité de production (PRAT)	1) Plan d'essai PRAT. 2) Résultats d'essai PRAT garantissant l'intégrité du châssis pour la fabrication	1) Plan PRAT exigé avant le début de la production. 2) Résultats d'essai PRAT après l'exécution du PRAT	Pas encore arrivé à échéance	
					Examen de la qualité finale des produits livrés	Dossiers d'examen de qualité démontrant une qualité adéquate	Pendant la production	Pas encore arrivé à échéance	

Tableau A.2 – Tableau des preuves pour un système Y

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
Conception		La fiabilité du système répond aux besoins du client	Les exigences relatives à la sûreté de fonctionnement sont bien identifiées par le client et/ou sont complètes	Risque que les attributs du système de sûreté de fonctionnement critiques n'aient pas été identifiés, donnant lieu à des exigences non satisfaites	Analyse des écarts de fonctionnalités. Analyse opérationnelle	Le document relatif aux exigences a été signé par les principaux intervenants, actant de son exhaustivité et de sa pertinence	Très tôt dans la phase de conception, avant la soumission du dossier initial	Rapport ee édition 03 en date de vvv	Accepté
			Aspects relatifs à la sûreté de fonctionnement traités dans l'ingénierie des systèmes. Par conséquent, l'impact de la sûreté de fonctionnement sur la fonctionnalité est entièrement compris. Les exigences relatives à la sûreté de fonctionnement sont SMART	Le risque que la sous-affirmation ne soit pas satisfaite est traité par: 1) développement des objectifs de disponibilité de la phase d'utilisation. 2) Numéros de système adéquats. 3) Objectifs de sûreté de fonctionnement initiaux associés à la disponibilité de la phase d'utilisation. 4) Évaluation de l'impact de la sûreté de fonctionnement sur l'efficacité opérationnelle ne montrant aucun effet défavorable	Études des besoins et des quantités (avec entrée de la sûreté de fonctionnement). Modélisation de la disponibilité	Le document inclut les objectifs de disponibilité opérationnelle dans la section de durabilité et découpe d'abord les objectifs de sûreté de fonctionnement			

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
Conception (suite)		Le client a correctement géré la sûreté de fonctionnement afin d'obtenir de bonnes caractéristiques de sûreté de fonctionnement. Les ressources adaptées et efficaces sont en place	Les coûts en aval sont optimisés/limités suite à la gestion efficace de la sûreté de fonctionnement	Risque que le client ne fasse pas le lien entre la sûreté de fonctionnement et le coût de propriété donnant lieu à des coûts en aval plus important	Contribution de la sûreté de fonctionnement dans la prise de décision d'investissement et la modélisation du coût du cycle de vie, y compris le coût (et la durée) d'obtention du niveau exigé de sûreté de fonctionnement	Plans clairement alignés sur la production des précédents projets. Les estimations réalistes du financement et des nombres d'équipements ont été préparées et incluses dans le plan d'exécution du projet en garantissant que la disponibilité et la fiabilité sont incluses dans ces études préalables comme moteurs de coût. Équipe en place.	Très tôt dans la phase de conception, avant la soumission du dossier initial	Plan d'exécution du projet réf. ff édition 02 en date de uuu	Accepté
			Le programme satisfait aux exigences d'échelle de temps du mécène	Risque que le client n'arrive pas à considérer l'impact des exigences sur le besoin d'une technologie complexe ou nouvelle, retardant le programme	Évaluation des risques technologiques, y compris les études de faisabilité examinant la maturité de la technologie susceptible d'être utilisée dans les options de solution	1) Rapports montrant les avancées de la recherche. Formulation de plans de démonstration des technologies. 2) Contribution de l'industrie via des équipes partenaires		1) Rapport gg édition 01 en date du ttt .Rapport hh édition 01 en date du sss.2) Équipe mobilisée	Rapport gg accepté. Rapport hh rejeté et réécrit
			Les risques temporels sont correctement gérés et limités	Risque que le client ne comprenne pas les risques temporels clés, donnant lieu à un manque de fiabilité et/ou des retards dans le programme	Évaluation des risques temporels par comparaison à des projets analogues, connexes ou historiques	Analyses pour montrer que les échelles de temps ont été planifiées conformément aux risques technologiques et techniques. Planning accepté et convenu		Planning ii édition 07 en date de rrr	Accepté

