IEC 60300-3-15

Edition 1.0 2009-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability management – Part 3-15: Application guide – Engineering of system dependability

Gestion de la sûreté de fonctionnement – Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub

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 It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) 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 CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 60300-3-15

Edition 1.0 2009-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Dependability management – Part 3-15: Application guide – Engineering of system dependability

Gestion de la sûreté de fonctionnement – Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE CODE PRIX XA

ICS 03.120.01

ISBN 2-8318-1048-4

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 3-15: Application guide – Engineering of system dependability

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication should be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability should 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 should not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-3-15 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1315/FDIS	56/1321/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.

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

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

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

INTRODUCTION

Systems are growing in complexity in today's application environments. System dependability has become an important performance attribute that affects the business strategies in system acquisition and the cost-effectiveness in system ownership and operations. The overall dependability of a system is the combined result of complex interactions of system elements, application environments, human-machine interfaces, deployment of support services and other influencing factors.

This part of IEC 60300 gives guidance on the engineering of the overall system to achieve its dependability objectives. The engineering approach in this standard represents the application of appropriate scientific knowledge and relevant technical disciplines for realizing the required dependability for the system of interest.

The four main aspects for engineering dependability concerning systems are addressed in terms of

– process,
– achievement,
– assessment, and
– measurement.

The engineering disciplines consist of technical processes that are applicable to the various stages of the system life cycle. Specific technical processes described in this part of IEC 60300 are supported by a sequence of relevant process activities to achieve the objectives of each system life cycle stage.

This part of IEC 60300 is applicable to generic systems with interacting system functions consisting of hardware, software and human elements to achieve system performance objectives. In many cases a function can be realized by commercial off-the-shelf products. A system can link to other systems to form a network. The boundaries separating a product from a system, and a system from a network, can be distinguished by defining the application of the entity. For example, a digital timer as a product can be used to synchronize the operation of a computer; the computer as a system can be linked with other computers in a business office for communications as a local area network. The application environment is applicable to all kinds of systems. Examples of applicable systems include control systems for power generation, fault-tolerant computing systems and systems for provision of maintenance support services.

Guidance on dependability engineering is provided for generic systems. It does not classify systems for special applications. The majority of systems in use are generally repairable throughout their life cycle operation for economic reasons and practical applications. Non-repairable systems such as communication satellites, remote sensing/monitoring equipment, and one-shot devices are considered as application-specific systems. They require further identification of specific application environment, operational conditions and additional information on unique performance characteristics to achieve their mission success objectives. Non-repairable subsystems and components are considered as throwaway items. The selection of applicable processes for engineering dependability into a specific system is carried out through the project tailoring and dependability management process.

This part of IEC 60300 forms part of the framework standards on system aspects of dependability to support IEC 60300-1 and IEC 60300-2 on dependability management. References are made to project management activities applicable to systems. They include identification of dependability elements and tasks relevant to the system and guidelines for dependability management reviews and tailoring of dependability projects.

DEPENDABILITY MANAGEMENT –

Part 3-15: Application guide – Engineering of system dependability

1 Scope

This part of IEC 60300 provides guidance for an engineering system's dependability and describes a process for realization of system dependability through the system life cycle.

This standard is applicable to new system development and for enhancement of existing systems involving interactions of system functions consisting of hardware, software and human elements.

This standard also applies to providers of subsystems and suppliers of products that seek system information and criteria for system integration. Methods and tools are provided for system dependability assessment and verification of results for achievement of dependability objectives.

2 Normative references

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

IEC 60300-1, *Dependability management – Part 1: Dependability management systems*

IEC 60300-2, *Dependability management – Part 2: Guidelines for dependability management*

3 Terms and definitions

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

3.1
system
set of interrelated items considered as a whole for a defined purpose, separated from other items

NOTE 1 A system is generally defined with the view of performing a definite function.

NOTE 2 The system is considered to be bound by an imaginary surface that intersects the links between the system and the environment and the other external systems.

NOTE 3 External resources (i.e. outside the system boundary) may be required for the system to operate.

NOTE 4 A system structure may be hierarchical, e.g. system, subsystem, component, etc.

3.2
subsystem
system that is part of a more complex system

3.3
operating profile
complete set of tasks to achieve a specific system objective

NOTE 1 Configurations and operating scenarios form part of the mode of system operation.

NOTE 2 An operating profile is the sequence of required tasks to be performed by the system to achieve its operational objective. The operating profile represents a specific operating scenario for the system in operation.

3.4
function
elementary operation performed by the system which, when combined with other elementary operations (system functions), enables the system to perform a task

[IEC 61069-1 :1991, 2.2.5] [1][1]

3.5
element
combination of components that form the basic building block to perform a distinct function

NOTE 1 An element may comprise hardware, software, information and/or human components.

NOTE 2 For some systems, information and data are an important part of the system operations.

3.6
integrity
ability of a system to sustain its form, stability and robustness, and maintain its consistency in performance and use

4 System dependability engineering and applications

4.1 Overview of system dependability engineering

Dependability is the ability of a system to perform as and when required to meet specific objectives under given conditions of use. Dependability characteristics include availability and its inherent or external influencing factors, such as: reliability, fault tolerance, recoverability, integrity, security, maintainability, durability and maintenance support. The dependability of a system infers that the system is trustworthy and capable of performing the desirable service upon demand to satisfy user needs. The system objective, structure, properties, and influencing conditions affecting system dependability performance are described in IEC 62347 [2] which provides guidance for determination of relevant system functions for specifying system dependability.

There are four main aspects for engineering dependability into systems:

a) **dependability process** – establishes the technical processes for engineering dependability into systems. The process consists of a sequence of activities implemented at each respective life cycle stage to achieve specific dependability objectives in system performance. The dependability process shall be fully integrated into the design and management processes;

b) **dependability achievement** – implementation of the effective engineering effort and knowledge experience applied at appropriate system life cycle stages. The aim is for progressive accomplishment of dependability objectives of the constituent system functions suitable for subsystem realization and system integration (reliability growth);

c) **dependability assessment** – evaluates the dependability attributes and determines their effectiveness when implemented into systems. The process identifies the specific dependability attributes to meet project needs and provides the methodology and rationale on how these attributes can be determined;

d) **dependability measurement** – quantifies the dependability attributes for contracting, specification and assessment purposes. The process is to assign a quantitative value or number to designate a target entity representing a specific dependability characteristic.

[1] Figures in square brackets refer to the bibliography.

The aim is to express a statement of intent in quantifiable terms to facilitate mutual understanding of the issue involved and to serve as basis for negotiation in reaching agreements.

4.2 System dependability attributes and performance characteristics

System dependability attributes are those specific dependability related features and time-dependent performance characteristics inherent in the system by design and construction. Some features, such as system performance characteristics can be quantified and measured. Other dependability features which are not quantifiable may present certain value or useful information pertinent to those attributes. These non-quantifiable features can be described in qualitative terms to establish its value for subjective dependability assessment. Both quantifiable and non-quantifiable features are important to describe the system dependability attributes. Examples of non-quantifiable features include product brand value, user friendly operation, and informative instructions. Examples of quantifiable performance characteristics include uptime duration, downtime frequency, mean-time-between-failures, and time for restoration from a degraded state back to normal system performance.

The main attributes of system dependability are as follows:

a) **availability**: the ability of the system to be in a state to perform a required function when a demand is placed upon the system. Availability performance is characterized in terms of measures such as percentage uptime for the duration of system performance operation upon demand; outage frequency and downtime duration;

b) **reliability**: the ability of the system to perform a required function for a given period of time under given conditions of use. Reliability performance is characterized in terms of measurements such as mean-time-between-failures and failure-free duration;

c) **maintainability**: the ability of the system to be restored to a state in which it can provide a required function following a failure, or retained in such an up-state, under given conditions of use and maintenance. Maintainability performance is characterized in terms of measurements such as mean-time-to-restore and recovery time;

d) **maintenance support**: ability of an organization to provide, when required, the resources required to maintain a system, under given conditions. Maintenance support performance is characterized in terms of measures such as utilization of maintenance resources, training needs, enabling tools and facilities, logistics delay time and turn-around time for spares provisioning.

There are other attributes related to dependability for specific system applications. They include but are not limited to:

e) **recoverability**: ability of a system to be restored to a state in which it can perform a required function following a failure without repair of hardware or software. It is characterized in terms of measurements such as mean-time-to-recover;

f) **testability**: ability of a system to be tested at designated maintenance levels for replace/repair action to determine fault coverage. It is characterized in terms of measurements such as percentage of test coverage;

g) **service accessibility**: ability of a service to be obtained within specified tolerances and other given conditions when requested by the user. It is characterized in terms of measurements such as probability of access to a service;

h) **service retainability**: ability of a service, once obtained, to continue to be provided under given conditions for a requested duration. It is characterized in terms of measurements such as probability of retention in time duration.

Recoverable performance is dependent on the design of system architecture, fault-tolerant and self-healing features incorporated into the system. Service performance is dependent on the properties of the system facilities, construction and infrastructure of resource deployment. The attributes of system performance in general are inherent in the system design. The performance attributes are derived from the capability of the system and the dependability feature of the system.

System performance characteristics are derived from time and incident measurements. An incident is an undesirable or unexpected event observed during system tests or in-service operation indicating that a failure might have occurred. All incidents should be recorded and investigated. This is to determine whether the incident is caused by a genuine failure, or it is due to human error or mistaken observation. A failure is a departure from the required performance functions of the system. However, at the time of observation, a failure may not cause complete cessation of the system functions, but may deteriorate system performance. The extent of deterioration before classification as failure should be defined and established for the measurements.

5 Managing system dependability

5.1 Dependability management

Dependability is a technical discipline and is managed by engineering principles and practices. IEC 60300-1 and IEC 60300-2 are used in this part of IEC 60300 for formulation of dependability management strategies and general application of technical approaches for implementation of dependability elements and tasks. Additional management processes are introduced to address system specific management issues. Dependability management involves project planning, resource allocation, dependability task assignments, monitoring and assurance, measurement of results, data analysis and continual improvement. Dependability activities should be conducted in conjunction with other technical disciplines to attain the needed synergistic effects and add values to the project outcomes. Project tailoring is emphasized for cost-effective management of system projects. Where applicable, life cycle cost analysis should be used for resource allocation and optimization for evaluation of acquisition and ownership costs.

5.2 System dependability projects

Dependability is a key decision factor in project management. Dependability affects the cost of project implementation. It focuses on specific dependability application issues in project tasks that need effective resolutions. Dependability has extensive impact on the results in project deliveries to meet customer expectations. From a system engineering perspective, realization of dependability in systems is an important business decision issue that needs full integration of engineering and design with the management decision process. Managing obsolescence, project risk assessment, technical design trade-offs, life cycle costing, outsourcing and supply-chain coordination are some examples of dependability activities in systems engineering practices.

Not all projects involve complete new system development. Most systems are built by integration of subsystems and application of commercial-off-the-shelf products for realization of system functions. In major system development or for system enhancement projects, it may involve multiple developers of subsystems and subcontractors on supplies and services to achieve on-time project delivery of the system. In this respect, project management is essential for coordination of various project efforts. System dependability projects may involve specific dependability activities such as:

a) adoption of new technology;

b) development of dependability specifications for system and subsystems;

c) dependability evaluation of commercial-off-the-shelf products for use in system functions;

d) assessment of supplier’s capability in fulfilment of dependability project requirements;

e) assurance of dependability for system acceptance.

System dependability activities may occur at any stage of the system life cycle. Some dependability task assignments may demand special skills and training in specific technical disciplines such as software engineering, logistics support, and human reliability.

5.3 Tailoring to meet project needs

A system dependability project is initiated to resolve specific dependability issues of concern to the system. The purpose of tailoring is to manage the allocation of available project resources and select the appropriate methods for effective problem resolution. Examples of system dependability project activities appropriate for tailoring include:

a) budget planning for allocation of dependability resources to meet project delivery targets;

b) evaluation of alternative technologies for high reliability product acquisition;

c) outsourcing of subsystem development to meet stringent criteria in software capability maturity model requirements where process monitoring is crucial;

d) training time required to gain sufficient experience to use a new reliability analysis tool;

e) selection of subcontractors for provision of on-site maintenance of critical systems for high availability performance expectations with no scheduled downtime permitted.

Guidelines for the tailoring process are described in IEC 60300-2.

5.4 Dependability assurance

Dependability assurance activities should form part of the quality assurance process for system dependability projects. This is to ensure that all planned and systematic activities implemented within the quality system, and demonstrated as needed, provide adequate confidence that the system and product quality requirements are fulfilled. Key activities involve project planning, technical and management responsibility assignment, verification of dependability assessment results, validation of dependability performance data for system acceptance, monitoring of dependability process effectiveness, failure reporting and data analysis for prompt corrective and preventive actions, documentation of relevant dependability information and maintenance of test records to support objective evidence, and management review to initiate process improvements. IEC 60300-2 provides additional information on selection of dependability program elements and tasks for tailoring of system dependability projects.

6 Realization of system dependability

6.1 Process for engineering dependability into systems

6.1.1 Purpose of dependability process

Establishing a process is essential for successful management of project tasks and coordination of activities. The dependability process should be integrated into the technical processes to facilitate engineering dependability into the system. The dependability process provides specific inputs at major project decision points of the system life cycle to facilitate project implementation. These major decision points occur at the completion of critical project management phases for market identification, system development, product realization, system acceptance, in-service operation, enhancement and retirement. Dependability information is crucial at these major decision points to justify business investments.

6.1.2 System life cycle and processes

The starting point for engineering dependability into a system should be at the earliest life cycle stage. The user should apply an effective engineering process at this life cycle stage.

The description of system life cycle stages can be viewed from a generic systems engineering perspective. There are other system life cycle descriptions. IEC 60300-2 describes the product life cycle phases from a project management view. ISO/IEC 15288 [3] provides a similar system life cycle description from an information technology and software engineering view. The guidance provided by this part of IEC 60300 is based on the concept of system life cycle stages, as described in Figure 1. System stages are precise technical transition points, whereas project phases may overlap by management discretions to reach major business

decisions. Project risk management as referred to in IEC 60300-2 applies throughout the life cycle processes.

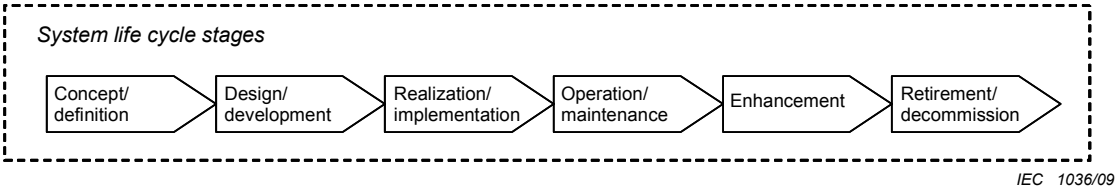

Figure 1 – An overview of a system life cycle

The technical processes for engineering consist of a sequence of process activities implemented at each respective life cycle stage to achieve the intended system performance and dependability objectives. Engineering dependability into a system is not completed in isolation. It is performed in conjunction with other technical disciplines (e.g. structural design) and supporting activities (e.g. quality assurance) for realization of system functions for their intended applications. Annex A describes a typical sequence of the system life cycle processes.

The key process activities in a system life cycle are as follows:

a) requirements definition identifies the users' needs and constraints of system applications;

b) requirements analysis transforms the users' view on system applications into a technical view for engineering the system and will include development of an operational use profile/timeline/design reference mission;

c) architectural design synthesizes a solution that satisfies system requirements for operating scenarios by allocating the required system functions to hardware, software and human elements;

d) functional design and evaluation determines the practical means for realizing the functions to facilitate design trade-off and optimization;

e) system design documentation captures the system information, including dependability data, suitable for system design;

f) system design and subsystem development creates the specified system and subsystem functions;

g) realization produces the system and subsystem elements in hardware and software forms;

h) integration assembles the system and subsystems consistent with the architectural design;

i) verification confirms that the specified design requirements are fulfilled by the system;

j) installation/transition establishes the system capability to provide the required performance service in a specified operational environment;

k) validation/commissioning provide objective evidence that the system fulfils the functional requirements;

l) operation engages the system to deliver its operational service;

m) maintenance support sustains the system capability for operational service;

n) enhancement improves the system performance with added features;

o) retirement/decommissioning ends the existence of the system entity.

6.1.3 Process applications through the system life cycle

A process is an integrated set of interrelated or interacting activities that transforms inputs into outputs. Processes are used as reference models for functional organization (e.g. quality

management systems (QMS), project management), business transactions (e.g. acquisition, supply-chain agreement), and technical planning and implementation (e.g. product development, system assessments). This part of IEC 60300 focuses on the technical processes for engineering dependability into systems.

Figure 2 shows an example of a process model. In the context of engineering, the primary inputs usually consist of data providing a set of requirements, or the expressed needs of the customer. The outputs may consist of processed data describing a desired solution such as a specification, the fabrication of a product or the delivery of a service. There are other inputs associated with the process for controlling and enabling purposes. The process activities transform or convert the primary inputs to the desired outputs. This conversion is subject to the conditions set by the enabling mechanisms and associated influencing factors. Some influencing factors are controllable such as operating procedures for activating the process; others may be uncontrollable such as the weather conditions or sudden climate change. Enabling mechanisms such as methods and tools are essential for the conversion to take effects. This process model is used for implementing the technical processes described in this part of IEC 60300.

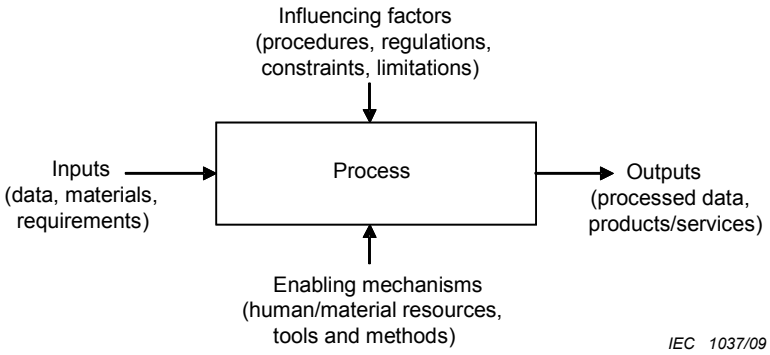

Figure 2 – Example of a process model

The technical processes serve two purposes:

a) to perform engineering tasks and conduct re-engineering activities during system conception and development;

b) to perform operation, maintenance and disposal activities with respect to the system.

The applications of technical processes are both recursive and iterative so as to complete the desired solution. This applies to all stages of the system life cycle. The relationships of the technical processes are independent of system size and structure. Process activities such as requirements definition, requirements analysis and architectural design are “top-down” technical approaches to engineer the desired solution (i.e. breaking the system down to its component elements); whereas integration and verification are “bottom-up” approaches to realize the system configuration and validate its performance (i.e. building the elements up to construct the system). The transition from “top-down” to “bottom-up” approaches during the implementation stage occurs at the completion of system installation where commissioning begins. This is known as the “V” model in engineering practice as described in ISO/IEC 15288 [3].

NOTE For further information on the “V” model refer to ISO/IEC/TR 15271 [4].

ISO/IEC 12207 [5] establishes a framework for software life cycle processes. It contains processes, activities and tasks that can be applied during the acquisition of a software product or service and during the supply, development, operation, maintenance and disposal of software products. ISO/IEC 12207 [5] can be used either alone or in conjunction with ISO/IEC 15288 [3].

Typical examples of process applications at each system life cycle stage can be found in Annex A. Knowledge of the system type and application environment is essential for tailoring the process application at the appropriate system life cycle stages in order to meet specific project needs.

6.2 Achievement of system dependability

6.2.1 Purpose of system dependability achievements

Achievement is the action of accomplishing an objective. It reflects the results brought about by successful problem resolution. The actions required for achieving system dependability can be accomplished by means of effective engineering effort and knowledge experience applied at appropriate system life cycle stages. The aim is for progressive accomplishment of dependability objectives of the constituent system functions leading to system integration. Achievement of system dependability is an important project objective that needs to be coordinated and demonstrated for system acceptance. System acceptance is usually a contractual agreement to meet customer requirements. The ultimate goal is to satisfy users' expectations of system performance.

6.2.2 Criteria for system dependability achievements

System dependability is achieved by successful incorporation of pertinent dependability attributes and related performance features into the system. The criteria for system dependability achievements should reflect:

a) a sound understanding of system performance objectives;

b) a sound understanding of operating conditions;

c) the effective implementation of dependability principles into the operational infrastructure;

d) the conditions of use;

e) the application of appropriate processes for system realization;

f) the utilization of knowledge and experience for cost-effective introduction of system services.

These criteria can be accomplished by focusing on key factors affecting dependability issues related to the system. The important criteria are identified which support process applications and realization of system objectives. Rationales are provided to clarify the significance of dependability implementation. These criteria should be considered in project planning and implementation. The user should tailor the appropriate dependability activities to meet specific project needs from a system life cycle perspective.

1) **dependability management policy** – this criterion influences the operational infrastructure, the allocation of appropriate resources, responsibility assignment for management accountability and dependability project leadership. The significance of dependability policy reflects a customer focus on dependability management strategy and commitments, collaborative effort, and systematic process approach towards effective application of dependability management principles as described in IEC 60300-1. The dependability management policy described in IEC 60300-1 applies throughout the engineering processes described in this part of IEC 60300;

2) **dependability knowledge base** – this criterion affects the accuracy of interpreting market needs, the adequacy of relevant information required for project initiation, the applications of available standards and specifications, the competitive leverage in contract negotiation and substantiation of dependability for objective evidence. The significance of dependability knowledge base lies in the market competitive advantage and technology leadership when dealing with new challenges in system dependability issues;

3) **design architecture** – this criterion affects the use of technologies for system applications, the selection of hardware, software, and human elements for realization of system functions, system integration and system in-service operation, and facilitating system enhancement and upgrade. Design architecture establishes a cohesive and

constructive framework for system integrity and realization. It facilitates capability enhancement, capacity expansion, cost-effective operation, and provision of quality of service. Appropriate technology utilization permits design trade-off by incorporation of advanced features and broadening the technical limits for applications;

4) **supply-chain cooperation** – this criterion affects make-buy decisions, outsourcing and subcontracting schemes, verification and validation procedures and documentations, and the monitoring and assurance processes. The significance of supply-chain management is based on purchaser-supplier cooperation and sharing of relevant information in the procurement and acquisition process. The supply-chain provides the necessary linkage for tracking important information. The impact on business is expediency in the administrative process, reduction in provisioning costs, and incentives for delivery of quality products and services;

5) **enabling systems** – this criterion affects the use of methods and tools, expediency of design throughputs, skills training needs, new product introduction and system deployment, maintenance and logistics support strategies. The significance of enabling systems is seen in the improvement of the design and delivery process and the effective utilization of methods and tools to expedite problem resolution. Enabling systems are not always technically complex requiring special skills for their comprehension and use. Some of the methodologies are simple checklists and instructions facilitating the operators and maintainers for on-site decisions to take proper actions. Further information on enabling systems is given in standard ISO/IEC 15288 [3];

6) **customer feedback and information management** – this criterion affects customer relations in terms of satisfaction and loyalty, provision of effective customer care services, accuracy in incident reporting, service data capture for analysis, effective implementation of corrective and preventive actions, establishment of system performance trends and records of dependability performance history. The significance of relevant feedback information is the ability to establish performance trends, identify critical areas requiring attention and provide objective evidence for verification and validation.

6.2.3 Methodology for system dependability achievements

The selection of applicable methods can proceed with the knowledge of criteria and the understanding of their significance for system dependability achievements. The objective is to utilize these methods to build dependability into the system. The application is aimed at incorporation of relevant dependability attributes into system functions.

The methodology for implementing dependability into system functions can be viewed from two perspectives:

a) top-down approach to synthesize system dependability based on specified system requirements and market information to develop the system architecture;

b) bottom-up approach to build dependability into system functions based on dependability design rules for simplification, fault tolerance, risk reduction and mitigation.

Both approaches involve the identification of dependability attributes and determination of their values. Dependability attributes are the fundamental measures for assessment and achievement of system dependability.

Dependability attributes that are relevant to system performance characteristics are time dependent. They can be quantified and derived from time and incident measurements. Examples include the percentage uptime for system availability performance, the probability of success of an operating system function with failure-free duration to demonstrate reliability, and the completion of system restoration within scheduled downtime to show expediency in maintenance support actions.

However, not all dependability attributes can easily be demonstrated due to time and cost constraints, technical limitations, or for other reasons related to the project. Examples include highly reliable complex systems, new systems with limited field deployment experience,

generic software systems for use in new application environment, and some commercial-off-the-shelf products with no performance reliability history. Other methods are needed to provide confidence for use and dependability assurance. It should be noted that system dependability attributes are stochastic or probabilistic in nature. They may encompass indirectly assessable features other than those performance characteristics that can be derived from direct measurements. Typical methods applicable include R&M case studies, simulated test cases, capability maturity models, and reliability growth programs.

Numbers and quantifiable values often need interpretation. A failure rate measurement may not be meaningful without proper reference to its context or explanation of the surrounding issues of concern. While the failure rate numbers may be used as indicators for comparison of alternative design options, the underlying assumptions are critical to support the rationale and justification. This allows application of statistical tools to determine inference bounds and confidence limits of potential risk exposures. In a business example, the mean-time-between-failures of a copying machine may not be too meaningful to the business owner, but the number of disposed void copies per month of machine usage would indicate the cost of wastage.

Annex B provides examples of applicable methods and tools to facilitate system dependability achievements. Knowledge of the system operating functions and its application environment described in Annex C is necessary for the selection of relevant methods and tools. Effective applications should focus on critical issues in solving technical problems. The limitations of these methods and tools for their specific applications should be noted to permit proper interpretation of results.

6.2.4 Realization of system functions

System functions can be realized by using hardware, software, or human elements, or any of their combinations to achieve specific system performance objectives. The following describes the general issues related to the selection and application of these elements for successful dependability achievements.

a) **Hardware element** – hardware is commonly used in system constructions. Hardware can consist of mechanical, electrical, electronic, optical, and other physical components. They are used in various configurations to realize the hardware functions. Most electronic products built today with hardware elements are relatively mature in technology applications. The design rules are well established. Electronic products exhibit consistency in production under controlled manufacturing process environment. Product quality and dependability can be ascertained by appropriate assurance programs. There are also ample 'experience' databases to support reliability performance of these hardware-based electronic products. However, some products with active electronic components are sensitive to varying application environments. The physics of failures of these components dominate the hardware failures and infant mortality phenomenon. Proper reliability design, packaging and screening can help significant reduction in early failures. Some hardware elements may wear-out due to operation or extensive use while others may have limited shelve-lives. These inherent reliability problems can be resolved by implementation of preventive and scheduled maintenance efforts. Hardware system structure is hierarchical. The maintenance support strategy can be deployed by proper functional design and packaging strategy of the lowest replaceable assembly or unit. This facilitates maintainability design and logistics support activities to improve system availability performance.

b) **Software element** – software can consist of coded instructions, computer programs, established rules and procedures for system operation. Coded commands are used to instruct a software program for execution of system function for application. Software codes are difficult to test for coding errors unless it is run in actual computer operation. A software program error resulting in a system failure is due to the activation of a latent fault or "bug" within the software program. Software design disciplines are essential to minimize the potential of generating unintended errors in design. The approaches used include fault avoidance, fault removal and fault tolerance. They are formal methods in software design disciplines. Although software does not wear-out, its functions can deteriorate as a consequence of changes. Because the software is created in one form or

another by human origin, the design control disciplines are focused on the software design environment. Adopting an infrastructure using methodology such as the Capability Maturity Models as a framework for software development can facilitate the achievement of dependability in software functions. Software issues and versions for upgrades should be controlled by a system configuration management process to sustain interoperability of functions and enhance dependability in performance;

c) **Human element** – human interactions with system operation can be viewed as part of the system functions or as an end user of the system. The role of the human in system performance can be beneficial with the human's ability to mitigate or control the on-going situations. However, most industrial incidents reported and major accidents studied can be traced back to human errors as the primary cause of system malfunction or disruption in performance service. Systems designed for human operation or use should incorporate human factors in the system design to minimize the risk of critical system failures, loss of properties, security violations or safety threats. Dependability can be achieved by application of human factors in design rules and simplification of tasks for human operation. The study of human factors involves a multi-disciplinary effort on gathering information about human capabilities and limitations for applications affecting human-system performance. The engineering aspects consist of the application of human factors information to the design of tools, machines, systems, tasks, jobs, and environment for safe, comfortable, and effective human use. Training and education are important prerequisites for any system operation requiring human interaction. Human factors standardization facilitates system integration, enhances interoperability of system elements, and improves serviceability and overall dependability performance.

Most system functions in today's electronic products use combined hardware and software elements in system designs. They offer a broad range of design features for diverse applications. Dependability of system functions is achieved by incorporation of design rules and established processes for applications. Design trade-off can be attained by proper combination of technologies suitable to meet specific application needs. Economic values can be gained through modular packaging and standardization for mass-scale production. System functions can be automated for self-checking to improve performance effectiveness by means of built-in-test or other monitoring schemes. Human intervention in system functions is only necessitated by safety and security regulations, or dictated by social and economic reasons. Annex D provides checklists for hardware, software, and human factor design applications.

6.2.5 Approaches to determine achievement of system dependability

There are three generic approaches to determine that system dependability has been achieved. They serve different purposes with varying degree of engineering rigour. In practice, a combination of these approaches is likely to be used:

a) **Demonstration** – this is achieved by means of actual system operation in an application environment over a scheduled time period to demonstrate dependability performance. Typical examples include:
   - dependability performance history of systems in field operation;
   - formal reliability demonstration;
   - availability performance during warranty period.

b) **Inference** – this is achieved by means of statistical methods using observed data of constituent system functions based on established criteria and assumptions to arrive at a numerical value representing system dependability attributes (characteristics / performance). Typical examples include:
   - prediction of system of given configuration;
   - system simulation;
   - capability maturity models;
   - test case verification of system performance.

c) **Progressive evidence** – this is achieved by progressive accomplishment of project milestones with auditable arguments to support objective evidence. Typical examples include:

- R&M case;
- reliability growth program.

6.2.6 Objective evidence of achievements

The following are key statements on system dependability characteristics for use as objective evidence to support system and product acceptance at applicable system life cycle stages. Objective evidence needs to be documented and authenticated for auditing and contracting purposes.

a) a statement on system dependability attributes and operating environment to reflect user expectations in commercial specification or proposal based on market research information. This provides information to start project planning and develop system dependability specification;

b) a statement on system performance characteristics in system dependability specification. This provides information for establishing dependability design objectives and system architecture;

c) a statement on reliability and maintainability performance characteristics for each system function in functional design specification. This provides information for technology selection, make-buy decisions, and establishing procurement requirements;

d) a statement on reliability and maintainability characteristics for system in-service operation and maintenance. This provides information for logistics support planning, contract maintenance, and special training needs;

e) a statement on relevant dependability characteristics for product acceptance, verification compliance, and validation of system performance results. This forms the basis for fulfilment of contractual agreements for deliverable contract items;

f) all dependability project reports containing dependability analysis data, test status and demonstration results. This provides information for project reviews, design changes, procedural updates, corrective and preventive actions for progressive improvement.

6.3 Assessment of system dependability

6.3.1 Purpose of system dependability assessments

Assessment is an evaluation of the status or outcome of a specific dependability activity or issue. The purpose of assessment is to determine how a problem can be solved. The findings are used to support recommended actions with rationale and justification. The assessment process facilitates the identification of possible alternatives or options for resolution of the problem. This permits design trade-offs and preferred product selection. The assessment effort in system dependability should be tailored to meet specific project needs and for process enhancement.

6.3.2 Types of assessments

Assessment can be objective or subjective. Objective assessment is by direct measurement of an entity to obtain the results. Subjective assessment is to assign a value on the nature, character, or quality of its findings. For example, to assess the quality of a software function in system application, we may gain insights on how the software is developed. Reviewing its design process to form a subjective opinion for appraisal could do this. The purpose is to ensure user confidence of the software's adequacy for application. We cannot be sure until we run the software in a computer system to ascertain its quality features in actual performance. This provides the crucial demonstration for objective evidence. In engineering practice, both objective and subjective assessments are used which complement each other in the evaluation process.

The following provides major project objectives associated with the assessment of system dependability at major decision points of the system life cycle:

a) **market identification –** the objective is to identify the market needs to justify investments for new system development or enhancing an existing system for competition. Market analysis is essential to justify major investments involving resource commitments. Systems engineering activities involve capability and resource identification, evaluation of new technology for feasible application, competitive analysis and user expectation of system performance, the extent of maintenance support necessary to sustain new or enhanced service operation, time and cost constraints for market entry and regulatory and environmental impact on system introduction. Initial system structure and configuration should be considered to meet applicable system operating scenarios. System life cycle costs should be examined on a return-on-investments basis. Key dependability assessment to support market identification include:
   - prediction of system dependability to meet anticipated market needs;
   - evaluation of new technology maturity suitable for system applications affecting dependability performance;
   - identification on critical dependability issues relating to serviceability impact and operability influence;
   - dependability capability evaluation of potential suppliers and subcontractors;
   - assurance of continuation of maintaining service, availability and safety until the system is fully retired.

b) **system design and development** – the objective is to rationalize the system design approach and evaluate design alternatives and options. The selected design is followed by system development. This is a major commitment to both capital and resource investments. System engineering activities involve requirements analysis, architectural design configuration, functional design and technology evaluation, outsourcing of subcontract work and selection of suppliers, system realization and integration, qualification testing and verification, system installation and transition for the required operation services. Key dependability assessment to support design and development decision include:
   - evaluation of system functions affecting dependability performance;
   - evaluation of system structure for reliability optimization of system configuration;
   - evaluation of access for maintenance;
   - system availability performance simulation and performance evaluation to determine critical system malfunction, failure mitigation and service support needs;
   - reliability verification and problem analysis for corrective actions;
   - evaluation of dependability programs of suppliers and subcontractors;
   - manufacturability assessment for production yield affecting reliability growth;
   - evaluation of reliability warranty incentives and logistics support requirements.

c) **system realization and implementation –** the objective is to execute make-buy decisions for acquisition and deployment of subsystem elements, and to implement resource commitments for system construction and integration. Key dependability assessment to support system realization and implementation include:
   - assessment of system elements and COTS products conformance to dependability requirements for subsystem integration;
   - assessment of subsystem conformance to dependability requirements;
   - assessment of quality assurance process;
   - evaluation of subsystem test performance results for system integration;
   - evaluation of system test performance results for preparation of system acceptance.

d) **system acceptance for in-service operation** – the objective is to assure customer confidence for system acceptance. This involves the hand-over of responsibility to the customer for in-service operation. It initiates the warranty period to ensure system

performance meets the end users' expectations. Key dependability assessment to ensure system acceptance include:

- evaluation of system performance by introduction of field tracking and incident reporting schemes;
- assess training needs and competency of customer operators and maintainers;
- establishing a focal point for data collection and incident report analysis to determine dependability performance trends and criticality of system malfunction requiring immediate corrective actions;
- evaluation of system maintenance service and logistics support effectiveness;
- procedures for design change authorization and configuration management.

e) **system enhancement** – the objective is to justify investment for enhancement, or upgrading of the existing system. This involves similar activities as for new system design and development for the enhancement part of the system. The legacy issues of the existing system shall be addressed to ensure interoperability and capability improvement of service. Key dependability assessment to support system enhancement decision includes:

- cost benefits analysis for change incorporation;
- evaluation of dependability performance impact due to changes with added new features;
- customer reaction to proposed changes;
- risk and value assessments.

f) **system retirement** – the objective is to retire the system from service. Key dependability assessment to support retirement decision include:

- evaluation of cost impact for termination of system service;
- evaluation of regulatory and environmental impact for termination of system service.

