IEC 60987

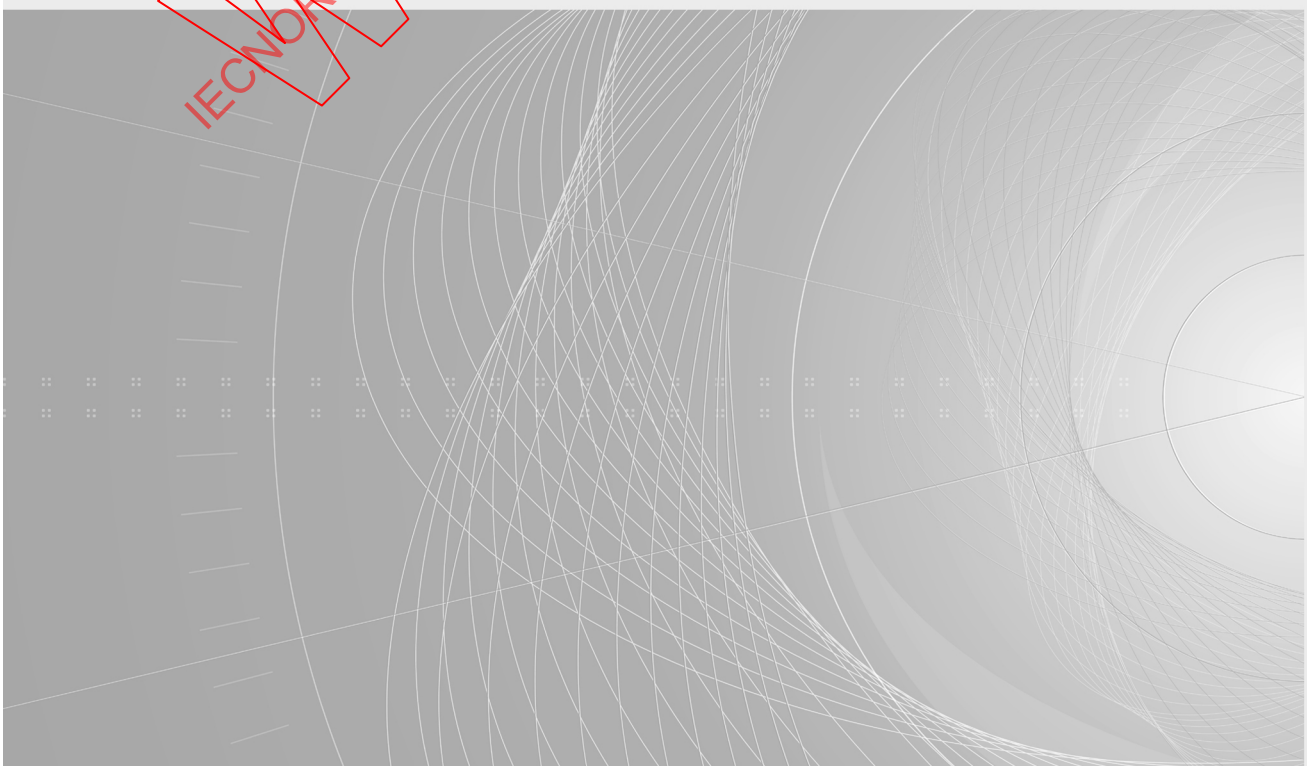
Edition 2.0 2007-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés



IEC 60987:2007

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 It also gives information on projects, withdrawn and replaced publications.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 60987

Edition 2.0 2007-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX V

ICS 27.120.20

ISBN 2-8318-9285-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – HARDWARE DESIGN REQUIREMENTS FOR COMPUTER-BASED SYSTEMS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC 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 shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60987 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1989. This edition includes the following significant technical changes with respect to the previous edition:

- account has been taken of the fact that computer design engineering techniques have advanced significantly in the intervening years;
- update of the format to align with the current IEC/ISO directives on the style of standards;
- alignment of the standard with the new revisions of IAEA documents NS-R-1 and NS-G-1.3, which includes as far as possible an adaptation of the definitions;

- replacement, as far as possible, of the requirements associated with standards published since the first edition, especially IEC 61513, IEC 60880, edition 2, and IEC 62138;
- review of the existing requirements and updating of the terminology and definitions.

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

FDIS	Report on voting
45A/662/FDIS	45A/666/RVD

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

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

The committee has decided that the contents of this publication will remain unchanged until the 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

a) Technical background, main issues and organization of the standard

The basic principles for the design of nuclear instrumentation, as specifically applied to the safety systems of nuclear power plants, were first interpreted in nuclear standards with reference to hardwired systems in IAEA Safety Guide 50-SG-D3 which has been superseded by IAEA Guide NS-G-1.3.

IEC 60987 was first issued in 1989 to cover the hardware aspects of digital systems design for systems important to safety, i.e. safety systems and safety-related systems.

Although many of the requirements within the original issue continue to be relevant, there were significant factors which justified the development of this revised edition of IEC 60987, in particular:

– a new standard has been produced which addresses in detail the general requirements for nuclear systems important to safety (IEC 61513);
– the use of pre-developed system platforms, rather than bespoke developments, has increased significantly.

b) Situation of the current standard in the structure of the IEC SC 45A standard series

The first-level IEC SC 45A standard for computer-based systems important to safety in nuclear power plants (NPPs) is IEC 61513. IEC 60987 is a second-level IEC SC 45A standard which addresses the generic issue of hardware design of computerized systems.

IEC 60880 and IEC 62138 are second-level standards which together cover the software aspects of computer-based systems used to perform functions important to safety in NPPs. IEC 60880 and IEC 62138 make direct reference to IEC 60987 for hardware design.

The requirements of IEC 60780 for equipment qualification are referenced within IEC 60987. For modules to be used in the design of a specific system important to safety, relevant and auditable operating experience from nuclear or other applications as described in IEC 60780, in combination with the application of rigorous quality assurance programmes, may be an acceptable method of qualification.

For more details on the structure of the SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of the standard

It is important to note that this standard establishes no additional functional requirements for Class 1 or Class 2 systems (see IEC 61513 for system classification requirements).

Aspects for which special recommendations have been produced (so as to assure the production of highly reliable systems), are:

– a general approach to computing hardware development;
– a general approach to hardware verification and to the hardware aspects of computer system validation.

It is recognized that computer technology is continuing to develop and that it is not possible for a standard such as this to include references to all modern design technologies and techniques. To ensure that the standard will continue to be relevant in future years the emphasis has been placed on issues of principle, rather than specific hardware design technologies. If new design techniques are developed then it should be possible to assess the suitability of such techniques by adapting and applying the design principles contained within this standard.

The scope of this standard covers digital systems hardware for Class 1 and Class 2 systems. This includes multiprocessor distributed systems and single processor systems; it covers the assessment and use of pre-developed items, for example, commercial off-the-shelf items (COTS), and the development of new hardware.

d) Description of the structure of the SC 45A standard series and relationships with other IEC, IAEA and ISO documents

The top-level document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

IEC 61513 refers direct to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common-cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced direct at this second level should be considered together with IEC 61513 as a consistent document set.