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	Réf.	Affirmation	Sous-affirmation	Preuves exigées	Activité de sûreté de fonctionnement	Critères de réussite/d'acceptation		Statut d'acceptation	
						Preuves	Échéance	Réf., Publication, date:	Statut d'approbation
Conception (suite)			L'assurance de sûreté de fonctionnement par le fournisseur satisfait aux normes	Risque que le client n'arrive pas à souligner la stratégie d'assurance, donnant lieu à une absence de preuves adaptées et provoquant l'insatisfaction du client	Un plan de sûreté de fonctionnement convenu	Un projet de plan de sûreté de fonctionnement soulignant les éléments, le travail et la stratégie pour traiter les principaux risques. Déclaration de travail pour les études de la phase de conception dans le dossier initial. Le plan inclut les critères d'acceptation du client	Très tôt dans la phase de conception, avant la soumission du dossier initial	Rapport jj projet C en date de qqq	Accepté
Appel d'offres (pour le développe-ment)		Les preuves étayant la sûreté de fonctionnement sont pertinentes et correctes, et satisfont aux besoins/attentes du client	Le client et le fournisseur ont communiqué et se sont entendus sur les exigences et les objectifs	Risque que le fournisseur ne comprenne pas les exigences du client, les preuves étayant la sûreté de fonctionnement étant de ce fait développées de manière ad hoc et ne répondant pas aux besoins/attentes du client	Prévisions de la fiabilité basées sur les taux de défaillance des équipements similaires et les facteurs appliqués en raison de différences dans le cycle de service, l'utilisation, la complexité, etc., donnant lieu aux exigences de sûreté de fonctionnement	Exigences de sûreté de fonctionnement claires avec les preuves exigées contenues dans le rapport d'étude de sûreté de fonctionnement adressé au fournisseur	Très tôt dans la phase de développement, avant la soumission du dossier final	Pas encore arrivé à échéance	
					Détails de l'analyse de la phase d'utilisation et études de la disponibilité opérationnelle	Registre des risques initial			

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	Réf.	Affirmation	Sous-affirmation	Preuves exigées	Activité de sûreté de fonctionnement	Critères de réussite/d'acceptation		Statut d'acceptation	
						Preuves	Échéance	Réf., Publication, date:	Statut d'approbation
Appel d'offres (pour le développement) (suite)		Le client sélectionne la solution optimale du point de vue de la sûreté fonctionnelle, de manière à atteindre les objectifs de sûreté de fonctionnement	Le mécanisme de sélection inclut la sûreté de fonctionnement et a été rigoureusement et efficacement utilisé	Risque que le mécanisme de sélection n'arrive pas à traiter rigoureusement la sûreté de fonctionnement, de sorte que la sûreté de fonctionnement n'est pas atteinte	Estimations de la fiabilité des options de conception. Études d'évaluation permettant d'entrer les estimations de sûreté de fonctionnement avec d'autres attributs dans un système de sélection d'option structuré	Rapports de sélection d'option démontrant que la sûreté de fonctionnement a été intégrée dans le processus de sélection	Dans la phase de développement, avant la soumission du dossier final	Pas encore arrivé à échéance	
				Risque qu'une importance inappropriée soit donnée à la sûreté de fonctionnement dans la méthode d'évaluation de la sûreté de fonctionnement, de sorte que les autres attributs soient affectés, quelle que soit l'importance de la sûreté de fonctionnement	Ébauche de questions concernant l'évaluation de la sûreté de fonctionnement, garantissant qu'il est accordé un poids égal à la performance, au temps et au coût en matière de sûreté de fonctionnement	Les scores finals de l'évaluation de l'offre, plus les principaux risques et étapes de réalisation de la sûreté de fonctionnement nécessaires pour s'engager pour la production de preuves de sûreté de fonctionnement sont contenus dans le rapport d'étude de sûreté de fonctionnement	Dans la phase de développement, avant la soumission du dossier final		
				Risque que les risques technologiques liés à chaque option ne soient pas correctement évalués, les exigences n'étant alors	Évaluation de la complexité logicielle potentielle via des mesures de	Les rapports de sélection d'option incluent une évaluation de la sûreté de fonctionnement logicielle	Dans la phase de développement, avant la soumission du	Pas encore arrivé à échéance	