6.3.3 Methodology for system dependability assessments

The assessment methodology addresses the implementation issues concerning processes, approaches and strategies.

The assessment methodology embraces two important processes:

a) **verification –** the verification process is a method of confirming the assessment results. It should be conducted to support major decision points at each system life cycle stage.

b) **validation –** the validation process provides objective evidence that the system meets the actual requirements and satisfies user expectations.

The approaches for assessment are often unique to suit various project implementation situations. They include a combination of the following approaches:

1) **analytical approach** – this involves activities such as design analysis, system performance simulation, standardization conformance, and compliance specification evaluation.

2) **experimental approach** – this involves activities such as performance testing and technical evaluation of system functions, physical assemblies, suppliers' products, subsystems integration, and the actual system acceptance.

3) **consultative approach** – this involves activities such as expert reviews, use of industry best practices, suppliers' consultation on product information, customer survey and user feedback, supply-chain participation, infrastructure development and enhancement.

4) **negotiated approach** – this involves activities such as establishing acceptable risk limits for system operating exposure to the environment, conditions for product deployment in specific regions, recycling of by-products and waste disposals, economic incentives and social benefits in contract agreements, and compliance to changing regulations.

The assessment strategies should focus on two main aspects in engineering dependability into systems:

i) **application focus** – this relates to meeting project specific applications for compliance of contractual requirements. The essential assessment activities are focused on the evaluation and analysis of system dependability at major decision points of the applicable system life cycle. The methods and tools deployed for assessment are commonly used for product verification and system or subsystem validation.

ii) **technology focus** – this relates to technology evaluation of design strategy and system support schemes to facilitate dependability performance achievements. The essential assessment activities are focused on evaluating the technology leverage that can be exploited for the system designs, and determining the viability of enabling systems to support continuity of system in-service operation. Issues concerning technology evolution and obsolescence should form part of the assessment strategies.

6.3.4 Assessment value and implications

Assessment is a prerequisite and crucial input for decision-making in projects. The assessment effort should be rationalized for practical application. The resolution of the issues of concern should be completed within reasonable time limits to realize the expected value or benefits to the project. This would establish the needed confidence to support project decisions. The following key issues that exemplify the value of assessment are noted for illustration. Typical examples are shown to highlight their major implications to the project outcomes.

a) Timing of assessment is crucial to provide meaningful results. The assessment value greatly diminishes when the assessment results are not available at the time needed to support major decisions. For example, a reliability prediction conducted during system design may provide valuable insights into the proper technology selection, architectural design structure, partitioning configuration, and choice of system elements and components for realizing system functions. A prediction done after design completion has limited value when the system is configured and ready for production.

b) Justifying the cost benefits of the assessment prior to its initiation is prudent for project planning and effective management. For example, the “plan-do-check-act” process in quality management systems (QMS) is commonly used as basis for planning assessment activities. Investment analysis related to assessment is critical to justify major capital expenditures and new acquisitions.

c) Ensuring the infrastructure support is adequate for implementation of assessment tools. This may involve technical procedure changes and cultural adjustments that would consume both time and effort. For example, migrating from the software capability maturity model process to the software capability maturity model integration process is a major endeavour for any corporation. Both technical resources and management culture would need adjustments to attain the industry recognized status and certification.

d) Contingency planning is essential to avoid unexpected project outcomes or unscheduled delays. This may impact resource allocation and work redeployment, supply-chain distribution and delivery of supplier products, and affect the scheduled commitments for system commissioning and customer acceptance. For example, at major decision points, contingency plans should be included as part of the assessment process, such as identifying alternate suppliers in case of supplier disruption, the deployment of technical expertise to work on critical designs to meet stringent delivery targets, and exploring the means of viable financing for capital investments.

6.4 Measurement of system dependability

6.4.1 Purpose of system dependability measurements

From an engineering perspective, system dependability measurements represent the process of assigning quantitative value to characterize the dependability attribute. The quantitative value is derived from observed or estimated data on time duration and the number of incident occurrences to reflect the dependability performance characteristics. The measurement process involves:

a) identifying the type and objective of measurement under contractual, operational, or for specific conditions such as product evaluation requiring quantification of dependability attributes;

b) determining the relevant data and the nature of the data sources for measurements;

c) utilizing effective enabling systems to facilitate the measurement process such as deployment of data collection systems, failure reporting, analysis and corrective action systems, survey questionnaires, or other support schemes;

d) interpreting the measurement results to establish performance trends, identify critical issues, and recommend management actions with rationales and justifications;

e) documenting the measurement findings for record retention, quality audits, and objective evidence.

f) ISO/IEC 15939 [6] defines a measurement process applicable to system and software engineering.

6.4.2 Classification of system dependability measurements

There are four general classes of dependability measurements to meet specific project needs.

a) **Measurement of inherent system dependability attributes** – the objective is to assign numerical figure-of-merits to represent the inherent dependability attributes of the system. This class of measurement is useful for comparison of dependability attributes of different design architectures and system configurations. The measurement process is conducted during system concept/definition stage to determine the inherent dependability performance capability of alternate options. The purpose is aimed at providing evidence of the system capability in meeting dependability objectives for proposal or contract inquiries. The numerical values can be stated in terms of probability of success, mean operating time between failures, life times or failure rates that quantify the system availability or reliability performance characteristics. The measurements are commonly carried out by prediction methods as described in IEC 60300-3-1 [7].

b) **Measurement of system dependability for performance evaluation and in-service operation** – the objective is to assign a number to designate system dependability performance in actual operation. This class of measurement is useful for assessment of dependability attributes during design/development stage where products and subsystems are tested to verify the adequacy of performance. It is also used during the system operation/maintenance stage to determine compliance to established operational objectives for dependability achievements. The measurement process is conducted by progressive testing of products, subsystems and the integrated system for performance verification and validation, and by tracking performance status of the system in-service operation. The measurement data come from product qualification tests, suppliers test results on subsystems, acceptance testing, and field performance records and incident reports. The numerical values can be stated as reliability, failure probability, failure free time (time to first failure), lifetime, percentage uptime (availability), outage frequency and duration.

c) **Measurement of system dependability for performance improvements** – the objective is to assign value to quantify and qualify the degree of customer satisfaction, or to determine the extent of customer value for performance improvements. This is an indirect measurement that helps to identify the impact of significant dependability attributes in system performance. This class of measurement is aimed at seeking direct user feedback on system performance, or to determine the value of service provision during system operation/maintenance stage. The measurement process is conducted by means of customer surveys, performance audits, value assessments, and direct contacts and dialogues with customers and suppliers. Customer satisfaction surveys are focused on identifying current issues of customer concerns. Quality function deployment is commonly utilized for performance value assessment to defining customer needs and translating them into appropriate technical requirements for actions in meeting those needs. The value assignment can be stated in a scale of 1 to 5 inclusive to indicate ratings such as from poor to excellent.

d) **Measurement of system dependability for risk exposures** – the objective is to assign numerical values to indicate the extent of risk exposures when the system is used for safety and security applications. This is an indirect measurement to identify the criticality of the dependability attributes affecting system performance functions. This class of measurement is conducted during system concept/definition stage to identify critical system functions and elements for specific system operation or mission. The assessment process includes the determination of threat or harm by designation of its severity and frequency of occurrence. The classification of risks can be established qualitatively by a range of catastrophic, critical, major, minor or negligible events. Probabilistic values can be assigned to indicate the severity of the situation by a statement such as a critical failure occurring once in every 10 years. IEC 60300-3-9 [8] describes the technological risk assessment methods affecting the dependability attributes of system performance. A similar method is used in the IEC 61508 series [9] on safety-integrity levels for ranking safety functions (refer to IEC 61508-1 [10] for more details).

6.4.3 Sources of measurements

Measurements of system dependability attributes can be ascertained by direct performance testing under simulated conditions or in actual operating environment where the relevant data can be collected. System dependability attributes can also be assessed by means of predictions based on field performance history of similar systems, or they can be derived from established reliability database with knowledge of the system configuration and the operating functions of its constituent system elements.

Measurement data related to dependability attributes can also come from other sources such as suppliers test programs, maintenance support data, warranty information, and customer surveys. It is important that the integrity of the data used for dependability assessment be validated for assurance purposes.

6.4.4 Enabling systems for dependability measurements

Data integrity in dependability measurements is important to assure the accuracy, credibility and consistency of the data acquisition and collection process. It ensures that relevant data are used correctly in data analysis and permits proper interpretation of the analysis results. The system design and format should be simple and straightforward to capture relevant information needed. Automated data entries and interactive web-based information access would enhance expediency for system implementation. There are various supporting systems utilized in engineering practice to enable cost-effective data collection and facilitate dependability measurements. These systems are essential parts of the dependability management system infrastructure. For their specific supportive roles, these systems can be classified as enabling systems to facilitate engineering dependability into the system of interest. Typical enabling systems commonly used for data collection, incidents reporting, problem analysis and corrective action include:

a) failure reporting, analysis and correction action system to capture non-conformance information and test failure data during system development, testing and integration;

b) test yield data acquisition system to capture manufacturing anomalies to track production yield rates for problem identification and root-cause analysis during product assembly;

c) incidents reporting during system in-service operation to capture incidents affecting the continuity of system performance service, report on-site maintenance actions, assign criticality of the incident, and record follow-up support requests and time required for resolution;

d) spares provisioning system to capture spares consumption data and turn-around-time for spares replenishment, spares distribution, and stock reordering;

e) information feedback system to capture customer complaints, suppliers concerns, and employee suggestions for infrastructure improvement, strategic planning, and problem resolution that add value to projects and organizational management.

6.4.5 Interpretation of dependability measurements

The proper interpretation of measurement results is essential for prompt corrective and preventive actions to support cost-effective operation. The following examples show the importance of measured or analysed data when transcribed and interpreted for follow-up actions.

a) The acquisition and collection of relevant data should provide value to meet current project needs. This infers proper planning and design of experiments. It takes time and effort to acquire data. If such data cannot be used to help resolve current problems, then it should not be collected. The objectivity of the measurement process should be clearly defined. For example, the collection of field performance data of old systems deployed many years ago that are no longer in production nor supported would not be too useful for the new system design using a different technology.

b) The transcribed measurements and interpreted results should present logical conclusion for recommended actions. The measured data and captured information should permit further analysis if necessary to support the underlying rationales or arguments in reaching a logical decision to justify the recommended actions. It should be noted that different interpretation of dependability measurements may lead to diverse understanding by the recipients, usually someone who needs the information for making decisions. For example, an availability performance number of 99,999 7 % assigned to a switching system may be an appropriate number to use in probability calculation of system functions, but it would be difficult to devise a scheme for system availability demonstration.

c) The dependability problems identified should address the criticality of the issues at hand to alert management actions. Such problems identified in a process of concern regarding dependability usually occur under situations that may cause significant safety or security impact if not promptly attended to. These dependability issues may have potential liability issues and risks exposure if not properly assessed at the time they occur. System in-service operation follows established operating procedures. System outage incidents are reported according to on-site assessment of their criticality. Some critical issues should be resolved immediately or within a limited time period. Other non-critical issues may be deferred to a later system update or maintenance enhancement. For example, a field modification of a system design to fix a temporary problem without proper design change authorization may create unknown long-term safety hazards. Temporary software patches to fix a localized problem without thorough investigation may lead to security violation or crashing the entire system operation. Dependability design may incorporate fault-tolerant protection features. Such protection features are no longer effective if they have been disarmed or disconnected due to a bypassing of access for temporary fixes without proper authorization. Interpretation process should identify and alert potential problem issues to avoid the reoccurrence of such incidents. Warning signs and labels placed in proper locations could draw attentions.

Annex A
(informative)

System life cycle processes and applications

A.1 System life cycle processes

A.1.1 Description of system life cycle processes

Figure A.1 provides a logical sequence of process activities applicable to each stage of the life cycle for engineering dependability into the system.

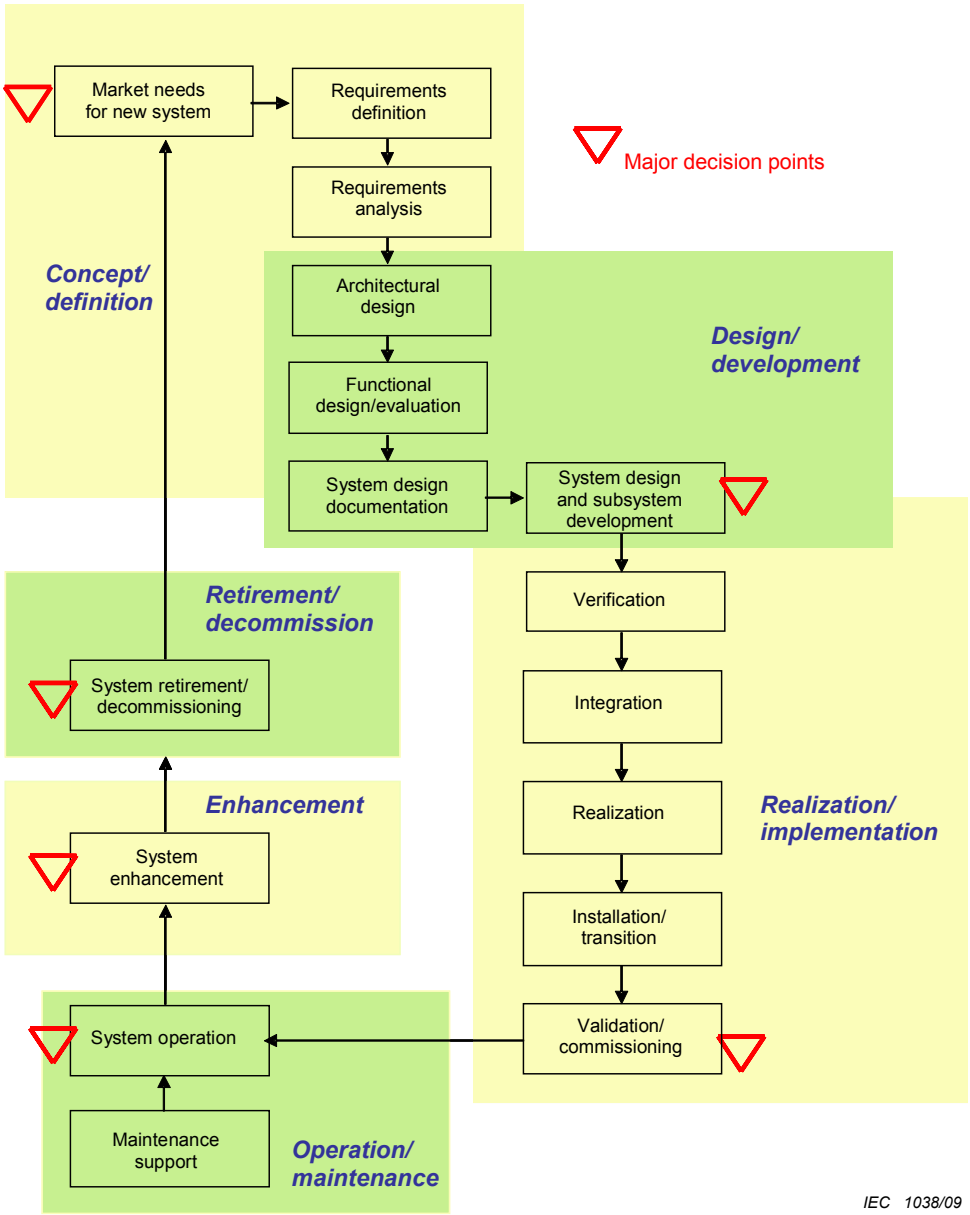

Figure A.1 – Overview of system life cycle processes

The first three stages of the system life cycle, i.e. concept/definition, design/development, and realization/implementation, before transition to operation/maintenance stage, overlap each other due to iteration of the processes. This indicates the need to provide continuity of workflow depending on the project needs. The extent of engineering effort crossing the arbitrarily defined boundaries of adjacent stages is dependent upon the project timeline and coordination activities. This can also be used to acquire sufficient system information to support the technical and business decision-making process. The following provides a brief description of each stage of the system life cycle:

a) The **concept/definition** stage is to identify the market needs, define/identify the operational use environment/timeline, define preliminary system requirements and confirm feasible design solutions by producing technical specifications for the system design. Selection of design options is based on risk analysis, impact evaluation, and practical engineering approaches. The process activities involve requirements definition, requirements analysis, architectural design, and functional design/evaluation to provide high-level system specifications.

b) The **design/development** stage is to plan and execute selected engineering design solutions for realization of system functions. This is transcribed into appropriate system development effort including engineering modelling, prototype construction, risk assessment, and interface identification of system and subsystem elements. Systematic evaluation of the integrated system functions is conducted to verify interoperability of system performance and interactions with external environments to validate final system configuration. Maintenance support planning, maintenance access, operation procedures, and assurance as well as support processes should be well established prior to system realization.

c) The **realization/implementation** stage is to execute make-buy decisions for acquisition and deployment of subsystem elements. The realization efforts deal with activities such as technology applications, manufacturing, packaging and supplies sourcing to ensure the complete transformation from system design to the specified product or subsystem elements. The realized products or elements may comprise a combination of hardware and software functions. Implementation includes such activities as integration of system functions, verification of subsystems, and installation of the system. System acceptance procedures should be established with the customer for system trials in the actual operating environment prior to commissioning. Validation should be a part of the trial to provide objective evidence of conformance to system specification. It should be noted that verification and validation are activities that take place at each life cycle stage and not just at system integration as indicated in Figure 2.

d) The **operation/maintenance** stage is used to deploy the system for delivery of service and to support system operational capability by means of maintenance. The process activities include operating and maintaining the system for service in accordance with system performance requirements, operators and maintainers training to maintain skills competency, customer interface to establish service relationship, and record keeping on system performance status and reporting failure incidents to initiate timely corrective and preventive actions. The system performance should be monitored and checked on a regular basis to ensure that reliability and quality of service objectives are met.

e) The **enhancement** stage is to improve system performance with added features to meet growing user demands on the system. The process activities include software upgrade, hardware addition, skills training, simplifying procedures to improve operational efficiency, obsolescence management, organizational restructuring to increase expediency and customer value.

f) **retirement/decommissioning** stage is to end the existence of the system entity. Upon termination of system service to the customer, the system may be disassembled, redeployed for other use, or disposed of where possible without affecting the environment. For complex systems, a strategy for decommissioning should be established to formalize planning and implementation of the decommissioning process to meet regulatory requirements. For consumer products regulatory rules concerning return and reuse or disposal may be in existence.

A.1.2 Process activities for system life cycle stages

Figure A.1 also shows the linkage of process activities from stage to stage in a system life cycle. Major decision points are shown to indicate the start and end of the process activities at each stage where resource commitments are made to advance the technical processes. Relevant data are captured during the process activities. They provide the essential information for life cycle cost analysis and risk evaluation to support technical resolutions and business decisions.

The relevant data captured includes the key inputs necessary to initiate the process activities of each stage, the major dependability activities to be performed, the relevant influencing factors for consideration, and the outputs resulting from the process generated efforts. When possible, the priority and impact relevant to the process activities should be indicated. This provides useful information for risk assessment and life cycle costing. Where appropriate, the technical approaches and engineering methods used for the process activities should be identified.

A.2 Examples of engineering process applications

A.2.1 Process for the system concept/definition stage

Inputs:

- customer requirements, needs and wants;
- regulatory requirements related to health, safety, security, and environmental concerns;
- company policy on bid decisions;
- market intelligence and competitions.

Key process activities	*Dependability related activities*
Requirements definition	
• Identify customer of the system, how the system is to be used, and for how long. • Identify system application environments. • Identify constraints related to potential system solutions. • Identify legacy issues related to interoperability with existing systems. • Establish system operating profile. • Document system specification. • Identify schedules and system deliverable targets. • Respond to customer RFP (request for proposal) if applicable.	• Identify dependability needs associated with the system applications. • Identify system availability and allowable outage downtimes acceptable by the customer • Identify technology constraints related to the scope and extent of achieving dependability objectives. • Gain knowledge of field performance history of existing or similar systems if available.

Requirements analysis	
• Determine system boundaries, operating functions and performance characteristics from the set of defined system requirements. • Evaluate the constraints identified affecting architectural design. • Determine technical approaches and feasibility for system realization. • Determine technical and quality measures enabling system assessments. • Identify capability to undertake the system work. • Identify potential partnership and suppliers requirements.	• Determine operating scenario for dependability assessments. • Define system failures and performance degradation limits. • Identify risk exposures and criticality of system failures. • Determine the number of maintainers and their associated skill level required. • Analyse system structure and breakdown of system functions. • Analyse system availability contributed by functional configuration of architectural design. • Perform fault tree analysis to determine critical areas requiring design attention. • Conduct system level failure modes and effects and criticality analysis to support design alternatives and justifications. • Evaluate system availability and cost trade-off affecting design options. • Determine means for dependability assessments.
Architectural design	
• Determine appropriate logical architectural design options. • Establish system configuration. • Partition system functions. • Establish design criteria and interfaces. • Formulate make/buy decisions of system functions. • Select technologies for design and choice of hardware/software for realization of functions. • Formulate solution to meet system requirements. • Establish means for verification and integration of system functions.	• Establish plan for dependability evaluation. • Availability allocation of system functions. • Determine failure criteria of system functions. • Evaluate reliability of each partitioned function and recommend alternate design options if required. • Identify critical functions requiring attention. • Establish maintainability criteria for design. • Establish testability of system function for diagnostics and recommend maintenance actions.

Functional design/evaluation	
• Formalize the functional design process. • Identify design composition of hardware/software elements for each function. • Incorporate test functions for performance verification. • Establish human factors design criteria. • Establish environmental design criteria. • Establish ergonomics design criteria. • Establish EMC design criteria. • Establish safety, security and reliability design criteria. • Establish hardware design rules. • Establish software maturity design schemes. • Simulate system performance at the functional level to determine fault coverage and system recovery strategy. • Verify performance limits and interoperability of the functional design to meet architectural design requirements.	• Conduct reliability assessment. • Conduct maintainability evaluation. • Conduct functional level failure modes and effects and criticality analysis. • Conduct functional level design trade-off, fault tolerance and risk evaluation. • Establish maintenance and logistics support plan. • Establish process for supplier evaluation for quality assurance and reliability conformance. • Establish process for commercial off-the-shelf product evaluation and acceptance.
System design documentation	
• Document system specifications.	• Incorporate dependability requirements in system specifications.

Influencing factors for consideration:

- competitions;
- economic issues;
- technology issues;
- capability issues;
- environmental issues;
- legal issues;
- timing for investments issues.

Enabling mechanisms for process applications:

- human resources;
- financial resources;
- facilities;
- integrated design and implementation processes;
- assurance process.

Outputs:

- system specifications;
- systems design knowledge.

A.2.2 Process for the system design/development stage

Inputs:

- system specifications;
- architectural design requirements;
- dependability plan.

Key process activities	*Dependability related activities*
System design	
• Establish system design/development plan. • Specify system/subsystem interface requirements. • Establish linkage with interacting systems. • Establish human interface requirements. • Establish configuration management plan and design change procedures. • Establish physical dimensions and standardize assembly footprints. • Establish emission and susceptibility rules for facility construction, cabling and wiring inside and outside of buildings and equipment housing structures. • Reach agreements with suppliers for development and acquisition of hardware/software elements. • Initiate prototype construction of subsystems. • Establish system integration procedures. • Establish test plan and system acceptance criteria. • Establish system monitoring, diagnostic schemes, incidents reporting and data management system. • Establish training programs.	• Establish system dependability program. • Establish quality assurance program. • Formalize dependability requirements for system, subsystems and functions. • Establish suppliers' dependability programs. • Establish dependability acceptance criteria and reliability growth programs. • Establish system maintenance and logistics support program. • Establish failure reporting, analysis, data collection and feedback system. • Define human reliability criteria. • Define warranty conditions.
Subsystem development	
• Initiate in-house development for subsystems. • Initiate interface development for interoperability. • Monitor and collaborate with material outsourcing and contracting external development efforts. • Prepare production plan. • Prepare operation plan. • Prepare maintenance and logistics support plan. • Prepare packaging, handling, storage and transportation plan. • Prepare installation plan. • Prepare integration plan. NOTE The listed plans may be integrated as activities in the master project plan for ease of update and coordination of project activities.	• Implement subsystem dependability program. • Implement supplier's dependability program. • Develop spares provisioning program. • Develop software test and diagnostic program.

Influencing factors for consideration:

- availability and access to relevant skills resources;
- commitment targets for development schedules;
- project risks.

Enabling mechanisms for process applications:

- availability of specific tools required for development;
- training needs.

Outputs:

- system prototype;

- system and subsystem support requirements.

A.2.3 Process for the system realization/implementation stage

Inputs:

- system prototype.

Key process activities	*Dependability related activities*
Realization	
• Carry out physical production of subsystems. • Realize construction of hardware/software elements. • Perform test evaluation of functions. • Carry out training of operators and maintainers. • Ensure test equipment and test facility are ready. • Ensure packaging, handling, storage and transportation instructions are ready.	• Implement system dependability program. • Implement quality assurance program. • Implement suppliers' dependability programs. • Implement system maintenance and logistics support program. • Implement failure reporting, analysis, data collection and feedback system.
Integration	
• Execute integration plan. • Assemble and integrate system entity. • Prepare verification and validation plans and procedures. • Prepare system acceptance plan.	• Implement integration related system dependability program. • Implement integration related quality assurance program.
Verification	
• Implement verification plan. • Document verification test results. • Prepare system acceptance plan. • Check verification results against system acceptance plan	• Conduct subsystem dependability assessments • Document failure reports from verification tests. • Generate incident reports for recommended corrective/preventive actions. • Resolve anomalies found during verification.
Installation/transition	
• Execute installation plan. • Document installation records and procedures. • Evaluate transition strategy for improvement.	• Establish shared maintenance support and reporting schemes with customer maintainers on system installed on customer premises. • Monitor turn-around-time for system restoration and replenishment of spares. • Maintain adequate spares inventory on maintainer's/customer's site.
Validation/commissioning	
• Implement validation plan. • Document validation test results. • Execute system acceptance plan. • Implement warranty schemes if applicable. • Customer sign-off for system acceptance to initiate system operation.	• Validate that system performance fulfils the dependability requirements. • Document failure reports from validation tests. • Generate non-conformance reports for recommended corrective/preventive actions. • Resolve anomalies found during validation. • Resolve warranty issues with customers.

Influencing factors for consideration:

- transition management;
- commitment targets for system delivery schedule;

- warranty requirements and incentives.

Enabling mechanisms for process applications:

- project management;
- customer training.

Outputs:

- system operation for service;
- customer support.

A.2.4 Process for the system operation/maintenance stage

Inputs:

- system in full service operation.

Key process activities	*Dependability related activities*
Operation	
• Implement operation strategy. • Monitor system performance. • Provide customer value.	• Implement reliability growth program. • Implement field data collection system. • Conduct customer satisfaction survey.
Maintenance	
• Implement maintenance support strategy. • Monitor system maintenance efforts. • Provide customer care service. • Implement maintenance activities for adaptive corrections.	• Analyse failure trends. • Conduct root-cause analysis of problem areas. • Recommend design or procedural changes for continual improvement. • Determine quality of service.

Influencing factors for consideration:

- system service capacity;
- supply chain for spares provisioning;
- responsive maintenance actions.

Enabling mechanisms for process applications:

- project management;
- operators and maintainers training.

Outputs:

- dependable system performance;
- customer satisfaction results.

A.2.5 Process for the system enhancement stage

Inputs:

- new customer requirements;
- enhanced features.

Key process activities	*Dependability related activities*
Enhancement	
• Identify new requirements. • Establish enhancement strategy and plan. • Evaluate the need for change and resulting benefits. • Implement enhancement efforts. • Implement activities for perfective corrections.	• Evaluate impact on dependability performance due to changes with added new features. • Conduct life cycle cost impact study for change incorporation. • Conduct risk and value assessments. • Conduct customer satisfaction survey resulting from change reactions.

Influencing factors for consideration:

- timing for change;
- return-on-investments.

Enabling mechanisms for process applications:

- change management;
- obsolescence management;
- customers “buy-in” or reaction to new service features incorporation.

Outputs:

- enhanced system performance;
- customer satisfaction results comparison before and after enhancement efforts.

A.2.6 Process for the system retirement/decommission stage

Inputs:

- status of aging system performance capability;
- competitiveness and marketability of existing operation service;
- increased maintenance and support costs.

Key process activities	*Dependability related activities*
Retirement/decommissioning	
• Execute system retirement/ decommissioning plan. • Implement reuse and redeployment strategy. • Implement waste treatment on disposal items. • Notify the customers on service termination. • Provide information on new or alternative service provision.	• Evaluate constraints on system deactivation and impact on removal of system from operation. • Evaluate impact on environments of disposal items. • Conduct customer satisfaction survey due to termination of service.

Influencing factors for consideration:

- timing for retirement;
- technology obsolescence;
- regulatory constraints;
- social impact due to termination of service.

Enabling mechanisms for process applications:

- project management.

Outputs:

- termination of service.

Annex B
(informative)

Methods and tools for system dependability development and assurance

B.1 General

Methods and tools are useful aids for solving generic technical problems including engineering dependability into systems at various life cycle stages. There are numerous tools and a multitude of tool vendors in the market. Some of the tools are standard forms and simple checklists; others are complex interactive systems often requiring licensing agreements for database access and technical support. Methods and tools are commonly developed in-house based on past engineering experience, or they can be purchased from tool vendors to facilitate staff training and multiple project usage. The selection of the appropriate methods for technical solution should be at the discretion of the engineers or practitioners performing the dependability task. Since investments are involved in the choice of tools, the engineer or practitioner should consider the relevancy of the class of dependability engineering problems that need to be solved, the frequency of tool usage, the training effort required to effectively use the tool to achieve results, and the availability of alternative methods of using simpler techniques to solve the same problem with a simple tool set developed in-house. The following provide typical examples of general applications, hardware specific applications and software specific applications of methods and tools for engineering dependability into systems.

B.2 General applications of methods and tools for engineering dependability into systems

B.2.1 Reliability and maintainability case

The reliability and maintainability (R&M) case tool is used by a system acquirer to ensure that the R&M requirements of the purchaser are determined and understood by both the supplier and purchaser of a system. The tool also provides a means of achieving progressive assurance that the R&M requirements are being or will be satisfied throughout the life of the system.

The tool provides a framework for:

a) the R&M case – a reasoned auditable argument to support the contention that a defined system satisfies the R&M requirements;

b) the R&M case report – a summary or abstract of the R&M evidence and arguments from the R&M case to support programme milestones; and

c) progressive assurance of R&M throughout the project milestones.

Reference document: DEF STAN 00-42 [11].

B.2.2 Reliability growth programs

Reliability growth programs are used for system reliability improvement during the system design/development stage. The objective of reliability growth is to realize the potential of system reliability targets by step-wise improvements using techniques in design analysis and reliability testing of the system modules or functions. The critical dependability activity is to identify and remove design weaknesses in the system for progressive reliability enhancement. Typical systems that would benefit from the application of reliability growth programs are those systems using novel architectural design techniques, new and unproven system components, and software intensive contents for incorporation in system operation. The

reliability growth concept is to reduce the probability of failure occurrence due to design weaknesses via progressive design improvements of the system and its constituent functions throughout the design and development process. Reliability growth programs should be integrated into the system design and evaluation process to achieve cost-effective solutions. reliability growth program is described in IEC 61014 [12]. The reliability growth models and estimation methods for reliability growth assessments based on failure data captured in the reliability growth program are described in IEC 61164 [13].

B.2.3 Configuration management

The management of the various and successive system configurations is a major concern for dependability (i.e. maintenance support). This is due to the variety of interfaces generated through different configurations. The increasing demand for inter-changeability of components (hardware and software) and interoperability of systems has direct commercial relevance and implies specific attention to configuration management. This is particularly true for long-life systems with shorter life components, which may change frequently in technology over the life of the system. During system development, a sound configuration management system contributes significantly to effective dependability achievement. Configuration management is essential for system change controls and meaningful dependability assessments. Guidance on general configuration management is described in ISO 10007 [14].

B.2.4 Bayesian belief networks

Bayesian belief networks (BBNs) are a powerful graphical formalism to support reasoning about uncertain events using diverse forms of evidence. They enable modelling of uncertainty and the combination of different types of evidence, including both subjective information based on expert judgement and ‘hard’ evidence from measurement. A BBN will accept as much or as little evidence as the user has available or wishes to enter, so it can make a prediction with missing or incomplete data. This methodology offers a useful approach to predicting dependability of a system at all life cycle stages when a mixture of indirect and direct dependability measurements is available.

There are numerous commercial Bayesian Network products available which facilitate the entry of data and setup of BBNs.

B.3 Hardware specific applications of methods and tools for engineering dependability into systems

B.3.1 Reliability enhancement

System reliability enhancement for hardware elements focuses on the inherent properties of the system functions and the influencing factors affecting the system reliability performance. The primary focus is on the technology used in system construction, the system operating environment, and the application of system functions to achieve system performance objectives. There are many classical reliability methods and techniques applicable for reliability assessments as described in IEC 60300-3-1. Reliability improvement can be achieved by proper incorporation of the recommended results with practical solutions based on relevant reliability assessment inputs. In most cases, design trade-off is necessary to determine the best solution. Some of these methods can be used for checks and balance to verify the analysis results of assessments done on the same hardware element.

Typical examples in the use of reliability methods and tools include:

- using reliability block diagram (RBD) to determine redundancy needs versus using a single higher reliability hardware element of new technology with a cost premium;
- using Markov analysis for reliability evaluation of complex system structures and complex maintenance strategies;
- using fault tree analysis (FTA) to identify critical failures in a system;

- using failure modes and effects analysis (FMEA) to determine the potential failure modes, effects and causes, and associated criticality of the risk exposures;
- using failure rate prediction to estimate the inherent reliability of hardware elements.

It should be noted that there are limitations to the use of reliability methods and tools. Assumptions made in problem formulation are essential for justification and rationalization of the technical approach taken. Engineering judgement based on practical experience is needed for interpretation of reliability assessment results prior to the recommendations.

Because thermal effect and electromagnetic interference affect the performance of electronic components in system functions, it is prudent for system analysis to develop a means for thermal budgeting and electromagnetic compatibility budgeting to limit the risk exposure of catastrophic system failure. This approach presents a viable engineering analysis method for achievement of system reliability performance. Fault avoidance and fault tolerant designs are crucial for design incorporated in critical system applications.

B.3.2 Maintainability enhancement

For maintainability enhancement it is important to consider the ease of maintenance of a repairable hardware item in the form of an assembly unit. This implies that the item when malfunctioning or worn-out could be identified, isolated, removed and replaced with a new item. The criteria establishing maintainability in system design deal with the partitioning of the system assembly for easy access, the construction of the lowest replaceable unit for replacement, the testability of the lowest replaceable unit for fault detection, and the cost and reliability of the lowest replaceable unit for spares provisioning. This will also determine the economics of a throwaway item or a repairable lowest replaceable unit.

System maintainability generally deals with three basic levels of repairs:

a) **organization level** – system restoration at the system location that usually involves replacing the lowest replaceable unit as a plug-in module with relatively short isolation and replacement times;

b) **intermediate level** – restoration of the lowest replaceable unit at an intermediate shop facility to further test, diagnose, repair/rework and restore the unit to its operational state for recycle. This would require longer time duration;

c) **depot level** – more extensive repair and rework can be done to restore the item to its operational state for recycle. This would require much longer time duration.

If the lowest replaceable unit is a throwaway item then the system maintainability is much more simplified with only two levels of maintenance. Replacement of failed unit only occurs at the organization level and the supply of spare unit comes from the depot, which could be the factory or the original equipment manufacturer. No repair shop is required. The challenge and incentive here is to design a cost-effective throwaway item that is environmentally friendly for disposal.