At a third level, IEC SC 45A standards not referenced direct by IEC 61513 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC 45A standard series, corresponds to technical reports which are not normative documents.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework and provides an interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. Compliance with IEC 61513 will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In this framework, IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 refers to ISO 9001 as well as to IAEA 50-C-QA (now replaced by IAEA 50-C/SG-Q) for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA Code on the safety of NPPs and in the IAEA safety series, in particular the requirements of NS-R-1, establishing safety requirements related to the design of NPPs, and Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in NPPs. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – HARDWARE DESIGN REQUIREMENTS FOR COMPUTER-BASED SYSTEMS

1 Scope

1.1 General

This International Standard is applicable to NPP computer-system hardware for systems of Class 1 and 2 (as defined by IEC 61513).

The structure of this standard has not changed significantly from the original 1989 issue; however, some issues are now covered by standards which have been issued in the interim (for example, IEC 61513 for system architecture design) and references to new standards have been provided where applicable. The text of the standard has also been modified to reflect developments in computer system hardware design, the use of pre-developed (for example, COTS) hardware and changes in terminology.

Computer hardware facilities used for software loading and checking are not considered to form an intrinsic part of a system important to safety and, as such, are outside the scope of this standard.

NOTE 1 Class 3 computer-system hardware is not addressed by this standard, and it is recommended that such systems should be developed to commercial grade standards.

NOTE 2 In 2006 the development of a new standard to address hardware requirements for "very complex" hardware was discussed within IEC SC 45A. If such a standard is developed then that standard would be used for the development of "very complex" hardware in preference to IEC 60987.

1.2 Use of this standard for pre-developed (for example, COTS) hardware assessment

Although the primary aim of this standard is to address aspects of new hardware development, the processes defined within this standard may also be used to guide the assessment and use of pre-developed hardware, such as COTS hardware. Guidance has been provided in the text concerning the interpretation of the requirements of this standard when used for the assessment of such components. In particular, the quality assurance requirements of 4.3, concerning configuration control, apply.

Pre-developed components may contain firmware (as defined in 3.8), and, where firmware software is deeply imbedded, and effectively "transparent" to the user, then IEC 60987 should be used to guide the assessment process for such components. An example of where this approach is considered appropriate is in the assessment of modern processors which contain a microcode. Such a code is generally an integral part of the "hardware", and it is therefore appropriate for the processor (including the microcode) to be assessed as an integrated hardware component using this standard.

Software which is not firmware, as described above, should be developed or assessed according to the requirements of the relevant software standard (for example, IEC 60880 for Class 1 systems and IEC 62138 for Class 2 systems).

1.3 Applicability of this standard to programmable logic devices development

I&C components may include programmable logic devices that are given their specific application logic design by the designer of the I&C component, as opposed to the chip manufacturer. Examples of such devices include complex programmable logic devices (CPLD) and field programmable gate arrays (FPGA).

While the programmable nature of these devices gives the development processes used for these devices, some of the characteristics of a software development process and the design processes used for such devices, are very similar to those used to design logic circuits implemented with discrete gates and integrated circuit packages. Therefore, the design processes and design verification applied to programmable logic devices should comply with the relevant requirements of this standard (i.e. taking into account the particular features of the design processes of such devices). To the extent that software-based tools are used to support the design processes for programmable logic devices, those software tools should generally follow the guidance provided for software-based development tools in the appropriate software standard, i.e. IEC 60880 (Class 1 systems) or IEC 62138 (Class 2 systems).

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 60780, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

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

IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61513:2001, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

IEC 62138, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

ISO 9001, *Quality management systems – Requirements*

IAEA NS-G 1.3, *Instrumentation and control systems important to safety in nuclear power plants*

IAEA 50-C/SG-Q:1996, *Quality assurance for safety in nuclear power plants and other nuclear installations*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61513, as well as the following, apply.

3.1
ATE
automated test equipment

3.2
COTS
commercial off the shelf; COTS is a subset of pre-developed products

3.3
diversity
existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defence against common cause failure. It may be achieved by providing systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective in different ways

[IEC 60880:2006, definition 3.14]

NOTE This definition is wider than that used by the IAEA NS-G-1.3 which is as follows: "The presence of two or more systems or components to carry out an identified function, where the different systems or components have different attributes so as to reduce the possibility of common mode failure". [IEC 61226:2005, definition 3.5]

3.4
firmware
software which is closely coupled to the hardware characteristics on which it is installed. The presence of firmware is generally "transparent" to the user of the hardware component and, as such, may be considered to be effectively an integral part of the hardware design (a good example of such software being processor microcode). Generally, firmware may only be modified by a user by replacing the hardware components (for example, processor chip, card, EPROM) which contain this software with components which contain modified software (firmware). Where this is the case, configuration control of the hardware components by the users of the equipment effectively provides configuration control of the firmware. Firmware, as considered by this standard, is effectively software that is built in to the hardware

3.5
FMEA
failure modes and effects analysis

3.6
FTA
fault tree analysis

3.7
NPP
nuclear power plant

3.8
pre-developed
item which already exists, is available as a commercial or proprietary product, and is being considered for use in a computer-based system

NOTE This definition is consistent with the definition of pre-developed software provided by IEC 61513:2001.

3.9
qualified life
period for which a structure, system or component has been demonstrated, through testing, analysis or experience, to be capable of functioning within acceptance criteria during specific operating conditions while retaining the ability to perform its safety functions in a design basis accident or earthquake

[IAEA Safety Glossary:2006]

3.10
revealed hardware failure
a hardware failure which is detected automatically and reported, for example, a board failure where a watchdog circuit automatically detects the failure and raises an alarm

3.11
safety-related system
system important to safety that is not part of a safety system

[IAEA Safety Glossary:2006]

3.12
safety system
system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents

[IAEA Safety Glossary:2006]

3.13
single failure
failure which results in the loss of capability of a system or component to perform its intended safety function(s), and any consequential failure(s) which result from it

[IAEA Safety Glossary:2006]

3.14
single failure criterion (SFC)
criterion (or requirement) applied to a system such that it is capable of performing its safety task in the presence of any single failure

[IAEA Safety Glossary:2006]

3.15
systems important to safety
system that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public

[IAEA Safety Glossary:2006]

3.16
system validation
confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification as intended (functionality, response time, fault tolerance, robustness)

[IEC 60880:2006, definition 3.42]

3.17
unrevealed hardware failure
hardware failure which is not detected by a system automatically and which only becomes apparent when an attempt is made to use a function which depends upon the failed hardware. Such failures may be discovered by functional testing or when an operational demand is placed upon the system

3.18
verification
confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity (ISO 12207)

[IEC 62138:2004, definition 3.35]

4 Project structure

4.1 General

A project established to produce a computer-based system important to safety should be divided up into a number of phases. Each phase should be to some extent self-contained but will depend on other phases for input and will, in turn, provide outputs for other phases. The various project phases together are considered to form the overall safety life cycle (see IEC 61513, Clause 5, which provides requirements for system life cycles). IEC 61513 allows project phases to be performed in parallel providing the integrity of the development process is not compromised.