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
				pas satisfaites	la taille et de la complexité du logiciel	au cours de la durée de vie	dossier final		
Appel d'offres (pour le développe-ment) (suite)					Lignes directrices en matière de conception de la sûreté de fonctionnement du projet et définition de la manière dont ces lignes directrices doivent être affectées	L'acceptation des acteurs concernant les lignes directrices de conception de la sûreté de fonctionnement du projet a été obtenue	Dans la phase de développement, avant la soumission du dossier final	Pas encore arrivé à échéance	
Développement		Le fournisseur comprend parfaitement l'objet des exigences, les objectifs étant alors alignés avec ceux du client	Le fournisseur et le client ont communiqué et se sont entendus sur l'objet des exigences, eu égard en particulier au respect des contraintes environnementales	Risque que le fournisseur n'ait pas mesuré l'impact des contraintes environnementales sur la sûreté de fonctionnement, les exigences n'étant alors pas satisfaites	Analyse du cycle de service, des charges, des niveaux de température, des niveaux de vibrations. Analyse de l'environnement d'exploitation et des modes de fonctionnement exigés Analyse des effets d'accumulation des dommages, de la poussière, de l'infiltration de saletés, de	Le rapport d'étude de sûreté de fonctionnement du fournisseur démontre que les facteurs environnementaux et les charges du cycle de service ont été compris et influencent la conception	Fourni avec l'appel d'offres ou très tôt dans la phase de réalisation		

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
					l'humidité, etc.				
Développement (suite)		Le fournisseur a reconnu et traité les risques liés à la sûreté de fonctionnement de manière à satisfaire aux exigences de sûreté de fonctionnement	Une gestion adéquate des risques a été mise en place et a inclus la sûreté de fonctionnement aux risques du projet.	Risque que le fournisseur n'arrive pas à impliquer le personnel chargé de la sûreté de fonctionnement dans l'identification formelle des risques, les risques n'étant alors pas identifiés ni traités.	Identification des risques associés à la sûreté de fonctionnement. Analyse de la résistance de la conception des composants critiques par rapport aux charges du cycle de service.	Examen par le client de la matrice des risques fournisseur étayée par les rapports d'étude de sûreté de fonctionnement montrant:	Très tôt dans le processus de conception pour influencer la conception des équipements prototypes	Pas encore arrivé à échéance	
				Risque que les registres des risques ne soient pas intégrés, donnant lieu à un défaut d'alignement entre la sûreté de fonctionnement et les risques du projet.	Prévisions et modélisation pour identifier les systèmes critiques.	– la modélisation à l'aide d'entrées mesurées (charges), pour garantir que la résistance de conception des sous-systèmes et composants critiques est adéquate pour satisfaire aux besoins de la mission, et qu'ils présentent la durabilité nécessaire pour continuer à fonctionner pendant la durée de vie prévue des équipements;			
					Analyse des problèmes d'interface et	– une analyse structurée des modes de défaillance potentiels pour			

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
					d'intégration	garantir que tous les problèmes d'interface et d'intégration sont traités et ne sont pas ignorés comme causes de manque de fiabilité; – la modélisation de la fiabilité, les prévisions et les allocations pour déterminer la criticité			
Développement (suite)		Les composants OTS fonctionnent comme prévu pendant la phase de développement	Composants OTS adaptés utilisés dans la conception	Démonstration des prévisions de sûreté de fonctionnement étayées par les données en service pour les sous-systèmes OTS	Études d'évaluation où les estimations de la sûreté de fonctionnement pour les sous-systèmes OTS considèrent les données existantes et l'impact des différences entre la nouvelle application et celles applicables aux données sources	Rapport examiné de manière indépendante.	Fourni avec l'appel d'offres ou très tôt dans la phase de développement	Pas encore arrivé à échéance	
						Les rapports de sélection d'option incluent des prévisions réalistes pour la sûreté de fonctionnement des sous-systèmes OTS			