Testability is an importance parameter for hardware maintainability enhancement. The extent of diagnostics and test coverage of the failed unit often dictates the time and effort spent in determining no-fault-found item, which drains the maintenance resources. Repair policy should clearly track these no-fault-found items and identify how many times a failed item has gone through the repair/rework line before being discarded as a throwaway. The repair policy should also review and assure the accuracy and effectiveness of the test equipment to clearly identify and determine the faulty item.

The maintainability design should consider the human factors aspects to facilitate human interactions for system restoration and maintenance service operation. Safety and security issues should be taken into consideration during preventive and corrective maintenance work. Guidance for maintainability design and applications is described in IEC 60300-3-10 [15].

B.3.3 Maintenance and logistic support enhancement

System maintenance and logistic support focuses on sustaining system performance in meeting its operational objectives. The activities are mainly conducted during the system operation/maintenance stage. Enhancement for maintenance and logistic support can be achieved by improvement in the supportability of the system within the constraints of the established system configuration and operational scenario. There are values to be gained by improvement in customer 'care' service and simplification of service support procedures. Improvement can also be made by effective automation in maintenance activity reporting, and deployment of logistic support analysis system. The logistic support issues concerning centralized or decentralized support depot system, and strategic planning and scheduling of maintenance support tasks could result in reduction of maintenance time and effort. In today's competitive market environment where systems reside in customer premises and widely distributed on a global basis, it is prudent to consider that essential maintenance work to be done by third-party contract maintenance. The outsourcing of maintenance support work requires additional training of contract maintenance staff with the proper skills and competency to carry out the necessary service for the customers. They are the first line maintenance staff to deal with customer complaints. Information gathering of customer concerns on the service work done and the customer confidence in the system would become a major challenge for coordination of system maintenance support process. Various methods have been employed for such enhancement techniques including reliability centred maintenance (RCM) as described in IEC 60300-3-11[16] and the integrated logistic support (LSI) process described in IEC 60300-3-12 [17].

B.4 Software specific applications of methods and tools for engineering dependability into systems

B.4.1 Object oriented methodology

This is an approach to model a system as a set of interacting objects with associated data and behaviour. It is based on decomposing the requirements or design of a system into a hierarchical set of classes and objects.

B.4.2 Structured methodology

This is a technique based on decomposing the requirements or design of a system into a set of algorithmic processes interconnected by a defined data flow. The processes perform a transformation on input data to generate output data. The decomposition can be procedure-oriented, data-oriented, or information-oriented. Structured methodologies can also be characterized by whether or not the methodology is intended for real-time system.

a) **Procedure-oriented method –** an approach that views the algorithmic processes in the system model as its fundamental characterization. Data definition follows from the defined processes.

b) **Data-oriented method** – an approach that views the input and output parts of the system model as its fundamental characterization. The algorithmic processes are derived from the data structures.

c) **Information-oriented method** – an approach that uses a logical data model for integrating information system components. It emphasizes the strategic requirements for data across an enterprise level system. The information system components are then built based on the requirements of the logical data model.

B.4.3 Functional decomposition design

Functional decomposition design is an approach that focuses on the definition of modules and interfaces by partitioning the specified functions of a software system. The design process is usually undertaken after the system requirements are developed and a concept has been chosen for the system structure. The iterative process refines the design in a complementary top-down and bottom-up manner. This is achieved by breaking a system into interacting functions or the functionality of system elements. System design hierarchy generally consists

of three levels: the top-level design, the mid-level design, and the lowest level detailed design. The behaviour of each level of system hierarchy can be described by diagrammatically representing the inputs and outputs, and the process of transformation of the relevant functions. At each level a block diagram can be drawn by using the information obtained through the functional decomposition process. These diagrams show how the system elements in the system architecture can work together and the functional description of each block can relate to its operation. The approach is very similar to the reliability block diagram (RBD) method with different designation of block functions. The method of functional decomposition is a powerful tool for designing systems that provides a systematic approach to capture the description of system hierarchy and its constituent system functions. Formal application of functional design techniques improves the quality of designs and enhances the dependability of performance operability. Examples of functional decomposition design methods are step-wise refinement, structured design, and real-time design.

B.4.4 Error analysis

Error analysis consists of:

- the process of investigating an observed software fault with the purpose of tracing the fault to its source;
- the process of investigating an observed software fault to identify such information as the cause of the fault, the phase of development process during which the fault was introduced, methodology by which the fault could have been prevented or detected earlier, and the method by which the fault was detected;
- the process of investigating software errors, failures and faults to determine quantitative rates and trends.

Error analysis involves determining if the cause of the problem is hardware or software.

B.4.5 Delphi technique

This is a group forecasting technique, generally used for future events such as technological developments, that uses estimates from experts and feedback summaries of these estimates for additional estimates by these experts until reasonable consensus occurs. It has been used in various software cost-estimating activities, including estimation of factors influencing software costs. For a detailed understanding of the Delphi technique reference should be made to a document dedicated to the Delphi technique such as The Delphi method: Techniques and applications, edited by H. A. Linstone and M. Turoff".

B.4.6 Computer-aided software engineering (CASE) tools

CASE tools are computer-aided software engineering tools that help automate one or more aspects of the software engineering process. CASE tools are commonly used in software engineering development and maintenance work. There are numerous CASE tools created by software vendors and used for specific applications by various organizations. CASE tools are commercially available to facilitate software applications such as system structure analysis, requirements management, modelling and simulation, software graphic design, code generation, re-engineering, "bug" tracking, report generation, and help authoring. CASE tools are COTS software products. The selection and application of CASE tools should follow standard evaluation process for assurance purposes. Guidance on classification of CASE tools is described in IEEE Std 1175.1 [18]. Guideline for evaluation and selection of CASE tools is described in ISO/IEC 14102 [19].

B.4.7 Software engineering environments (SEE) services

SEE is a collection of software services, partially or fully automated by software tools that are used to support the execution of human activities in software engineering. SEE activities are usually carried out within a software development and maintenance project environment. They cover such areas as the specification, development, re-engineering or maintenance of

software-based systems. SEE applications may cover several situations; from running a few tools on the same operating system, to the fully integrated environment, able to handle, monitor, and control all the data, processes and activities in the software life cycle. A SEE provides support to human activities through a series of services that describe the capabilities of the environment. The software process supported by a SEE becomes an assisted or automated software process. SEE can be considered as an enabling system. Further information on SEE can be found in ISO/IEC 15940 [20].

B.4.8 Capability maturity models

Capability Maturity Model (CMM) is used by organizations to describe their software process maturity. The CMM ranks an organization on a level of 1 to 5:

– Level 1: considered ad hoc or chaotic
– Level 2: repeatable processes
– Level 3: defined processes (industry minimal standard on technical processes)
– Level 4: measured processes
– Level 5: optimized processes

CMM model is used in a systematic way based on a set of principles to derive a maturity questionnaire. A model can emerge by fully elaborating the maturity framework. It provides the organization using the model with effective guidance for establishing process improvement programs.

The CMM for software (SW-CMM) helps the organization increase the maturity of the software processes by using the knowledge acquired from software process assessments and extensive feedback from industry best practices.

CMM focuses on the development process. The process areas define the building blocks or bodies of knowledge based on industry practices. The maturity levels define the dependencies and priorities for improvement.

The Level 1 is to guide organizations by focusing on limited process improvement resources on the most important changes. The prioritization is important because most lower maturity software organizations do not have the historical data necessary to determine if a change is actually an improvement. That is, the change will produce a statistically significant improvement, within some predicted period of time, including all costs associated with making the change, as compared to not changing.

The Level 2 addresses mainly the management processes for better planning of schedule, time and resources, tracking, and project control.

The Level 3 establishes an organizationally defined repeatable development process that becomes the baseline for future measured improvements. It also establishes the mechanisms to collect process/product data and the methods to determine how process performance and quality tack against business goals.

The Level 4 addresses those variations that are not part of the system of common causes. It recognizes that the development process is a system and statistical techniques can be applied. It is used to predict performance and quality based on experience and data.

The Level 5 addresses common causes of variance, to analyse the cause of defects, measure potential changes intending to reduce or prevent those defects, and determine if the changes are actually improvements. This is the process of optimization or continuous improvement.

CMM provides a benchmark to compare organization's development process capability and to use that measure as a predictor of product quality.

As the use and experience with SW-CMM has increased, models have been developed for different disciplines and technical applications. One such model is the Systems Engineering Capability Maturity Model (SE-CMM). Software engineering capability is the ability of a software organization to perform successfully in terms of cost, schedule, product functionality, and quality. The capability has several dimensions including

1) the expertise, experience, training, and motivation of the people performing and managing the work,
2) the process capability, and
3) the technology that is available and applied.

The separate models for Software Engineering (SW-CMM) and Systems Engineering (SE-CMM) used by organizations have created confusion in the software industry. They have become redundant and often counter-productive in practice. The differences between the SW and SE models made it difficult for an organization to use both models concurrently.

The solution to this confusion is to deal with the mismatch by creating the Capability Maturity Model Integration (CMM*i*). The CMM*i* is to reconcile the inconsistencies in architecture, approach, terminology, and other compatibility issues between the SW-CMM, SE-CMM, and related models. The outcome of the creation is a set of models, and supporting infrastructure, collectively referred to as CMM*i*.

CMM was developed by Software Engineering Institute (SEI) registered to Carnegie Mellon University. Reference to CMM can be found in www.sei.cmu.edu [21].

Annex C
(informative)

Guidance on system application environment

C.1 Understanding system application environment

The guidance on system application environment presents a system view for the end product environment when integrated into system operation. This is to provide relevant information of the system operation environment for robust and dependable product designs and material selection suitable for system application. Relevant criteria for development or selection of hardware products are provided for functional design considerations. The examples shown in the application environment are for generic ground-based systems.

The value of presenting a comprehensive set of relevant design criteria is motivated by the following factors:

a) experience has shown that specific product designs or acquisitions often overlooked the linkages of human interfaces, electromagnetic, climatic, and mechanical conditions and other performance factors as viewed from a system perspective for end product applications. The approach presented herein would facilitate system architectural design and product integration to conform to global market requirements;

b) data gathering and cross referencing of standards against customer requirements could involve extensive effort. This guidance provides a ready reference and inputs for design specifications;

c) the current product development trend is moving away from designing to meet a specific customer's requirement because of time-to-market constraints. This guidance presents a broad range of application segments where the use environment and product needs could be rationalized for cost-effective product development and acquisition to facilitate system integration;

d) controls of environment and product performance characteristics are being progressively applied at the system, subsystem and product levels as cost-effective measures to achieve optimal design solutions to meet changing global market demands. It reflects the trend towards international collaboration and standards harmonization to facilitate system and product development.

C.2 Environmental requirements definition process

Figure C.1 presents an overview of the requirements definition process.

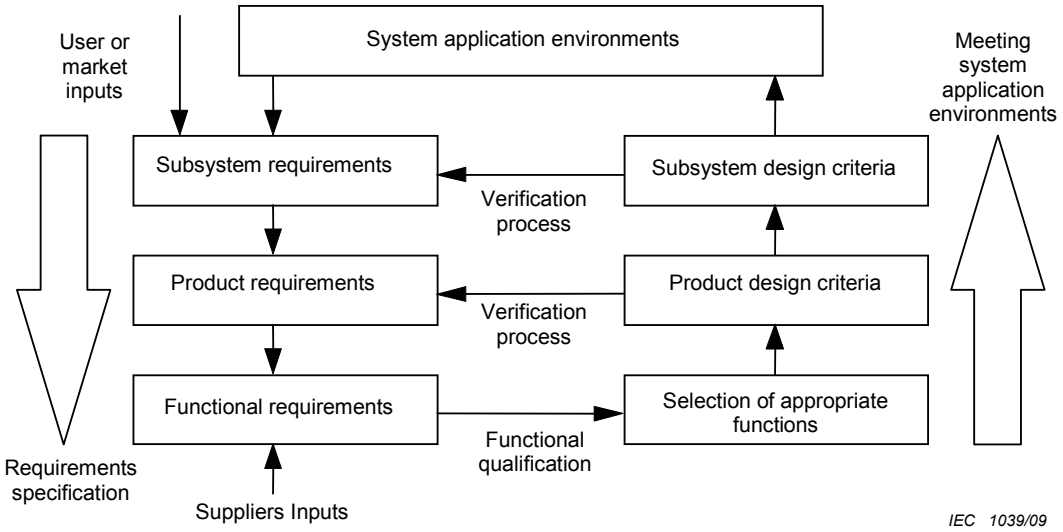

Figure C.1 – Environmental requirements definition process

Requirements definition is a top-down process whereby the system environment for the intended integration of subsystems, products and functional applications are defined. The system environment conditions are then translated into requirements for the constituent products and functions. User needs and market inputs are generally used to guide the development of requirements specification.

A parallel design verification process is employed to complement the requirements definition process. This is a bottom-up process to ensure the fulfilment of requirements at every stage of the intended design, from functional applications selection, through product development to system integration. The objective is to meet or exceed end use system application performance requirements.

The end use system environment conditions are provided in Clause C.3. The requirements pertaining to the use environment applicable to products integrated in the system are identified in terms of specific performance characteristics. They permit product environment classifications and identification of applicable environmental exposures.

C.3 System environment conditions

C.3.1 Classification of system environment conditions

Figure C.2 illustrates the mapping of system application environments to exposures. The noted electromagnetic, climatic and mechanical conditions, as exposed to a designated system application, provide the design envelope for a specific product environment classification.

The linkage between exposures and the performance characteristics associated with the attributes of the product designs should be noted (see the IEC 60721 series) [22].

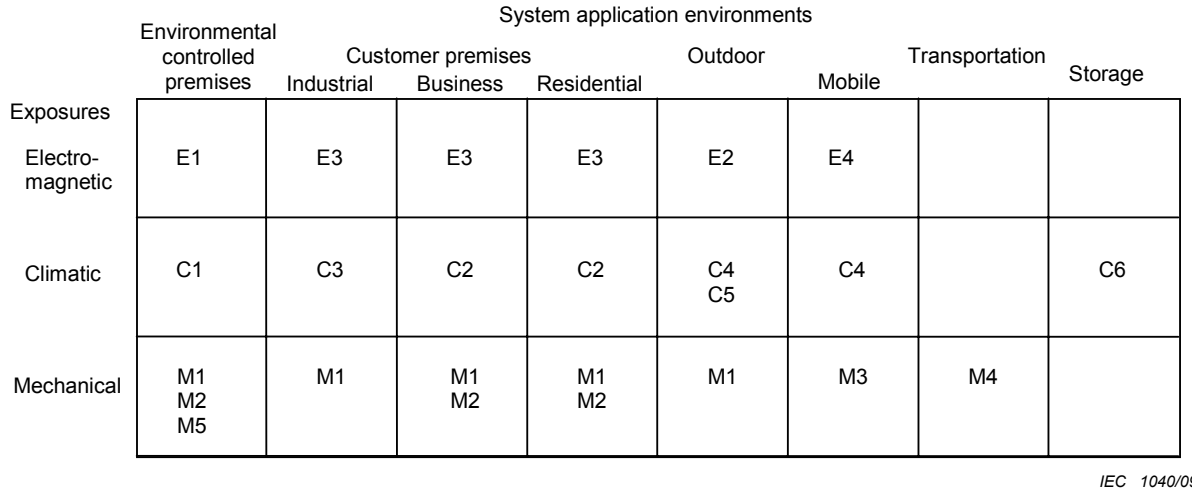

Figure C.2 – Mapping of system application environments to exposures

C.3.2 Electromagnetic conditions

Electromagnetic conditions consist of the following environmental exposures:

E1 Environmental controlled premises (e.g. laboratories, clean rooms)
E2 Outdoor locations
E3 Customer premises
E4 Portable and mobile applications

C.3.3 Climatic conditions

Climatic conditions consist of the following environmental exposures:

C1 Controlled climate (e.g. laboratories, clean rooms)
C2 Indoor temperature controlled
C3 Indoor temperature not controlled (e.g. unheated garage)
C4 Outdoor protected (e.g. sheltered)
C5 Outdoor unprotected (e.g. open field)
C6 Storage

C.3.4 Mechanical conditions

Mechanical conditions consist of the following environmental exposures:

M1 Stationary
M2 Portable
M3 Mobile
M4 Transportation
M5 Earthquake

C.4 Design characteristics influenced by system application environment

Design characteristics are influenced by the system application environment. These characteristics are inherent in the system performance attributes. They affect the system design architecture, the technologies used in system functions, and the packaging strategy to achieve optimum performance operation. Correlation and mapping of the design

characteristics to the end-use environment are essential for development of system application environment. The mapping process is to identify common characteristics and worst case constraints for product design suitable for system application. The aim is to ensure integrity and robustness of the product when integrated into the system for use in different environment conditions. The mapping exercise provides a technical approach for consideration of product design options and selection of alternate technologies.

System performance attributes	*Design characteristics influenced by system application environment*
• Electromagnetic compatibility	• System design architecture • EMC budget and emission limits • Clock rates • Shielding and filtering requirements
• Thermal	• Power consumption and distribution • Thermal budget and temperature limits • Cooling methods • Heat transfer mechanisms
• Quality	• Quality process • Acceptance criteria • Non-conformance monitoring and elimination • Supplier qualification
• Dependability	• Availability performance and permissible downtime/frequency • Mean-time-between-failures • Mean-time-to-restoration • Maintenance support and spares provisioning strategy • Life times and failure free periods
• Environmental compatibility	• Environmental life cycle process • Design for reduce, reuse and recycle • Environmental impact • Risk exposures

C.5 System performance attributes for design considerations

C.5.1 General

The information contained in the correlation and mapping of Figure C.2 and Figure C.3 can facilitate the design of specific system function or product for use in designated system application environment. The following descriptions of specific system performance attributes provide useful background information essential for design considerations.

C.5.2 EMC design considerations

Electromagnetic compatibility (EMC) is the capability of a product to function without emitting or being affected by electromagnetic noise. Emission is the electromagnetic energy or unwanted noise emanating from a source. This can come from sources such as a high frequency clock embedded in an electronic circuit or module contained in a product. Immunity is the ability of a product to resist electromagnetic noise. This can come from nearby operation of radio and television transmitters, or from electrostatic discharges. Emission levels are regulated in many countries to prevent interference. Electronic product designs should meet their respective emission limits for product marketing and application purpose. Partitioning is the technique used for designing a product to meet EMC requirements. The translation of EMC requirements from the system level down to the product level, and to the module level requires an EMC budgeting process. This involves detailed analysis of the devices used in the module, shielding strategy and placement of components, routing of cables and printed wiring. The contributions from all available emission sources within the module are used to determine the level of design margins. This is the margin of tolerance in the module design that may impact the performance of the module within a product when integrated into a system exposed to electromagnetic environment.

C.5.3 Thermal design considerations

Thermal requirements are highly influenced by the application system function and the environmental exposures subjected to the product or the modules operating inside the system. The fundamental thermal issue is concerning the heat generation and heat removal to permit sustainable performance integrity. Heat generation is influenced by the device function needed for the application, the power consumption and dissipation of all components within the confines of the module physical design envelope. Heat removal strategy could be conductive, convective, and by radiation. Typical system cooling situations are forced air or natural convection. The performance of a high density packaging module is sensitive to heat sources generated internally within the module contributed by the devices used in the module design. The ambient temperature of the module operating environment or surrounding will also affect the module performance. Abnormal temperature rise due to undesirable internal heat sources or external heat transfer will affect the reliability performance of the module. Thermal budgeting of the power dissipation of potential heat generating sources would provide the basis for identification, reduction and removal of unwanted heat generated within the module. Thermal design should take into consideration the power dissipation, the temperature rise, the rate of cooling, and the thermal operating limits of devices. Thermal budgeting should be managed at all levels of the system hierarchy from a system perspective.

C.5.4 Quality design considerations

Quality embraces all inherent characteristics of an entity (system, product, module, or component) that bear on its ability to satisfy stated and implied needs. Quality implies the conformance to requirements; hence the acceptance criteria and control procedures are established for conformance acceptance. This is to ensure continuous compliance to established standards with appropriate mechanisms built into the system or process to facilitate continuous improvement. Quality assurance and quality control processes are well established within the industries. Quality design methods are described in literature and quality design considerations will not be elaborated here.

C.5.5 Dependability design considerations

Dependability is the inherent capability of a system to provide availability performance to provide a level of satisfactory service upon demand. Availability is a performance characteristic dependent on its influencing factors consisting of performance functions of reliability, maintainability, and maintenance support. Dependability design considerations have been addressed in other sections of this part of IEC 60300 and will not be elaborated here.

C.5.6 Environmental compatibility design considerations

Environmental compatibility is essential in today's market place. Environmental impact of the product and module at the time of replacement or disposal presents a challenging situation to the developers and manufacturers of the products. Typical user or customer demands are in the form of a take back contract whereby the provider or supplier of the product is subjected to take back the replacement product prior to the installation of a new product for service. Buy back contracts are also common in today's business where the supplied quantity of spares retained or purchased by a user or customer is not being used at the end of an agreed time period, the provider or supplier will need to buy back the spares. In the design and manufacturing of products and modules, consideration should be given to the re-use of disposal parts. Recycle of by-products in the production process to minimize waste disposal is another factor to be considered in the environmental impact studies. Reduction of emissions and wastes from the product environmental life cycle process should also be taken into consideration.

Annex D
(informative)

Checklists for system dependability engineering

D.1 Checklists for system dependability project management

D.1.1 General

The system dependability checklists are applicable to the system life cycle at the major decision points to facilitate project management reviews. These checklists identify the critical issues that need to be addressed to validate the completion of key system dependability activities of each project phase. Regular project reviews between major decision points are recommended for progressive implementation of tasks for dependability achievements. This is to ensure that all critical issues have been assessed and resolved. The review records can be used as objective evidence to support the project dependability assurance process. The checklists reflect the processes for transfer of project responsibilities and transition of system ownerships during the entire system life cycle. These checklists can be used by the supplier and the customer for project tailoring to meet their specific application needs.

D.1.2 Market identification checklist

a) The nature and applications of system dependability performance are defined and the intent to replace an existing system or to enhance its performance is known.

b) Timing for new system introduction with specific dependability features has been established.

c) The system operating environments, specific dependability influencing factors and related regulatory issues have been identified.

d) Technical capabilities for dependability engineering of system development have been identified.

e) The resources required to support the dependability project have been identified and estimated.

f) Capital investments and acquisition of specific dependability tools and enabling mechanisms for system development have been identified.

g) Potential customers and probable competitors interested in system development with dependability performance focus have been identified.

h) The expected system performance requirements and special system features are defined including the identification of unique dependability issues and customer expectations e.g. software robustness.

i) The system dependability operating scenarios, interoperability with other systems, technological design preference, and legacy issues involved has been identified.

j) The system maintenance and logistics support requirements for dependable operation have been identified.

k) A marketing strategy and plan for leveraging dependability in system performance has been established.

l) A project team for proposal and technical work with dependability expertise support has been established.

m) Go/no go decision for system development can be justified with a strategic dependability performance focus.

D.1.3 System development checklist

a) A project development plan for implementation of dependability tasks has been established.

b) System requirements are analysed and dependability characteristics assessed.

c) Design strategy, technology selection and dependability activities for system development have been determined.

d) Quality plan and dependability assurance process are established and implemented.

e) Standardization process and dependability design rules have been implemented.

f) System architecture and physical configuration in meeting system performance requirements have been determined.

g) System and subsystem integration plan has been established.

h) Hardware partitioning, software interfaces, and human factors designs to meet system performance requirements have been determined;

i) System dependability performance requirements and operating conditions are specified;

j) System test strategy, test coverage and functional evaluation are completed;

k) System functions to meet dependability performance needs have been evaluated;

l) System designs and dependability of system functions have been validated;

m) Outsourced project work, development partnerships and preferred suppliers are coordinated and accomplished;

n) Second sources have been identified and coordinated to support alternate project needs;

o) Applicable enabling systems and support strategy are deployed for system dependability achievements;

p) Manufacturability for product realization and related dependability issues are determined;

q) Design documentations, training instructions, and test procedures are completed.

r) System operation and support plan have been established.

s) Logistics support plan is established.

t) Maintenance policy and the levels of repair of lowest level assembly are established.

u) Go/no go decision for product realization can be justified.

D.1.4 Product realization checklist

a) Product implementation plan has been established.

b) Product quality and dependability assurance tasks are implemented.

c) Supplier product coordination and control for dependability assessment are completed.

d) Commercial-off-the-shelf products required for incorporation in system functions have been evaluated.

e) Product and subsystem evaluation for dependability verification are completed.

f) System and subsystem test and performance evaluation have been completed.

g) System integration and subsystem incorporation have been achieved.

h) Design freeze and configuration control plan is established.

i) System performance requirements have been validated.

j) System acceptance strategy has been established.

k) Failure reporting analysis and corrective action system has been established and implemented.

l) Go/no go decision for system transfer and customer acceptance can be justified.

D.1.5 System acceptance checklist

a) System acceptance plan is established with customer consultation.

b) System dependability performance demonstration plan and applicable warranty period have been established and accepted by the customer.

c) Incident reporting system is implemented and criteria for reporting established.

d) System operation and support plan to achieve dependability performance are implemented.

e) Training for system operators and maintainers is conducted and the trainees are certified, where applicable.

f) System support for third-party participation such as calibration services has been identified, coordinated and approved.

g) System hand-over procedures are established for transfer to customer operation.

h) Legal transfer of system ownership to the customer under contract is completed.

i) Go/no go decision for system in-service operation can be justified.

D.1.6 In-service operation checklist

a) System operation and support plan are implemented.

b) System performance monitoring and control procedures are implemented.

c) Incident reporting system is implemented to track dependability performance, service continuity operation, maintenance support activities, and corrective and preventive actions.

d) Maintenance actions are tracked.

e) Design change procedures and configuration control plan are activated.

f) Logistics support plan is implemented.

g) System operational analysis is implemented.

h) Operational anomalies and areas for improvement are identified.

i) System dependability performance trend is established.

j) End user satisfaction surveys are conducted.

k) Go/no go decision for retention of existing system in-service operation can be justified.

D.1.7 Enhancement checklist

a) Market needs for system enhancement have been established.

b) Risk and value assessments are conducted to justify the enhancement effort.

c) Impact on dependability performance due to enhancement changes is verified.

d) Impact on the environment and other influencing factors including regulatory, safety and security issues concerning the enhancement changes are investigated and validated.

e) The cost and time schedules for the enhancement work estimated.

f) The resources needed for the enhancement work are determined.

g) Go/no go decision for system enhancement can be justified.

D.1.8 Retirement checklist

a) The need and timing for system retirement has been established.

b) The causes for retirement such as technology obsolescence, economic and regulatory constrains have been determined.

c) Replacement system to provide continued system service is determined.

d) Social implications due to termination of service are assessed.

e) Go/no go decision for system retirement can be justified.

f) Plan for seamless transition from old to new system has been established and assured.

D.2 Checklists for hardware, software, and human factors design applications

D.2.1 General

The checklists for hardware, software, and human factors design applications can be used for engineering dependability into systems. They facilitate the process for product designs and system development. The selection of combined hardware and software elements for designing system functions often presents an opportunity for trade-offs to facilitate human interactions. Human factors play an important role to maximize system dependability performance. System designs should consider the checklists complementary for optimal design applications.

D.2.2 System hardware design checklists

a) System hardware requirements have been established.

b) The hardware elements selected for designing system functions have been identified.

c) The hardware technology and reliability history is known and has been assessed.

d) The system hardware configuration is determined.

e) Hardware design specifications have been established.

f) The hardware packaging concept and modularization scheme have been determined.

g) The thermal budget in an operating profile has been analysed to determine hot spots and cooling schemes with respect to the module ambient conditions and system operating environment.

h) The electro-magnetic compatibility budget in an operating profile has been established to identify the extent for shielding, filtering, partitioning and placement requirements.

i) Functional module interface and connectivity has been established.

j) Power feed and supply plan and voltage standardization for the system have been determined.

k) System reliability performance modeling has been evaluated for redundancy and design options.

l) Functional analysis and reliability allocation for each system function have been determined.

m) System and subsystem integration plan has been developed.

n) System maintainability and testability have been analysed and test coverage determined.

o) Built-in test capability and self-checking features where applicable are incorporated into the module design to facilitate fault identification and fault isolation..

p) Fault tolerant and fault avoidant designs are incorporated into critical system functions.

q) System maintenance concept and the levels of maintenance have been established.

r) Spares provisioning of the lowest level assemblies has been determined.

s) Turn-around-time for spares replenishment has been determined.

t) System simulation where needed to demonstrate availability performance has been conducted.

u) System test cases for fault detection, isolation and repair, and restoration time have been verified.

v) Commercial off-the-shelf hardware products are evaluated for incorporation into system functions.

w) System, subsystem, and functional module test plans and procedures are developed.

x) Design documentation is complete for hardware product and assembly production.

D.2.3 System software design checklists

a) System software requirements have been established.

b) The system architecture is determined.

c) Software standards are implemented for software design and development.

d) Software tools and services are acquired to support software development.

e) Software partitioning and allocation of functions has been established.

f) Software functions interface and protocol has been established.

g) Software design specifications have been established.

h) Software delivery schedules and plans for preliminary design and detailed design are established.

i) Software module functions are tested and verified to meet design specification.

j) Commercial-off-the-shelf software products are evaluated for incorporation into system functions.

k) Acceptance criteria of software product and subsystem have been established.

l) Acceptance testing has been conducted to determine the software product and subsystem in meeting acceptance criteria.

m) Software system test and evaluation are validated to meet performance specification.

n) Software tools for system operation and maintenance support have been identified.

o) Design documentation is complete for software product replications.

D.2.4 Human factors design checklists

a) The objective for human factors design is defined.

b) The human factors plan has been established for design applications.

c) The human factors design concepts are established for usability, operational suitability, function allocation and level of automation, recognition of the human capabilities and limitations in system operation and maintenance.

d) The human system interfaces have been evaluated in terms of design simplicity, identical functions for consistency in operation, compatibility with other existing systems of that kind and user awareness of the information displays and communications.

e) The human to computer interfaces have been evaluated in terms of screen design to facilitate user friendly interaction, input controls and control mechanisms, ease of data entry and editing, graphic information and display, update and interrupt features, file management functions, message windows and help services. It is important that system messages are correct, complete, not misleading and easy to understand.

f) The system designs have incorporated fail-safe features, error resistance and tolerance, ease of handing of critical situations and emergencies, ease of enabling and disabling automated functions, simple diagnostic routines for fault management and easy to navigate through degraded mode of system operation for corrective action.

g) The system designs have incorporated ease of access to replace removable units and lowest level assemblies, adequate labelling for safety warning and operation, and access to technical manuals and support documents for maintenance, installation and repair instructions;

h) The system designs for operation have determined the level of automation and the skills and training needs for the operators and maintainers.

i) Design documentation is complete for development of system operation and maintenance manuals.

D.2.5 Environmental compatibility design checklist

a) The objective of designing for the environment is defined.

b) The environmental design requirements have been established for design applications.

c) The environmental standards and regulations have been reviewed and incorporated in the environmental design concepts and implementation plan focusing on reducing the number of hardware assemblies and parts and aiming at reuse or recycling.

d) The number of parts used in an assembly has been minimized to reduce assembly and disassembly time to improve recycling process efficiency.

e) Modular design for the lowest level replaceable unit with a single function has been considered to permit service options, functional upgrade, and recycling of parts.

f) Grouping non-recycled parts in one location has been considered to facilitate disassembly and quick removal for disposal.

g) Placement of high value part in a location for easy access has been considered to enable partial disassembly for optimum return and salvage.

h) Designing parts for ruggedness and stability has been considered to enhance manual disassembly.

i) Avoidance of moulded-in metal inserts and reinforcement in plastic parts in assembly has been considered to enhance separation and recycling of plastic parts.

j) Making access and break points obvious in logical sequence has been considered to enhance disassembly and maintenance service training.

k) Power down or standby condition whenever possible to save energy and reduce pollution.

l) The number of fasteners has been minimized to reduce assembly and disassembly time.

m) Standardizing the use of tools for assembly and disassembly has been considered to save tooling cost and time.

n) Easy access to fastening points has been considered to enhance maintainability and servicing.

o) Using snap-fits where applicable and practical has been considered to enhance disassembly and ease of parts removal.

p) Using compatible fastening materials with connecting parts has been considered to enhance recycling of parts.

q) Making incompatible parts easily separable when joining together has been considered to enhance parts separation for recycling.

r) Use of adhesives are generally not recommended due to difficulty of disassembling the parts, especially when the two joined materials are incompatible in recycling. Further even for compatible materials the adhesives can contaminate the materials making recycling difficult.

s) The number and length of interconnecting wires and cables should be minimized to reduce assembly and disassembly time and avoid potential electromagnetic interference.

t) Designing breakable connections for throwaway parts should be considered to enhance disassembly.

D.3 Checklists for use of commercial-off-the-shelf (COTS) products in systems

D.3.1 General

Commercial-off-the-shelf (COTS) products are widely used in system applications due to engineering economics and time-to-market situations in system development. COTS products are generally market driven and their fitness for use has been demonstrated by a broad spectrum of commercial applications. A COTS product, in the form of hardware or software, or in their various combinations, provides a ready-made package for commercial purchase. Typical examples of COTS products include but are not limited to power supplies, business applications software, and programmable electronic control equipment. The purchaser of a COTS product has no influence on the product features and its operational specifications. Selecting the right COTS products for system incorporation is of prime importance in engineering dependability into the system of interest. There are certain risks involved in selecting a COTS product and validating its suitability for a specific system application, irrespective of the COTS product claims and its demonstrated compliance. This is due to the absence of the purchaser influence on the product features and performance characteristics. Using a COTS product for critical system application would require additional evaluation effort

for assurance. The checklists are provided to facilitate requirements identification, performance evaluation and assurance of the COTS product for suitable incorporation into system application.

D.3.2 Checklists for requirements identification

a) The COTS product is commercially available with a unique identification for purchase and has sufficient product information and functional description for evaluation of its fitness for use for the intended application.

b) There are multiple suppliers of similar products in the commercial market to choose from.

c) The product identification is designated by name, model or version, and serial number or date on the manufacturer's product label.

d) The product description contains product specification, instructions for installation and operation of the product, procedures for product connections and interface requirements for applications, and the need and extent for product maintenance and support services.

e) Warning labels and procedures for safety related operations where applicable are provided.

f) Product warranty information is provided.

g) Product reliability and maintainability information, performance history, and supporting test data are available for verification.

h) A statement of product quality attestation is provided.

D.3.3 Checklists for evaluation of documented performance records

a) Product performance records containing relevant documentations to substantiate conformance to product specification are available for verification.

b) The relevant documentations including test plan, test procedures, test environment and conditions, and test records are used to demonstrate product conformance to specification.

c) Test cases designed to evaluate fault tolerant conditions where applicable to the product claims are available for verification.

D.3.4 Checklists for product assurance

a) Product quality information and quality records are available for verification.

b) Product conformity assessment data are available for verification.

c) Product field data is available to support reliability performance claims.

d) Product return rates and failure trends are available for verification.

e) Product maintenance records are available for verification.

f) Product risk assessment and evaluation of product features and related process attributes are completed for critical system application. Specific evaluation includes but not limited to fault detection, redundancy needs, and establishing the integrity level of the COTS product appropriate for critical system operation. Integrity level is the denotation of a range of values of the product property necessary to maintain system risks within tolerable limits. The methodology for determining integrity levels is described in ISO/IEC 15026 [23].