A quality assurance plan shall be applied to the hardware production process.

4.2 Project subdivision

The following general requirements define the hardware development life-cycle requirements for computer-based systems within the scope of this standard.

a) The hardware development life cycle shall be compatible with the whole system life cycle (Annex A).

b) Each sub-phase of the hardware development life cycle shall consist of well-defined and documented activities.

c) Pre-existing hardware products (for example, COTS) to be included in the design shall be checked, verified and tested as appropriate before use.

d) Adequate means (i.e. spare parts, devices for test and maintenance, etc.) and accommodation (i.e. laboratories, workshops, space, etc.) shall be provided to carry out the tasks associated with each development phase.

e) Each development phase shall include the production of appropriate documentation.

f) Each development phase shall be concluded by performing verification (see Clause 7).

g) Every verification activity shall result in auditable records documenting the conclusions reached and any design changes resulting from the verification performed.

h) All work activities shall be scheduled to ensure that adequate time is allowed for the following:

   1) the resolution of any interactions between the hardware and software development phases required to ensure system hardware/software compatibility;

   2) the production of documentation, and the performance of testing, verification and quality assurance activities.

4.3 Quality assurance

The design and development process shall meet the relevant requirements of IAEA 50-C/SG-Q (compliance with ISO 9001 is one acceptable method of meeting these requirements). A

hardware quality assurance plan shall exist either as a separate document (or documents) or as part of an overall quality assurance plan. The plan shall address the use of pre-existing hardware and the development of hardware as required. All hardware quality-related activities to be performed by the plant operator, owner, contractors and subcontractors as part of the hardware development process should be included in the quality assurance plan.

4.3.1 The plan should address the following phases, as they are applicable to any particular system or development:

a) design and development;

b) procurement;

c) manufacturing;

d) construction and commissioning;

e) operation and maintenance.

4.3.2 It is not a requirement that all the phases listed above be addressed before the design process begins, but, before each phase is initiated, a plan addressing the requirements of that phase shall be in place.

4.3.3 The quality assurance plan(s) should describe the organization, management and execution of quality related activities, including, as relevant:

a) documentation configuration control;

b) the design process;

c) the procurement process for goods and services;

d) configuration control of build instructions, build procedures and drawings;

e) configuration control of materials and items to be used to build the system hardware;

f) quality control activities, such as formal inspections;

g) control of test equipment;

h) control of hardware handling/storage/shipping;

i) the testing process;

j) monitoring of nonconformances raised and the implementation of corrective actions;

k) the procedure for storing quality assurance records;

l) the procedure for internal audits.

5 Hardware requirements

5.1 General

5.1.1 The hardware requirements shall be consistent with the requirements of the system and form part of the computer-system specification (see IEC 61513:2001, Clause 6). The computer-system specification is a description of the combined hardware/software system and states the design objectives for the system and the functions to be performed by the computer system (systems may be developed for a particular application or may be developed generically, i.e. platform development, in which case development is based upon derived generic system requirements).

5.1.2 The hardware requirements shall be specified in the system hardware requirements specification, or in some other suitable document.

5.1.3 Hardware requirements shall be presented according to a technique or method whose format shall not preclude readability, i.e. the hardware requirements should not be difficult to understand.

5.1.4 Functional hardware requirements shall be unambiguous, testable and/or verifiable and achievable.

5.1.5 The hardware requirements specification should give an overview of hardware requirements, identify the hardware functions important to nuclear safety (however, if these are provided in combination with the system software they should be defined in the system requirements specification), identify the hardware design requirements, state hardware reliability requirements, and state the hardware environmental withstand requirements.

5.1.6 The hardware requirements for computer systems may include requirements which are applicable to hardware in general as well as requirements which are particular to computer system hardware (for example; cabling, surface preparation of enclosures).

5.1.7 The hardware functional requirements should generally describe what has to be done and not how it has to be done. However, the use of pre-existing components/platforms may result in a degree of bottom-up hardware design. Before such pre-existing components are selected for use, an assessment shall be performed to confirm that the hardware performance characteristics (for example; failure modes) are consistent with system requirements. If any anomalies are found then these shall be reconciled, either by modifying the hardware design or the system design (while ensuring that system nuclear safety requirements are not compromised).

5.2 Functional and performance requirements

5.2.1 The hardware functional and performance requirements shall be consistent with the functional and performance requirements of the system important to safety.

5.2.2 The hardware functional and performance requirements, combined with the software requirements (to the extent necessary to address all hardware requirements), shall be verified for compliance with the system requirements.

5.2.3 All parts of the system, down to the component level, which contain software shall be assessed as described in 1.2 of this standard.

a) The hardware functional requirements shall include, but are not restricted to, the definition of
   1) the purpose of the overall computer system hardware and of each hardware sub-system;
   2) the numbers and types of sensors and actuators to be connected to the computer system;
   3) the numbers and types of devices for the man/machine interface such as displays, printers and keyboards.

b) Each component or subsystem delivered by a supplier, and which is to be integrated into the system, should be accompanied by a specification which addresses all safety-related aspects of the performance of that item. If such a specification is not provided, then an analysis shall be performed to determine the hardware design characteristics of the component to the extent necessary to confirm its suitability.

c) The hardware performance requirements shall include (as applicable to any particular application)
   1) required data acquisition rate;
   2) required data handling capability;
   3) required computational capacity;

4) required reliability/availability;
5) required communications interfaces (protocols, transmission speeds);
6) required computational and conversion accuracy;
7) required signal noise rejection capability;
8) required response times;
9) physical size limitations;
10) geographic requirements (for example, length of data transmission lines);
11) required level of spare capacity (if required);
12) environmental withstand qualification requirements;
13) electrical power supply requirements.

d) Any constraints imposed upon the hardware design by the system or software design shall be stated.

5.3 Reliability/Availability requirements

5.3.1 The hardware reliability/availability requirements shall be consistent with the overall reliability requirements of the system. They shall include a description of any types of failure which have to be tolerated without loss, or with a defined limited loss, of function. Hardware reliability targets should be provided.

NOTE Hardware reliability in this context is concerned with random hardware failures and excludes any consideration of failures due to logical design errors.

5.3.2 Irrespective of the hardware reliability/availability requirements, the overall I&C architecture for a NPP shall meet the IAEA NS-G-1.3 single failure criteria (see 3.6).

5.3.3 The hardware requirements should give target figures for the hardware reliability parameters (such as mean time between failure (revealed), mean time between failure(unrevealed), mean time to repair (for revealed failures)). Any requirement for reliability claims to be supported with detailed analysis of the hardware design should be stated, for example, subunit, card-level or component-level analysis.

5.3.4 The methods which may be used to analyse the reliability and the effects of system hardware failures include

– FTA, which is concerned with the identification and analysis of conditions and factors which cause or contribute to the occurrence of a defined undesirable event (see IEC 61025 for advice concerning this technique);
– FMEA, which identifies failures which have significant consequences affecting the system performance, for example, reliability, safety, availability (see IEC 60812 for advice concerning this technique).