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
Développement (suite)		Les essais sont efficaces, les résultats d'essai pouvant être correctement formulés	La conception se sert de la notification automatique de l'utilisation et des défauts pour enregistrer l'état et l'utilisation du système	Risque que les événements ne puissent pas être formulés pendant les essais, tous les paramètres d'entrée n'étant pas connus et, de ce fait, la sûreté de fonctionnement ne pouvant pas être mesurée	HUMS à mettre en application de manière effective et efficace comme une partie du processus de conception	Rapport d'analyse de maintenabilité identifiant les fonctions couvertes par l'HUMS	Fourni avec l'appel d'offres ou très tôt dans la phase de développement	Pas encore arrivé à échéance	
		Le système a atteint les niveaux de sûreté de fonctionnement exigés suite à la transition du développement à l'utilisation	La transition du développement à l'utilisation est correctement gérée, et les activités exigées sont réalisées	Risque que le fournisseur s'attende à ce que les problèmes de sûreté de fonctionnement soient traités par le client pendant l'utilisation, donnant lieu à une faible sûreté de fonctionnement et une insatisfaction du client	Identification des risques et des activités de sûreté de fonctionnement planifiées pour traiter ces risques, avec la fonctionnalité technique, les ressources et les contrôles/critères de réussite pour garantir que cela se produit	Plan de sûreté de fonctionnement du fournisseur comprenant: – gestion de la sûreté de fonctionnement et structure organisationnelle claires; – plan systématique des activités pour satisfaire aux exigences de sûreté de fonctionnement définies par rapport aux risques identifiés; – activités de sûreté de fonctionnement avec des objectifs clairs et des critères de réussite; – activités de sûreté de fonctionnement planifiées en temps voulu pour influencer la conception;	Pendant des propositions du projet et aux étapes préliminaires de développement	Pas encore arrivé à échéance	

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
						– allocations d'objectifs de sûreté de fonctionnement aux sous-traitants; – plans et rapports d'étude de sûreté de fonctionnement des sous-traitants; – plan d'essai et d'évaluation clair; – étapes de sûreté de fonctionnement planifiées pour la réalisation de la sûreté de fonctionnement avec des examens périodiques			
Développement (suite)		Le fournisseur effectue des essais adéquats pour fournir des preuves suffisantes afin de démontrer les exigences à la satisfaction du client	Les critères d'essai et d'évaluation ont été formellement convenus entre le fournisseur et le client	Démonstration de la sûreté de fonctionnement par des données de conception, d'essai et d'évaluation assurant un niveau de fiabilité technique et statistique selon lequel la conception du prototype de préproduction a satisfait aux exigences de sûreté de fonctionnement	Exécuter, surveiller et examiner les activités du plan de sûreté de fonctionnement, modifier si nécessaire	Acceptation des rapports de justification de la sûreté de fonctionnement du fournisseur par le client, montrant: – les changements de conception résultant des conclusions des études de conception (analyse des contraintes, AMPEC, etc.); DRACAS détaillé et efficace; – résultats d'essai des composants;	Pendant le développement avant l'acceptation et la réalisation du système	Pas encore arrivé à échéance	

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
						– résultats d'essai des sous-systèmes; – autres résultats d'essai; – résultats d'essai de développement de la fiabilité; – essais de démonstration de la fiabilité; – résultats d'essais d'exploitation et de maintenance; – résultats d'essais de performance; – informations sur l'action de revue de conception; – données sur le terrain des autres utilisateurs			
Développement (suite)		La fiabilité des progiciels OTS n'est pas affectée lors de l'intégration dans le système	Les interfaces OTS sont compatibles avec l'architecture logicielle du système	Démonstration que les essais d'intégration dans le laboratoire d'intégration logicielle n'ont aucun impact sur les résultats de la sûreté de fonctionnement. Inclue le processus d'essai, d'analyse et de correction signalé par le DRACAS formel	Rapport DRACAS issu des activités d'essai et de développement	Le rapport DRACAS montre les preuves de ce qui suit: – modifications de conception entraînant une fiabilité accrue; – entrée dans les rapports de prévision de la sûreté de fonctionnement pour	Pendant le développement avant la phase d'acceptation et de réalisation du système	Pas encore arrivé à échéance	

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
						couvrir les cycles des taux de défaillance logicielle potentielle			
Réalisation		Le système a atteint les niveaux de sûreté de fonctionnement exigés suite à la transition du développement à l'utilisation	Le fournisseur a pris en compte et géré l'étendue des changements entre le prototype et le système de production	Risque que la transition du développement à l'utilisation soit mal gérée et que les activités ne soient pas effectuées par manque de temps, entraînant une faible sûreté de fonctionnement initiale	Preuves que les leçons tirées des constructions prototypes de préproduction ont influencé le processus de production.	Rapports d'étude de sûreté de fonctionnement du fournisseur montrant ce qui suit: – résultats des essais de confirmation/qualification de la production; – résultats du premier lot d'essais d'acceptation de la fiabilité de production (PRAT); – preuves des changements de procédures de production et de qualité pour capturer les défauts; – indicateurs de fonctionnalités des processus Six Sigma	Avant et pendant la phase de réalisation initiale	Pas encore arrivé à échéance	
					Données d'essai et d'évaluation suffisantes et garantie technique et statistique que la norme de construction de production satisfait aux exigences de sûreté de fonctionnement et montrer que la				