Bibliography

[1] IEC 61069-1:1991, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 1 General considerations and methodology*

[2] IEC 62347, *Guidance on system dependability specifications*

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

[4] ISO/IEC TR15271, *Information technology – Guide for ISO/IEC 12207 (Software Life Cycle Processes)*

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

[6] ISO/IEC 15939, *Systems and software engineering – Measurement process*

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

[8] IEC 60300-3-9, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*

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

[10] IEC 61508-1, *Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 1 General requirements*

[11] DEF STAN 00-42, Part 3. *Reliability and Maintainability Assurance Guide – Reliability and Maintainability Case*

[12] IEC 61014, *Programmes for reliability growth*

[13] IEC 61164, *Reliability growth – Statistical test and estimation methods*

[14] ISO 10007, *Quality management systems – Guidelines for configuration management*

[15] IEC 60300-3-10*, Dependability management – Part 3-10: Application guide – Maintainability*

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

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

[18] IEEE Std 1175.1, *IEEE guide for CASE tool interconnections – Classification and description*

[19] ISO/IEC 14102, *Information technology – Guideline for the evaluation and selection of CASE tools*

[20] ISO/IEC 15940, *Information Technology – Software Engineering Environment Services*

[21] *www.sei.cmu.edu.*

[22] IEC 60721(all parts), *Classification of environmental conditions*

[23] ISO/IEC 15026, *Information technology – System and software integrity levels*

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

IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61025, *Fault tree analysis (FTA)*

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

IEC 61508-7, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

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

IEC 61713, *Software dependability through the software life-cycle processes – Application guide*

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

IEC 62198, *Project risk management – Application guidelines*

IEC 62308, *Equipment reliability – Reliability assessment methods*

IEC PAS 62508, *Guidance on human factors engineering for system dependability life cycle applications*

ISO 13407, *Human-centred design processes for interactive systems*

ISO/TR 18529, *Ergonomics – Ergonomics of human-system interaction – Human-centred lifecycle process descriptions*

ITU-T Recommendation E.800, *Terms and definitions related to the quality of service and network performance including dependability*

QFD Institute, *The official source for Quality Function Deployment,* http://www.qfdi.org

References for functional analysis and modelling

EN 1325-1, *Value management, value analysis, functional analysis vocabulary – Part 1: Value analysis and functional analysis*

EN 12973, *Value management*

EN 14514, *Space engineering standards – Functional analysis*

NF X 50-153, Value Analysis – Recommendation for the implementation

IEC/TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*

Federal Information Processing Standards (FIPS) Publication 183: *Integration definition for function modeling (IDEF0)* US National Institute of Standards and Technology

The Delphi method: *Techniques and applications,* edited by H. A. Linstone and M. Turoff

SOMMAIRE

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

_____

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI 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, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 60300-3-15 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1315/FDIS	56/1321/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/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 60300, sous le titre général *Gestion de la sûreté de fonctionnement*, est disponible sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI 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

Les systèmes utilisés dans les environnements d'application actuels sont de plus en plus complexes. La sûreté de fonctionnement constitue désormais un attribut d'aptitude à la fonction important affectant les stratégies d'entreprise en termes d'acquisition de systèmes et de rentabilité en termes de propriété et d'exploitation de ces derniers. La sûreté de fonctionnement globale d'un système résulte de l'association d'interactions complexes entre éléments de systèmes, environnements d'application, interfaces homme-machines, de la mise en œuvre de services d'assistance et d'autres facteurs influents.

Cette partie de la CEI 60300 donne des lignes directrices pour l'ingénierie d'un système global, pour l'atteinte des objectifs en matière de sûreté de fonctionnement. L'approche technique décrite dans la présente norme est la mise en application de connaissances scientifiques appropriées et de disciplines techniques pertinentes permettant de réaliser la sûreté de fonctionnement requise pour le système étudié.

Les quatre principaux aspects de la sûreté de fonctionnement d'ingénierie des systèmes sont traités en termes

– de processus,
– de réalisation,
– d'évaluation et
– de mesure.

Les disciplines techniques consistent en des processus techniques applicables aux différentes étapes du cycle de vie d'un système. Une séquence d'activités de processus pertinentes vient à l'appui des processus techniques spécifiques décrits dans la présente partie de la CEI 60300, afin d'atteindre les objectifs de chaque étape du cycle de vie d'un système.

La présente partie de la CEI 60300 s'applique aux systèmes génériques ayant des fonctions système interactives et consistant en des éléments matériels, logiciels et humains permettant d'atteindre les objectifs d'aptitude à la fonction desdits systèmes. Dans de nombreux cas, une fonction peut être réalisée par des produits du commerce. Un système peut être associé à d'autres systèmes pour former un réseau. Les limites qui séparent un produit d'un système et un système d'un réseau, peuvent être différenciées par la définition de l'application de l'entité. Par exemple, une horloge numérique peut être utilisée en tant que produit pour la synchronisation du fonctionnement d'un ordinateur; un ordinateur peut, en tant que système, être associé à d'autres ordinateurs dans un bureau à des fins de communications sous forme de réseau local d'entreprise. La prise en considération de l'environnement d'application vaut pour tous les types de systèmes. Les systèmes de commande pour la production d'énergie, les ordinateurs tolérants aux pannes et les systèmes de prestation de services de logistique de maintenance sont des exemples de systèmes.

Des lignes directrices portant sur l'ingénierie de la sûreté de fonctionnement sont données pour les systèmes génériques. Elles ne classent pas les systèmes en fonction d'applications spéciales. La majorité des systèmes utilisés peuvent généralement être réparés tout au long de leur cycle de vie selon des considérations économiques et d'applications pratiques. Les systèmes non réparables tels que les satellites de communication, les matériels de télédétection/télésurveillance et les dispositifs à mission unique sont considérés comme des systèmes spécifiques à une application. Pour atteindre leurs objectifs, ils requièrent une identification propre de l'environnement d'application spécifique, des conditions d'exploitation et d'informations supplémentaires relatives à des caractéristiques uniques d'aptitude à la fonction. Les sous-systèmes et composants non réparables sont considérés comme des articles jetables. La sélection de processus applicables à ingénierie de la sûreté de fonctionnement dans un système spécifique est menée au moyen d'une adaptation du projet et du processus de la gestion de la sûreté de fonctionnement.

La présente partie de la CEI 60300 fait partie intégrante du jeu de normes traitant des aspects système de la sûreté de fonctionnement et venant à l'appui de la CEI 60300-1 et de la CEI 60300-2 en matière de gestion de la sûreté de fonctionnement. Il y est fait référence aux activités de gestion de projet applicables aux systèmes. Elle traite de l'identification des éléments de la sûreté de fonctionnement et des tâches appropriées au système, ainsi que des lignes directrices pour les revues de gestion de la sûreté de fonctionnement et l'adaptation des projets de sûreté de fonctionnement.

GESTION DE LA SÛRETÉ DE FONCTIONNEMENT –

Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes

1 Domaine d'application

La présente partie de la CEI 60300 donnent des lignes directrices pour l'ingénierie de la sûreté de fonctionnement des systèmes et elle décrit un processus de réalisation de la sûreté de fonctionnement tout au long du cycle de vie des systèmes.

Cette norme s'applique au développement de nouveaux systèmes et à l'amélioration de systèmes existants impliquant des interactions de fonctions système et consistant en des éléments matériels, logiciels et humains.

Cette norme s'applique également aux fournisseurs de sous-systèmes et de produits qui recherchent des informations relatives aux systèmes et des critères relatifs à l'intégration des systèmes. Des méthodes et des outils sont donnés pour évaluer la sûreté de fonctionnement des systèmes et la vérifier des résultats afin d'atteindre les objectifs de sûreté de fonctionnement.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

CEI 60300-2, *Gestion de la sûreté de fonctionnement – Partie 2: Lignes directrices pour la gestion de la sûreté de fonctionnement*

3 Termes et définitions

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

3.1
système
ensemble d'éléments interdépendants considérés dans leur totalité et distinctement d'autres éléments, dans le contexte d'un objectif défini

NOTE 1 Un système est généralement défini avec pour objectif l'exécution d'une fonction définie.

NOTE 2 Le système est considéré comme étant délimité par une surface imaginaire sécante avec les liaisons entre le système et l'environnement et les autres systèmes externes.

NOTE 3 Le fonctionnement du système peut nécessiter des ressources externes (c'est-à-dire hors des limites du système).

NOTE 4 La structure d'un système peut être hiérarchique, par exemple système, sous-système, composant, etc.

3.2
sous-système
système qui fait partie intégrante d'un système plus complexe

3.3
profil opérationnel
ensemble complet des tâches à accomplir pour atteindre l'objectif d'un système spécifique

NOTE 1 Les configurations et les scénarios de fonctionnement font partie intégrante du mode d'exploitation d'un système.

NOTE 2 Un profil opérationnel est la séquence des tâches requises que le système doit accomplir pour atteindre son objectif opérationnel. Le profil opérationnel représente un scénario de fonctionnement spécifique pour le système en exploitation.

3.4
fonction
opération élémentaire effectuée par le système qui, combinée à d'autres opérations élémentaires (fonctions du système), permet au système d'effectuer une tâche donnée

[CEI 61069-1 :1991, 2.2.5] [1][1]

3.5
élément
combinaison de composants formant un bloc de base pour réaliser une fonction distincte

NOTE 1 Un élément peut comprendre du matériel, du logiciel, de l'information et/ou des composantes humaines.

NOTE 2 Pour certains systèmes, les informations et les données constituent une part importante des opérations du système.

3.6
intégrité
capacité d'un système à conserver sa forme, sa stabilité et sa robustesse, et à maintenir sa cohérence en matière d'aptitude à la fonction et d'utilisation

4 Ingénierie de la sûreté de fonctionnement des systèmes et applications

4.1 Vue d'ensemble de l'ingénierie de la sûreté de fonctionnement des systèmes

La sûreté de fonctionnement est la capacité d'un système à fonctionner de manière à satisfaire aux objectifs spécifiques dans les conditions d'utilisation données. Les caractéristiques de la sûreté de fonctionnement incluent la disponibilité et ses facteurs influents intrinsèques ou externes, tels que la fiabilité, la tolérance aux pannes, la restaurabilité, l'intégrité, la sûreté, la maintenabilité, la durabilité et la logistique de maintenance. La sûreté de fonctionnement d'un système implique que l'on puisse compter sur lui et qu'il soit capable d'exécuter sur demande le service souhaité afin de satisfaire aux besoins de l'utilisateur. L'objectif, la structure, les propriétés et les conditions d'influence du système qui affectent l'aptitude à la fonction de la sûreté de fonctionnement du système sont décrits dans la CEI 62347 [2] qui donne des lignes directrices pour la détermination des fonctions système appropriées pour la spécification de la sûreté de fonctionnement du système considéré.

L'ingénierie de la sûreté de fonctionnement des systèmes comporte quatre aspects principaux:

a) **processus de la sûreté de fonctionnement** – établit les processus techniques d'ingénierie de la sûreté de fonctionnement des systèmes. Le processus consiste en une séquence d'activités mises en œuvre à chaque phase du cycle de vie pour atteindre les

[1] Les chiffres entre crochets se réfèrent à la bibliographie.

objectifs de sûreté de fonctionnement spécifiques en termes d'aptitude à la fonction du système. Le processus de sûreté de fonctionnement doit être entièrement intégré aux processus de conception et de management;

b) **réalisation de la sûreté de fonctionnement** – mise en œuvre de la prestation d'ingénierie et de l'expérience appliqués aux étapes du cycle de vie appropriées du système. L'objectif consiste ici à atteindre progressivement les objectifs de sûreté de fonctionnement des fonctions système constitutives, en adéquation avec la réalisation des sous-systèmes et l'intégration des systèmes (croissance de la fiabilité);

c) **évaluation de la sûreté de fonctionnement** – évalue les attributs de la sûreté de fonctionnement et détermine leur efficacité lorsqu'ils sont mis en œuvre dans les systèmes. Le processus identifie les attributs de la sûreté de fonctionnement spécifiques visant à satisfaire les besoins du projet et fournit la méthodologie et les principes de détermination de ces attributs;

d) **mesure de la sûreté de fonctionnement** – quantifie les attributs de la sûreté de fonctionnement à des fins de passation de contrats, de spécification et d'évaluation. Le processus consiste à assigner une valeur quantifiée ou un nombre afin de désigner une entité cible représentant une caractéristique de sûreté de fonctionnement spécifique. L'objectif consiste à exprimer une déclaration d'intention en termes quantifiables afin de faciliter une compréhension mutuelle de la version concernée et à l'utiliser comme base de négociation pour la conclusion d'accords.

4.2 Attributs et caractéristiques d'aptitude à la fonction de sûreté de fonctionnement des systèmes

Les attributs de la sûreté de fonctionnement des systèmes sont les caractéristiques liées à la sûreté de fonctionnement et les caractéristiques temporelles d'aptitude à la fonction spécifiques intrinsèques au système par conception et construction. Certaines caractéristiques, telles que les caractéristiques d'aptitude à la fonction des systèmes, peuvent être quantifiées et mesurées. D'autres caractéristiques de la sûreté de fonctionnement, non quantifiables, peuvent présenter certaines valeurs ou informations utiles adaptées à ces attributs. Ces caractéristiques non quantifiables peuvent être décrites en termes qualitatifs pour établir la valeur d'évaluation subjective de la sûreté de fonctionnement. Les caractéristiques quantifiables et non quantifiables sont toutes les deux aussi importantes pour décrire les attributs de la sûreté de fonctionnement des systèmes. La valeur commerciale du produit, l'exploitation conviviale et les instructions informatives sont des exemples de caractéristiques non quantifiables. La durée de disponibilité, la fréquence des arrêts, la durée moyenne entre défaillances et le temps de restauration d'un état détérioré en un fonctionnement normal du système sont des exemples de caractéristiques d'aptitude à la fonction quantifiables.

Les principaux attributs de la sûreté de fonctionnement d'un système sont les suivants:

a) **disponibilité**: capacité du système à exécuter sur demande une fonction requise expresse. L'aptitude à la fonction de disponibilité se caractérise en termes de mesures telles que le pourcentage de la durée de disponibilité pour le fonctionnement sur demande du système, la fréquence d'états hors service et la durée des arrêts;

b) **fiabilité**: capacité du système à réaliser une fonction requise dans des conditions d'utilisation et une durée données. L'aptitude à la fonction de fiabilité se caractérise en termes de mesures telles que la durée moyenne entre défaillances et la durée sans défaillance;

c) **maintenabilité**: capacité du système à recouvrer après une défaillance un état dans lequel il peut réaliser une fonction requise, ou à être maintenu dans l'état de disponibilité, dans des conditions d'utilisation et de maintenance données. L'aptitude à la fonction de maintenabilité se caractérise en termes de mesures telles que le temps moyen avant restauration et le temps de recouvrement;

d) **logistique de maintenance**: capacité d'un organisme à fournir, le cas échéant, les ressources nécessaires pour maintenir un système, dans les conditions données. L'aptitude à la fonction de logistique de maintenance se caractérise en termes de mesures telles que l'utilisation des ressources de maintenance, les besoins en formation,

les outils et les équipements de validation, le temps de réponse de la logistique et le délai d'approvisionnement pour les pièces de rechange.

Il existe d'autres attributs relatifs à la sûreté de fonctionnement pour des applications système spécifiques. Ces attributs incluent, sans toutefois s'y limiter:

e) **la restaurabilité**: capacité d'un système à être restauré après une défaillance, dans un état dans lequel il peut réaliser une fonction requise sans nécessiter la réparation du matériel ou du logiciel. La restaurabilité se caractérise en termes de mesures telles que la durée moyenne de panne;

f) **la testabilité**: capacité d'un système à être soumis à des essais à des niveaux de maintenance désignés en vue d'une action de remplacement/réparation, afin de déterminer le taux de couverture de pannes. La testabilité se caractérise en termes de mesures telles que le pourcentage de couverture des essais;

g) **l'accessibilité d'un service**: capacité d'un service à être obtenu dans les tolérances spécifiées et autres conditions données lorsque l'utilisateur le demande. L'accessibilité d'un service se caractérise en termes de mesures telles que la probabilité d'accès à un service;

h) **la continuabilité d'un service**: capacité d'un service, une fois obtenu, à continuer à être fourni dans les conditions données pendant une durée demandée. La continuabilité d'un service se caractérise en termes de mesures telles que la probabilité de conservation dans la durée.

L'aptitude à la fonction récupérable dépend de la conception de l'architecture du système, des caractéristiques de tolérance aux pannes et de réparation automatique intégrées au système. L'aptitude à la fonction de service dépend des propriétés des installations système, de la construction et de l'infrastructure de mobilisation des ressources. Les attributs d'aptitude à la fonction du système sont en général intrinsèques à la conception des systèmes. Les attributs d'aptitude à la fonction sont issus de la capacité et de la caractéristique de sûreté de fonctionnement du système.

Les caractéristiques d'aptitude à la fonction du système sont issues des mesures du temps et des incidents. Un incident est un événement indésirable ou inattendu observé au cours des essais du système ou d'une exploitation indiquant qu'une défaillance peut s'être produite. Il convient d'enregistrer et d'analyser tous les incidents. Cette opération est destinée à déterminer si l'incident est dû à une défaillance, ou s'il est dû à une erreur humaine ou à une observation erronée. Une défaillance constitue un écart par rapport aux fonctions d'aptitude à la fonction requises du système. Toutefois, au moment de l'observation, une défaillance peut ne pas entraîner une interruption complète des fonctions système, mais peut détériorer l'aptitude à la fonction du système. Il convient de définir et d'établir l'étendue de la détérioration avant son classement comme défaillance.

5 Gestion de la sûreté de fonctionnement des systèmes

5.1 Gestion de la sûreté de fonctionnement

La sûreté de fonctionnement est une discipline technique gérée par des principes et des pratiques d'ingénierie. La présente partie de la CEI 60300 utilise les CEI 60300-1 et 60300-2 pour formuler les stratégies de gestion de la sûreté de fonctionnement et d'application générale des approches techniques dans la mise en oeuvre des éléments et tâches de la sûreté de fonctionnement. Des processus de gestion supplémentaires sont introduits pour traiter des questions de gestion spécifiques au système. La gestion de la sûreté de fonctionnement implique la planification des projets, la répartition des ressources, l'assignation de tâches de sûreté de fonctionnement, la surveillance et l'assurance, la mesure de résultats, l'analyse de données et l'amélioration continue. Il convient de mener les activités de sûreté de fonctionnement conjointement à d'autres disciplines techniques afin d'atteindre les effets de synergie nécessaires et apporter de la valeur ajoutée aux résultats du projet. L'adaptation du projet est renforcée pour une gestion rentable des projets système. Le cas

échéant, il convient d'utiliser l'analyse du coût du cycle de vie pour la répartition et l'optimisation des ressources, ceci afin d'évaluer les coûts d'acquisition et de propriété.

5.2 Projets de sûreté de fonctionnement des systèmes

La sûreté de fonctionnement est un facteur décisionnel clé dans la gestion des projets. La sûreté de fonctionnement affecte le coût de mise en œuvre des projets. Elle met l'accent sur les questions spécifiques à l'application de la sûreté de fonctionnement dans des tâches de projet, et devant être résolues. La sûreté de fonctionnement a un impact important sur les fournitures du projet afin de satisfaire aux attentes des clients. Du point de vue de l'ingénierie système, la réalisation de la sûreté de fonctionnement des systèmes est une décision opérationnelle importante nécessitant l'intégration complète de l'ingénierie et de la conception dans le processus décisionnel de gestion. La gestion de l'obsolescence, l'évaluation des risques liés aux projets, les compromis techniques de conception, l'évaluation du coût du cycle de vie, l'externalisation et la coordination de la chaîne d'approvisionnement constituent quelques exemples des activités de sûreté de fonctionnement dans les pratiques d'ingénierie des systèmes.

Les projets n'impliquent pas tous un développement complet des nouveaux systèmes. La plupart des systèmes sont constitués par l'intégration de sous-systèmes et l'application de produits de série pour la réalisation des fonctions système. Dans le cas des grands projets de développement de systèmes ou d'amélioration des systèmes, ceci peut impliquer de nombreux développeurs de sous-systèmes et sous-traitants de fournitures et services, pour assurer la réalisation du projet du système dans les délais prévus. A cet égard, la gestion des projets est essentielle pour la coordination des différentes prestations liées à leur mise en œuvre. Les projets de sûreté de fonctionnement des systèmes peuvent impliquer des activités de sûreté de fonctionnement spécifiques telles que:

a) l'adoption de nouvelles techniques;

b) le développement de spécifications de sûreté de fonctionnement pour le système et les sous-systèmes;

c) l'évaluation de la sûreté de fonctionnement des produits de série destinés à être utilisés dans les fonctions système;

d) l'évaluation de la capacité du fournisseur à satisfaire aux exigences relatives aux projets de sûreté de fonctionnement;

e) l'assurance de la sûreté de fonctionnement pour l'acceptation des systèmes.

Des activités de sûreté de fonctionnement des systèmes peuvent être réalisées à toute étape du cycle de vie des systèmes. Certaines assignations de tâches liées à la sûreté de fonctionnement peuvent exiger des compétences et une formation spéciales dans des disciplines techniques telles que le génie logiciel, la logistique et le facteur humain.

5.3 Adaptation afin de satisfaire aux besoins d'un projet

Un projet de sûreté de fonctionnement est développé pour résoudre les problèmes de sûreté de fonctionnement spécifiques au système concerné. L'adaptation a pour objectif de gérer la répartition des ressources disponibles pour le projet et de choisir les méthodes appropriées pour la résolution effective des problèmes. Des exemples d'activités liées aux projets de sûreté de fonctionnement des systèmes appropriées à l'adaptation sont:

a) la planification budgétaire relative à la répartition des ressources liées à la sûreté de fonctionnement afin d'atteindre les objectifs de réalisation des projets;

b) l'évaluation des techniques alternatives d'acquisition de produits d'une grande sûreté de fonctionnement;

c) l'externalisation du développement des sous-systèmes afin de répondre aux critères stricts des exigences relatives au modèle de maturité de la capacité logicielle pour lesquelles la surveillance de processus est fondamentale;

d) le temps de formation requis pour acquérir une expérience suffisante permettant d'utiliser un nouvel outil d'analyse de fiabilité;

e) le choix de sous-traitants pour la prestation d'une maintenance sur site des systèmes critiques en termes de rendement, de grande disponibilité, pour lesquels aucune immobilisation programmée n'est par ailleurs admise.

Les lignes directrices du processus d'adaptation sont décrites dans la CEI 60300-2.

5.4 Assurance de la sûreté de fonctionnement

Il convient que les activités d'assurance de la sûreté de fonctionnement fassent partie intégrante du processus d'assurance de qualité des projets, pour ce qui relève de la sûreté de fonctionnement des systèmes. Cette intégration est destinée à assurer que toutes les activités planifiées et systématiques mises en œuvre au sein du système de qualité, et démontrées si nécessaire, permettent d'assurer en toute confiance la satisfaction des exigences relatives à la qualité des systèmes et des produits. Les activités clés impliquent la planification du projet, l'attribution des responsabilités en termes de technique et de gestion, la vérification des résultats de l'évaluation de la sûreté de fonctionnement, la validation des données d'aptitude à la fonction de sûreté de fonctionnement pour l'acceptation des systèmes, le contrôle de l'efficacité du processus de la sûreté de fonctionnement, le compte rendu des défaillances et l'analyse des données pour des actions correctives et préventives rapides, la documentation des informations pertinentes relatives à la sûreté de fonctionnement et la conservation des enregistrements d'essai venant à l'appui des preuves tangibles, ainsi que la revue de direction visant à la mise en œuvre d'améliorations de processus. La CEI 60300-2 donne des informations supplémentaires concernant la sélection d'éléments et de tâches de programmes de sûreté de fonctionnement pour l'adaptation des projets liés à la sûreté de fonctionnement des systèmes.

6 Réalisation de la sûreté de fonctionnement des systèmes

6.1 Processus d'ingénierie de la sûreté de fonctionnement des systèmes

6.1.1 Objet du processus de sûreté de fonctionnement

La mise en place d'un processus est essentielle à la gestion satisfaisante des tâches liées aux projets et à la coordination des activités. Il convient d'intégrer le processus de sûreté de fonctionnement aux processus techniques afin de faciliter l'ingénierie de la sûreté de fonctionnement des systèmes. Le processus de sûreté de fonctionnement fournit des entrées spécifiques aux principaux points de décision relatifs au cycle de vie des systèmes, ceci facilitant la mise en œuvre du projet. Ces principaux points de décision interviennent à l'achèvement des phases critiques de la gestion de projet en vue de l'identification des marchés, du développement des systèmes, de la réalisation des produits, ainsi que de l'acceptation, de l'exploitation, de l'amélioration puis du retrait des systèmes. Les informations relatives à la sûreté de fonctionnement sont lors de ces principaux points de décision, fondamentales pour justifier les investissements de nature commerciale.

6.1.2 Cycle de vie des systèmes et processus

Il convient que le point de départ de l'ingénierie de la sûreté de fonctionnement d'un système figure dans la première étape du cycle de vie. Il convient que l'utilisateur applique un processus d'ingénierie efficace lors de cette étape du cycle de vie.

La description des étapes du cycle de vie d'un système peut être présentée du point de vue de l'ingénierie de systèmes génériques. Il existe d'autres descriptions du cycle de vie des systèmes. La CEI 60300-2 décrit les étapes du cycle de vie d'un produit du point de vue de la gestion de projet. L'ISO/CEI 15288 [3] donne une description similaire du cycle de vie d'un système du point de vue des technologies de l'information et de l'ingénierie logicielle. Les lignes directrices données par la présente partie de la CEI 60300 sont basées sur le concept des étapes du cycle de vie d'un système, tel que décrit à la Figure 1. Ces étapes constituent des points de transition technique précis, tandis que les phases d'un projet peuvent se

chevaucher selon les volontés du management afin de respecter des décisions d'entreprise importantes. La gestion des risques liés à un projet, à laquelle il est fait référence dans la CEI 60300-2, s'applique tout au long des processus du cycle de vie.

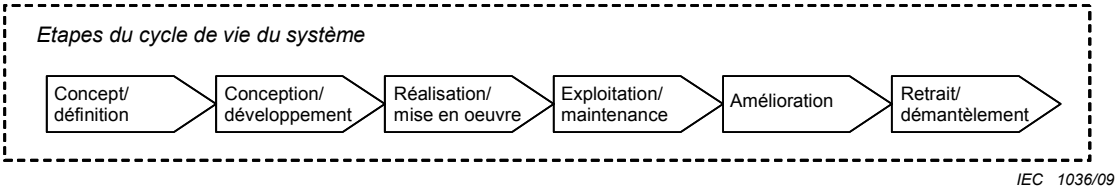

Figure 1 – Présentation du cycle de vie d'un système

Les processus techniques de mise en oeuvre de l'ingénierie consistent en une séquence d'activités de processus exécutées à chaque étape respective du cycle de vie pour atteindre les objectifs fixés d'aptitude à la fonction et de sûreté de fonctionnement des systèmes. L'ingénierie de la sûreté de fonctionnement d'un système n'est pas une activité isolée. Elle est réalisée conjointement à d'autres disciplines techniques (par exemple conception des structures) et activités de soutien (par exemple assurance de qualité) pour la réalisation des fonctions système en vue de leurs applications prévues. L'Annexe A décrit une séquence type des processus du cycle de vie des systèmes.

Les activités de processus clés du cycle de vie d'un système sont les suivantes:

a) la définition des exigences identifie les besoins des utilisateurs et les contraintes des applications système;

b) l'analyse des exigences transforme la vision de l'utilisateur sur les applications du système en une vision technique pour l'ingénierie du système et comprend le développement d'un profil d'utilisation opérationnel / d'un calendrier / d'une mission nominale de référence;

c) la conception de l'architecture synthétise une solution qui satisfait aux exigences du système pour des scénarios de fonctionnement, en affectant les fonctions système nécessaires aux éléments matériels, logiciels et humains;

d) la conception fonctionnelle et l'évaluation déterminent les moyens pratiques de réalisation des fonctions pour faciliter les compromis de conception et l'optimisation;

e) la documentation de la conception du système fournit les informations sur le système, y compris les données de sûreté de fonctionnement appropriées pour la conception du système;

f) la conception des systèmes et le développement de sous-systèmes génèrent les fonctions système et sous-système spécifiées;

g) la réalisation produit les éléments système et sous-systèmes sous formes matérielles et logicielles;

h) l'intégration assemble le système et les sous-systèmes conformément à la conception architecturale;

i) la vérification confirme le fait que les exigences de conception spécifiées sont satisfaites par le système;

j) l'installation/transition établit la capacité du système à fournir le service d'aptitude à la fonction requis dans un environnement opérationnel spécifié;

k) la validation/mise en service fournit des preuves tangibles de la satisfaction des exigences de fonctionnement par le système;

l) l'exploitation consiste pour le système à assurer son service opérationnel;

m) la logistique de maintenance pérennise la capacité du système en termes de service opérationnel;

n) l'amélioration renforce l'aptitude à la fonction du système par l'ajout de caractéristiques supplémentaires;

o) le retrait/démantèlement met fin à l'existence de l'entité système.

6.1.3 Applications de processus au cours du cycle de vie d'un système

Un processus est un ensemble intégré d'activités liées entre elles ou interactives qui transforme des éléments d'entrée en éléments de sortie. Les processus sont utilisés comme modèles de référence pour l'organisation fonctionnelle (par exemple systèmes de management de la qualité (SMQ), gestion de projet), transactions commerciales (par exemple acquisition, contrat pour la chaîne d'approvisionnement), planification et mise en œuvre technique (par exemple développement d'un produit, évaluations de systèmes). La présente partie de la CEI 60300 concerne plus particulièrement les processus techniques relatifs à l'ingénierie de la sûreté de fonctionnement des systèmes.

La Figure 2 illustre un exemple de modèle de processus. Dans un contexte d'ingénierie, les éléments d'entrée primaires consistent habituellement en des données fournissant un ensemble d'exigences ou les besoins exprimés par le client. Les éléments de sortie peuvent consister en des données transformées décrivant une solution souhaitée telle qu'une spécification, la fabrication d'un produit ou la prestation d'un service. Il existe d'autres éléments d'entrée associés au processus de contrôle et d'activation. Les activités de processus transforment ou convertissent les éléments d'entrée primaires en éléments de sortie souhaités. Cette conversion est soumise aux conditions établies par les mécanismes d'activation et les facteurs influents associés. Certains facteurs influents tels que les procédures d'exploitation pour l'activation du processus sont contrôlables; d'autres facteurs peuvent ne pas être contrôlables, par exemple les conditions météorologiques ou un changement climatique soudain. Les mécanismes d'activation tels que les méthodes et les outils, sont essentiels pour que la conversion soit effective. Ce modèle de processus permet de mettre en œuvre les processus techniques décrits dans la présente partie de la CEI 60300.

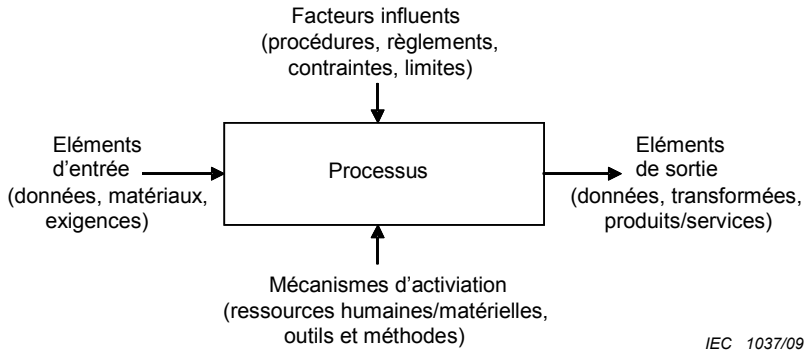

Figure 2 – Exemple de modèle de processus

Les processus techniques ont un double objectif:

a) exécuter les tâches d'ingénierie et mener les activités de réingénierie lors de la conception et du développement des systèmes ;

b) exécuter les activités d'exploitation, de maintenance et de retrait par rapport au système.

Les applications des processus techniques, qu'elles soient récursives et itératives, permettent de parvenir à la solution souhaitée. Ceci s'applique à toutes les étapes du cycle de vie des systèmes. Les relations des processus techniques sont indépendantes de la taille et de la structure des systèmes. Les activités de processus telles que la définition et l'analyse des exigences, et la conception architecturale sont des approches techniques « descendantes » permettant de façonner la solution souhaitée (c'est-à-dire la répartition du système en ses éléments constitutifs); l'intégration et la vérification constituent en revanche des approches « ascendantes » permettant de réaliser la configuration du système et de valider son aptitude

à la fonction (c'est-à-dire la constitution des éléments visant à la construction du système). La transition entre les approches « descendantes » et « ascendantes » au cours de l'étape de mise en œuvre intervient à la fin de l'installation du système au moment où commence sa mise en service. Ceci est connu sous l'appellation modèle « V » dans la pratique d'ingénierie, tel que décrit dans l'ISO/CEI 15288 [3].

NOTE Pour plus d'informations sur le modèle en V, se reporter à l'ISO/CEI/TR 15271 [4].

L'ISO/CEI 12207 [5] établit un cadre pour les processus du cycle de vie des logiciels. Cette norme contient les processus, activités et tâches pouvant être appliqués au cours de l'acquisition d'un produit ou d'un service logiciel et au cours des phases d'approvisionnement, de développement, d'exploitation, de maintenance et de retrait des produits logiciels. L'ISO/CEI 12207 [5] peut être utilisée seule ou conjointement à l'ISO/CEI 15288 [3].

Des exemples types d'applications de processus à chaque étape du cycle de vie d'un système sont donnés à l'Annexe A. La connaissance du type de système et de l'environnement d'application est essentielle pour l'adaptation de l'application du processus aux étapes appropriées du cycle de vie du système afin de répondre aux besoins spécifiques d'un projet.

6.2 Réalisation de la sûreté de fonctionnement d'un système

6.2.1 Objet de la réalisation de la sûreté de fonctionnement d'un système

La réalisation est l'action effective de l'atteinte d'un objectif. Elle reflète les résultats obtenus par la résolution aboutie des problèmes rencontrés. Les actions requises pour la réalisation de la sûreté de fonctionnement d'un système peuvent être accomplies par une prestation d'ingénierie, des connaissances et l'expérience aux étapes appropriées du cycle de vie d'un système. L'objectif consiste ici en une réalisation progressive des objectifs de sûreté de fonctionnement des fonctions système constitutives aboutissant à l'intégration du système. La réalisation de la sûreté de fonctionnement d'un système constitue un objectif important du projet nécessitant coordination et démonstration en vue de l'acceptation du système. L'acceptation d'un système constitue généralement un accord contractuel visant à répondre aux exigences du client. L'objectif final est de satisfaire les attentes des utilisateurs en termes d'aptitude à la fonction du système.

6.2.2 Critères de réalisation de la sûreté de fonctionnement d'un système

La réalisation de la sûreté de fonctionnement d'un système s'effectue par l'intégration réussie des attributs de la sûreté de fonctionnement pertinents et des caractéristiques d'aptitude à la fonction associées dans le système. Il convient que les critères de réalisation de la sûreté de fonctionnement d'un système reflètent:

a) une parfaite compréhension des objectifs d'aptitude à la fonction du système;

b) une parfaite compréhension des conditions d'exploitation;

c) l'application effective des principes de la sûreté de fonctionnement dans l'infrastructure opérationnelle;

d) les conditions d'utilisation;

e) l'application de processus appropriés pour la réalisation du système;

f) l'utilisation des connaissances et de l'expérience acquises pour une introduction rentable de services fonctionnels.

Ces critères peuvent être remplis par une concentration sur les facteurs clés qui affectent les questions portant sur la sûreté de fonctionnement du système. Les critères importants sont identifiés, ces derniers soutenant par ailleurs les applications de processus et la réalisation des objectifs fonctionnels. Des éléments de justification sont fournis pour clarifier l'importance de la mise en œuvre de la sûreté de fonctionnement. Il convient que la planification et la mise en œuvre des projets tiennent compte de ces critères. Il convient que l'utilisateur adapte les

activités de sûreté de fonctionnement appropriées afin de répondre aux besoins spécifiques du projet du point de vue du cycle de vie du système.