Where relevant, a suitable analysis technique shall be applied to Class 1 and Class 2 hardware systems to ensure that any potential hardware failures do not have unacceptable nuclear safety effects.

5.3.5 A technique such as FTA when combined with known component failure data may be used to provide calculated values for system hardware reliability characteristics. Such an approach shall be used to analyse the hardware of Class 1 systems (see IEC 61513), unless sufficient operating experience is available to give high confidence that the target hardware reliability targets will be achieved. Such a technique should also be applied for Class 2 systems, or, alternatively, a justification of adequate reliability provided on the basis of qualitative reasoning (for example, quality of components, hardware redundancy, operating experience, proportion of revealed hardware failures versus unrevealed hardware failures, etc.), particularly if hardware reliability requirements are not overly demanding.

5.3.6 Strategies and provisions to assure reliability and availability over the lifetime of the computer system shall be defined. These measures shall be documented as maintenance requirements. They shall include requirements to prevent maintenance activities introducing faults which may lead to common-cause failures. Maintenance activities on multiple train systems are generally considered to be the most likely means of introducing such faults and therefore systems shall be designed to reduce the necessity for such activities to the extent practical. Where maintenance activities having the potential to result in common-cause failures are required, then the design requirements shall specify how the risk of such failures shall be minimized.

5.3.7 Maintenance requirements should address (as applicable to any particular system)

a) requirements for system operation during hardware maintenance activities;
b) consumable replacement, for example, air filters;
c) any requirements for the regular replacement of subsystems, modules and/or components;
d) the extent of hardware revalidation (for example, testing) required following hardware maintenance activities.

5.3.8 However, given that the requirements specification should define "what", rather than "how", it may not be practicable to define maintenance requirements in detail at the requirement specification phase of a project, in which case these requirements should be fully defined at a later phase of the development process.

5.4 Environmental withstand requirements

5.4.1 The hardware environmental withstand requirements shall address physical constraints, climatic, seismic, chemical, electrical and radiation conditions as applicable. Any particular requirements applicable during installation and commissioning should also be included.

5.4.2 The degree of immunity to electromagnetic interference shall be specified as required by the operational environment, and tested according to applicable standards, for example, IEC 61000. The electromagnetic operational environment could potentially be affected by a wide variety of electrical interference sources, for example, switchgear, mobile phones, relays, walkie-talkies, electrostatic discharges, lightning, earth faults.

5.4.3 The electromagnetic qualification levels specified should be in accordance with realistic estimates of the operational conditions under all credible worst-case circumstances.

5.4.4 The hardware requirements shall identify any prohibited construction materials and any requirements for particular materials to be used, or for particular types of production processes.

5.4.5 If a particular hardware qualification process is required, then this should be documented in the hardware requirements.

5.5 Documentation requirements

The hardware documentation requirements shall be specified as part of the documentation requirements of the computer system (see IEC 61513). The documentation to be produced should include (as relevant):

a) design documents (system hardware components, hardware design of interfaces, etc.);
b) operators' manuals;
c) maintenance manuals.

6 Design and development

6.1 General

This clause is applicable to system, subsystem and module level hardware design and development.

6.1.1 The design and development process for new hardware should take as an input the hardware requirements specification. The design process should progress through various design stages which result in the production of hardware which meets the hardware requirements specification.

6.1.2 The more general level of design activity may be termed the "preliminary" design, consisting of the analysis of different design alternatives in order to define the hardware system architecture in terms of subsystems and modules.

6.1.3 Preliminary design is generally followed by one or more detailed design levels. The detailed design activities shall expand the preliminary design to address the detailed design of subsystems, modules and components to the extent that the overall hardware design description is sufficiently complete to be implemented.

6.1.4 Prototype hardware may be built, not only to demonstrate successful interaction between hardware modules, but also to check hardware and software compatibility.

6.1.5 Pre-developed (for example, COTS) components could be used for all system hardware or for a subset of hardware components. Subclauses 6.2 to 6.7 mainly consider the situation where bespoke hardware development is required; however, where appropriate, guidance is also provided which defines how the requirements of these subclauses may be applied to the use of pre-developed components.

6.2 Design activities

6.2.1 System performance requirements which are dependant upon hardware performance shall be addressed by the hardware design, and evidence shall be made available, either through analysis or testing, to show that the hardware design meets these requirements. Such requirements may include calculation accuracy, time response, environmental withstand capabilities and electrical supply requirements (for pre-existing components, the component hardware specification shall be verified against the system hardware requirements to ensure that the pre-existing components meet the specified requirements, or hardware performance shall be verified by test).

6.2.2 Any discrepancies against hardware requirements shall be reconciled, by either changing the design or changing the requirements (the impact of any changes shall be fully assessed and documented).

6.2.3 The hardware designers shall identify such tests as are necessary to show that the required performance has been achieved. Such tests may be performed on the hardware alone, or performed when the hardware is integrated with the software, i.e. as part of the system integration testing phase.

6.2.4 The hardware designers shall specify any maintenance activities required to provide confidence that the performance and reliability requirements are achieved during the full operational life of the equipment. These may include operational tests, calibration, repair, periodic replacement and maintenance procedures. Such activities should be performed to an extent which provides sufficient confidence in correct operation of the equipment and yet reduces human interference and the performance of intrusive work with the systems to a minimum, so as to reduce the likelihood of faults (such as potential common-mode failure faults) being introduced through maintenance activities.

6.2.5 Where a qualified target life is specified, justification shall be provided that this target is realistic and achievable.

6.3 Reliability

6.3.1 Reliability requirements should be specified in the hardware requirements documentation (see 5.3).

6.3.2 As required to support the system-level safety analysis, an analysis of the potential for hardware failures shall be made during design. Where multiple trains of a system or multiple systems (each of which may have a single or multiple trains of equipment) are used to implement a nuclear safety function then proper consideration of the potential for common-cause hardware failures shall be included in this analysis. Potential means of hardware based common-cause failure are as follows:

– maintenance activities performed simultaneously or sequentially on multiple trains of equipment (particularly where such activities may introduce unrevealed hardware faults);
– periodic testing;
– coincident unrevealed random hardware failures on multiple trains of equipment which affect the same nuclear safety function(s);
– latent design faults affecting multiple equipment trains, and which were not revealed by the design process.

6.3.3 Methods which may be used to analyse hardware reliability and the effects of system hardware failures include FTA and FMEA (see 5.3.4).

6.3.4 The hardware design should minimize the potential impact on nuclear safety of the following factors:

– maintenance activities;
– system failure due to random hardware failure;
– hardware failure due to environmental conditions.

6.3.5 If the estimated hardware reliability is considered to be inadequate for a particular role then compensating actions shall be taken. These may take the form of design improvements or operational changes (such as an increase in the frequency of operational testing). However, care should be taken when the option of increased operational testing is chosen, as any intrusive activities on operational plant carries an intrinsic degree of risk as faults may be induced or introduced (i.e. the net overall effect upon safety of operational testing may be negative). Ideally, all testing should be performed when potential faults in the testing process would not have a nuclear safety impact, for example, during station outages or when the equipment to be tested is isolated from operational plant.