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
					fiabilité n'a pas été dégradée par le processus de production				
Réalisation (suite)					Processus de production et de qualité matures tout au long de la conception du prototype de préproduction.				
					Procédures d'étude et de correction des défauts, défaillances et pannes				
		Les articles produits sont de qualité acceptable.	Le fournisseur a un site et des processus de production matures.	Démonstration de la qualité de fabrication consistante (plan d'essais PRAT)		Résultats d'essais du lot PRAT.	Aux points convenus pendant la phase de réalisation	Pas encore arrivé à échéance	
			Le fournisseur effectue une surveillance adaptée et suffisante.	Démonstration de la mise en œuvre de procédures de qualité efficaces		Dossiers d'examen de qualité			
		Les composants OTS fonctionnent comme prévu pendant la réalisation	Les informations d'assemblage des équipements OTS sont adaptées à l'application	Démonstration de la qualité d'assemblage/d'intégration cohérente des composants OTS grâce au plan d'essais PRAT.		Résultats d'essais du lot PRAT. Dossiers d'examen de qualité	Aux points convenus pendant la phase de réalisation	Pas encore arrivé à échéance	
				Démonstration de la mise en œuvre de procédures					

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
				de qualité efficaces pour l'assemblage et l'intégration					
Utilisation		Le changement d'utilisation, d'environnement et de support est identifié et bien géré	Le client a spécifié les exigences de prise en charge du système	Risque de dégradation de la sûreté de fonctionnement suite à une prise en compte inappropriée du changement d'utilisation, de prise en charge et d'environnement	Données d'utilisation et de défaillance des équipements avec analyse appropriée pour fournir les estimations de fiabilité et les tendances des défaillances. Identification des modes de défaillance systématiques et introduction de modifications via des services postconception Données sur les coûts de réparation et les ressources	Résultats d'essais de démonstration d'exploitation et de maintenance (OMD). Résultats d'étude de sûreté de fonctionnement OMD. Collecte et analyse des données OMD	Au début et pendant la phase d'utilisation	Pas encore arrivé à échéance	
Utilisation/mise hors service		Des leçons ont été tirées du projet afin d'éviter les problèmes dans les projets à venir	Les responsabilités relatives à la propriété et à la notification du système sont définies par le client	Risque que les leçons tirées ne soient pas appliquées aux projets futurs, n'ayant pas été capturées ou diffusées par le client, ce qui entraîne des problèmes récurrents	Dossier complet de tous les éléments du travail de sûreté de fonctionnement, de la conception à l'utilisation ou à la mise hors service, issu des leçons régulières tirées des	Résultats d'études anticipés	Pendant toute la durée d'utilisation et de mise hors service	Pas encore arrivé à échéance	

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	**Réf.**	**Affirmation**	**Sous-affirmation**	**Preuves exigées**	**Activité de sûreté de fonctionnement**	**Critères de réussite/d'acceptation**		**Statut d'acceptation**	
						Preuves	**Échéance**	**Réf., Publication, date:**	**Statut d'approbation**
					activités				
Utilisation/mise hors service (suite)			L'équipe du client est uniquement démobilisée lorsque l'assurance et les leçons tirées ont été réalisées		Rassemblement de l'ensemble des documents d'exigences, données de sûreté de fonctionnement et rapports dans un référentiel de données d'entreprise	Exigences de sûreté de fonctionnement matures			
					Production d'un rapport final des leçons tirées donnant des informations sur l'efficacité du plan et les estimations de sûreté de fonctionnement finales atteintes	Extraits du plan de gestion au cours de la durée de vie.			
						Résultats des réunions de sûreté de fonctionnement (plan de sûreté de fonctionnement, etc.).			
						ITEAP et rapports d'acceptation			

Tableau des preuves pour un système Y					Publication:	Date:		Signature:	
Phase du cycle de vie	Réf.	Affirmation	Sous-affirmation	Preuves exigées	Activité de sûreté de fonctionnement	Critères de réussite/d'acceptation		Statut d'acceptation	
						Preuves	Échéance	Réf., Publication, date:	Statut d'approbation
						Étude de sûreté de fonctionnement entièrement renseignée avec tous les rapports de preuves sur la sûreté de fonctionnement Étude de sûreté de fonctionnement entièrement renseignée avec tous les rapports de preuves sur la sûreté de fonctionnement (notamment l'utilisation en matière d'exploitation et de maintenance)			
						Analyse des leçons tirées			