1) **politique de gestion de la sûreté de fonctionnement** – ce critère influence l'infrastructure opérationnelle, la répartition des ressources appropriées, l'attribution des responsabilités en termes de gestion et de management de projets de sûreté de fonctionnement. L'importance de la politique de sûreté de fonctionnement reflète l'écoute du client en matière de stratégies et d'engagements relatifs à la gestion de la sûreté de fonctionnement, de collaboration et d'approche par processus systématiques, en direction d'une application effective des principes de gestion de la sûreté de fonctionnement décrits dans la CEI 60300-1. La politique de gestion de la sûreté de fonctionnement décrite dans la CEI 60300-1 s'applique tout au long des processus d'ingénierie décrits dans la présente partie de la CEI 60300;

2) **base de connaissances de la sûreté de fonctionnement** – ce critère concerne l'exactitude de l'interprétation des besoins du marché, le caractère approprié des informations requises pour le lancement du projet, les applications des normes et des spécifications disponibles, la compétitivité de l'entreprise en termes de négociation de contrats et de justification de la sûreté de fonctionnement pour des preuves tangibles. L'importance de la base de connaissances de la sûreté de fonctionnement réside dans l'avantage concurrentiel du marché et le leadership technologique lors de la relève de nouveaux défis portant sur les questions de sûreté de fonctionnement des systèmes;

3) **architecture de la conception** – ce critère concerne l'utilisation des techniques relatives aux applications systèmes, le choix des éléments matériels, logiciels et humains nécessaires à la réalisation des fonctions système, l'intégration et l'exploitation des systèmes, et la facilitation de l'amélioration et de la mise à niveau de ces derniers. L'architecture de calcul établit un cadre cohérent et constructif destiné à l'intégrité et à la réalisation des systèmes. Elle facilite l'amélioration et l'extension de la capacité, l'exploitation rentable et la fourniture d'une qualité de service. L'emploi approprié des techniques permet de parvenir à un compromis de conception par l'intégration de caractéristiques avancées et l'extension des limites techniques relatives aux applications;

4) **coopération de la chaîne d'approvisionnement** – ce critère concerne les décisions achat-fabrication, les programmes d'externalisation et de sous-traitance, les procédures et documents de vérification et de validation, et les processus de contrôle et d'assurance. L'importance de la gestion de la chaîne d'approvisionnement est basée sur la coopération acheteur-fournisseur et sur le partage des informations pertinentes dans le processus d'approvisionnement et d'acquisition. La chaîne d'approvisionnement fournit les liens nécessaires à la traçabilité des informations importantes. L'effet sur l'entreprise constitue une opportunité réelle dans les processus administratifs, la réduction des coûts d'approvisionnement et les incitations à fournir des produits et des services de qualité;

5) **systèmes d'activation** – ce critère concerne l'utilisation des méthodes et outils, l'opportunité d'accroître l'efficacité de conception, les besoins de formation en compétences reconnues, l'introduction et l'installation de nouveaux produits et systèmes et les stratégies de maintenance et de support logistique. L'importance des systèmes d'activation est observée dans l'amélioration du processus de conception et d'approvisionnement et dans l'utilisation effective des méthodes et outils qui visent à accélérer la résolution des problèmes. Les systèmes d'activation ne présentent pas toujours une complexité technique requérant des compétences particulières pour leur compréhension et leur utilisation. Certaines méthodologies constituent de simples listes de contrôle et instructions qui permettent aux opérateurs et aux spécialistes de la maintenance de prendre des décisions pratiques pour l'exécution d'actions appropriées sur site. L'ISO/CEI 15288 [3] fournit des informations supplémentaires sur les systèmes d'activation;

6) retour d'information du client et gestion de l'information – ce critère concerne les relations avec le client en termes de satisfaction et de fidélité, la prestation de services efficaces d'assistance à la clientèle, la précision du compte rendu des incidents, la saisie des données de service pour analyse, la mise en œuvre effective des actions correctives et préventives, l'établissement de tendances d'aptitude à la fonction des systèmes et d'enregistrements d'historique d'aptitude à la fonction de la sûreté de fonctionnement. L'importance des informations rétroactives pertinentes est la capacité à établir des

tendances d'aptitude à la fonction, à identifier des domaines critiques requérant une attention particulière et à fournir des preuves tangibles pour vérification et validation.

6.2.3 Méthodologie pour la réalisation de la sûreté de fonctionnement des systèmes

Le choix des méthodes applicables peut être fait sur la base de la connaissance des critères et de la compréhension de leur importance pour la réalisation de la sûreté de fonctionnement des systèmes. L'objectif est d'utiliser ces méthodes pour établir la sûreté de fonctionnement du système. L'application de ces méthodes vise à intégrer des attributs de la sûreté de fonctionnement pertinents aux fonctions système.

La méthodologie de mise en œuvre de la sûreté de fonctionnement des fonctions système peut être perçue selon deux points de vue différents:

a) approche descendante de synthèse de la sûreté de fonctionnement des systèmes sur la base des exigences système et des informations sur le marché spécifiées, ceci afin de développer l'architecture des systèmes;
b) approche ascendante de constitution de la sûreté de fonctionnement des fonctions système sur la base des règles de conception relatives à la simplification, la tolérance aux pannes, la réduction et l'atténuation des risques.

Les deux approches impliquent l'identification des attributs de la sûreté de fonctionnement et la détermination de leurs valeurs. Les attributs de la sûreté de fonctionnement constituent les mesures fondamentales d'évaluation et de réalisation de la sûreté de fonctionnement des systèmes.

Les attributs de la sûreté de fonctionnement importants pour les caractéristiques d'aptitude à la fonction des systèmes sont de nature temporelle. Ils peuvent être quantifiés et déduits des mesures du temps et des incidents. Le pourcentage de la durée de disponibilité pour l'aptitude à la fonction de disponibilité des systèmes, la probabilité d'exécution aboutie d'une fonction système d'exploitation avec une durée sans défaillance afin de démontrer la fiabilité, et la réalisation de la restauration du système dans une période d'immobilisation programmée afin de révéler l'opportunité des actions de logistique de maintenance sont des exemples d'attributs de cette nature.

Toutefois, en raison de contraintes de temps et de coût, de limites techniques ou pour d'autres raisons liées au projet, les attributs de la sûreté de fonctionnement ne peuvent pas tous être démontrés. Les systèmes complexes d'une grande sûreté de fonctionnement, les nouveaux systèmes dont l'application sur site est limitée, les systèmes logiciels génériques destinés à être utilisés dans un nouvel environnement d'application, et certains produits du commerce pour lesquels il n'existe aucun historique de fiabilité d'aptitude à la fonction sont des exemples d'attributs de cette nature. D'autres méthodes sont nécessaires à la confiance d'utilisation et à l'assurance de la sûreté de fonctionnement. Il convient de noter que les attributs de la sûreté de fonctionnement des systèmes sont stochastiques ou probabilistes par nature. Ils peuvent englober des caractéristiques à évaluation indirecte autres que les caractéristiques d'aptitude à la fonction pouvant être déduites de mesures directes. Les études de cas de fiabilité et de maintenabilité (R&M), les cas d'étude simulés, les modèles de maturité de la capacité et les programmes de croissance de la fiabilité sont des méthodes typiques applicables.

Les nombres et valeurs quantifiables doivent souvent être interprétés. La mesure du taux de défaillance peut ne pas être significative sans une référence appropriée à son contexte ou à l'explication des préoccupations associées. Alors que les taux de défaillance peuvent être utilisés comme indicateurs aux fins de comparaison d'options de conception alternatives, les hypothèses de base sont importantes pour venir à l'appui des principes de justification. Ceci permet d'appliquer des outils statistiques pour déterminer les limites d'inférence et de confiance relatives aux expositions aux risques incertains. Par exemple dans une entreprise, la durée moyenne entre les défaillances d'une photocopieuse peut ne pas se révéler trop significative pour le propriétaire, le nombre de photocopies nulles perdues par mois d'utilisation de la machine indiquant toutefois le coût du gaspillage.

L'Annexe B fournit des exemples de méthodes et outils applicables dans le but de faciliter la réalisation de la sûreté de fonctionnement des systèmes. La connaissance des fonctions d'exploitation du système et de son environnement d'application décrit dans l'Annexe C est nécessaire pour le choix de méthodes et outils pertinents. Il convient que les applications se concentrent sur les questions critiques portant sur la résolution des problèmes techniques. Il convient de noter les limites de ces méthodes et outils applicables à leurs applications spécifiques afin d'interpréter les résultats de manière appropriée.

6.2.4 Réalisation des fonctions d'un système

Les fonctions d'un système peuvent être réalisées en utilisant les éléments matériels, logiciels ou humains, ou l'une quelconque de leurs combinaisons pour atteindre des objectifs d'aptitude à la fonction spécifiques du système. Les paragraphes ci-dessous décrivent les questions générales liées au choix et à l'application de ces éléments pour une réalisation réussie de la sûreté de fonctionnement.

a) **Élément matériel** – les constructions de systèmes utilisent couramment des éléments matériels. Le matériel peut consister en des composants mécaniques, électriques, électroniques, optiques et autres composants physiques. Ces composants sont utilisés dans diverses configurations pour réaliser les fonctions matérielles. La plupart des produits électroniques constitués de nos jours d'éléments matériels présentent une maturité certaine dans les applications technologiques. Les règles de conception sont correctement établies. La production des produits électroniques est constante dans un environnement à processus de fabrication contrôlé. La qualité et la sûreté de fonctionnement des produits peuvent être déterminées par des programmes d'assurance appropriés. Il existe également des bases de données « d'expériences » importantes qui viennent à l'appui de l'aptitude à la fonction de fiabilité de ces produits électroniques matériels. Toutefois, certains produits à composants électroniques actifs sont sensibles à la variation des environnements d'application. La nature de la physique des défaillances de ces composants domine dans les défaillances matérielles et le phénomène de la mortalité infantile. Une conception, un conditionnement et un examen appropriés de la fiabilité permettent de réduire les défaillances précoces de manière significative. Certains éléments matériels peuvent se dégrader par usure du fait de l'exploitation ou d'une utilisation extensive, tandis que d'autres peuvent avoir des durées de conservation limitées. Ces problèmes de fiabilité intrinsèque peuvent être résolus par la mise en œuvre de mesures de prévention et de maintenance programmée. La structure des systèmes matériels est hiérarchique. La stratégie de logistique de maintenance peut être déployée par une conception fonctionnelle et une stratégie de conditionnement appropriées du plus petit ensemble ou de la plus petite unité remplaçable. Ceci facilite l'exécution des activités de conception de la maintenabilité et de logistique qui visent à améliorer l'aptitude à la fonction de disponibilité des systèmes.

b) **Élément logiciel** – peut consister en des instructions codées, des programmes d'ordinateur, et des règles et procédures établies pour l'exploitation des systèmes. Les instructions codées servent à indiquer à un programme logiciel d'exécuter une fonction système pour application. Il est difficile de vérifier par essai les codes logiciels afin de détecter les erreurs de codage, à moins que ceux-ci ne soient utilisés pour le fonctionnement réel de l'ordinateur. Une erreur dans un programme logiciel entraînant la défaillance du système a pour origine l'activation d'une panne ou d'un « bogue » latent(e) interne au programme logiciel. Les techniques de conception logicielle sont essentielles pour réduire au minimum le potentiel de génération d'erreurs de conception intempestives. Les approches employées incluent l'évitement et l'élimination des pannes, ainsi que la tolérance aux pannes. Elles constituent des méthodes formelles dans les techniques de conception logicielle. Bien que le logiciel ne s'use pas, ses fonctions peuvent se détériorer du fait des modifications opérées. Dans la mesure où le logiciel est, sous une forme ou une autre, une création de l'homme, les techniques de contrôle de la conception se concentrent sur l'environnement de conception de ce dernier. L'adoption d'une infrastructure qui utilise une méthodologie telle que les modèles de maturité de la capacité comme cadre de développement des logiciels, peut faciliter la réalisation de la sûreté de fonctionnement des fonctions des logiciels. Il convient qu'un processus de gestion de la configuration des systèmes contrôle les éditions et versions logicielles

améliorées afin de maintenir l'interopérabilité des fonctions et d'améliorer l'aptitude à la fonction de sûreté de fonctionnement.

c) **Élément humain** – les interactions de l'homme avec le fonctionnement des systèmes peuvent être considérées soit comme une partie intégrante des fonctions du système, soit comme le fait de l'utilisateur final du système. Le rôle de l'homme dans l'aptitude à la fonction d'un système peut être bénéfique, dans la mesure où l'opérateur humain est capable de pallier ou de contrôler les situations en cours. Toutefois, la plupart des incidents industriels signalés et les principaux accidents étudiés sont dus à des erreurs humaines qui constituent la cause principale du dysfonctionnement d'un système ou de l'interruption d'un service d'aptitude à la fonction. Il convient que l'ergonomie soit intégrée dans les systèmes conçus pour être exploités ou utilisés par des individus afin de réduire au minimum le risque de défaillances critiques, la perte de biens, les atteintes à la sécurité ou les menaces pour la sécurité. La sûreté de fonctionnement peut être réalisée par l'introduction de l'ergonomie dans les règles de conception et par la simplification des tâches exécutées par un opérateur. L'étude de l'ergonomie implique une prestation pluridisciplinaire de recueil d'informations sur les aptitudes humaines et les limites relatives aux applications qui affectent l'aptitude à la fonction homme-système. Les aspects relatifs à l'ingénierie résident dans l'application des informations relatives à l'ergonomie à la conception des outils, machines, systèmes, tâches et activités, ainsi que dans l'environnement pour une utilisation sûre, confortable et efficace par la personne. La formation et l'éducation constituent des conditions préalables importantes pour toute exploitation d'un système nécessitant une interaction humaine. La normalisation de l'ergonomie facilite l'intégration des systèmes, améliore l'interopérabilité des éléments d'un système, ainsi que l'aptitude à la fonction de l'aptitude à l'emploi et de la sûreté de fonctionnement générale.

La plupart des fonctions système des produits électroniques actuels combinent des éléments matériels et logiciels dans les conceptions des systèmes. Elles proposent par ailleurs un large éventail de caractéristiques de conception pour diverses applications. La sûreté de fonctionnement des fonctions système est réalisée par l'intégration de règles de conception et de processus d'applications établis. Un compromis de conception peut être trouvé par une combinaison appropriée de techniques permettant de répondre aux besoins d'application spécifiques. Des économies sont réalisables grâce à un conditionnement modulaire et à la normalisation d'une fabrication en série. Les fonctions d'un système peuvent être automatisées en vue de leur autocontrôle et ce, afin d'améliorer l'efficacité de l'aptitude à la fonction par un essai intégré ou d'autres programmes de contrôle. Seuls des règlements de sûreté et de sécurité ou des raisons d'ordre social ou économique imposent l'intervention de l'homme dans les fonctions système. L'Annexe D fournit des listes de contrôle pour les applications de conception des éléments matériels et logiciels, ainsi que de l'ergonomie.

6.2.5 Approches pour déterminer la réalisation de la sûreté de fonctionnement d'un système

Trois approches génériques permettent de déterminer que la sûreté de fonctionnement d'un système a été obtenue. Ces approches ont des objectifs différents avec un degré variable de rigueur technique. Dans la pratique, l'utilisation d'une combinaison de ces trois approches est la plus vraisemblable.

a) **Démonstration** – opération réalisée par l'exploitation réelle du système dans un environnement d'application sur une période programmée, afin de démontrer l'aptitude à la fonction de la sûreté de fonctionnement. Des exemples typiques sont:

   – l'historique de l'aptitude à la fonction de sûreté de fonctionnement des systèmes exploités sur site;

   – une démonstration de fiabilité formelle;

   – l'aptitude à la fonction de disponibilité pendant la période de garantie.

b) **Inférence** – opération réalisée par des méthodes statistiques utilisant les données observées des fonctions système constitutives sur la base de critères et d'hypothèses établis, afin d'atteindre une valeur qui représente les attributs de la sûreté de fonctionnement du système (caractéristiques / aptitude à la fonction). Des exemples typiques sont:

- la prévision d'un système de configuration donnée;
- la simulation du système;
- les modèles de maturité de la capacité;
- la vérification de l'aptitude à la fonction du système par un cas d'essai.

c) **Preuve progressive** – opération réalisée par l'exécution progressive des étapes d'un projet avec des argumentations auditables venant à l'appui des preuves tangibles. Des exemples typiques sont:

- l'étude de cas de fiabilité et de maintenabilité;
- un programme de croissance de fiabilité.

6.2.6 Preuves tangibles des réalisations

Les informations suivantes constituent des énoncés fondamentaux concernant les caractéristiques de sûreté de fonctionnement d'un système, destinées à être utilisées comme preuves tangibles venant à l'appui d'un système et d'un produit aux étapes applicables du cycle de vie d'un système. La documentation et l'authentification des preuves tangibles sont nécessaires à des fins d'audit et de passation de contrats.

a) une formulation des attributs de la sûreté de fonctionnement du système et de l'environnement d'exploitation afin de refléter les attentes de l'utilisateur dans une spécification ou une proposition commerciale basée sur les renseignements relatifs aux études de marchés. Cette formulation fournit des informations permettant d'engager la planification d'un projet et d'élaborer une spécification portant sur la sûreté de fonctionnement du système;

b) une formulation des caractéristiques d'aptitude à la fonction du système dans une spécification portant sur la sûreté de fonctionnement de ce dernier. Cette formulation fournit des informations pour la définition d'objectifs de conception de la sûreté de fonctionnement et l'établissement de l'architecture du système;

c) une formulation des caractéristiques d'aptitude à la fonction de la fiabilité et de la maintenabilité pour chaque fonction système dans une spécification de conception fonctionnelle. Cette formulation fournit des informations pour le choix des techniques, les décisions achat-fabrication et l'établissement d'exigences relatives à l'approvisionnement;

d) une formulation des caractéristiques de fiabilité et de maintenabilité pour l'exploitation et la maintenance du système. Cette formulation fournit des informations pour la planification de la logistique, la maintenance contractuelle et les besoins de formation spéciaux;

e) une formulation des caractéristiques pertinentes de la sûreté de fonctionnement pour l'acceptation des produits, la conformité de la vérification et la validation des résultats d'aptitude à la fonction du système. Cette formulation constitue la base de l'accomplissement des accords contractuels pour les fournitures;

f) tous les rapports de projets dédiés à la sûreté de fonctionnement et contenant les données d'analyse de la sûreté de fonctionnement, la condition d'essai et les résultats de démonstration. Cette formulation fournit des informations pour les revues de projets, les modifications de conception, les actualisations de procédures, et les actions correctives et préventives pour une amélioration progressive.

6.3 Evaluation de la sûreté de fonctionnement d'un système

6.3.1 Objet des évaluations de la sûreté de fonctionnement d'un système

L'évaluation consiste à déterminer l'état ou le résultat d'une activité ou d'une question spécifique liée à la sûreté de fonctionnement. L'évaluation a pour objectif de déterminer comment un problème peut être résolu. Les constatations permettent de soutenir les actions recommandées par des principes et des éléments de justification. Le processus d'évaluation facilite l'identification des alternatives ou des options potentielles de résolution du problème. Ceci permet la réalisation de compromis de conception et un choix des produits préférentiels. Il convient que le niveau d'évaluation dans la sûreté de fonctionnement d'un système soit adapté de manière à répondre aux besoins spécifiques du projet et à améliorer le processus impliqué.

6.3.2 Types d'évaluation

L'évaluation peut être objective ou subjective. L'évaluation objective consiste en une mesure directe d'une entité pour obtenir les résultats. L'évaluation subjective consiste à assigner une valeur à la nature, au caractère ou à la qualité de ses constatations. Par exemple, l'évaluation de la qualité d'une fonction logicielle dans l'application du système permet d'avoir une vision élargie sur la méthode de développement du logiciel. La revue de son processus de conception pour se forger une opinion d'appréciation subjective pourrait y parvenir. L'objectif est d'assurer la confiance de l'utilisateur par rapport au caractère approprié du logiciel pour son application. Cette confiance ne peut être garantie que lorsque le logiciel est utilisé dans un système informatique afin de déterminer ses caractéristiques de qualité en aptitude à la fonction réelle. Cette disposition fournit les éléments fondamentaux nécessaires à la démonstration des preuves tangibles. L'ingénierie utilise aussi bien les évaluations objectives que subjectives, qui se complètent dans le processus d'évaluation.

Les éléments suivants donnent les principaux objectifs d'un projet associés à l'évaluation de la sûreté de fonctionnement d'un système aux principaux points de décision du cycle de vie du système:

a) **identification du marché –** l'objectif consiste à identifier les besoins du marché afin de justifier les investissements nécessaires au développement de nouveaux systèmes ou à l'amélioration d'un système existant à des fins de concurrence. L'analyse du marché est essentielle pour justifier les principaux investissements qui impliquent l'engagement de ressources. Les activités d'ingénierie des systèmes impliquent l'identification de la capacité et des ressources, l'évaluation des nouvelles techniques pour une application réalisable, l'analyse concurrentielle et l'attente des utilisateurs en termes d'aptitude à la fonction du système, l'étendue de la logistique de maintenance nécessaire à l'exploitation continue d'un nouveau service ou d'un service amélioré, les contraintes de temps et de coût pour une entrée sur le marché, et l'influence des règlements et de l'environnement sur l'introduction du système. Il convient de tenir compte de la structure et de la configuration initiales du système afin de satisfaire les scénarios applicables d'exploitation du système. Il convient d'examiner les coûts du cycle de vie du système sur la base d'un rendement du capital investi. L'évaluation clé de la sûreté de fonctionnement venant à l'appui de l'identification du marché inclut:

   – la prévision de la sûreté de fonctionnement du système afin de répondre aux besoins éventuels du marché;

   – l'évaluation de la maturité des nouvelles techniques appropriées aux applications système qui affectent l'aptitude à la fonction de sûreté de fonctionnement;

   – l'identification des questions critiques relatives à la sûreté de fonctionnement relatives à l'effet sur l'aptitude à l'emploi et à l'influence sur l'exploitabilité;

   – l'évaluation de la capacité de sûreté de fonctionnement des fournisseurs et sous-traitants potentiels;

   – l'assurance de la pérennité du maintien du service, de la disponibilité et de la sécurité du système jusqu'à son retrait complet.

b) **conception et développement du système** – l'objectif consiste ici à rationaliser l'approche de conception du système et à évaluer les alternatives et options de conception. Le développement du système suit la conception choisie. Ceci représente un engagement considérable tant sur le plan des investissements en termes de capital que des investissements en termes de ressources. Les activités d'ingénierie du système impliquent l'analyse des exigences, la configuration de conception de l'architecture, l'évaluation de la conception et des techniques fonctionnelles, l'externalisation des travaux de sous-traitance et le choix des fournisseurs, la réalisation et l'intégration du système, les essais et la vérification de la qualification, l'installation et la transition du système pour les services opérationnels requis. L'évaluation clé de la sûreté de fonctionnement venant à l'appui de la décision de conception et de développement inclut:

   – l'évaluation des fonctions du système qui affectent l'aptitude à la fonction de sûreté de fonctionnement;

- l'évaluation de la structure du système pour l'optimisation de la fiabilité de la configuration du système;
- l'évaluation de l'accès pour les opérations de maintenance;
- la simulation de l'aptitude à la fonction de disponibilité du système et l'évaluation de l'aptitude à la fonction afin de déterminer un dysfonctionnement critique du système, une réduction des défaillances et les besoins en logistique de service;
- la vérification de la fiabilité et l'analyse des problèmes en vue d'actions correctives;
- l'évaluation des programmes de sûreté de fonctionnement des fournisseurs et sous-traitants;
- l'évaluation de la capacité de fabrication pour les résultats de production qui affectent la croissance de la fiabilité;
- l'évaluation des incitations à la garantie de fiabilité et des exigences relatives à la logistique.

c) **réalisation et mise en œuvre du système** – l'objectif consiste ici à appliquer les décisions achat-fabrication pour l'acquisition et l'installation d'éléments de sous-système, et à respecter les engagements en termes de ressources pour la construction et à l'intégration du système. L'évaluation clé de la sûreté de fonctionnement venant à l'appui de la réalisation et de la mise en œuvre du système inclut:

- l'évaluation de la conformité des éléments de système et des produits du commerce aux exigences relatives à la sûreté de fonctionnement pour l'intégration des sous-systèmes;
- l'évaluation de la conformité des sous-systèmes aux exigences relatives à la sûreté de fonctionnement;
- l'évaluation du processus d'assurance de qualité;
- l'évaluation des résultats de la réalisation des essais des sous-systèmes en vue de l'intégration du système;
- l'évaluation des résultats de la réalisation des essais des systèmes en vue de l'acceptation du système.

d) **acceptation du système pour l'exploitation** – l'objectif consiste ici à assurer la confiance de l'utilisateur par rapport à l'acceptation du système. Ceci implique le transfert des responsabilités au client pour une exploitation. L'acceptation déclenche la période de garantie afin de s'assurer que l'aptitude à la fonction du système répond aux attentes des utilisateurs finals. L'évaluation clé de la sûreté de fonctionnement visant à s'assurer de l'acceptation du système inclut:

- l'évaluation de l'aptitude à la fonction du système par l'introduction de programmes de poursuite en champ et de compte rendu d'incidents;
- l'évaluation des besoins en formation et de la compétence des opérateurs et des spécialistes de la maintenance du client;
- l'établissement d'un point focal pour le recueil des données et l'analyse des comptes rendus d'incidents afin de déterminer les tendances d'aptitude à la fonction de sûreté de fonctionnement et la criticité d'un dysfonctionnement du système nécessitant des actions correctives immédiates;
- l'évaluation de l'efficacité du service de maintenance du système et de la logistique;
- les procédures d'autorisation des modifications de conception et de gestion de la configuration.

e) **amélioration du système** – l'objectif consiste ici à justifier l'investissement pour l'amélioration ou l'extension du système existant. Ceci implique des activités similaires à celles nécessaires à la conception et au développement de nouveaux systèmes, comme dans le cas de l'amélioration du système. Les problèmes hérités relatifs au système existant doivent être traités afin d'assurer l'amélioration de l'interopérabilité et de la capacité du service. L'évaluation clé de la sûreté de fonctionnement venant à l'appui de la décision d'amélioration du système inclut:

- l'analyse coûts-avantages pour l'intégration des modifications;

- l'évaluation de l'influence de l'aptitude à la fonction de sûreté de fonctionnement due aux modifications avec ajout de nouvelles caractéristiques;
- la réaction du client aux modifications proposées;
- l'évaluation des risques et de la plus-value.

f) **retrait du système** – l'objectif consiste ici à retirer le système du service. L'évaluation clé de la sûreté de fonctionnement venant à l'appui de la décision de retrait du système inclut:

- l'évaluation de l'impact du coût pour l'interruption du service fonctionnel;
- l'évaluation de l'impact de la réglementation et de l'impact sur l'environnement pour l'interruption du service fonctionnel.

6.3.3 Méthodologie pour l'évaluation de la sûreté de fonctionnement du système

La méthodologie d'évaluation traite des problèmes de mise en œuvre concernant les processus, approches et stratégies.

La méthodologie d'évaluation comprend deux processus importants:

a) **vérification** – le processus de vérification constitue une méthode de confirmation des résultats d'évaluation. Il convient d'effectuer la vérification afin de soutenir les principaux points de décision à chaque étape du cycle de vie du système.

b) **validation** – le processus de validation fournit des preuves tangibles attestant que le système satisfait les exigences réelles et les attentes de l'utilisateur.

Les approches d'évaluation conviennent, souvent de façon exclusive, aux diverses situations de mise en œuvre d'un projet. Elles combinent par ailleurs les approches suivantes:

1) **approche analytique –** implique des activités telles que l'analyse de conception, la simulation de l'aptitude à la fonction du système, la conformité de normalisation et l'évaluation de la spécification de conformité.
2) **approche expérimentale –** implique des activités telles que les essais d'aptitude à la fonction et l'évaluation technique des fonctions système, les ensembles physiques, les produits des fournisseurs, l'intégration des sous-systèmes et l'acceptation réelle du système.
3) **approche consultative –** implique des activités telles que les revues d'experts, l'emploi des meilleures pratiques industrielles, la consultation des fournisseurs concernant les informations sur le produit, le sondage auprès de la clientèle et le retour d'information à l'utilisateur, la participation à la chaîne d'approvisionnement, le développement et l'amélioration des infrastructures.
4) **approche négociée –** implique des activités telles que la fixation de limites de risque acceptables pour l'exposition du système exploité au milieu environnant, les conditions de mise en place du produit dans des régions spécifiques, le recyclage des produits dérivés et des déchets, les incitations économiques et les avantages sociaux des accords contractuels et la conformité à des règlements nouveaux.

Il convient que les stratégies d'évaluation se concentrent sur deux aspects principaux de l'ingénierie de la sûreté de fonctionnement des systèmes:

i) **concentration sur l'application –** activité relative à la satisfaction des applications spécifiques au projet pour la conformité des exigences contractuelles. Les activités d'évaluation essentielles se concentrent sur l'évaluation et l'analyse de la sûreté de fonctionnement du système aux principaux points de décision du cycle de vie applicable de ce dernier. Les méthodes et outils d'évaluation sont utilisés couramment pour la vérification du produit et la validation du système ou du sous-système.

ii) **concentration sur la technologie –** activité relative à l'évaluation technologique de la stratégie de conception et des programmes de soutien au système, afin de faciliter la

réalisation de l'aptitude à la fonction de la sûreté de fonctionnement. Les activités essentielles d'évaluation se concentrent sur l'évaluation du niveau technologique pouvant être exploitée pour les modèles de systèmes, et sur la détermination de la viabilité des systèmes d'activation relatifs à la continuité du fonctionnement du système en exploitation. Il convient que les questions concernant l'évolution et l'obsolescence technique fassent partie intégrante des stratégies d'évaluation.

6.3.4 Valeur de l'évaluation et implications

L'évaluation constitue une condition préalable et un élément d'entrée crucial pour le processus décisionnel intervenant dans les projets. Il convient de rationaliser le processus d'évaluation pour une application donnée. Il convient de résoudre les problèmes rencontrés dans des délais raisonnables afin d'obtenir la valeur ou les avantages prévus pour le projet. Ce processus peut permettre d'instaurer la confiance nécessaire dans les décisions liées au projet. Les questions-clé suivantes qui donnent des exemples de la valeur de l'évaluation sont indiquées pour illustration. Des exemples types sont présentés pour souligner leurs implications principales sur les résultats liés au projet.

a) La synchronisation de l'évaluation est primordiale pour fournir des résultats significatifs. La valeur de l'évaluation se réduit fortement lorsque ses résultats ne sont pas disponibles le moment venu pour venir à l'appui des principales décisions. Par exemple, une prévision de fiabilité intervenant lors de la conception d'un système peut donner un aperçu de valeur du choix technologique approprié, de la structure de la conception architecturale, de la configuration de partitionnement et du choix des éléments et des composants du système pour la réalisation de leurs fonctions. Une prévision effectuée une fois la conception achevée est d'une valeur limitée lorsque le système est configuré et prêt à être fabriqué.

b) Il est prudent de justifier les coûts et avantages de l'évaluation avant de l'entreprendre et ce, pour la planification du projet et une gestion efficace. Par exemple, le processus « planifier, faire, vérifier, agir » dans les systèmes de management de la qualité (SMQ) sert couramment de base de planification des activités d'évaluation. L'analyse des investissements liée à l'évaluation constitue un élément critique pour justifier les principales dépenses d'investissement et les nouvelles acquisitions.

c) L'assurance du soutien de l'infrastructure convient à la mise en œuvre des outils d'évaluation. Ceci peut impliquer des modifications de procédures techniques et des adaptations culturelles qui nécessiteront à la fois du temps et des ressources. Par exemple, la migration du processus de modèles de maturité de la capacité logicielle vers le processus d'intégration de modèles de maturité de la capacité logicielle représente un effort important pour toute entreprise. Les ressources techniques et la culture managériale peuvent toutes deux faire l'objet d'ajustements pour parvenir au statut et à la certification reconnus par le secteur industriel.

d) La prise en compte des contingences dans la planification est essentielle pour éviter des résultats de projet inattendus ou des délais non programmés. Ceci peut avoir un impact sur la répartition des ressources et le redéploiement des tâches, la répartition de la chaîne d'approvisionnement et la livraison des produits du fournisseur, et influer sur les engagements programmés pour la mise en service du système et l'acceptation du client. Par exemple, il convient, aux principaux points de décision, d'inclure les plans d'urgence dans le processus d'évaluation, tels que l'identification de fournisseurs alternatifs en cas de défaillance d'un ou de plusieurs fournisseurs, l'application d'une expertise technique pour étudier des conceptions critiques afin de satisfaire des objectifs de livraison stricts, et l'analyse des moyens de financement viable pour les investissements en capital.

6.4 Mesure de la sûreté de fonctionnement d'un système

6.4.1 Objet des mesures de la sûreté de fonctionnement d'un système

Du point de vue de l'ingénierie, les mesures de la sûreté de fonctionnement d'un système représentent le processus d'assignation d'une valeur quantitative afin de caractériser l'attribut de la sûreté de fonctionnement. La valeur quantitative est déduite des données observées ou estimées relatives à la durée et du nombre d'incidents effectifs, afin de refléter les

caractéristiques de l'aptitude à la fonction de sûreté de fonctionnement. Le processus de mesure implique:

a) l'identification du type et de l'objectif de la mesure dans des conditions contractuelles, opérationnelles ou spécifiques, telles que l'évaluation du produit requérant la quantification des attributs de la sûreté de fonctionnement;

b) la détermination des données pertinentes et de la nature des sources de données pour les mesures;

c) l'utilisation de systèmes d'activation efficaces afin de faciliter le processus de mesure tels que la mise en place de systèmes de recueil de données, le compte rendu des défaillances, les systèmes d'analyse et d'actions correctives, les questionnaires d'enquête ou d'autres programmes de soutien;

d) l'interprétation des résultats de mesure afin d'établir des tendances d'aptitude à la fonction, d'identifier les questions critiques et de recommander des actions de gestion avec principes et justifications nécessaires;

e) la documentation des résultats de mesure pour la conservation des enregistrements, les audits qualité et les preuves tangibles.

f) l'ISO/CEI 15939 [6] définit un processus de mesure applicable à l'ingénierie système et au génie logiciel.