6.3.6 Where a probabilistic safety assessment is used to support the safety case of an NPP, the estimated probabilistic hardware reliability values (for example, as developed from FTA) may be fed into the NPP analysis, and so contribute to the accuracy of the overall station reliability calculations.

6.4 Maintenance

The hardware design shall address any specific maintenance requirements contained within the hardware requirements specification. In addition, where practicable, the design should include features to reduce the risk of faults being introduced due to maintenance activities; examples of such features are as follows:

– components that may require replacement due to failure should be easily accessible;

– replaceable components should be clearly identified so that maintenance staff may easily check that the correct components are used;
– there should be adequate spacing of terminals;
– there should be adequate provision of dedicated terminals for use during calibration/testing activities (so that plant wiring does not have to be disconnected to facilitate such activities);
– hardware design should have a structured layout with clear labelling to reduce the potential for maintenance errors.

6.5 Interfaces

IEC 61513, 6.1.1.2.1, provides system interface requirements which aim to prevent the propagation of failures across system interfaces.

6.6 Modification

To the extent required by the hardware requirements specification, the hardware shall be designed to be capable of being modified (see Clause 12).

6.7 Power failure

To the extent required by the hardware requirements specification, the computer system shall be designed to be insensitive to the consequences of short-term power failures and to potential variations of the power supply (voltage/frequency). System features shall be provided to notify operators and maintenance staff of such power fluctuations (this role may not be allocated to hardware, and hence may be out of scope of this standard).

6.8 Component selection

Where pre-existing components are to be used, the design of the components shall be compatible with their role within the system hardware.

6.9 Design documentation

6.9.1 The hardware design documentation shall describe the hardware design and the means by which the hardware requirements have been addressed. Standardized forms of design documentation and the use of automated hardware design tools are recommended.

6.9.2 A hierarchy of design documents addressing the computer system hardware should be produced which consist of a number of documentation 'levels'. The design documentation at each level should specify the design aspects relevant to that level and define the hardware requirements for the lower levels. Documents (as applicable) for manufacturing/assembly, factory testing, installation, commissioning, maintenance and operation shall be produced during the design process.

6.9.3 A preliminary hardware design description may be produced which defines the hardware architecture, i.e. the structure and relationship between the different parts of the system. It should include the general layout of hardware, with block diagrams of the subsystems and modules of the lower levels. It should also include hardware requirements for the detailed design, such as:

– the number and types of central processor units and other processors;
– computer memory hardware requirements;
– the number and types of interfaces;
– the number and types of data links and busses.

6.9.4 At the conclusion of the design and development of the hardware, documentation shall be produced which contains a full and final description that conveys both the design details down to the lower level and the capabilities, limitations and other characteristics of the hardware.

6.9.5 This final description documentation shall provide the following information:

a) a design overview;

b) cross-references to supporting design documents;

c) a description of the subdivision of the hardware in terms of hardware subsystems;

d) a description of each subsystem in terms of its major modules and components (using for example, block diagrams, circuit diagrams);

e) a description of subsystem hardware interfaces. Interfaces shall be described as appropriate in logical, physical, electrical or other terms;

f) a description of the computer system hardware interfaces. Interfaces with any other systems either within or outside the nuclear plant, shall be identified showing the specific interfaces and related hardware requirements;

g) the physical layout – a description with diagrams of the physical layout of the equipment should be provided;

h) qualification data (see Clause 8), including the definition of any necessary actions (such as exchange of components) required to maintain the specified qualification lifetime. Qualification data relevant to shelf life of spare parts should also be provided where relevant;

i) maintenance requirements;

j) a description of how the requirements for hardware reliability and fail-safe properties are fulfilled.

7 Verification and validation

7.1 General

7.1.1 The design and development process shall include formal checks that the hardware design deliverables from each phase of design and development meet the requirements imposed by the previous phase.

7.1.2 The hardware verification process is generally considered to begin with the verification of the hardware design requirements against the system design requirements, and is considered to be complete when the system software is integrated into the hardware. For Class 1 and Class 2 systems, IEC 60880 and IEC 62138, respectively, provide relevant requirements for the hardware/software integration phases.

7.2 Verification plan

A formal verification plan shall be prepared to define the approach to be used to verify the hardware design and to control the verification process. The plan shall be prepared prior to initiating verification actions. The plan (or plans) should document the personnel/organization to be used, organizational structure, verification methods to be used, level of verification to be performed, schedules and other significant project activities related to verification.

a) Verification may be performed in parallel with the design process (providing adequate configuration control arrangements are in place) so that errors may be detected and corrected as soon as possible.

b) Formal verification actions shall not take place until design components are released for verification by the design personnel. Once released for verification, the design and related documentation shall be maintained under formal configuration control.

c) After release for verification, the design change process shall ensure that all subsequent changes to the hardware design are adequately verified (i.e., as required by 7.7).

7.3 Independence of verification

7.3.1 For Class 1 hardware design, verifiers should be managerially independent from the hardware designers; for example, they may be in different departments of the same organization or from a different organization. For Class 2 systems, verifiers shall not have designed the items to be verified; however, persons involved with verification may be from the same organization as the individuals responsible for the design. In addition to these requirements:

a) the verification personnel shall be technically competent;

b) any verification findings and responses to those findings by the design team shall be formally documented;

c) verification shall be performed according to documented procedures.

7.3.2 For Class 2 hardware development where ATE is used to verify the correctness of hardware, then the detailed independence requirements defined above apply to the personnel who design the ATE, rather than the personnel monitoring the performance of the tests being performed by the ATE. However, for the development of all Class 1 hardware, individuals shall not be responsible for performing tests (with or without ATE) on hardware components which they have designed.

7.4 Methods

Critical reviews, audits, analysis, manual tests or tests performed using ATE, or a combination of these methods, may be used to provide hardware design verification. The basis for the choice of verification method(s) to be used shall be documented in sufficient detail to allow auditing by personnel who are not directly involved in the design or verification activities.

a) When choosing the appropriate verification method, the following issues shall be considered when relevant:
   - the safety-related classification of the system (i.e. Class 1/2, with Class 1 requiring the most rigorous techniques);
   - the documented reviews and tests which will be performed on the integrated hardware and software as part of the system verification and validation processes, i.e. to eliminate such activities from the hardware verification and validation processes, so as not to inefficiently utilise resources by duplicating work;
   - previous verification activities performed on the hardware or on systems containing the hardware (i.e. where equipment has been effectively pre-qualified);
   - system design characteristics, for example, size, maturity/novelty of design principles used, failure modes and complexity;
   - supporting data which may be available from other sources, such as that obtained from quality assurance and environmental qualification processes.

b) Appropriate tools and methods shall be available to support the testing of subsystems and electronic components to ensure that they can be thoroughly tested. ATE should be used to improve the repeatability and thoroughness of testing where effective.

c) Test instruments used in the verification or testing process shall be calibrated where necessary to confirm accuracy, in which case procedures shall ensure that only calibrated instruments are used.

d) Software-based test tools shall be validated prior to use and shall be placed under configuration control.

e) The results of all formal testing shall be recorded (informal testing may be performed during the design process as a precursor to formal testing). Auditable records of formal

testing shall be available which are sufficient to demonstrate that all tests have been performed, and that any test anomalies have been successfully reconciled.