Annexe B
(informative)

Exigences générales relatives au rapport d'étude de sûreté de fonctionnement

B.1 Généralités

Cette annexe fournit les en-têtes et décrit le contenu des sections dans le rapport d'étude de sûreté de fonctionnement. Il n'est pas envisagé que cette structure soit adaptée à chaque projet, mais elle permet de fournir des lignes directrices sur les informations qu'il convient de trouver dans les rapports.

Le rapport d'étude de sûreté de fonctionnement fournit les preuves de la sûreté de fonctionnement à une étape spécifique convenue du cycle de vie. Les rapports présentent un argument basé sur les affirmations qui, à son tour, est basé sur les preuves et hypothèses que le système satisfait aux exigences de sûreté de fonctionnement. Il n'est pas prévu que le rapport contienne toutes les preuves produites jusqu'à cette étape, mais résume et fait office de "panneau de signalisation", indiquant où les preuves détaillées peuvent être trouvées.

La présente norme fait référence à la sûreté de fonctionnement qui pourrait être considérée pour suggérer que les preuves documentaires de la fiabilité et de la maintenabilité sont résumées dans un seul rapport. Si le tableau des preuves exige des rapports séparés, ou si le client ou le fournisseur considère qu'avoir des rapports séparés présente une image plus claire ou fournit une approche plus ciblée, les rapports d'étude de fiabilité et de maintenabilité séparés sont considérés comme parfaitement acceptables.

Si approprié, pour améliorer la lecture et le transfert d'informations, il convient que les rapports d'étude de sûreté de fonctionnement associés à un projet donné essaient d'adopter un format commun.

B.2 Éléments nécessaires pour un rapport d'étude de fonctionnement

Il convient que chaque rapport d'étude de sûreté de fonctionnement liste et fasse référence aux exigences dans le tableau des preuves, par rapport auquel les preuves doivent être évaluées et être traçables en relation avec les exigences originales du client.

Il convient que le rapport d'étude de sûreté de fonctionnement souligne également le contexte, l'objet et le domaine d'application du rapport, en détaillant par exemple:

a) une vue d'ensemble des circonstances qui ont conduit au besoin et au développement du rapport d'étude de sûreté de fonctionnement;
b) l'objet du rapport d'étude de sûreté de fonctionnement, à savoir pourquoi et pour qui il a été produit;
c) le domaine d'application et les limites du rapport d'étude de sûreté de fonctionnement;
d) ce que couvre (et ne couvre pas) le rapport;
e) les limites de responsabilités eu égard au contrôle managérial et aux autres acteurs;
f) les relations avec d'autres rapports, si applicable;
g) l'applicabilité et le respect des réglementations et normes en vigueur.

B.3 Contexte et hypothèses

B.3.1 Acteurs

Cet article décrit les acteurs intéressés par le système, leurs attentes et les exigences qui en résultent.

B.3.2 Description du système

Il convient que la description du système comporte les points ci-dessous:

a) Description physique – il convient que ce point décrive brièvement les caractéristiques physiques ou fonctionnelles du système.

b) Limites du système – il convient que ce point décrive brièvement les limites physiques ou fonctionnelles du système. Les blocs-diagrammes peuvent fournir une bonne méthode pour illustrer les limites du système considérées dans l'étude de la sûreté de fonctionnement (voir IEC 61078).

c) Exploitation – il convient que ce point décrive le rôle principal ou la fonction principale du système et les rôles secondaires. Il convient que ce point inclue son cycle de service anticipé type.

d) Environnement – il convient que ce point décrive les environnements d'exploitation du système.

e) Interfaces avec les autres équipements/systèmes – il convient que ce point définisse les équipements associés aux entrées, conclusions et services pour le système concerné. Si approprié, il convient que ce point décrive également ces équipements situés physiquement à côté du système installé.

f) Utilisateurs et interfaces homme-machine exigées – il convient que ce point décrive les personnes qui utilisent le système et les interfaces qu'elles ont avec le système.

g) Norme de construction/version logicielle – il convient que ce point fasse référence à une norme de construction spécifique du système, notamment les versions logicielles, si approprié.

h) Contrôle de configuration – pour garantir que le rapport reflète la dernière norme de construction/version, il convient que la description indique où la dernière norme de construction/version est définie, par exemple, l'index des enregistrements principal.

i) Niveaux de qualification du personnel – il convient de décrire le niveau de qualification et la formation exigés pour exploiter et entretenir le système.

j) Politique de maintenance – il convient que celle-ci décrive les systèmes de prise en charge pour chaque rôle du système ou profil de cycle de service anticipé.