6.4.2 Classification des mesures de la sûreté de fonctionnement d'un système

Il existe quatre classes générales de mesures de la sûreté de fonctionnement qui visent à répondre aux besoins d'un projet.

a) **Mesure des attributs intrinsèques de la sûreté de fonctionnement du système –** l'objectif consiste ici à assigner des facteurs de qualité numériques afin de représenter les attributs intrinsèques de la sûreté de fonctionnement du système. Cette classe de mesure est utile pour comparer les attributs de la sûreté de fonctionnement d'architectures, de conception et de configurations système différentes. Le processus de mesure est appliqué au cours de l'étape de conception/définition du système afin de déterminer la capacité intrinsèque de l'aptitude à la fonction de sûreté de fonctionnement d'options diverses. L'objectif consiste à fournir des preuves de la capacité du système à satisfaire les objectifs de sûreté de fonctionnement dans le cadre d'enquêtes commerciales ou contractuelles. Les valeurs numériques peuvent être indiquées en termes de probabilité de succès, de temps moyen de fonctionnement entre défaillances, de durées de vie ou de taux de défaillance qui quantifient les caractéristiques d'aptitude à la fonction de disponibilité ou de fiabilité du système. Les méthodes de prévisions décrites dans la CEI 60300-3-1 [7] permettent d'effectuer les mesures.

b) **Mesure de la sûreté de fonctionnement du système pour l'évaluation de l'aptitude à la fonction et de l'exploitation –** l'objectif consiste à assigner un nombre pour désigner l'aptitude à la fonction de sûreté de fonctionnement du système en exploitation réelle. Cette classe de mesure est utile pour l'évaluation des attributs de la sûreté de fonctionnement au cours de l'étape de conception/développement pendant laquelle les produits et sous-systèmes sont soumis à l'essai pour vérifier le caractère approprié de l'aptitude à la fonction. Elle est également utilisée au cours de l'étape d'exploitation/maintenance du système afin de déterminer la conformité aux objectifs opérationnels établis pour la réalisation de la sûreté de fonctionnement. Le processus de mesure est appliqué au moyen d'essais progressifs des produits, des sous-systèmes et du système intégré pour la vérification et la validation de l'aptitude à la fonction, et par la traçabilité de l'état d'aptitude à la fonction de l'exploitation du système. Les données de mesure proviennent des essais de qualification des produits, des résultats des essais des fournisseurs portant sur les sous-systèmes, des essais de réception, des enregistrements d'aptitude à la fonction sur site et des comptes rendus d'incidents. Les valeurs numériques peuvent être indiquées en termes de fiabilité, probabilité de défaillance, temps de fonctionnement sans défaillance (durée de fonctionnement avant la première défaillance), durée de vie, temps de disponibilité en pourcentage (disponibilité), fréquence et durée de panne.

c) **Mesure de la sûreté de fonctionnement du système pour l'amélioration de l'aptitude à la fonction –** l'objectif consiste à assigner une valeur pour quantifier et qualifier le degré de satisfaction du client, ou à déterminer l'étendue de la plus-value apportée au client par l'amélioration de l'aptitude à la fonction. Il s'agit d'une mesure indirecte qui permet d'identifier l'impact des attributs significatifs de la sûreté de fonctionnement sur l'aptitude à la fonction du système. Cette classe de mesure a pour objectif la recherche d'un retour d'information direct de l'utilisateur sur l'aptitude à la fonction du système ou la détermination de la valeur de la prestation du service au cours de l'étape d'exploitation/maintenance du système Le processus de mesure est appliqué par l'intermédiaire de sondages auprès de la clientèle, d'audits d'aptitude à la fonction, d'évaluations de plus-value, de contacts et de dialogues directs avec les clients et les fournisseurs. Les enquêtes de satisfaction du client ont pour objectif d'identifier les sources actuelles de préoccupation des clients. L'application de la fonction qualité est couramment utilisée pour l'évaluation de la valeur d'aptitude à la fonction afin de définir les besoins des clients et de les traduire en exigences techniques appropriées exprimées en termes d'actions visant à satisfaire lesdits besoins. L'assignation de la valeur peut être définie selon une échelle de 1 à 5 inclus mentionnant des appréciations telles que mauvais à excellent.

d) **Mesure de la sûreté de fonctionnement du système pour les expositions aux risques –** l'objectif consiste à assigner des valeurs numériques pour indiquer l'étendue des expositions aux risques lorsque le système est utilisé pour des applications de sécurité et de sûreté. Il s'agit d'une mesure indirecte destinée à identifier la criticité des attributs de la sûreté de fonctionnement qui affectent les fonctions d'aptitude à la fonction du système. Cette classe de mesure s'applique au cours de l'étape de conception/définition du système afin d'identifier les fonctions et les éléments critiques de ce dernier pour une exploitation ou une mission spécifique. Le processus d'évaluation inclut la détermination d'une menace ou d'un préjudice par la désignation de sa gravité et de sa fréquence d'occurrence. La classification de risques peut être établie de manière qualitative par différents événements à caractère catastrophique, critique, majeur, mineur ou négligeable. Des valeurs probabilistes peuvent être assignées pour indiquer la gravité de la situation par une déclaration telle qu'une défaillance critique se produisant une fois tous les 10 ans. La CEI 60300-3-9 [8] décrit les méthodes d'appréciation des risques technologiques qui affectent les attributs de la sûreté de fonctionnement relatives à l'aptitude à la fonction du système. Une méthode similaire est utilisée dans la série de la CEI 61508 [9] concernant les niveaux d'intégrité de sécurité pour le classement des fonctions de sécurité (se reporter à la CEI 61508-1 [10] pour plus de détails).

6.4.3 Sources de mesures

Les mesures des attributs de la sûreté de fonctionnement du système peuvent être déterminées par des essais d'aptitude à la fonction directs dans des conditions simulées ou dans l'environnement d'exploitation réel dans lequel les données pertinentes peuvent être recueillies. Les attributs de la sûreté de fonctionnement du système peuvent également être évalués par des prévisions sur la base de l'historique d'aptitude à la fonction sur site de systèmes similaires; ils peuvent également être déduits de la base de données de fiabilité établie sur la foi de la configuration du système et des fonctions opérationnelles de ses éléments constitutifs.

Les données de mesure relatives aux attributs de la sûreté de fonctionnement peuvent également provenir d'autres sources telles que les programmes d'essai des fournisseurs, les données de logistique de maintenance, les informations sur la garantie et les sondages auprès de la clientèle. Il est important, à des fins d'assurance, de valider l'intégrité des données utilisées pour l'évaluation de la sûreté de fonctionnement.

6.4.4 Systèmes d'activation pour les mesures de la sûreté de fonctionnement

L'intégrité des données dans les mesures de la sûreté de fonctionnement est importante pour assurer la précision, la crédibilité et la cohérence du processus d'acquisition et de recueil des données. Cette intégrité permet d'assurer que les données pertinentes sont utilisées correctement dans l'analyse et permet par ailleurs une interprétation correcte des résultats de l'analyse. Il convient que la conception et le format du système soient simples et directs pour

recueillir les informations pertinentes nécessaires. Des entrées de données automatisées et un accès à des informations virtuelles interactives contribueraient à l'amélioration de l'opportunité de mise en œuvre du système. Différents systèmes de soutien sont utilisés dans la pratique d'ingénierie pour permettre le recueil de données économiques et faciliter les mesures de la sûreté de fonctionnement. Ces systèmes constituent des éléments essentiels de l'infrastructure des systèmes de gestion de la sûreté de fonctionnement. Ces systèmes peuvent, pour leurs rôles d'appui spécifiques, être classés comme systèmes d'activation afin de faciliter l'ingénierie de la sûreté de fonctionnement du système étudié. Les systèmes d'activation typiques utilisés couramment pour le recueil des données, le compte rendu d'incidents, l'analyse des problèmes et la mise en œuvre d'actions correctives comprennent:

a) un système de compte rendu et d'analyse des défaillances, ainsi que de mise en œuvre d'actions correctives, destiné à recueillir les informations de non-conformité et les données de défaillance d'essai lors du développement, de l'essai et de l'intégration des systèmes;

b) un système d'acquisition des données de rendement des essais pour détecter les défauts de fabrication afin d'assurer la traçabilité des rendements de production en vue de l'identification des problèmes et de l'analyse des causes profondes lors de la fabrication des produits;

c) le compte rendu d'incidents lors de l'exploitation du système afin d'identifier les incidents qui affectent la continuité du service d'aptitude à la fonction du système, de rendre compte des actions de maintenance sur site, d'assigner un degré de criticité de l'incident, ainsi que d'enregistrer les demandes d'assistance et de suivi et le temps de résolution nécessaire;

d) un système d'approvisionnement en pièces de rechange dédié au recueil des données relatives à la consommation desdites pièces et au délai d'achèvement du réapprovisionnement, de la distribution et de la reconstitution des stocks de ces mêmes pièces;

e) un système de retours d'information dédié au recueil des réclamations de clients, des préoccupations des fournisseurs et des suggestions du personnel pour une amélioration des infrastructures, une planification stratégique et la résolution des problèmes apportant une valeur ajoutée aux projets et à la gestion organisationnelle.

6.4.5 Interprétation des mesures de la sûreté de fonctionnement

L'interprétation correcte des résultats de mesure est essentielle à la mise en œuvre d'actions correctives et préventives rapides venant à l'appui d'une exploitation rentable. Les exemples suivants montrent l'importance des données mesurées ou analysées lorsqu'elles sont transcrites et interprétées pour les actions de suivi.

a) Il convient que l'acquisition et le recueil des données pertinentes apportent de la valeur ajoutée permettant de répondre aux besoins du projet. Cela suppose une planification et une organisation des expériences appropriées. L'acquisition des données réclame du temps et un investissement. Si ces données ne peuvent pas servir à résoudre plus facilement les problèmes actuels, il convient alors de ne pas les recueillir. Il convient de définir clairement l'objectivité du processus de mesure. Par exemple, l'utilité du recueil des données d'aptitude à la fonction sur site de systèmes anciens mis en place il y a de nombreuses années, et qui ne sont plus fabriqués ni soumis à maintenance, peut ne pas être très utile pour la conception des nouveaux systèmes utilisant une technologie différente.

b) Il convient que les mesures transcrites et les résultats interprétés présentent une conclusion logique pour les actions recommandées. Il convient que les données mesurées et les informations recueillies permettent si nécessaire, une analyse ultérieure dans le cadre d'arguments pour étayer une décision par la justification des actions recommandées. Il convient de noter qu'une interprétation différente des mesures de la sûreté de fonctionnement peut aboutir à une compréhension diverse des destinataires, qui sont généralement des individus ayant besoin de ces informations pour prendre des décisions. Par exemple, un indice d'aptitude à la fonction de disponibilité de 99, 999 7 % assigné à un commutateur peut se révéler être un nombre approprié pour un calcul de

probabilité des fonctions système, un programme de démonstration de la disponibilité du système étant toutefois difficile à formuler.

c) Il convient que les problèmes de sûreté de fonctionnement identifiés traitent de la criticité des questions en suspens pour alerter les actions du management. Les problèmes de cette nature identifiés dans un processus considéré concernant la sûreté de fonctionnement apparaissent habituellement dans des situations susceptibles d'avoir un impact sur la sécurité ou la sûreté si les personnes concernées n'y prêtent pas rapidement attention. Ces problèmes de sûreté de fonctionnement peuvent comporter des questions de responsabilités éventuelles et une exposition aux risques s'ils ne font pas l'objet d'une évaluation correcte au moment de leur occurrence. L'exploitation d'un système suit des procédures d'exploitation établies. Les incidents d'interruption du système sont consignés dans un rapport selon l'évaluation sur site de leur criticité. Il convient de résoudre certaines questions critiques de manière immédiate ou dans une période limitée. Les autres questions non critiques peuvent être reportées à une actualisation ou à une amélioration de maintenance ultérieure du système. Par exemple, une modification sur site d'un modèle de système pour résoudre un problème temporaire sans une autorisation appropriée de la modification de la conception peut engendrer des risques pour la sécurité à long terme inconnus. Des sous-programmes logiciels de modification provisoires destinés à résoudre un problème localisé sans examen approfondi peuvent aboutir à une atteinte à la sécurité ou à une panne générale du système. La conception de la sûreté de fonctionnement peut intégrer des caractéristiques de tolérance aux pannes. De telles fonctions de protection ne sont plus efficaces si elles ont été désactivées ou déconnectées pour appliquer une modification logicielle provisoire sans autorisation préalable appropriée. Il convient que le processus d'interprétation identifie et signale les problèmes potentiels afin d'éviter toute nouvelle occurrence de ce type d'incidents. Des panneaux et étiquettes d'avertissement placés en des lieux appropriés peuvent attirer l'attention.

Annexe A
(informative)

Processus du cycle de vie des systèmes et applications

A.1 Processus du cycle de vie des systèmes

A.1.1 Description des processus du cycle de vie des systèmes

La Figure A.1 illustre une séquence logique d'activités de processus applicables à chaque étape du cycle de vie pour l'ingénierie de la sûreté de fonctionnement du système.

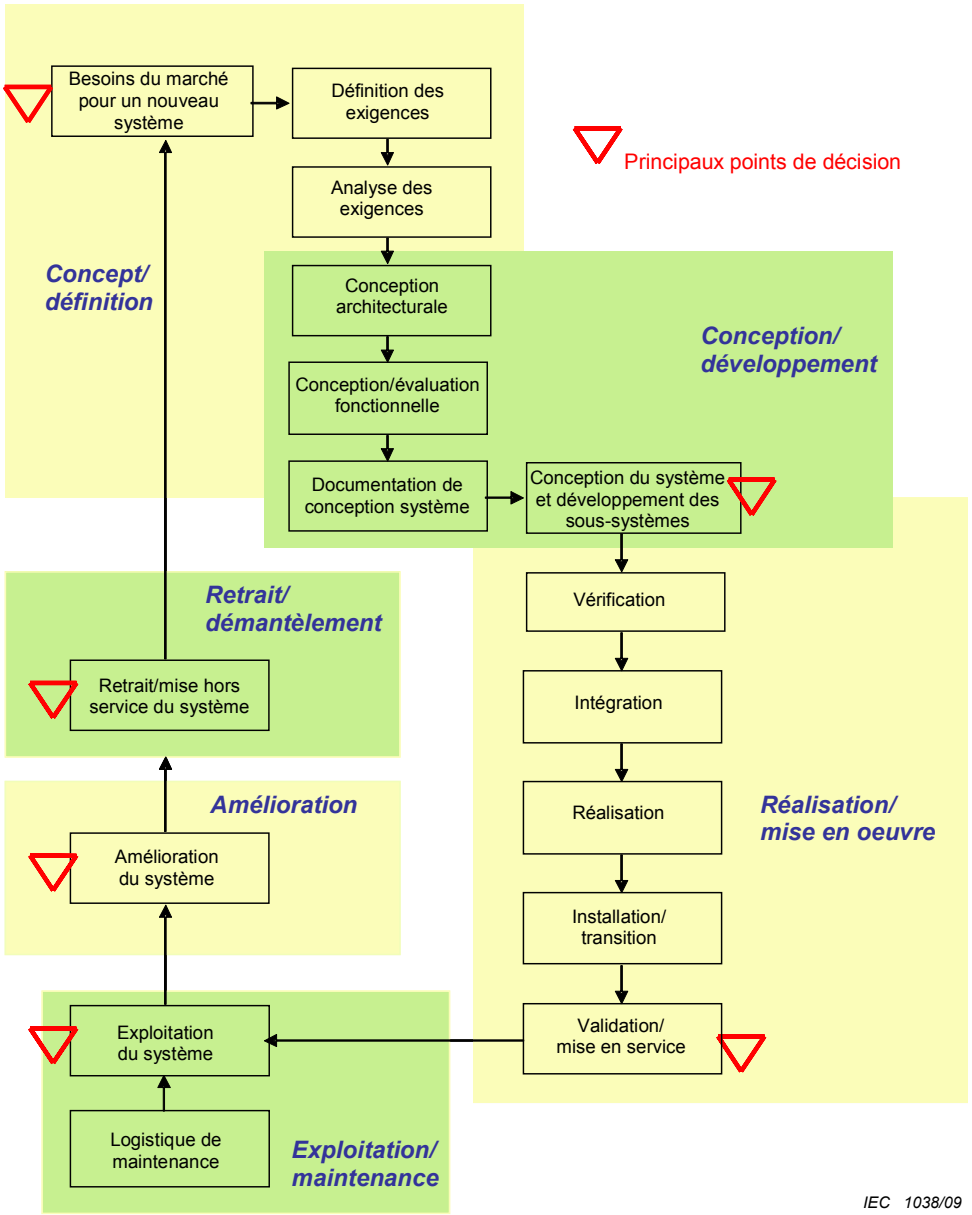

Figure A.1 – Présentation générale des processus du cycle de vie d'un système

Les trois premières étapes du cycle de vie d'un système, c'est-à-dire concept/définition, conception/développement et réalisation/mise en œuvre, avant la transition vers l'étape

d'exploitation/maintenance, se chevauchent du fait que ces processus sont itératifs. Ceci indique la nécessité d'assurer la continuité du flux de travaux selon les besoins du projet. L'étendue de la prestation d'ingénierie au-delà des limites définies de manière arbitraire des étapes voisines, dépend du calendrier d'exécution du projet et des activités de coordination. Cette prestation peut également servir à recueillir un nombre suffisant d'informations destinées à venir à l'appui du processus technique et de prise de décisions opérationnelles. Chaque étape du cycle de vie du système est décrite de manière succincte ci-dessous:

a) L'étape de **concept/définition** consiste à identifier les besoins du marché, définir/identifier l'environnement d'application/calendrier d'exécution opérationnels, définir les exigences système préliminaires et à confirmer les solutions de conception réalisables par la production de spécifications techniques pour la conception du système. Le choix des options de conception repose sur l'analyse des risques, l'évaluation d'incidence et les approches d'ingénierie. Les activités de processus impliquent la définition et l'analyse d'exigences, la conception architecturale et la conception/évaluation fonctionnelles afin de définir des spécifications système de haut niveau.

b) L'étape de **conception/développement** consiste à planifier et à exécuter les solutions de conception technique choisies pour la réalisation des fonctions du système. Cette étape se transcrit en une prestation de développement du système approprié, y compris la modélisation technologique, la construction de prototypes, l'évaluation des risques et l'identification de l'interface des éléments du système et des sous-systèmes. Une évaluation systématique des fonctions du système intégrées permet de vérifier l'interopérabilité de l'aptitude à la fonction et les interactions du système avec des milieux externes, afin de valider la configuration définitive du système. Il convient de définir correctement la planification de la logistique de maintenance, l'accès pour la maintenance, les procédures opérationnelles, ainsi que les processus d'assurance et de soutien, préalablement à la réalisation du système.

c) L'étape de **réalisation/mise en œuvre** consiste à exécuter les décisions achat-fabrication pour l'acquisition et la mise en place d'éléments de sous-systèmes. Les prestations de réalisation traitent des activités telles que les applications technologiques, la fabrication, le conditionnement et l'approvisionnement en fournitures de manière à assurer la transformation complète de la conception du système en éléments de produits ou de sous-systèmes spécifiés. Les produits ou éléments réalisés peuvent combiner des fonctions matérielles et logicielles. La mise en œuvre inclut des activités telles que l'intégration des fonctions du système, la vérification des sous-systèmes et l'installation du système. Il convient d'établir les procédures de réception du système en collaboration avec le client, afin de mettre en place des essais du système dans l'environnement d'exploitation réel avant la mise en service. Il convient que la validation fasse partie intégrante de l'essai afin de fournir les preuves tangibles de la conformité à la spécification du système. Il convient de noter que la vérification et la validation sont des activités se déroulant à chaque étape du cycle de vie et non juste au moment de l'intégration du système, tel qu'indiqué à la Figure 2.

d) L'étape **d'exploitation/maintenance** permet de mettre en place le système pour la fourniture du service et de venir à l'appui de la capacité opérationnelle du système grâce à la maintenance. Les activités de processus incluent l'exploitation et le maintien du système en service conformément aux exigences d'aptitude à la fonction de ce dernier, la formation des opérateurs et des spécialistes de la maintenance afin de pérenniser les compétences et qualifications, l'interface client destinée à établir une relation de service, la tenue de registres portant sur l'état d'aptitude à la fonction du système et le compte rendu des incidents de type défaillance afin de déclencher les actions correctives et préventives dans les délais impartis. Il convient de contrôler et de vérifier l'aptitude à la fonction du système de manière régulière afin de s'assurer du respect de la fiabilité et de la qualité des objectifs de service.

e) L'étape **d'amélioration** consiste à améliorer l'aptitude à la fonction du système par l'ajout de fonctionnalités afin de satisfaire les demandes croissantes des utilisateurs concernant

le système. Les activités de processus incluent une mise à jour logicielle, l'ajout de matériel(s), la formation professionnelle, la simplification des procédures afin d'améliorer l'efficacité opérationnelle, la gestion de l'obsolescence, la restructuration organisationnelle de manière à renforcer l'opportunité et à accroître la plus-value pour le client.

f) L'étape de **retrait/démantèlement** consiste à mettre fin à l'existence de l'entité système. Au terme du service du système au client, le système peut être démonté, réinstallé pour une autre utilisation ou éliminé, dans toute la mesure du possible sans affecter l'environnement. Il convient, pour les systèmes complexes, d'établir une stratégie de démantèlement afin de formaliser la planification et la mise en œuvre du processus de démantèlement, de manière à satisfaire les exigences réglementaires. Des dispositions réglementaires peuvent exister concernant le retour et la réutilisation ou l'élimination des produits de consommation.

A.1.2 Activités de processus pour les étapes du cycle de vie d'un système

La Figure A.1 illustre également les relations des activités de processus d'une étape à l'autre du cycle de vie d'un système. Les principaux points de décision indiquent le début et la fin des activités de processus à chaque étape d'exécution des engagements en termes de ressources en vue de la progression des processus techniques. Les données pertinentes sont recueillies au cours des activités de processus. Elles fournissent les informations essentielles pour l'analyse du coût du cycle de vie et l'évaluation des risques afin de venir à l'appui des résolutions techniques et des décisions opérationnelles.

Les données pertinentes recueillies comprennent les éléments d'entrée clés nécessaires au déclenchement des activités de processus de chaque étape, les principales activités de sûreté de fonctionnement à exécuter, les facteurs influents appropriés à étudier, et les éléments de sortie issus des actions générées par le processus. Il convient, dans toute la mesure du possible, d'indiquer la priorité et l'impact sur les activités de processus. Ces éléments fournissent des informations utiles pour l'appréciation des risques et le calcul du coût du cycle de vie. Le cas échéant, il convient d'identifier les approches techniques et les méthodes d'ingénierie utilisées pour les activités de processus.

A.2 Exemples d'applications de processus d'ingénierie

A.2.1 Processus applicable à l'étape de concept/définition du système

Eléments d'entrée:

- exigences, besoins et souhaits des clients;
- dispositions réglementaires relatives à la santé, la sécurité, la sûreté et les préoccupations environnementales;
- politique d'entreprise concernant les décisions en matière d'appels d'offres;
- informations commerciales et concurrence des marchés.

Activités de processus clés	*Activités liées à la sûreté de fonctionnement*
Définition des exigences	
• Identifier l'utilisateur (client) du système, la méthode et la durée d'utilisation de ce dernier. • Identifier les environnements d'application du système. • Identifier les contraintes liées aux solutions d'utilisation du système potentielles. • Identifier les problèmes héréditaires liés à l'interopérabilité avec les systèmes existants. • Etablir le profil opérationnel du système. • Documenter la spécification du système. • Identifier les calendriers et les cibles réalisables du système. • Répondre à la demande de proposition du client, le cas échéant.	• Identifier les besoins en termes de sûreté de fonctionnement associés aux applications du système. • Identifier la disponibilité du système et les temps d'interruption acceptables par le client • Identifier les contraintes technologiques liées au domaine d'application et à l'étendue de réalisation des objectifs de sûreté de fonctionnement. • Prendre connaissance de l'historique d'aptitude à la fonction sur site des systèmes existants ou de systèmes similaires, lorsqu'ils existent.
Analyse des exigences	
• Déterminer les limites du système, les fonctions opérationnelles et les caractéristiques d'aptitude à la fonction à partir de l'ensemble des exigences fonctionnelles définies. • Evaluer les contraintes identifiées qui affectent la conception architecturale. • Déterminer les approches techniques et la faisabilité de réalisation du système. • Déterminer les mesures techniques et de qualité qui permettent les évaluations du système. • Identifier la capacité de fonctionnement du système. • Identifier les exigences potentielles relatives aux partenariats et aux fournisseurs.	• Déterminer le scénario d'exploitation pour les évaluations de la sûreté de fonctionnement. • Définir les défaillances du système et les limites de dégradation des aptitudes à la fonction. • Identifier les expositions aux risques et la criticité des défaillances du système. • Déterminer le nombre de spécialistes de la maintenance et leur niveau de compétence associé requis. • Analyser la structure du système et la répartition de ses fonctions. • Analyser la disponibilité du système à laquelle contribue la configuration fonctionnelle de la conception architecturale. • Effectuer l'analyse par arbre de panne afin de déterminer les zones critiques requérant une attention sur la conception. • Effectuer une analyse des modes de défaillance système, ainsi que des effets et de la criticité afin de venir à l'appui des alternatives et des justifications de conception. • Evaluer la disponibilité du système et l'étude comparative des coûts qui affectent les options de conception. • Déterminer les moyens d'évaluation de la sûreté de fonctionnement.

Conception architecturale	
• Déterminer les options de conception architecturale logique appropriées. • Etablir la configuration du système. • Partager les fonctions du système. • Etablir les critères et les interfaces de conception. • Formuler les décisions achat/fabrication relatives aux fonctions du système. • Choisir les techniques de conception et le matériel/logiciel propres à la réalisation de ces fonctions. • Définir une solution visant à satisfaire les exigences du système. • Définir les moyens de vérification et d'intégration des fonctions du système.	• Elaborer un plan d'évaluation de la sûreté de fonctionnement. • Allocation de la disponibilité des fonctions du système. • Déterminer les critères de défaillance des fonctions du système. • Evaluer la fiabilité de chaque fonction partagée et recommander des options de conception alternatives si nécessaire. • Identifier les fonctions critiques nécessitant une attention particulière. • Définir les critères de maintenabilité de conception. • Etablir la testabilité de la fonction système à des fins de diagnostic et pour les actions de maintenance recommandées.
Conception/évaluation fonctionnelles	
• Formaliser le processus de conception fonctionnelle. • Identifier la composition de conception des éléments matériels/logiciels pour chaque fonction. • Intégrer les fonctions d'essai pour la vérification des aptitudes à la fonction. • Etablir les critères de calcul relatifs aux facteurs humains. • Etablir les critères de calcul environnementaux. • Etablir les critères de calcul ergonomique. • Etablir les critères de calcul de la CEM. • Etablir les critères de calcul de la sécurité, sûreté et fiabilité. • Définir les règles de conception matérielle. • Définir des programmes de calcul de la maturité des logiciels. • Simuler l'aptitude à la fonction du système au niveau fonctionnel afin de déterminer le taux de couverture de pannes et la stratégie de remise en état du système. • Vérifier les limites d'aptitude à la fonction et l'interopérabilité de la conception fonctionnelle afin de satisfaire aux exigences de conception architecturale.	• Effectuer l'évaluation de la fiabilité. • Evaluer la maintenabilité. • Effectuer une analyse des modes de défaillance fonctionnelle, ainsi que des effets et de la criticité. • Evaluer les compromis de conception fonctionnelle, la tolérance aux pannes et les risques. • Elaborer un plan de maintenance et de support logistique. • Etablir un processus d'évaluation des fournisseurs eu égard à la conformité de l'assurance qualité et de la fiabilité. • Etablir le processus d'évaluation et de réception des produits de série.
Documentation de conception du système	
• Documenter les spécifications du système	• Intégrer les exigences de sûreté de fonctionnement dans les spécifications du système.

Facteurs influents à prendre en considération:

- différentes formes de concurrence;
- questions économiques;
- questions technologiques;
- questions liées à la capacité;
- questions environnementales;
- problèmes héréditaires;
- synchronisation des questions liées aux investissements.

Mécanismes d'activation des applications de processus:

- ressources humaines;
- ressources financières;
- installations;
- processus de conception et de mise en œuvre intégrés;
- processus d'assurance.

Eléments de sortie:

- spécifications du système;
- connaissances relatives à la conception des systèmes.

A.2.2 Processus applicable à l'étape de conception/développement du système

Eléments d'entrée:

- spécifications du système;
- exigences relatives à la conception architecturale;
- plan de sûreté de fonctionnement.

Activités de processus clé	*Activités liées à la sûreté de fonctionnement*
Conception du système	
• Elaborer un plan de conception/développement du système. • Spécifier les exigences relatives à l'interface système/sous-système • Etablir les liens avec les systèmes interactifs. • Définir les exigences relatives à l'interface humaine. • Elaborer un plan de gestion de la configuration et les procédures de modification de la conception. • Définir les dimensions physiques et normaliser les encombrements d'assemblage. • Etablir des règles d'émission et de susceptibilité pour la construction d'installations, le câblage et la pose de canalisations électriques à l'intérieur et à l'extérieur de bâtiments et de structures d'hébergement de matériel(s). • Conclure des accords avec les fournisseurs pour le développement et l'acquisition d'éléments matériels/logiciels. • Engager la construction de prototypes de sous-systèmes. • Etablir des procédures d'intégration des systèmes. • Elaborer un plan d'essai et établir les critères d'acceptation du système. • Etablir un processus de surveillance du système, des programmes de diagnostic, ainsi qu'un système de compte rendu des incidents et de gestion des données. • Etablir des programmes de formation.	• Etablir un programme de sûreté de fonctionnement du système. • Etablir un programme d'assurance qualité. • Définir des exigences de sûreté de fonctionnement pour le système, les sous-systèmes et les fonctions. • Etablir les programmes de sûreté de fonctionnement des fournisseurs. • Etablir des critères d'acceptation de la sûreté de fonctionnement et des programmes de croissance de la fiabilité. • Etablir un programme de maintenance du système et de support logistique. • Elaborer un système de compte rendu des défaillances, d'analyse, de recueil des données et de retour d'information. • Définir des critères de fiabilité du personnel. • Définir les conditions de garantie.

Développement des sous-systèmes	
• Engager le développement interne de sous-systèmes. • Engager le développement de l'interface d'interopérabilité. • Contrôler et collaborer avec les services de développement externe de l'externalisation et de la sous-traitance des matériaux. • Préparer un plan de production. • Préparer un plan d'exploitation. • Préparer un plan de maintenance et de support logistique. • Préparer un plan de conditionnement, manutention, stockage et transport. • Préparer un plan d'installation. • Préparer un plan d'intégration. NOTE Les plans énumérés peuvent être intégrés en tant qu'activités dans le plan de projet principal afin de faciliter la mise à jour et la coordination des activités du projet.	• Mettre en oeuvre un programme de sûreté de fonctionnement des sous-systèmes. • Mettre en œuvre le programme de sûreté de fonctionnement du fournisseur. • Développer un programme d'approvisionnement en pièces de rechange. • Développer un programme d'essai logiciel et de diagnostic.

Facteurs influents à prendre en considération:

- disponibilité et accès aux ressources professionnelles appropriées;
- objectifs d'engagement pour les programmes de développement;
- risques liés au projet.

Mécanismes d'activation des applications de processus:

- disponibilité d'outils spécifiques nécessaires au développement;
- besoins en formation.

Eléments de sortie:

- prototype du système;
- exigences relatives au soutien du système et des sous-systèmes.

A.2.3 Processus applicable à l'étape de réalisation/mise en œuvre du système

Eléments d'entrée:

- prototype du système.

Activités de processus clé	*Activités liées à la sûreté de fonctionnement*
Réalisation	
• Engager la production de sous-systèmes. • Engager la construction d'éléments matériels/logiciels. • Evaluer les fonctions par essai. • Former les opérateurs et les spécialistes de la maintenance. • S'assurer de la disponibilité des matériels et des installations d'essai. • S'assurer de la disponibilité des instructions de conditionnement, manutention, stockage et transport.	• Mettre en œuvre un programme de sûreté de fonctionnement du système. • Mettre en œuvre un programme d'assurance de qualité. • Mettre en œuvre les programmes de sûreté de fonctionnement des fournisseurs. • Mettre en œuvre un programme de maintenance et de support logistique du système. • Mettre en œuvre un système de compte rendu des défaillances, d'analyse, de recueil des données et de retour d'information.

Intégration	
• Mettre en œuvre le plan d'intégration. • Assembler et intégrer une entité système. • Préparer des plans et des procédures de vérification et de validation. • Préparer un plan d'acceptation du système.	• Mettre en œuvre un programme de sûreté de fonctionnement du système lié à l'intégration. • Mettre en œuvre un programme d'assurance de qualité lié à l'intégration.
Vérification	
• Appliquer un plan de vérification. • Documenter les résultats de l'essai de vérification. • Préparer un plan d'acceptation du système. • Contrôler les résultats de vérification par rapport au plan d'acceptation du système	• Procéder à des évaluations de la sûreté de fonctionnement. • Documenter les comptes rendus de défaillances à partir des essais de vérification. • Générer des comptes rendus d'incidents pour les actions correctives/préventives recommandées. • Résoudre les anomalies constatées lors de la vérification.
Installation/transition	
• Appliquer un plan d'installation. • Documenter les registres et procédures d'installation. • Evaluer la stratégie d'amélioration de transition.	• Etablir des programmes de logistique de maintenance et de compte rendu partagés avec les spécialistes de la maintenance du client concernant le système installé dans les locaux du client. • Contrôler le délai d'achèvement de la restauration du système et du réapprovisionnement en pièces de rechange. • Etablir un inventaire des pièces de rechange adéquates sur le site du spécialiste de maintenance/client.
Validation/mise en service	
• Mettre en œuvre le plan de validation. • Documenter les résultats de l'essai de validation. • Appliquer le plan d'acceptation du système. • Mettre en œuvre les programmes de garantie le cas échéant. • Signature écrite du client pour l'acceptation du système en vue de son exploitation.	• Valider le fait que l'aptitude à la fonction du système satisfait les exigences relatives à la sûreté de fonctionnement. • Documenter les comptes rendus de défaillance à partir des essais de validation. • Produire des rapports de non conformité pour les actions correctives/préventives recommandées. • Résoudre les anomalies constatées lors de la validation. • Résoudre les problèmes de garantie avec les clients.

Facteurs influents à prendre en considération:

- gestion de la transition ;
- objectifs d'engagement pour le délai de livraison du système;
- exigences et incitations relatives à la garantie.

Mécanismes d'activation des applications de processus:

- gestion de projet;
- formation du client.

Eléments de sortie:

- exploitation du système;
- soutien au client.

A.2.4 Processus applicable à l'étape d'exploitation/maintenance du système

Eléments d'entrée:

- système exploité à sa capacité maximale.

Activités de processus clé:	*Activités liées à la sûreté de fonctionnement*
Exploitation	
• Mettre en oeuvre une stratégie d'exploitation. • Contrôler l'aptitude à la fonction du système. • Fournir une plus-value au client.	• Mettre en œuvre un programme de croissance de fiabilité. • Mettre en œuvre un système de recueil des données sur site. • Effectuer une enquête de satisfaction du client.
Maintenance	
• Mettre en oeuvre une stratégie de logistique de maintenance. • Contrôler les prestations de maintenance du système. • Prévoir un service d'assistance à la clientèle. • Exécuter des activités de maintenance en vue de corrections adaptatives.	• Analyser les défaillances les plus fréquentes. • Analyser les causes profondes des domaines de problèmes. • Recommander des modifications de conception ou de procédure en vue d'une amélioration continue. • Déterminer la qualité du service.

Facteurs influents à prendre en considération:

- capacité de service du système;
- chaîne d'approvisionnement en pièces de rechange;
- actions de maintenance corrective;

Mécanismes d'activation des applications de processus:

- gestion de projet;
- formation des opérateurs et des spécialistes de la maintenance.

Eléments de sortie:

- aptitude à la fonction de système fiable;
- résultats de l'enquête de satisfaction de la clientèle.

A.2.5 Processus applicable à l'étape d'amélioration du système

Eléments d'entrée:

- nouvelles exigences du client;
- fonctionnalités améliorées.

Activités de processus clé	*Activités liées à la sûreté de fonctionnement*
Amélioration	
• Identifier les nouvelles exigences. • Etablir une stratégie et un plan d'amélioration. • Evaluer la nécessité d'une modification et les avantages qui en résultent. • Mettre en oeuvre les efforts d'amélioration. • Exécuter les activités visant à des corrections perfectives.	• Evaluer l'impact sur l'aptitude à la fonction de sûreté de fonctionnement dû aux modifications apportées par l'ajout de nouvelles fonctionnalités. • Effectuer une étude d'impact sur le coût du cycle de vie en vue de l'intégration des modifications. • Effectuer une appréciation des risques et de la plus-value apportée. • Effectuer une enquête de satisfaction du client suite aux réactions face aux modifications opérées.