7.5 Documentation

Auditable records resulting from verification activities shall include the verification programme plan, test procedures, test results, design change records and documentation of any discrepancies which are discovered during the hardware verification process (together with records showing how each discrepancy was reconciled).

a) Test procedures should be clearly written, provide step-by-step instructions for hardware verification and should contain detailed information of the test set-up.

b) Test procedures shall contain unambiguous pass/fail criteria.

c) Test procedures implemented by software shall be documented.

7.6 Discrepancies

Discrepancies found during the verification process shall be formally documented and transmitted to the relevant personnel for resolution. The response shall be formally documented to provide a traceable path to assure that all discrepancies are assessed and any identified design deficiencies corrected or accepted. Where design deficiencies are accepted, all impacts on system documentation shall be fully addressed.

7.7 Changes and modifications

7.7.1 All design changes shall be subject to design impact assessment to determine which documentation requires amendment and what design and verification processes should be repeated.

7.7.2 Modified parts shall be identified in accordance with the relevant quality control procedures.

7.8 Installation verification

Verification of correct system installation shall be in accordance with Clause 10.

7.9 Validation

System validation of the integrated hardware and software shall be performed as required by IEC 61513, IEC 60880 or IEC 62138 as applicable.

7.10 Verification of pre-existing equipment platforms

Where a pre-existing equipment platform is to be used, then the suitability of the platform for its intended use shall be assessed. The assessment process shall consider the following design aspects:

a) design process used to develop the hardware, i.e. assess against the relevant requirements of Clause 6;

b) experience of use (where actual hardware reliability data provides confirmation that hardware reliability targets are achievable, then considerable confidence in the performance of the hardware in the proposed application may be gained). Relevant experience-of-use data which support the required hardware reliability target may be used to compensate for discrepancies in the development methods used, as identified by item a) above;

c) if item a) above does not provide adequate information to justify the hardware for its intended use, then additional work may be performed to support the assessment, for example, testing, analysis, justification.

8 Qualification

IEC 60780 provides requirements concerning the qualification of hardware for nuclear safety applications and the relevant requirements of the standard should be applied. Annex B provides an informative outline of the qualification process.

9 Manufacture

Where subsystems, modules and components used in the computer system include pre-developed (for example, COTS) products and bespoke hardware products, they shall be built and/or assessed in accordance with the relevant requirements of this standard.

10 Installation and commissioning

10.1 Packing, handling, transport, storage and unpacking shall be such as to prevent any damage to the system.

10.2 Before the system is unpacked and installed, the environment in which the system is to be installed shall be verified to conform to the hardware environmental requirements, as covered by 5.4.

10.3 Adequate procedures and information shall be available to enable the system to be installed, cabled and wired in accordance with the design requirements; for example, earthing requirements. Identification of items of equipment shall form part of this information. For this purpose, a quality plan shall be applied. The system shall be installed, cabled, tested and set to work in accordance with defined procedures.

10.4 The proper working of the system at site shall be checked by planned and specified commissioning tests, as required by IEC 61513.

10.5 The tests shall be performed in accordance with relevant standards, for example, IEC 61000.

10.6 The severity level of electromagnetic interference tested shall be chosen in such a way that it equals or surpasses the worst estimated conditions to which the system may be subjected while required to operate.

10.7 For Class 1 and 2 systems off-site type testing of electromagnetic interference withstand should be performed. For Class 2 systems this type of testing should generally be considered to provide adequate assurance of correct operation. For Class 1 systems on-site testing should also be performed if practicable and effective.

10.8 On the completion of installation and commissioning, and when it has been confirmed that all acceptance criteria have been addressed (or concessions agreed), ownership of the system may be transferred to the user, as described in IEC 61513.

11 Maintenance

Hardware maintenance comprises

– tests, checks and calibration (which may be either periodic, within specified maximum intervals, or following the replacement, exchange, overhaul or repair of components [i.e. revalidation]);

– maintenance such as is required to maintain the computer hardware in good working order, for example, replacement of expendables, or the preventative exchange or overhaul of equipment, subunits, parts or components;

– repairs, i.e. the restoration of the operability of failed equipment, subunits and parts.

11.1 Maintenance requirements

11.1.1 A formal procedure (or procedures) shall be specified and applied to control the execution and the documentation of maintenance activities (see Annex C).

This shall take into account

– preventative actions required to reduce the potential for faults to be introduced and the potential for personal injuries to occur;

– organizational and operational preparations required if the maintenance activities have the potential to affect plant operation, or the availability of safety functions or safety-related functions.

11.1.2 Maintenance shall be undertaken by qualified and authorized personnel. It shall be performed according to specified procedures. The procedures shall make provision for personal certification (by an authorized person, or by automated test) to the effect that, where tasks may have a direct impact upon safety, each task has been completed satisfactorily.

All relevant information, such as time and date, replacements fitted, etc., shall be recorded.

11.1.3 The records arising from maintenance work shall be made available for audit if required.

11.1.4 For some critical components, rather than performing component replacement only when failure occurs, a preventative maintenance regime may be adopted. In this case, controls should be applied to ensure that components are replaced after a period of time not longer than their qualified life (if applicable, see IEC 60780).

11.1.5 Spare parts held by the operating organization shall be kept in a store which meets any environmental conditions relevant to the parts to be stored there. The shelf life of spare parts shall be controlled and modified as necessary with the passage of time in accordance with the ageing characteristics of the hardware. Any activities needed to preserve the state of readiness of the spares, such as periodic energization, shall be addressed.

11.1.6 Spares should be qualified to a standard equivalent to that used to qualify operational components. Any proposal to reduce the qualification requirements of a Class 1 or 2 system component, or to extend the qualification life of such a component, should be treated as a system modification and assessed as such; see Clause 12 (IEC 61513 specifies the controls to be placed on system modifications).

11.1.7 All spares shall be under configuration control and shall have adequate identification marking or labelling.

11.1.8 It is recommended that the future supply of spare components should be secured to the extent practicable (for example, either through the holding of spares, assurances from suppliers or by having access to manufacturing capability).

11.2 Failure data

11.2.1 Failure data acquired during equipment operation constitutes a major source of information which can be used to improve

– component reliability data knowledge (by taking into account real operating environment conditions);
– equipment reliability evaluations (by determining actual field failure data and by observing availability in operating conditions);
– maintenance policy (through better spare parts optimization, better preventative maintenance schedules and better maintenance personnel training requirements).

11.2.2 Accordingly, field failure data (from information available from maintenance reports) should be logged in a failure data bank.

11.2.3 The maintenance reports shall contain (if relevant and if known)

– identification of the system with the failed component;
– failure circumstances and failure effects;
– failed component identification;
– component location within the system;
– description of the fault which caused the failure;
– date of intervention;
– age of failed component;
– identification of person(s) who raised the report;
– identification of person(s) who diagnosed the fault.