B.3.3 Exigences relatives à la sûreté de fonctionnement

Il convient que cette section reflète les exigences du client et la compréhension de ces exigences par le fournisseur et comment elles doivent être mesurées. Il convient que les exigences soient considérées dans leur plus large contexte de manière à ce qu'elles incluent les exigences relatives à l'environnement et à l'utilisation, ainsi que les exigences de sûreté de fonctionnement explicitement définies. Il convient que le fournisseur décrive comme les exigences ont été interprétées pour la solution de conception proposée et développées dans la sûreté de fonctionnement visée du projet.

B.3.4 Limites d'utilisation

Il convient que cette section définisse les limites d'utilisation du système ou le contexte dans lequel les arguments sont émis, ce qui, en cas de dépassement, signifie que les affirmations de sûreté de fonctionnement pourraient ne pas être valides. Ces limites incluent les paramètres d'exploitation du système, l'environnement et les activités de maintenance importantes.

B.3.5 Hypothèses

Il convient que toutes les hypothèses soient explicitement identifiées, soit dans le rapport d'étude de sûreté de fonctionnement soit dans un registre d'hypothèses séparé. Si possible, il convient que les activités pour valider les hypothèses soient identifiées et incluses dans le tableau des preuves.

B.4 Risques

Grâce à l'analyse des exigences de sûreté de fonctionnement, il convient que le fournisseur identifie les risques associés au système qui ne satisfont pas aux exigences de sûreté de fonctionnement et comment ces risques seront ou ont été traités pendant le projet. Ces informations se trouvent en principe dans le tableau des preuves.

B.5 Plan de sûreté de fonctionnement

Il convient que le fournisseur détermine comment il a l'intention de satisfaire aux exigences et de le démontrer et de fournir l'assurance nécessaire. Cette section justifie les activités dans le plan de sûreté de fonctionnement du fournisseur et identifie les critères de réussite de ces activités.

B.6 Tableau des preuves

Il convient que cette section fournisse une vue d'ensemble complète des preuves, que ce soit pendant les phases de développement et de réalisation ou pendant l'utilisation du système. Il convient également d'indiquer quand et par qui les rapports d'étude de sûreté de fonctionnement doivent être établis. Les entrées spécifiques dans le tableau des preuves peuvent être sélectionnées par le client et peuvent être associées aux étapes de paiement à des fins de contrôle.

B.7 Élément de preuve

Il convient que cette section indexe les preuves existantes. Voir 5.3 pour des exemples de types de preuves qui pourraient être inclus. Il convient que chaque élément de preuve soit référencé dans le tableau des preuves et dans les affirmations qu'il démontre ou les risques qu'il traite.

Il convient que l'élément de preuve trace également l'historique des révisions et mises à jour de la philosophie de conception de la sûreté de fonctionnement, des objectifs et du plan, qui les adaptent avec le statut variable des risques d'origine, ainsi que les nouveaux risques/risques émergents. Il convient que l'élément de preuve fasse la distinction entre les preuves factuelles et les arguments ou la déduction tirée des faits.

B.8 Examen des preuves actuelles

Il convient que cette section fournisse un examen équilibré de l'élément de preuve en termes d'intégralité, de ponctualité et d'acceptabilité eu égard aux critères contenus dans le tableau des preuves.

B.9 Affirmations et argument de la sûreté de fonctionnement

Cette section contient l'argument qui étaie les affirmations selon lesquelles le système satisfait à chacune des exigences de sûreté de fonctionnement. Il convient que cette section fournisse le raisonnement expliquant pourquoi chacune des exigences est, ou sera, satisfaite pendant l'utilisation, en fonction du contexte, des preuves et des hypothèses.

Il convient que toutes les hypothèses soient listées explicitement ou qu'une liste d'hypothèses soit référencée. Au début de la phase d'utilisation, il convient que les principales hypothèses restantes soient explicitement soulignées, avec les limites d'utilisation qui peuvent en résulter.