Facteurs influents à prendre en considération:

- calendrier des modifications;
- retour sur investissements.

Mécanismes d'activation des applications de processus:

- gestion des modifications;
- gestion de l'obsolescence;
- « rachat » des clients ou réaction à l'incorporation de nouvelles fonctionnalités de service.

Eléments de sortie:

- meilleure aptitude à la fonction du système;
- comparaison des résultats de l'enquête de satisfaction du client avant et après les efforts d'amélioration.

A.2.6 Processus applicable à l'étape de retrait/démantèlement du système

Eléments d'entrée:

- état de la capacité d'aptitude à la fonction du système vieillissant;
- compétitivité et possibilité de commercialisation du service opérationnel existant;
- coûts de maintenance et de soutien accrus.

Activités de processus clés	*Activités liées à la sûreté de fonctionnement*
Retrait/démantèlement	
• Exécuter le plan de retrait/démantèlement du système. • Mettre en œuvre la stratégie de réutilisation et de réinstallation. • Appliquer le traitement des déchets pour les articles non recyclables/réutilisables • Notifier la fin du service aux clients. • Fournir des informations sur la prestation d'un nouveau service ou d'un service alternatif.	• Evaluer les contraintes sur la désactivation du système et l'impact sur le retrait du service du système. • Evaluer l'impact des articles non recyclables/réutilisables sur l'environnement. • Effectuer une enquête sur la satisfaction du client suite à la fin du service.

Facteurs influents à prendre en considération:

- calendrier de retrait;
- obsolescence des technologies;
- contraintes réglementaires;

- Impact social suite à la fin du service.

Mécanismes d'activation des applications de processus:

- gestion de projet.

Eléments sortants:

- fin du service.

Annexe B
(informative)

Méthodes et outils pour le développement et l'assurance de la sûreté de fonctionnement d'un système

B.1 Généralités

Les méthodes et outils constituent une aide à la résolution des problèmes techniques génériques, y compris l'ingénierie de la sûreté de fonctionnement des systèmes à diverses étapes du cycle de vie. Il existe de nombreux outils et fournisseurs d'outils sur le marché. Certains outils se présentent sous des formes normalisées et de simples listes de contrôle; d'autres constituent des systèmes interactifs complexes qui requièrent souvent des contrats de licence pour l'accès à des bases de données et un soutien technique. Les méthodes et outils sont couramment développés en interne sur la base de l'expérience technique acquise, ou peuvent être achetés auprès de fournisseurs afin de faciliter la formation du personnel et un usage multiple. Il convient que le choix des méthodes appropriées pour une solution technique donnée soit laissé à la discrétion des ingénieurs ou des spécialistes en charge de la tâche de sûreté de fonctionnement. Dans la mesure où le choix des outils implique des investissements, il convient que l'ingénieur ou le spécialiste tienne compte de la pertinence des problèmes techniques liés à la sûreté de fonctionnement devant être résolus, de la fréquence d'utilisation des outils, de la prestation de formation requis pour l'utilisation efficace de l'outil concerné afin d'obtenir des résultats, et de la disponibilité de méthodes alternatives d'emploi de techniques plus simples destinées à résoudre le même problème à l'aide d'un jeu d'outils simple développé en interne. Des exemples typiques d'applications générales et d'applications spécifiques matérielles et logicielles des méthodes et outils pour l'ingénierie de la sûreté de fonctionnement des systèmes sont fournis ci-dessous.

B.2 Applications générales des méthodes et outils pour l'ingénierie de la sûreté de fonctionnement des systèmes

B.2.1 Cas de fiabilité et de maintenabilité

L'outil de fiabilité et de maintenabilité (R&M) est utilisé par l'acquéreur du système afin de s'assurer que les exigences qu'il a spécifiées sont déterminées et comprises tant par le fournisseur que par l'acheteur du système. L'outil permet également de s'assurer de manière progressive que les exigences R&M sont ou seront satisfaites tout au long du cycle de vie du système.

L'outil fournit un cadre pour:

a) le cas R&M – une argumentation rationnelle auditable venant à l'appui de la déclaration selon laquelle un système défini satisfait les exigences R&M;

b) le rapport de cas R&M – une synthèse ou un résumé des preuves et argumentations R&M issues du cas R&M venant à l'appui des points-clés du ou des programmes et

c) assurance progressive du cas R&M sur l'ensemble des points-clés du projet.

Document de référence: DEF STAN 00-42 [11].

B.2.2 Programmes de croissance de fiabilité

Les programmes de croissance de fiabilité sont utilisés pour améliorer la fiabilité du système au cours de l'étape de conception/développement du système. L'objectif de la croissance de fiabilité est de réaliser le potentiel d'objectifs de fiabilité du système par des améliorations progressives à l'aide de techniques d'analyse de la conception et d'essai de fiabilité des modules ou des fonctions du système. L'activité critique relative à la sûreté de

fonctionnement consiste à identifier et à supprimer les défauts de conception du système en vue d'une amélioration progressive de la fiabilité. Les systèmes typiques qui peuvent tirer avantage de l'application des programmes de croissance de fiabilité sont les systèmes qui utilisent des techniques nouvelles de conception architecturale, de nouveaux composants système non éprouvés, et des constituants logiciels importants destinés à être intégrés au fonctionnement du système. Le concept de croissance de fiabilité consiste à réduire la probabilité d'occurrence de défaillances dues à des défauts de conception, grâce à des améliorations progressives de la conception du système et de ses fonctions constitutives tout au long du processus de conception et de développement. Il convient d'intégrer les programmes de croissance de fiabilité à la conception du système et au processus d'évaluation pour réaliser des systèmes rentables. Un programme de croissance de fiabilité est décrit dans la CEI 61014 [12]. Les modèles de croissance de fiabilité et les méthodes d'estimation applicables aux évaluations de la croissance de fiabilité basés sur les données de défaillance recueillies dans le programme de croissance de fiabilité sont décrits dans la CEI 61164 [13].

B.2.3 Gestion de la configuration

La gestion des diverses configurations successives d'un système est une préoccupation majeure pour la sûreté de fonctionnement (c'est-à-dire la logistique de maintenance). Ceci est dû au grand nombre d'interfaces générées par les différentes configurations. La demande croissante pour une interchangeabilité des composants (matériel et logiciel) et une interopérabilité des systèmes a un intérêt commercial direct et implique une attention spécifique à la gestion de la configuration. Ceci est particulièrement vrai pour les systèmes à longue durée avec des composants ayant une durée de vie plus réduite, et dont la technologie peut changer souvent au cours de la durée de vie du système. Une gestion solide de la configuration contribue de manière significative, au cours du développement d'un système, à la réalisation d'une sûreté de fonctionnement efficace. La gestion de la configuration est essentielle pour le contrôle des modifications apportées au système et pour des évaluations significatives de la sûreté de fonctionnement. Un guide sur la gestion de la configuration générale est décrit dans l'ISO 10007 [14].

B.2.4 Réseaux de croyances bayésiens (BBN)

Ces réseaux constituent un formalisme graphique puissant venant à l'appui d'un raisonnement portant sur des événements incertains, en utilisant diverses formes de preuves. Ces mêmes réseaux permettent de modéliser l'incertitude et de combiner différents types de preuves, y compris à la fois des informations subjectives basées sur un jugement autorisé et des preuves « tangibles » issues d'une mesure. Un réseau de croyances bayésien acceptera autant ou aussi peu de preuves à disposition de l'utilisateur ou que ce dernier souhaite intégrer, de manière à pouvoir formuler une prévision en l'absence de données ou avec des données incomplètes. Cette méthodologie propose une approche utile de prévision de la sûreté de fonctionnement d'un système à toutes les étapes du cycle de vie lorsqu'une combinaison de mesures indirectes et directes de la sûreté de fonctionnement est disponible.

De nombreux produits de réseaux bayésiens sont disponibles dans le commerce, qui facilitent la saisie de données et la constitution de réseaux de croyances bayésiens.

B.3 Applications de méthodes et outils spécifiques au matériel, pour l'ingénierie de sûreté de fonctionnement des systèmes

B.3.1 Amélioration de la fiabilité

L'amélioration de la fiabilité des éléments matériels d'un système est concentrée sur les propriétés intrinsèques des fonctions du système et les facteurs influents qui affectent l'aptitude à la fonction de fiabilité de ce dernier. Cette amélioration porte principalement sur la technologie utilisée dans la construction du système, l'environnement d'exploitation de ce dernier, et l'application des fonctions système pour atteindre les objectifs d'aptitude à la fonction du système. Il existe de nombreuses méthodes et techniques classiques de fiabilité applicables aux évaluations de la fiabilité, tel que décrites dans la CEI 60300-3-1.

L'amélioration de la fiabilité peut être réalisée par l'intégration correcte des résultats recommandés aux solutions pratiques, sur la base d'éléments d'évaluation de la fiabilité pertinents. Dans la plupart des cas, un compromis de conception se révèle nécessaire pour déterminer la meilleure solution. Certaines méthodes peuvent être utilisées pour des automatismes régulateurs afin de vérifier les résultats d'analyse des évaluations effectuées avec le même élément matériel.

Les exemples typiques d'utilisation de méthodes et outils de fiabilité comprennent:

- l'utilisation d'un bloc-diagramme de fiabilité (BDF) pour déterminer les besoins de redondance par rapport à l'utilisation d'un seul élément matériel de plus grande fiabilité et de technologie nouvelle avec une prime de coût;
- l'utilisation de l'analyse de Markov pour l'évaluation de la fiabilité de structures de systèmes complexes et de stratégies de maintenance complexes;
- l'utilisation de l'analyse par arbre de panne (AAP) afin d'identifier les défaillances critiques d'un système;
- l'utilisation de l'analyse des modes de défaillance et de leurs effets (AMDE) afin de déterminer les modes, effets et causes potentiels des défaillances, et la criticité associée des expositions aux risques;
- l'utilisation de la prévision des taux de défaillance pour estimer la fiabilité intrinsèque des éléments matériels.

Il convient de noter que des limites s'appliquent à l'utilisation des méthodes et outils de fiabilité. Les hypothèses exprimées dans la formulation d'un problème sont essentielles pour la justification et l'adaptation de l'approche technique adoptée. Un jugement technique fondé sur une expérience pratique est nécessaire pour pouvoir interpréter les résultats d'évaluation de la fiabilité préalablement aux recommandations.

Dans la mesure où l'effet thermique et l'interférence électromagnétique affectent l'aptitude à la fonction des composants électroniques des fonctions système, il est prudent en vue de l'analyse du système, de développer un moyen de budgétisation thermique et de compatibilité électromagnétique et cela afin de limiter l'exposition aux risques d'une défaillance catastrophique du système. Cette approche présente une méthode d'analyse technique viable qui permet de réaliser l'aptitude à la fonction de fiabilité du système. Les conceptions d'évitement des pannes et de tolérance aux pannes sont fondamentales pour leur intégration dans des applications systèmes critiques.

B.3.2 Amélioration de la maintenabilité

Il est important, pour l'amélioration de la maintenabilité, de prendre en considération la facilité de maintenance d'un élément matériel réparable sous la forme d'un ensemble. Ceci implique que l'élément pourrait, en cas de dysfonctionnement ou d'usure, être identifié, isolé, retiré et remplacé par un nouvel élément. Les critères de détermination de la maintenabilité de la conception du système traitent du partitionnement de l'ensemble système pour une facilité d'accès, de la construction de la plus petite unité remplaçable en vue de son remplacement, de la testabilité de cette dernière pour la détection des pannes, ainsi que du coût et de la fiabilité de cette même unité pour l'approvisionnement en pièces de rechange. Ces critères permettront également de déterminer l'aspect économique d'un article jetable ou d'une plus petite unité remplaçable et réparable.

La maintenabilité d'un système traite généralement de trois niveaux de réparation de base:

- **niveau de l'organisme** – restauration du système à son emplacement, qui implique habituellement le remplacement de la plus petite unité remplaçable comme module enfichable, avec des temps d'isolement et de remplacement relativement courts;
- **niveau intermédiaire** – restauration de la plus petite unité remplaçable à un local commercial intermédiaire pour soumettre à l'essai, diagnostiquer, réparer/ré-usiner et

restaurer ultérieurement l'unité à son état opérationnel en vue de son recyclage. Ce niveau nécessiterait une durée plus longue;

- **niveau du dépôt** – une réparation et un ré-usinage plus intensifs peuvent être effectués pour restaurer l'article à son état opérationnel en vue de son recyclage. Ce niveau nécessiterait une durée plus longue.

Si la plus petite unité remplaçable est un article jetable, la maintenabilité du système est alors bien plus simplifiée avec deux niveaux de maintenance uniquement. Le remplacement de l'unité défaillante intervient uniquement au niveau de l'organisation et la ou les pièces de rechange proviennent du dépôt, qui peut être l'usine ou l'équipementier d'origine. Aucun atelier de réparation n'est requis. Le défi et l'incitation en jeu consistent ici à concevoir un article jetable rentable et écologique pouvant être éliminé.

La testabilité est un paramètre important de l'amélioration de la maintenabilité du matériel. L'étendue du diagnostic et la couverture d'essai d'une unité défaillante détermine souvent le temps et l'effort consacrés à la détection d'une entité sans défaillance constatée et qui épuise les ressources de maintenance. Il convient que la politique de réparation assure la traçabilité de ces articles sans défaillance constatée et identifie le nombre de réparations/ré-usinages d'un article défaillant avant d'être éliminé comme article jetable. Il convient également que ladite politique examine et garantisse la précision et l'efficacité du matériel d'essai de manière à identifier clairement et à déterminer l'article défaillant.

Il convient que la conception de la maintenabilité prenne en considération les aspects de l'ergonomie afin de faciliter les interactions humaines en vue de la restauration du système et du fonctionnement du service de maintenance. Il convient que les travaux de maintenance préventive et corrective tiennent compte des questions liées à la sécurité et à la sûreté. Le guide pour la conception et les applications de la maintenabilité est décrit dans la CEI 60300-3-10 [15].

B.3.3 Amélioration de la maintenance et du support logistique

La maintenance et le support logistique sont concentrés sur la pérennité de l'aptitude à la fonction du système grâce à la réalisation de ses objectifs opérationnels. Les activités sont exécutées principalement au cours de l'étape d'exploitation/maintenance du système. L'amélioration de la maintenance et du support logistique peut être réalisée par l'amélioration de l'aptitude du système au soutien dans les contraintes du scénario établi de configuration et d'exploitation du système. L'amélioration du service "d'assistance" à la clientèle et la simplification des procédures de logistique de service permettent le gain d'une plus-value. L'amélioration est également possible par une automatisation efficace du compte rendu de l'activité de maintenance et la mise en place d'un système d'analyse du support logistique. Les questions liées au support logistique concernant un système centralisé ou décentralisé de dépôt de soutien, ainsi que la planification et la programmation stratégiques des tâches de support de maintenance, pourraient entraîner la réduction du temps et de la prestation de maintenance. Il est prudent, dans l'environnement actuel de marchés concurrentiels où les systèmes sont installés dans les locaux du client et distribués à grande échelle au niveau mondial, d'envisager que des travaux de maintenance essentiels soient effectués par un service de maintenance contractuel tiers. L'externalisation des travaux de support de maintenance nécessite une formation supplémentaire du personnel de maintenance contractuelle ayant les compétences et l'expertise appropriées pour exécuter le service nécessaire aux clients. Ce personnel, de premier niveau, traite des réclamations de clients. Le recueil d'informations relatives aux préoccupations des clients portant sur le travail de service effectué et la confiance des clients eu égard au système constituerait un défi essentiel pour la coordination du processus de logistique de maintenance du système. Diverses méthodes ont été employées pour ce type de techniques d'amélioration, y compris la maintenance basée sur la fiabilité (MBF) décrite dans la CEI 60300-3-11 [16] et le processus de support logistique intégré (SLI) décrit dans la CEI 60300-3-12 [17].

B.4 Applications spécifiques au logiciel des méthodes et outils pour l'ingénierie de la sûreté de fonctionnement des systèmes

B.4.1 Méthodologie orientée objets

C'est une approche de modélisation d'un système en qualité d'ensemble d'objets interactifs avec des données et un comportement associés. Cette méthodologie est basée sur la décomposition des exigences ou la conception d'un système en un ensemble hiérarchique de classes et d'objets.

B.4.2 Méthodologie structurée

C'est une technique basée sur la décomposition des exigences ou la conception d'un système en un ensemble de processus algorithmiques interconnectés par un flux de données défini. Les processus transforment les données d'entrée pour générer des données de sortie. La décomposition peut être procédurale, orientée données ou orientée informations. Les méthodologies structurées peuvent également être caractérisées par le fait que la méthodologie concernée est destinée ou non à un système temps réel.

a) **Méthode procédurale** – approche qui considère les processus algorithmiques utilisés dans le modèle de système comme la caractérisation fondamentale de ce dernier. La définition des données provient des processus définis.

b) **Méthode orientée données** – approche qui considère les éléments d'entrée et de sortie du modèle de système comme la caractérisation fondamentale de ce dernier. Les processus algorithmiques sont déduits des structures de données.

c) **Méthode orientée informations** – approche qui utilise un modèle de données logiques pour l'intégration des composants du système d'information. Cette approche souligne les exigences stratégiques relatives aux échanges de données dans un système d'entreprise. Les composants du système d'information sont ensuite établis sur la base des exigences du modèle de données logiques.

B.4.3 Conception de la décomposition fonctionnelle

C'est une approche qui est concentrée sur la définition de modules et d'interfaces par le partitionnement des fonctions spécifiées d'un système logiciel. Le processus de conception est habituellement appliqué après le développement des exigences du système et le choix d'un concept pour la structure de ce dernier. Le processus itératif affine la conception selon une méthode descendante et ascendante complémentaire. Cet affinement est effectif par la répartition d'un système en fonctions interactives ou la fonctionnalité des éléments du système. La hiérarchie de conception d'un système comprend généralement trois niveaux: la conception de haut niveau, la conception de niveau moyen, et la conception détaillée de plus bas niveau. Le comportement de chaque niveau hiérarchique d'un système peut être décrit par une représentation schématique des entrées et des sorties, et le processus de transformation des fonctions pertinentes. A chaque niveau, les informations obtenues par le processus de décomposition fonctionnelle permettent de tracer un bloc-diagramme. Les blocs-diagrammes montrent comment les éléments d'un système dans l'architecture de ce dernier peuvent "collaborer" et comment la description fonctionnelle de chaque bloc peut être associée à son exploitation. L'approche utilisée est très similaire à la méthode du bloc-diagramme de fiabilité (BDF) avec une désignation différente des fonctions. La méthode de la décomposition fonctionnelle est un outil utile de conception des systèmes qui fournit une approche systématique d'enregistrement de la description de la hiérarchie du système et de ses fonctions constituantes. L'application formelle de techniques de conception fonctionnelle améliore la qualité des modèles de système et renforce la sûreté de fonctionnement de l'opérabilité de l'aptitude à la fonction. L'affinement progressif, la conception structurée et la conception en temps réel constituent des exemples de méthodes de conception de la décomposition fonctionnelle.

B.4.4 Analyse d'erreur

Cette analyse se compose:

- du processus d'examen d'une défaillance logicielle observée afin d'assurer son traçage jusqu'à sa source;
- du processus d'examen d'une défaillance logicielle observée afin d'identifier une information telle que la cause de la défaillance, la phase du processus de développement au cours de laquelle la défaillance a été introduite, la méthodologie qui aurait pu éviter la défaillance ou la détecter plus tôt, et la méthode qui a permis de détecter la défaillance;
- du processus d'examen des erreurs, défaillances et pannes logicielles permettant de déterminer les taux et tendances quantitatives.

L'analyse d'erreur implique de déterminer si la cause du problème est matérielle ou logicielle.

B.4.5 Technique Delphi

C'est une technique de prévision de groupes, généralement utilisée pour les événements futurs tels que les développements technologiques, fondée sur les estimations d'experts et les synthèses de retours d'informations de ces estimations afin que ces experts puissent effectuer des estimations supplémentaires jusqu'à l'obtention d'un consensus raisonnable. Cette technique a été utilisée dans diverses activités d'estimation des coûts logiciels, y compris l'estimation des facteurs qui influencent les coûts logiciels. Il convient, pour une compréhension détaillée de la technique Delphi, de faire référence à un document dédié à la technique Delphi telle que The Delphi method: Techniques and applications, publiée par H. A. Linstone and M. Turoff.

B.4.6 Outils de génie logiciel assisté par ordinateur (CASE)

Ces outils permettent l'automatisation d'un ou de plusieurs aspects du processus d'ingénierie logicielle. Ils sont couramment utilisés dans le développement du génie logiciel et les travaux de maintenance. Les fournisseurs de logiciels créent de nombreux outils CASE qui sont utilisés pour des applications spécifiques par divers organismes. Les outils CASE disponibles dans le commerce facilitent les applications logicielles telles que l'analyse de la structure d'un système, la gestion des exigences, la modélisation et la simulation, la conception graphique logicielle, la génération de codes, la réingénierie, la localisation des "bogues", la production de rapports et la création de systèmes d'aide. Les outils CASE sont des produits logiciels du commerce. Il convient que le choix et l'application des outils CASE suivent un processus d'évaluation normal à des fins d'assurance. Le guide sur la classification des outils CASE est décrit dans la norme IEEE 1175.1 [18]. Les lignes directrices pour l'évaluation et le choix des outils CASE sont décrites dans l'ISO/CEI 14102 [19].

B.4.7 Services d'environnements de génie logiciel (SEE)

C'est une collection de services logiciels, partiellement ou totalement automatisés par des outils logiciels utilisés pour soutenir l'exécution des activités humaines dans le génie logiciel. Les activités SEE sont habituellement exécutées dans un environnement de projet de développement et de maintenance d'un logiciel. Elles couvrent des domaines tels que la spécification, le développement, la réingénierie ou la maintenance de systèmes logiciels. Les applications SEE peuvent couvrir plusieurs situations, par exemple de l'utilisation de quelques outils avec le même système d'exploitation, à l'environnement totalement intégré, capable de traiter, surveiller et contrôler tous les processus, données et activités du cycle de vie d'un logiciel. Un service SEE soutient les activités humaines grâce à une série de services qui décrivent les capacités de l'environnement. Le processus logiciel soutenu par un service SEE est un processus logiciel assisté ou automatisé. Un service SEE peut être considéré comme un système d'activation. Des informations supplémentaires sur les services SEE sont fournies dans l'ISO/CEI 15940 [20].

B.4.8 Modèles de maturité de la capacité

Le modèle de maturité de la capacité (MMC) est utilisé par les organismes pour décrire leur maturité de processus logiciels. Le MMC classe un organisme selon un niveau de 1 à 5:

– Niveau 1: considéré ad hoc ou chaotique
– Niveau 2: processus reproductibles
– Niveau 3: processus définis (norme minimale industrielle sur les processus techniques)
– Niveau 4: processus mesurés
– Niveau 5: processus optimisés

Le modèle MMC est utilisé de manière systématique basé sur un ensemble de principes afin de déduire un questionnaire de maturité. L'élaboration complète du cadre de maturité permet de générer un modèle. Ce cadre fournit à l'organisme qui utilise le modèle un guide efficace pour l'établissement de programmes d'amélioration des processus.

Le modèle de maturité de la capacité logicielle permet à l'organisme d'accroître la maturité des processus logiciels en utilisant les connaissances acquises par les évaluations desdits processus et un retour d'information extensif des meilleures pratiques industrielles.

Le MMC se concentre sur le processus de développement. Les domaines du processus définissent les blocs fonctionnels ou les blocs de connaissances basés sur les pratiques industrielles. Les niveaux de maturité définissent les dépendances et les priorités d'amélioration.

Le Niveau 1 consiste à aider les organismes à concentrer leurs prestations sur les ressources limitées d'amélioration de processus consacrées aux changements les plus importants. La hiérarchisation par ordre de priorité est importante dans la mesure où la plupart des sociétés de logiciels à maturité moindre ne disposent pas des données historiques nécessaires pour déterminer si un changement constitue effectivement une amélioration. En d'autres termes, le changement opéré entraînera une amélioration importante du point de vue statistique, dans un certain délai prévu, y compris tous les coûts associés à la réalisation du changement, par comparaison à une absence de changement.

Le Niveau 2 concerne principalement les processus de gestion en vue d'une meilleure planification du calendrier, de la durée et des ressources, d'une localisation et d'un contrôle du ou des projets.

Le Niveau 3 établit un processus de développement reproductible défini par l'organisme qui constitue la référence d'améliorations mesurées futures. Il établit également les mécanismes de recueil des données de processus/produits, ainsi que les méthodes permettant de déterminer comment l'aptitude à la fonction et la qualité du processus adhèrent aux objectifs de l'entreprise.

Le Niveau 4 concerne les variations qui ne font pas partie intégrante du système des causes communes. Ce niveau reconnaît que le processus de développement constitue un système en soi et que des techniques statistiques peuvent être appliquées. Le niveau 4 est utilisé pour prévoir l'aptitude à la fonction et la qualité sur la base de l'expérience acquise et des données disponibles.

Le Niveau 5 concerne les causes communes de variance pour analyser la cause des défauts, mesurer les changements potentiels destinés à réduire ou à prévenir ces défauts, et déterminer si les changements constituent des améliorations effectives. Il s'agit du processus d'optimisation ou d'amélioration continue.

Le MMC fournit un étalon de comparaison de la capacité du processus de développement de l'organisme, ledit étalon permettant par ailleurs d'utiliser cette mesure comme élément de prévision de la qualité du ou des produits.

Le développement de l'utilisation du modèle de maturité de la capacité logicielle et de l'expérience associée a permis de développer des modèles pour différentes disciplines et

applications techniques. Le modèle de maturité de la capacité de l'ingénierie systèmes constitue l'un de ces modèles. La capacité du génie logiciel est la capacité d'une société de logiciels à obtenir des résultats positifs en termes de coût, calendrier, fonctionnalité du ou des produits et qualité. La capacité comprend plusieurs dimensions incluant

1) l'expertise, l'expérience, la formation et la motivation du personnel qui exécute et gère le travail,
2) la capacité de processus, et
3) la technologie disponible et appliquée.

Les modèles distincts de génie logiciel (SW-CMM) et d'ingénierie systèmes (SE-CMM) utilisés par les organismes ont créé une certaine confusion dans l'industrie du logiciel. Ces modèles sont redondants et souvent inefficaces dans la pratique. Un organisme pouvait difficilement utiliser les deux modèles concurremment du fait des différences entre les modèles SW et SE.

La solution à cette confusion consiste à gérer ce décalage par la création de l'intégration de modèles de maturité de la capacité (CMM*i*). Cette dernière consiste à rapprocher les incohérences d'architecture, d'approche et de terminologie, ainsi que les autres problèmes de compatibilité entre les modèles SW-CMM, SE-CMM et les modèles associés. Le résultat de cette création est un ensemble de modèles, et d'infrastructure d'appui, désigné par le terme collectif CMM*i*.

Le MMC a été développé par le Software Engineering Institute (SEI) accrédité par la Carnegie Mellon University. Des références au MMC sont disponibles sur le site www.sei.cmu.edu [21].

Annexe C
(informative)

Guide sur l'environnement d'application d'un système

C.1 Compréhension de l'environnement d'application d'un système

Le guide sur l'environnement d'application d'un système présente l'environnement du produit fini d'un point de vue système et lorsque le produit est intégré dans l'exploitation du système. Ce guide permet de fournir les informations pertinentes de l'environnement d'exploitation du système pour le choix de modèles de produits et de matériels robustes et fiables, appropriés à l'application du système. Des critères pertinents relatifs au développement ou au choix de produits matériels sont fournis pour tenir compte de la conception fonctionnelle. Les exemples présentés dans l'environnement d'application s'appliquent aux systèmes terrestres génériques.

La valeur de présentation d'un ensemble complet de critères de calcul pertinents est motivée par les facteurs suivants:

a) l'expérience montre que les modèles ou les acquisitions de produits spécifiques ont souvent ignoré les liens des interfaces humaines, les conditions électromagnétiques, climatiques et mécaniques, ainsi que les autres facteurs d'aptitude à la fonction considérés du point de vue du système pour des applications de produits finis. L'approche présentée ici peut faciliter la conception architecturale du système et l'intégration du ou des produits afin de satisfaire aux exigences du marché mondial;

b) le recueil de données et la correspondance de normes par rapport aux exigences du client peuvent nécessiter un effort important. Ce guide fournit une référence effective et des éléments d'entrée pour des spécifications de conception;

c) la tendance actuelle de développement d'un produit s'éloigne du processus de conception habituel afin de satisfaire à une exigence spécifique du client en raison des contraintes de commercialisation. Ce guide présente un large éventail de segments d'application sur lesquels l'environnement d'utilisation et les besoins du produit peuvent être rationalisés en vue du développement et de l'acquisition d'un produit rentable pour faciliter l'intégration du système;

d) des contrôles de l'environnement et des caractéristiques d'aptitude à la fonction du produit s'appliquent progressivement aux niveaux du système, du sous-système et du produit sous forme de mesures rentables pour élaborer des solutions de conception optimales afin de satisfaire aux demandes évolutives du marché mondial. Ce marché reflète la tendance actuelle d'une collaboration internationale et d'une harmonisation des normes afin de faciliter le développement des systèmes et des produits.

C.2 Processus de définition des exigences environnementales

La Figure C.1 présente une vue d'ensemble du processus de définition des exigences.

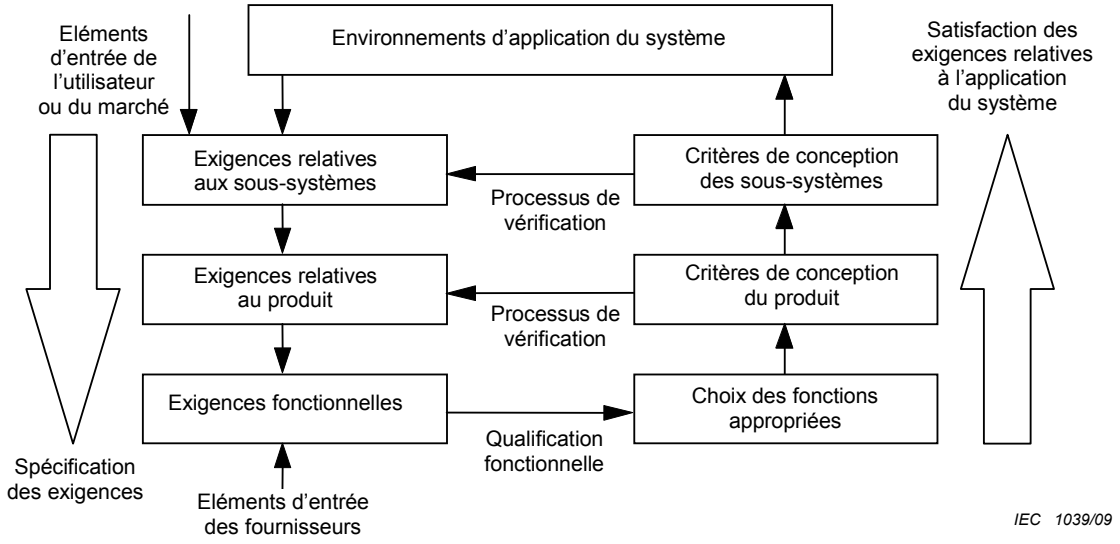

Figure C.1 – Processus de définition des exigences environnementales

La définition des exigences constitue un processus descendant permettant de définir l'environnement du système pour l'intégration prévue des sous-systèmes, produits et applications fonctionnelles. Les conditions environnementales du système sont ensuite traduites en exigences relatives aux produits et fonctions constitutifs. Les besoins de l'utilisateur et les informations du marché servent généralement de guide au développement de la spécification des exigences.

Un processus de vérification parallèle de la conception permet de compléter le processus de définition des exigences. Il s'agit d'un processus ascendant visant à assurer la satisfaction des exigences à chaque étape de la conception prévue, du choix des applications fonctionnelles et cela par le développement du produit, à l'intégration du système. L'objectif consiste à satisfaire ou à surpasser les exigences d'aptitude à la fonction d'application relatives à l'utilisation finale du système.

Les conditions de l'environnement d'utilisation finale du système sont décrites à l'Article C.3. Les exigences relatives à l'environnement d'utilisation applicable aux produits intégrés au système sont identifiées en termes de caractéristiques d'aptitude à la fonction spécifiques. Elles permettent de classer les environnements des produits et d'identifier les expositions environnementales applicables.

C.3 Conditions environnementales d'un système

C.3.1 Classement des conditions environnementales d'un système

La Figure C.2 illustre la cartographie des environnements d'application d'un système aux expositions. Les conditions électromagnétiques, climatiques et mécaniques indiquées, telles qu'exposées à une application système désignée, fournissent l'enveloppe de conception propre à le classement d'un environnement de produit spécifique.

Il convient de noter le lien entre les expositions et les caractéristiques d'aptitude à la fonction associées aux attributs des conceptions de produits (voir la série CEI 60721) [22].

Expositions	Environnements d'application du système							
	Locaux à environnement contrôlé	Locaux du client			Site extérieur		Transport	Stockage
		Industriels	Commerciaux	Résidentiels		Mobile		
Electro-magnétiques	E1	E3	E3	E3	E2	E4		
Climatiques	C1	C3	C2	C2	C4 C5	C4		C6
Mécaniques	M1 M2 M5	M1	M1 M2	M1 M2	M1	M3	M4	

IEC 1040/09

Figure C.2 – Cartographie des environnements d'application du système aux expositions

C.3.2 Conditions électromagnétiques

Elles comprennent les expositions environnementales suivantes:

E1 Locaux à environnement contrôlé (par exemple laboratoires, salles blanches)

E2 Sites extérieurs

E3 Locaux du client

E4 Applications portables et mobiles

C.3.3 Conditions climatiques

Elles comprennent les expositions environnementales suivantes :

C1 A environnement contrôlé (par exemple laboratoires, salles blanches)

C2 A régulation de la température intérieure

C3 Absence de régulation de la température intérieure (par exemple garage non chauffé)

C4 A protection extérieure (par exemple sous abri)

C5 Absence de protection extérieure (par exemple en champ libre)

C6 Stockage

C.3.4 Conditions mécaniques

Elles comprennent les expositions environnementales suivantes :

M1 Fixe

M2 Portable

M3 Mobile

M4 Transport

M5 Séisme

C.4 Caractéristiques de conception influencées par l'environnement d'application du système

Les caractéristiques de conception sont influencées par l'environnement d'application du système. Ces caractéristiques sont intrinsèques aux attributs d'aptitude à la fonction du

système. Elles affectent l'architecture de conception du système, les technologies appliquées dans les fonctions du système et la stratégie de conditionnement pour une aptitude à la fonction de fonctionnement optimale. La corrélation et l'évaluation cartographique des caractéristiques de conception par rapport à l'environnement d'utilisation finale sont essentielles pour le développement d'un environnement d'application du système. Le processus d'évaluation cartographique consiste à identifier les caractéristiques communes et les contraintes du cas le plus défavorable pour une conception de produit appropriée à une application système. L'objectif est de s'assurer de l'intégrité et de la robustesse du produit lorsqu'il est intégré au système pour une utilisation dans des conditions environnementales différentes. La cartographie fournit une approche technique qui vise à tenir compte des options de conception du produit et du choix de technologies alternatives.