11.2.4 Failure data for systems important to safety shall be subject to periodic review to ensure that the frequency of component failure remains within acceptable limits. Any statistically significant negative trends in the data should be extrapolated to ensure, to the extent practicable, that the equipment will continue to operate satisfactorily in the future period up to the next assessment of the failure data of the equipment, or until the equipment may be replaced (whichever is the shortest period).

11.3 Maintenance documentation

11.3.1 Instructions for maintenance shall be provided in written or electronic form by means of procedures, manuals, handbooks, etc.

11.3.2 Maintenance documents shall describe the hardware maintenance policy for the equipment in use, including identification of hardware components which require regular checking, re-calibration or replacement.

11.3.3 Maintenance documents shall describe any relevant diagnostic processes which should be used to detect the failure of specific modules.

11.3.4 Documentation shall describe the repair policy, i.e.

– the methods of repair or substitution of different subsystems, modules and components;
– any restrictions which the system should be subjected to during repair time (for example, the system or parts of the system which shall be switched off);
– the extent to which equipment shall be revalidated after a repair.

In addition to the procedures for scheduled periodic maintenance, diagnostic procedures should be provided, where relevant and practicable, which may be used to assist in the investigation of anomalous system behaviour and to identify failed components.

12 Modification

Hardware design modification may be required to correct defective performance or to address new or revised performance requirements.

12.1 The process controlling hardware design changes shall be compliant with the requirements of 6.3.6 of IEC 61513:2001.

12.2 Hardware design changes which have an impact beyond a single design phase (i.e. excluding any changes made by the designers while in the process of creating the design) shall be controlled by a documented procedure. This design change procedure should take account of any potential impacts to other aspects of the system design, such as other hardware components and software.

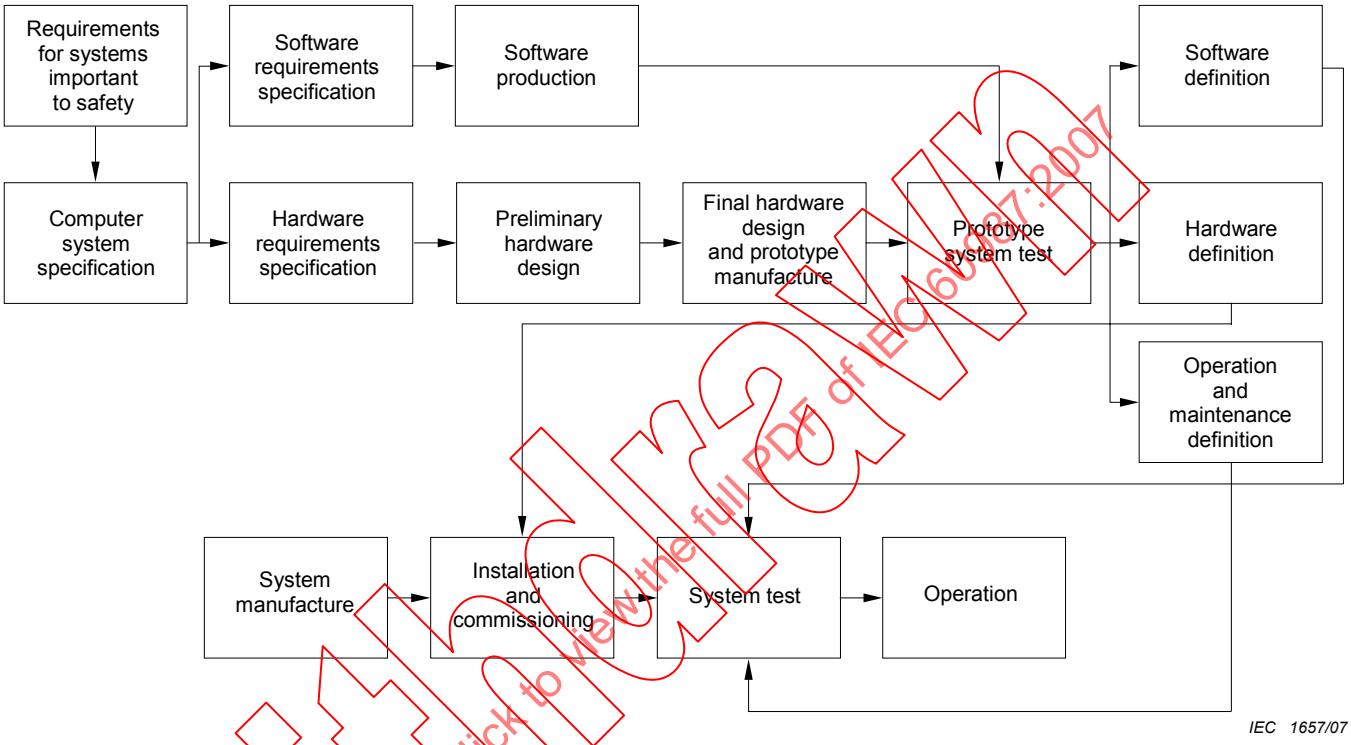
12.3 The design change procedure shall ensure that the impact of all hardware changes on the hardware and system verification, validation and qualification processes is identified and any required re-work is performed.

13 Operation

Relevant requirements for system operation are provided by IEC 61513 (IEC 60880 and IEC 62138 contain additional relevant information).

Annex A
(informative)