B.10 Conclusions et recommandations

Il convient que cette section contienne un journal des conclusions tirées des preuves de sûreté de fonctionnement accumulées jusqu'à présent, y compris s'il est probable que le système satisfasse à ses exigences de sûreté de fonctionnement. Ceci inclut de faire référence aux conclusions des publications précédentes du rapport d'étude de sûreté de fonctionnement et de décrire comment les arguments ont changé.

Dans les publications provisoires, il convient d'indiquer si le projet passe à l'étape suivante ou quel travail supplémentaire est exigé pour permettre au projet d'avancer. De plus, il convient d'indiquer les activités qu'il convient d'effectuer à l'avenir pour générer l'assurance nécessaire que les exigences de sûreté de fonctionnement sont satisfaites.

Il convient de résumer et traiter le statut des hypothèses, preuves, arguments, affirmations et risques résiduels. Il convient de tirer les conclusions eu égard au statut de l'assurance progressive et les activités nécessaires pour traiter les risques résiduels.

Il convient que les recommandations soient basées sur les pénuries actuelles de preuves disponibles et il convient de proposer des modifications, si approprié, de la philosophie de conception, des objectifs et des activités de sûreté de fonctionnement afin de garantir que le système satisfait à chacune des exigences de sûreté de fonctionnement.

Annexe C
(informative)

Liste de contrôle des points pour évaluer l'adéquation des preuves

La présente annexe fournit une liste de contrôle qu'il convient de considérer comme une invitation à initier une action lorsque les points de la liste de contrôle sont pertinents et n'impliquent pas de réponse "Oui" et "Non". Un jugement est nécessaire pour évaluer les preuves présentées. Il convient de ne pas considérer la liste de contrôle comme étant prescriptive ou exhaustive. Elle est générique et donne les lignes directrices venant à l'appui des lignes directrices générales fournies à l'Article 7 de la présente norme.

Liste de contrôle:

1) Les objectifs de l'activité sont-ils clairement définis?
2) L'activité a-t-elle été exécutée de manière systématique et est-elle terminée?
3) L'activité a-t-elle été exécutée à un moment qui permet d'influencer la conception?
4) L'activité reflète-t-elle correctement l'utilisation et l'environnement du système et est-ce que cela a été documenté?
5) L'activité a-t-elle été exécutée pour refléter les limites physiques et fonctionnelles du système?
6) Des hypothèses sont-elles enregistrées (par exemple, entrées d'autres systèmes ou services) et sont-elles réalistes et raisonnables?
7) Une justification est-elle donnée pour la méthode/technique d'activité utilisée, et est-elle raisonnable?
8) Qui a été consulté pendant l'activité (par exemple, utilisateur, agent de maintenance, concepteur)? Ce niveau de consultation était-il raisonnable?
9) Les recommandations relatives à l'activité sont-elles clairement définies, et sont-elles raisonnables?
10) Les preuves documentaires indiquent-elles que les recommandations ont été mises en application?
11) Les résultats de l'activité ont-ils été progressivement mis à jour pour refléter la dernière conception, et ont-ils été utilisés comme intrants dans les revues de conception?

Bibliographie

Documents pour structurer les arguments

Toulmin method – Toulmin, S., The Uses of Argument, 1958, 2nd edition, 2003

Goal Structuring Notation – GSN Community Standard

http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf

Documents pour parvenir à des accords formels

ISO/IEC 12207, *Ingénierie des systèmes et du logiciel – Processus du cycle de vie du logiciel*

ISO/IEC 15026, *Ingénierie du logiciel et des systèmes – Assurance du logiciel et des systèmes*

ISO/IEC 15288, *Ingénierie des systèmes et du logiciel – Processus du cycle de vie du système*

Documents relatifs à la sûreté de fonctionnement

IEC 60300-3-1, *Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique*

IEC 60300-3-4, *Gestion de la sûreté de fonctionnement – Partie 3-4: Guide d'application – Spécification d'exigences de sûreté de fonctionnement*

IEC 61078, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

IEC 62347, *Lignes directrices pour les spécifications de sûreté de fonctionnement des systèmes*

Documents relatifs à la gestion des risques

IEC/ISO 31010, *Gestion des risques – Techniques d'évaluation des risques*

IEC 62198, *Gestion des risques liés à un projet – Lignes directrices pour l'application*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

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

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