Attributs d'aptitude à la fonction du système	*Caractéristiques de conception influencées par l'environnement d'application du système*
• Compatibilité électromagnétique	• Architecture de conception du système • Budget CEM et limites d'émission • Fréquences d'horloge • Normes de blindage et de filtrage
• Effet thermique	• Consommation et distribution d'énergie • Budget thermique et limites de température • Méthodes de refroidissement • Mécanismes de transfert de chaleur
• Qualité	• Processus de qualité • Critères d'acceptation • Contrôle et élimination des non-conformités • Qualification du ou des fournisseurs
• Sûreté de fonctionnement	• Performance de disponibilité et temps d'arrêt/fréquence admissibles • Durée moyenne entre les défaillances • Temps moyen de restauration • Stratégie de logistique de maintenance et d'approvisionnement en pièces de rechange • Durées de vie et périodes sans défaillance
• Compatibilité environnementale	• Processus du cycle de vie environnemental • Conception pour réduction, réutilisation et recyclage • Impact sur l'environnement • Expositions aux risques

C.5 Attributs d'aptitude à la fonction d'un système pour les questions de conception

C.5.1 Généralités

Les informations contenues dans la corrélation et la cartographie des Figures C.2 et C.3 peuvent faciliter la conception d'une fonction système spécifique ou d'un produit destiné à une utilisation dans un environnement d'application d'un système. Les descriptions suivantes des attributs d'aptitude à la fonction spécifiques du système fournissent des informations générales utiles essentielles pour les questions de conception.

C.5.2 Prise en compte de la CEM dans la conception

La compatibilité électromagnétique (CEM) est la capacité d'un produit à fonctionner sans émettre ou sans être affecté par un bruit électromagnétique. L'émission est l'énergie électromagnétique ou le bruit parasite provenant d'une source. Cette émission peut provenir de sources telles qu'une horloge haute fréquence intégrée dans un circuit ou module électronique contenu dans un produit. L'immunité est la capacité d'un produit à résister au bruit électromagnétique. Ce bruit peut être dû au fonctionnement proche de radio-émetteurs et de postes de télévision, ou à des décharges électrostatiques. Les niveaux d'émission sont réglementés dans de nombreux pays pour prévenir toute interférence. Il convient que les conceptions de produits électroniques respectent leurs limites d'émission respectives à des

fins de commercialisation et d'application du produit. Le partitionnement est la technique utilisée pour concevoir un produit de sorte qu'il satisfasse les exigences CEM. La translation des exigences CEM du niveau du système au niveau du produit, ainsi qu'au niveau du module, nécessite un processus de budgétisation CEM. Ceci implique une analyse détaillée des dispositifs utilisés dans le module, de la stratégie de blindage et de la mise en place des composants, du cheminement des câbles et du câblage imprimé. Les contributions de toutes les sources d'émission disponibles dans le module sont utilisées pour déterminer le niveau des marges de conception. Ce niveau constitue la marge de tolérance dans la conception du module susceptible d'avoir une influence sur l'aptitude à la fonction du module dans un produit, lorsqu'il est intégré à un système exposé à l'environnement électromagnétique.

C.5.3 Prise en compte des contraintes thermiques dans la conception

Les exigences thermiques sont fortement influencées par le fonctionnement du système et les expositions environnementales appliquées au produit ou aux modules fonctionnant à l'intérieur du système. La question thermique fondamentale concerne la production et l'évacuation de chaleur afin de permettre une intégrité durable de l'aptitude à la fonction. La production de chaleur est influencée par la fonction de dispositif nécessaire à l'application, la consommation d'énergie et la dissipation de tous les composants dans les limites de l'enveloppe de conception physique du module. La méthode d'évacuation de la chaleur peut être conductrice, convective, et par rayonnement. La convection par air forcé ou la convection naturelle constituent des refroidissements typiques d'un système. L'aptitude à la fonction d'un module à haute densité de composants est sensible aux sources de chaleur internes générées dans le module par les dispositifs utilisés dans la conception de ce même module. La température ambiante de l'environnement de fonctionnement du module ou du milieu environnant affectera également l'aptitude à la fonction du module. Une montée en température anormale due à des sources de chaleur interne non souhaitables ou à un transfert de chaleur externe affectera l'aptitude à la fonction de fiabilité du module. La budgét thermique de la dissipation d'énergie des sources potentielles de production de chaleur peut fournir les informations nécessaires à l'identification, la réduction et l'élimination de la chaleur non désirée générée dans le module. Il convient que la conception thermique prenne en considération la dissipation d'énergie, la montée en température, le taux de refroidissement et les limites de fonctionnement thermique des dispositifs. Il convient de gérer le budget thermique à tous les niveaux hiérarchiques fonctionnels du point de vue du système.

C.5.4 Prise en compte de la qualité dans la conception

La qualité englobe toutes les caractéristiques intrinsèques d'une entité (système, produit, module ou composant) qui concernent sa capacité à satisfaire les besoins exprimés ou implicites. La qualité implique la conformité aux exigences; les critères d'acceptation et les procédures de contrôle sont de ce fait établis pour l'acceptation de la conformité, ceci afin de s'assurer de la conformité continue aux normes établies, les mécanismes appropriés étant par ailleurs intégrés au système ou au processus pour faciliter une amélioration continue. Les processus d'assurance et de contrôle de qualité sont bien établis dans l'industrie. Les méthodes de conception de la qualité étant décrites dans la documentation applicable, les questions relatives à la conception ne seront donc pas détaillées dans la présente norme.

C.5.5 Questions relatives à la conception de la sûreté de fonctionnement

La sûreté de fonctionnement est la capacité intrinsèque d'un système à assurer l'aptitude à la fonction de disponibilité afin de fournir un niveau de service satisfaisant sur demande. La disponibilité est une caractéristique d'aptitude à la fonction dont les facteurs influents consistent en des fonctions d'aptitude à la fonction de fiabilité, maintenabilité et logistique de maintenance. Les questions relatives à la conception de la sûreté de fonctionnement ont été traitées dans les autres articles de la présente partie de la CEI 60300 et ne feront donc pas l'objet d'une description détaillée dans la présente norme.

C.5.6 Prise en compte de la compatibilité environnementale dans la conception

La compatibilité environnementale est essentielle sur le marché actuel. L'impact environnemental du produit et du module lors de leur remplacement ou élimination constitue

une situation préoccupante pour les développeurs et les fabricants de produits. Les demandes typiques de l'utilisateur ou du client se présentent sous la forme d'un contrat de reprise par lequel le prestataire ou le fournisseur du produit est tenu de reprendre le produit retiré préalablement à la mise en place d'un nouveau produit destiné à être mis en service. Les contrats de rachat sont également pratique courante dans les opérations commerciales actuelles dans lesquelles la quantité fournie de pièces de rechange conservées ou achetées par un utilisateur ou un client n'est pas utilisée au terme d'une période convenue, le prestataire ou le fournisseur devant alors racheter les pièces de rechange. Il convient, dans la conception et la fabrication des produits et modules, de tenir compte de la réutilisation des pièces destinées à être éliminées. Le recyclage des produits dérivés dans le processus de fabrication afin de réduire au minimum les déchets, constitue un autre facteur dont les études de l'impact environnemental doivent tenir compte. Il convient également de prendre en considération la réduction des émissions et des déchets générés par le processus du cycle de vie environnemental du produit.

Annexe D
(informative)

Listes de contrôle applicables à l'ingénierie de la sûreté de fonctionnement d'un système

D.1 Listes de contrôle applicables à la gestion de projet de sûreté de fonctionnement d'un système

D.1.1 Généralités

Les listes de contrôle portant sur la sûreté de fonctionnement d'un système sont applicables au cycle de vie du système aux principaux points de décision, afin de faciliter les revues de direction de projet. Ces listes de contrôle identifient les questions critiques qui doivent être traitées afin de valider l'exécution accomplie des activités clés de sûreté de fonctionnement du système de chaque phase du projet. Il est recommandé d'effectuer des revues de projet de manière régulière entre les principaux points de décision pour une exécution progressive des tâches de réalisation de la sûreté de fonctionnement. Ceci permet de s'assurer de l'évaluation et de la résolution de tous les problèmes critiques. Les enregistrements des revues peuvent servir de preuves tangibles venant à l'appui du processus d'assurance de la sûreté de fonctionnement du projet. Les listes de contrôle reflètent les processus de transfert des responsabilités du projet et de transition de la propriété du système au cours de son cycle de vie complet. Ces listes de contrôle peuvent être utilisées par le fournisseur et le client pour l'adaptation du projet en vue de répondre à leurs besoins d'application spécifiques.

D.1.2 Liste de contrôle portant sur l'identification du marché

a) La nature et les applications de l'aptitude à la fonction de sûreté de fonctionnement du système sont définies et l'intention de remplacement d'un système existant ou d'amélioration de son aptitude à la fonction est connue.

b) Le calendrier d'introduction d'un nouveau système avec des caractéristiques de sûreté de fonctionnement spécifiques a été établi.

c) Les environnements d'exploitation du système, les facteurs influents spécifiques de la sûreté de fonctionnement et les questions réglementaires associées ont été identifiés.

d) Les capacités techniques applicables à l'ingénierie de la sûreté de fonctionnement pour le développement du système ont été identifiées.

e) Les ressources nécessaires au soutien du projet de sûreté de fonctionnement ont été identifiées et estimées.

f) Les investissements en capital et l'acquisition d'outils de sûreté de fonctionnement et de mécanismes d'activation spécifiques pour le développement du système ont été identifiés.

g) Les clients potentiels et les concurrents probables intéressés par le développement du système avec un objectif d'aptitude à la fonction de sûreté de fonctionnement ont été identifiés.

h) Les exigences attendues d'aptitude à la fonction du système et les caractéristiques spéciales de ce dernier sont définies, y compris l'identification des questions de sûreté de fonctionnement uniques et des attentes des clients tout aussi uniques, par exemple robustesse du logiciel.

i) Les scénarios d'exploitation de la sûreté de fonctionnement du système, l'interopérabilité avec d'autres systèmes, la préférence de conception technologique et les problèmes héréditaires ont été identifiés.

j) Les exigences relatives à la maintenance et au support logistique du système en vue d'un fonctionnement fiable ont été identifiées.

k) Une stratégie de commercialisation et un plan d'influence de la sûreté de fonctionnement dans l'aptitude à la fonction du système ont été établis.

l) Une équipe de projet chargée d'émettre des propositions et responsable du travail technique, et spécialisée dans le soutien à la sûreté de fonctionnement, a été créée.

m) La décision oui/non de mise en place du développement du système peut être justifiée par un objectif stratégique de l'aptitude à la fonction de sûreté de fonctionnement.

D.1.3 Liste de contrôle applicable au développement d'un système

a) Un plan de développement de projet pour l'exécution des tâches de sûreté de fonctionnement a été élaboré.

b) Les exigences système sont analysées et les caractéristiques de sûreté de fonctionnement sont évaluées.

c) La stratégie de conception, le choix de la technologie et les activités de sûreté de fonctionnement relatives au développement du système ont été déterminés.

d) Un plan qualité et un processus d'assurance de la sûreté de fonctionnement sont établis et mis en oeuvre.

e) Un processus de standardisation et des règles de conception de la sûreté de fonctionnement ont été mis en oeuvre.

f) L'architecture et la configuration physique du système visant à satisfaire aux exigences d'aptitude à la fonction du système ont été déterminées.

g) Un plan d'intégration du système et des sous-systèmes a été établi.

h) Le partitionnement du matériel, les interfaces logicielles et la conception de l'ergonomie visant à satisfaire aux exigences d'aptitude à la fonction du système ont été déterminés.

i) Les exigences relatives à l'aptitude à la fonction de sûreté de fonctionnement du système et les conditions d'utilisation sont spécifiées.

j) La stratégie d'essai du système, la couverture d'essai et l'évaluation fonctionnelle sont réalisées.

k) Les fonctions système destinées à répondre aux besoins d'aptitude à la fonction de sûreté de fonctionnement ont été évaluées.

l) Les conceptions de système et la sûreté de fonctionnement des fonctions système ont été validées.

m) Les travaux externalisés, les partenariats de développement et les services des fournisseurs préférentiels sont coordonnés et réalisés.

n) Les secondes sources ont été identifiées et coordonnées pour venir à l'appui des exigences de diversification du projet.

o) Les systèmes d'activation et la stratégie de soutien applicables sont mis en place pour réaliser la sûreté de fonctionnement du système.

p) La capacité de fabrication en vue de la réalisation du produit et les questions liées à la sûreté de fonctionnement associées sont déterminées.

q) Les documents de conception, instructions de formation et procédures d'essai sont achevés.

r) L'exploitation du système et le plan de soutien ont été établis.

s) Le plan de support logistique est établi.

t) La politique de maintenance et les niveaux de réparation de l'ensemble de plus bas niveau sont établis.

u) La décision de la réalisation du produit peut être justifiée.

D.1.4 Liste de contrôle applicable à la réalisation du produit

a) Le plan de mise en oeuvre du produit a été établi.

b) Les tâches d'assurance de la qualité et de la sûreté de fonctionnement du produit sont exécutées.

c) La coordination et le contrôle des produits du ou des fournisseurs pour l'évaluation de la sûreté de fonctionnement sont effectifs.

d) Les produits du commerce devant être intégrés aux fonctions du système ont été évalués.

e) L'évaluation des produits et sous-systèmes pour la vérification de la sûreté de fonctionnement est effectuée.

f) L'essai du système et des sous-systèmes, et l'évaluation de l'aptitude à la fonction ont été effectués.

g) L'intégration du système et l'incorporation des sous-systèmes sont effectives.

h) Le plan de gel de la conception et de contrôle de la configuration est établi.

i) Les exigences d'aptitude à la fonction du système ont été validées.

j) La stratégie d'acceptation du système a été établie.

k) L'analyse du compte rendu des défaillances et le système d'actions correctives ont été établis et mis en oeuvre.

l) La décision de la mise en place du transfert du système et de l'acceptation du client peut être justifiée.

D.1.5 Liste de contrôle applicable à l'acceptation du système

a) Un plan d'acceptation du système est établi avec consultation du client.

b) Un plan de démonstration de l'aptitude à la fonction de sûreté de fonctionnement du système et la période de garantie applicable ont été établis et acceptés par le client.

c) Le système de compte rendu des incidents est mis en oeuvre et les critères relatifs audit compte rendu sont établis.

d) L'exploitation du système et son plan de soutien sont établis afin de réaliser l'aptitude à la fonction de sûreté de fonctionnement.

e) La formation des opérateurs et des spécialistes de la maintenance du système est en place et les stagiaires sont certifiés, le cas échéant.

f) Le soutien au système en vue de la participation d'une tierce partie telle que les services d'étalonnage, a été identifié, coordonné et approuvé.

g) Des procédures de mise à disposition du système sont établies pour le transfert dudit système au client en vue de son exploitation.

h) Le transfert juridique de la propriété du système au client dans le cadre du contrat est achevé.

i) La décision de la mise en place de l'exploitation du système peut être justifiée.

D.1.6 Liste de contrôle applicable à l'exploitation

a) L'exploitation du système et le plan de soutien sont mis en oeuvre.

b) Les procédures de surveillance et de contrôle de l'aptitude à la fonction du système sont appliquées.

c) Le système de compte rendu des incidents est mis en oeuvre pour assurer la traçabilité de l'aptitude à la fonction de sûreté de fonctionnement, de la pérennité du service, des activités de logistique de maintenance et des actions correctives et préventives.

d) La traçabilité des actions de maintenance est assurée.

e) Les procédures de modification de conception et le plan de contrôle de la configuration sont activés.

f) Le plan de support logistique est mis en oeuvre.

g) L'analyse opérationnelle du système est effectuée.

h) Les anomalies de fonctionnement et les domaines d'amélioration sont identifiés.

i) La tendance d'aptitude à la fonction de la sûreté de fonctionnement du système est établie.

j) Les enquêtes de satisfaction de l'utilisateur final sont effectuées.

k) La décision du maintien de l'exploitation du système existant peut être justifiée.

D.1.7 Liste de contrôle applicable à l'amélioration

a) Les besoins du marché en termes d'amélioration du système ont été établis.

b) L'appréciation des risques et la détermination de la ou des plus-values sont effectués afin de justifier l'effort d'amélioration.

c) L'impact sur l'aptitude à la fonction de sûreté de fonctionnement dû aux modifications d'amélioration est vérifié.

d) L'impact sur l'environnement et les autres acteurs influents, y compris les questions réglementaires, de sécurité et de sûreté concernant les modifications d'amélioration sont examinés et validés.

e) Le calendrier et le barème des coûts propres aux travaux d'amélioration sont estimés.

f) Les ressources nécessaires aux travaux d'amélioration sont déterminées.

g) La décision de l'amélioration du système peut être justifiée.

D.1.8 Liste de contrôle applicable au retrait

a) La nécessité et le calendrier du retrait du système ont été établis.

b) Les causes de retrait telles que l'obsolescence technique ou les contraintes économiques et réglementaires ont été déterminées.

c) Le système de remplacement destiné à fournir un service continu du système est déterminé.

d) Les conséquences sociales de la fin du service sont évaluées.

e) La décision du retrait du système peut être justifiée.

f) Le plan de transition entre l'ancien et le nouveau système a été établi et garanti.

D.2 Listes de contrôle pour les applications de conception des éléments matériels et logiciels, et de l'ergonomie

D.2.1 Généralités

Les listes de contrôle pour les applications de conception des éléments matériels et logiciels, et de l'ergonomie peuvent être utilisées pour l'ingénierie de la sûreté de fonctionnement des systèmes. Elles facilitent le processus de conception des produits et de développement des systèmes. Le choix d'éléments matériels et logiciels combinés pour la conception des fonctions système offre souvent la possibilité de parvenir à des compromis afin de faciliter les interactions humaines. L'ergonomie a un rôle important dans la maximisation de l'aptitude à la fonction de sûreté de fonctionnement d'un système. Il convient que les conceptions de systèmes tiennent compte des listes de contrôle complémentaires pour des applications de conception optimales.

D.2.2 Listes de contrôle applicables à la conception matérielle d'un système

a) Les exigences matérielles du système ont été établies.

b) Les éléments matériels choisis pour la conception des fonctions du système ont été identifiés.

c) L'historique de la technologie et de la fiabilité matérielles est connu et a fait l'objet d'une évaluation.

d) La configuration matérielle du système est déterminée.

e) Les spécifications de conception matérielle ont été établies.

f) Le concept de conditionnement matériel et le programme de modularisation ont été déterminés.

g) Le budget thermique d'un profil d'exploitation a été analysé pour déterminer les points chauds et les programmes de refroidissement eu égard aux conditions ambiantes du module et à l'environnement d'exploitation du système.

h) Le budget de compatibilité électromagnétique d'un profil opérationnel a été établi afin d'identifier la portée des exigences en matière de blindage, filtrage, partitionnement et installation.

i) L'interface et la connectivité du module fonctionnel ont été établies.

j) Le plan d'alimentation et de fourniture en énergie et la normalisation de la tension pour le système ont été déterminés.

k) La modélisation de l'aptitude à la fonction de fiabilité du système a été évaluée pour les options de redondance et de conception.

l) L'analyse fonctionnelle et la répartition de la fiabilité pour chaque fonction du système ont été déterminées.

m) Le plan d'intégration du système et des sous-systèmes a été élaboré.

n) La maintenabilité et la testabilité du système ont été analysées et la couverture d'essai a été déterminée.

o) Une capacité d'essai intégrée et des caractéristiques d'autocontrôle, le cas échéant, sont intégrées à la conception du module afin de faciliter l'identification et la localisation des pannes.

p) Les conceptions tolérantes aux pannes et les conceptions qui évitent les pannes sont intégrées aux fonctions critiques du système.

q) Le concept de maintenance du système et les niveaux de maintenance ont été établis.

r) L'approvisionnement en pièces de rechange des ensembles de plus bas niveau a été déterminé.

s) Le délai d'achèvement du réapprovisionnement en pièces de rechange a été déterminé.

t) Une simulation du système, lorsqu'elle est nécessaire à la démonstration de l'aptitude à la fonction de disponibilité, a été effectuée.

u) Les cas d'essai applicables au système pour la détection, la localisation et la réparation des pannes, ainsi que le temps de restauration ont été vérifiés.

v) Les produits matériels du commerce sont évalués en vue de leur intégration aux fonctions du système.

w) Des plans et des procédures d'essai du système, des sous-systèmes et du module fonctionnel sont élaborés.

x) La documentation de conception est complète pour la fabrication de produits et d'ensembles matériels.

D.2.3 Listes de contrôle applicables à la conception logicielle d'un système

a) Les exigences logicielles du système ont été établies.

b) L'architecture du système est déterminée.

c) Des normes logicielles sont appliquées pour la conception et le développement du ou des logiciels.

d) Des outils et services logiciels sont mis à disposition pour venir à l'appui du développement logiciel.

e) Le partitionnement logiciel et la répartition des fonctions ont été établis.

f) L'interface et le protocole des fonctions logicielles ont été établis.

g) Les spécifications de conception logicielle ont été établies.

h) Les calendriers de livraison du ou des logiciels et les plans de conception préliminaire et détaillée ont été établis.

i) Les fonctions du module logiciel sont soumises à essai et vérifiées afin de satisfaire à la spécification de conception.

j) Les produits logiciels du commerce sont évalués en vue de leur intégration aux fonctions du système.

k) Les critères d'acceptation du produit et du sous-système logiciels ont été établis.

l) Un essai de réception a été effectué pour déterminer si le produit et le sous-système logiciels satisfont aux critères de réception.

m) L'essai et l'évaluation du système logiciel sont validés pour satisfaire à la spécification d'aptitude à la fonction.

n) Les outils logiciels dédiés à l'exploitation et à la logistique de maintenance du système ont été identifiés.

o) La documentation de conception est complète pour les reproductions de produits logiciels.

D.2.4 Listes de contrôle applicables à la conception de l'ergonomie

a) L'objectif de la conception de l'ergonomie est défini.

b) Le plan relatif à l'ergonomie a été établi pour les applications de conception.

c) Les études de conception de l'ergonomie sont établis pour la convivialité, l'évaluation des qualités opérationnelles, la répartition des fonctions et le niveau d'automatisation, la reconnaissance des capacités humaines et les limites propres à l'exploitation et à la maintenance du système.

d) Les interfaces homme-machine ont été évaluées en termes de simplicité de la conception, fonctions identiques pour la cohérence de l'exploitation, compatibilité avec les autres systèmes existants de ce type et la sensibilisation de l'utilisateur aux affichages et communications d'informations.

e) Les interfaces homme-machine ont été évaluées en termes de conception de l'écran afin de faciliter une interaction conviviale, les contrôles sur les entrées et les mécanismes de commande, l'entrée et la mise en forme des données, l'information et l'‘affichage graphiques, les fonctions d'actualisation et d'interruption, les fonctions de gestion de fichiers, les fenêtres de message tuteurs et les services d'aide. Il est important que les messages système soient corrects, complets, faciles à comprendre et non trompeurs.

f) Les conceptions de systèmes comportent des fonctionnalités à sécurité intégrée, de résistance et de tolérance aux pannes, de facilité de traitement des situations critiques et des urgences, et de facilité d'utilisation des fonctions automatisées d'activation et de désactivation, des programmes de diagnostic simples pour la gestion des pannes et une fonction de facilité de navigation par le biais d'un mode dégradé d'exploitation du système en vue d'une action corrective.

g) Les conceptions de systèmes intègrent une facilité d'accès pour le remplacement des unités démontables et des ensembles de plus bas niveau, un étiquetage adéquat dédié à un avertissement de sécurité et une exploitation en toute sécurité, et un accès aux manuels techniques et aux documents d'aide pour les instructions de maintenance, d'installation et de réparation.

h) Les conceptions de systèmes pour l'exploitation déterminent le niveau d'automatisation, ainsi que les compétences et les besoins en formation des opérateurs et des spécialistes de la maintenance.

i) La documentation de conception est complète pour l'élaboration de manuels d'exploitation du système et de maintenance.

D.2.5 Liste de contrôle applicable à la conception de la compatibilité avec l'environnement

a) L'objectif de conception environnementale est défini.

b) Les exigences de conception environnementale ont été établies pour les applications de conception.

c) Les normes et règlements applicables à l'environnement ont été examinés et intégrés aux concepts d'étude environnementale et au plan de mise en oeuvre qui vise à réduire le nombre d'ensembles et d'éléments matériels, et à leur réutilisation ou leur recyclage.

d) Le nombre d'éléments utilisés dans un ensemble a été minimisé afin de réduire le temps de montage et de démontage, pour une amélioration de l'efficacité du processus de recyclage.

e) La conception modulaire applicable à l'unité remplaçable de plus bas niveau à une seule fonction a été prise en compte afin de permettre des options de service, une amélioration fonctionnelle, et le recyclage des éléments.

f) Le regroupement des éléments non recyclés en un lieu donné a été pris en compte afin de faciliter le démontage et le retrait rapide pour élimination.

g) La mise en place d'un élément de valeur en un lieu donné pour une facilité d'accès a été prise en compte pour permettre un démontage partiel en vue d'un retour et d'une récupération optimum.

h) La conception des éléments pour une robustesse et une stabilité effectives a été prise en compte afin d'améliorer le démontage manuel.

i) L'évitement de chevilles métalliques intégrées et le renfort des pièces métalliques dans un ensemble ont été pris en compte pour améliorer la séparation et le recyclage des éléments plastiques.

j) La mise en évidence des points d'accès et d'interruption dans une séquence logique a été prise en compte afin d'améliorer la formation du service de démontage et de maintenance.

k) Mise hors tension ou état de veille dans toute la mesure du possible afin d'économiser l'énergie et de réduire la pollution.

l) Le nombre de fixations a été minimisé pour réduire les temps de montage et de démontage.

m) La normalisation de l'utilisation des outils de montage et de démontage a été prise en compte afin de réduire le coût et le temps de disponibilité de l'outillage.

n) Une facilité d'accès aux points de fixation a été prise en compte afin d'améliorer la maintenabilité et l'entretien.

o) L'utilisation de cliquets, le cas échéant et lorsque la pratique le permet, a été prise en compte afin d'améliorer le démontage et la facilité de retrait des éléments.

p) L'utilisation de matériels de fixation compatibles avec les éléments de connexion a été prise en compte afin d'améliorer le recyclage des pièces constitutives.

q) La possibilité d'une désolidarisation aisée des éléments incompatibles lorsqu'ils sont reliés entre eux a été prise en compte afin d'améliorer ladite désolidarisation en vue de leur recyclage.

r) L'utilisation d'adhésifs n'est généralement pas recommandée en raison de la difficulté de démontage des éléments, plus particulièrement lorsque les deux matériaux reliés entre eux ne peuvent pas être recyclés. Par ailleurs, y compris dans le cas de matériaux compatibles, les adhésifs peuvent contaminer les matériaux et rendre de ce fait tout recyclage difficile.

s) Il convient de minimiser le nombre et la longueur des fils et câbles d'interconnexion afin de réduire les temps de montage et de démontage et d'éviter toute interférence électromagnétique potentielle.

t) Il convient d'envisager la conception de raccords frangibles pour les éléments jetables afin d'améliorer leur démontage.

D.3 Listes de contrôle pour l'utilisation de produits du commerce (COTS) dans les systèmes

D.3.1 Généralités

Les produits du commerce (COTS) sont largement utilisés dans les applications système du fait de l'économie d'ingénierie et des contraintes de délai de mise sur le marché prises en compte dans le développement des systèmes. Les produits du commerce sont généralement tributaires du marché et leur aptitude à l'emploi a été démontrée par un large spectre

d'applications commerciales. Un produit du commerce, présenté sous une forme matérielle ou logicielle, ou dans diverses combinaisons, fournit un progiciel prêt à l'usage en vue d'un achat commercial. Les exemples typiques de produits du commerce incluent, sans toutefois s'y limiter, les blocs d'alimentation, logiciels d'applications commerciales et appareils de commande électroniques programmables. L'acheteur d'un produit du commerce n'exerce aucune influence sur les caractéristiques du produit et ses spécifications opérationnelles. Le choix de produits du commerce appropriés destinés à être intégrés au système est tout particulièrement important dans l'ingénierie de la sûreté de fonctionnement du système concerné. Certains risques sont associés au choix d'un produit du commerce et à la validation de son aptitude à l'emploi pour une application système spécifique, indépendamment des revendications à l'égard du produit du commerce et de sa conformité avérée. Ceci est dû à la au fait que l'acheteur ne peut influer sur les fonctions du produit et ses caractéristiques d'aptitude à la fonction. L'utilisation d'un produit du commerce pour l'application d'un système critique nécessiterait un effort d'évaluation supplémentaire pour acquérir une certitude. Les listes de contrôle sont destinées à faciliter l'identification des exigences, l'évaluation de l'aptitude à la fonction et l'assurance que le produit du commerce peut être effectivement intégré à l'application système.

D.3.2 Listes de contrôle applicables à l'identification des exigences

a) Le produit du commerce est mis en vente avec une identification unique d'achat. Les informations sur le produit sont par ailleurs suffisantes et la description fonctionnelle du produit permet d'évaluer son aptitude à l'emploi pour l'application prévue.

b) Le choix du produit peut être effectué parmi plusieurs fournisseurs de produits similaires présents sur le marché.

c) L'identification du produit est désignée par le nom, le modèle ou la version, ainsi que par le numéro de série ou la date apparaissant sur l'étiquette apposée par le fabricant sur le produit.

d) La description du produit contient la spécification de ce dernier, les instructions pour son installation et son utilisation, les procédures applicables aux connexions du produit et les exigences d'interface relatives aux applications, ainsi que la nécessité et l'étendue des services de maintenance et de soutien du produit.

e) Des étiquettes d'avertissement et des procédures applicables aux opérations relatives à la sécurité sont prévues, le cas échéant.

f) Des informations sur la garantie du produit sont fournies.

g) Les informations sur la fiabilité et la maintenabilité du produit, l'historique d'aptitude à la fonction et les données d'essai complémentaires peuvent être vérifiés.

h) Une déclaration d'attestation de la qualité du produit est fournie.

D.3.3 Listes de contrôle applicables à l'évaluation des enregistrements d'aptitude à la fonction documentés

a) Les enregistrements d'aptitude à la fonction du produit, contenant des documents pertinents destinés à valider la conformité à la spécification du produit, peuvent être vérifiés.

b) Les documents pertinents incluant le plan d'essai, les modes opératoires, l'environnement et les conditions d'essai, ainsi que les enregistrements d'essai, servent à démontrer la conformité du produit à la spécification.

c) Les cas d'essai conçus pour évaluer les conditions de tolérance aux pannes, le cas échéant, par rapport aux revendications à l'égard du produit, peuvent être vérifiés.

D.3.4 Listes de contrôle pour l'assurance du produit

a) Les informations et les enregistrements relatifs à la qualité du produit peuvent être vérifiés.

b) Les données d'évaluation de la conformité du produit peuvent être vérifiées.

c) Les données d'exploitation du produit sont disponibles pour venir à l'appui des revendications à l'égard de l'aptitude à la fonction de fiabilité.

d) Les taux de retour du produit et les défaillances les plus fréquentes peuvent être vérifiés.

e) Les dossiers de maintenance du produit peuvent être vérifiés.

f) L'évaluation des risques liés au produit et l'évaluation des fonctionnalités de ce dernier et des attributs de processus associés sont effectuées pour les applications critiques du système. Une évaluation spécifique comprend, sans toutefois s'y limiter, la détection des pannes, les besoins de redondance et la détermination du niveau d'intégrité du produit du commerce approprié à l'exploitation d'un système critique. Le niveau d'intégrité constitue la dénotation d'une plage de valeurs de la propriété du produit, nécessaire au maintien des risques, auxquels est exposé le système, dans des limites tolérables. La méthodologie qui permet de déterminer le niveau d'intégrité est décrite dans l'ISO/CEI 15026 [23].

Bibliographie

[1] CEI 61069-1 :1991, *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 1: Considérations générales et méthodologie*

[2] CEI 62347, *Lignes directrices pour les spécifications de sûreté de fonctionnement des systèmes*

[3] ISO/CEI 15288, *Ingénierie des systèmes et du logiciel – Processus de cycle de vie du système*

[4] ISO/CEI TR 15271, *Technologies de l'information – Guide pour l'ISO/CEI 12207 (Processus du cycle de vie du logiciel)*

[5] ISO/CEI 12207, *Ingénierie des systèmes et du logiciel – Processus du cycle de vie du logiciel*

[6] ISO/CEI 15939, *Ingénierie des systèmes et du logiciel – Processus de mesure*

[7] CEI 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*

[8] CEI 60300-3-9, *Gestion de la sûreté de fonctionnement – Partie 3: Guide d'application - Section 9: Analyse du risque des systèmes technologiques*

[9] CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

[10] CEI 61508-1, Sécurité fonctionnelle des systèmes *électriques/ électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

[11] DEF STAN 00-42, Part 3. *Reliability and Maintainability Assurance Guide – Reliability and Maintainability Case*

[12] CEI 61014, *Programmes de croissance de fiabilité*

[13] CEI 61164, *Croissance de la fiabilité – Tests et méthodes d'estimation statistiques*

[14] ISO 10007, *Systèmes de management de la qualité – Lignes directrices pour le management de configuration*

[15] CEI 60300-3-10*, Gestion de la sûreté de fonctionnement – Partie 3-10: Guide d'application - Maintenabilité*

[16] CEI 60300-3-11, *Gestion de la sûreté de fonctionnement – Partie 3-11: Guide d'application - Maintenance basée sur la fiabilité*

[17] CEI 60300-3-12, *Gestion de la sûreté de fonctionnement – Partie 3-12: Guide d'application - Soutien logistique intégré*

[18] IEEE Std 1175.1, *IEEE guide for CASE tool interconnections – Classification and description*

[19] ISO/CEI 14102, *Technologies de l'information – Lignes directrices pour l'évaluation et la sélection d'outils CASE*

[20] ISO/CEI 15940, *Technologies de l'information – Services d'environnement en ingénierie du logiciel*

[21] www.sei.cmu.edu.

[22] CEI 60721 (toutes les parties), *Classification des conditions d'environnement*

[23] ISO/CEI 15026: *Technologies de l'information – Niveaux d'intégrité du système et du logiciel*

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

CEI 60812, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

CEI 61025, *Analyse par arbre de panne (AAP)*

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

CEI 61508-7, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

CEI 61709, *Composants électroniques – Fiabilité – Conditions de référence pour les taux de défaillance et modèles d'influence des contraintes pour la conversion*

CEI 61713, *Sûreté de fonctionnement des logiciels pendant leurs processus de cycle de vie – Guide d'application*

CEI 61882, *Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application*

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

CEI 62308, *Fiabilité de l'équipement – Méthodes d'évaluation de la fiabilité*

IEC PAS 62508, *Guidance on human factors engineering for system dependability life cycle applications* (disponible uniquement en anglais)

ISO 13407, *Processus de conception centrée sur l'opérateur humain pour les systèmes interactifs*

ISO/TR 18529, *Ergonomie – Ergonomie de l'interaction homme/système – Descriptions des processus cycle de vie centrées sur l'opérateur humain*

ITU-T Recommendation E.800, *Terms and definitions related to the quality of service and network performance including dependability* (disponible uniquement en anglais)

QFD Institute, *The official source for Quality Function Deployment,* http://www.qfdi.org

Références pour l'analyse fonctionnelle et la modélisation:

EN 1325-1, *Vocabulaire du management de la valeur, de l'analyse de la valeur et de l'analyse fonctionnelle – Partie 1: Analyse de la valeur et analyse fonctionnelle*

EN 12973, *Management par la valeur*

EN 14514, *Ingénierie spatiale – Analyse fonctionnelle*

NF X 50-153, *Analyse de la valeur – Recommandations pour sa mise en oeuvre*

CEI/TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment électroniques* (disponible uniquement en anglais)[2]

Federal Information Processing Standards (FIPS) Publication 183: *Integration definition for function modeling (IDEF0)* US National Institute of Standards and Technology

The Delphi method: *Techniques and applications*, edited by H. A. Linstone and M. Turoff

_____

[2] *Manuel des données de fiabilité – Modèle universel de prévision de la fiabilité des composants, cartes de circuits imprimés et matériels*

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