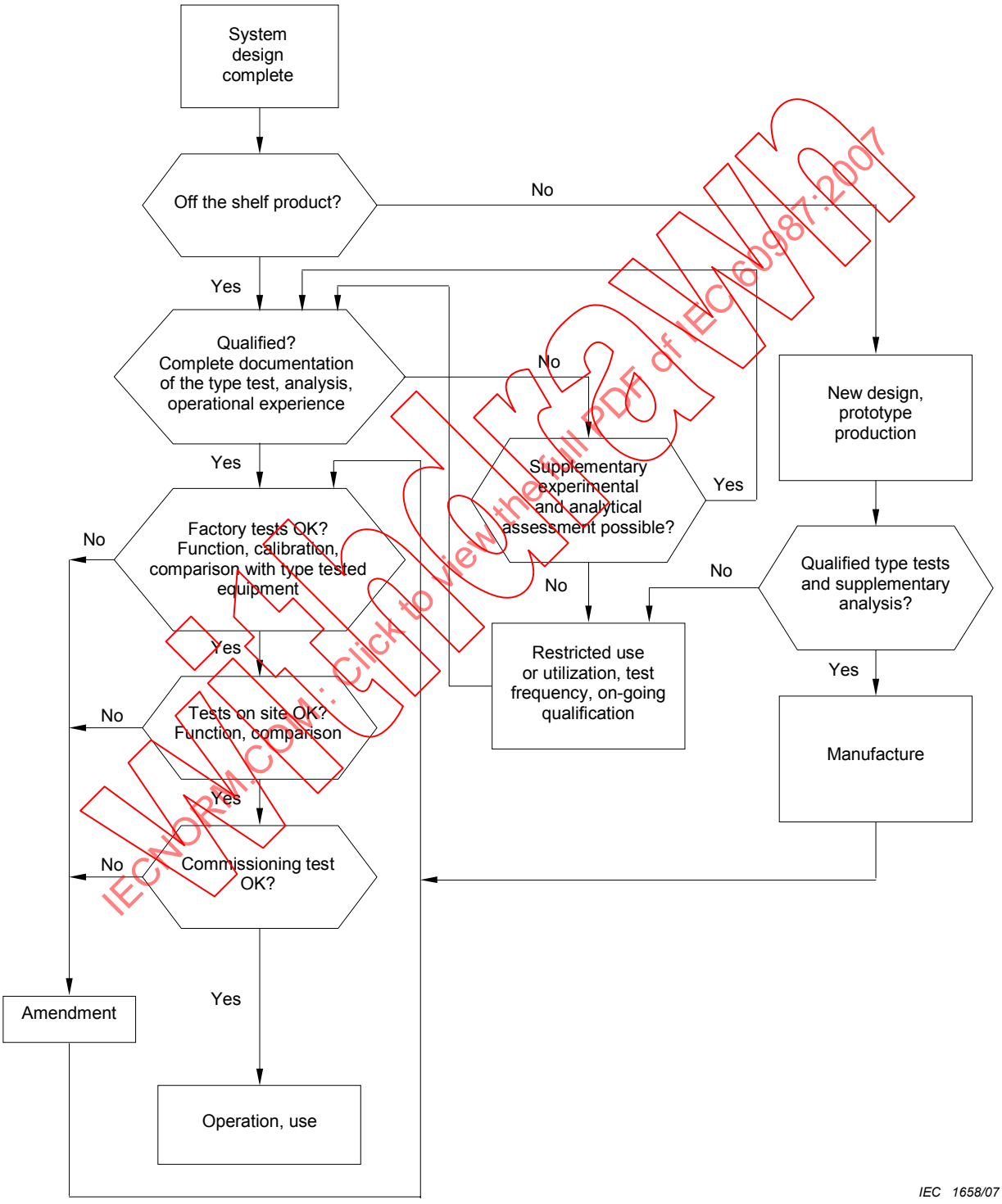
Overview of system life cycle



NOTE In the interest of clarity, the feedback paths have not been shown.

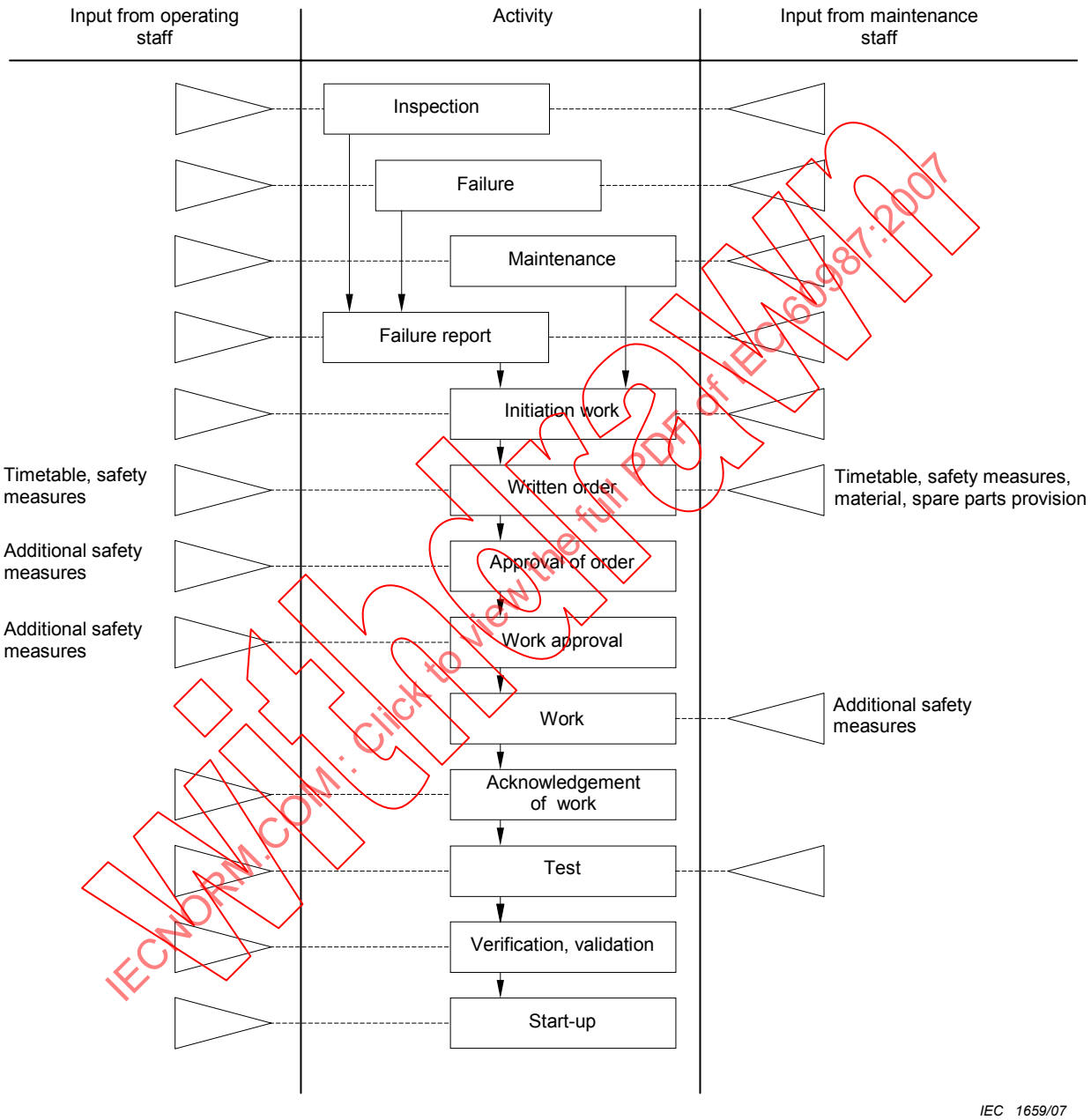
Annex B
(informative)

Outline of qualification



Annex C
(informative)

Example of maintenance procedure



Legend

Signifies staffing related to activity shown

Bibliography

The following references contain information of some relevance to this standard.

IEC 61226, *Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions*

ISO 12207, *Information technology – Software life cycle process*

IAEA Safety Glossary:2006

IAEA NS-R-1:2000, *Safety of nuclear power plants: Design*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES APPLICABLES À LA CONCEPTION DU MATÉRIEL DES SYSTÈMES INFORMATISÉS

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 60987 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Cette deuxième édition annule et remplace la première édition parue en 1989. Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- prise en compte du fait que les techniques de conception du matériel des systèmes informatisés ont progressé de façon significative ces dernières années;
- mise à jour du format de la norme pour être conforme aux directives ISO/CEI portant sur le style des normes;
- mise en cohérence de la norme avec les nouvelles révisions des documents de l'AIEA NS-R-1 et NS-G-1.3, cela comprenant autant que possible une adaptation des définitions;

- remplacement, autant que faire se peut, des exigences associées aux normes publiées depuis la parution de la première édition de la CEI 60880, plus particulièrement la CEI 61513, la CEI 60880, édition 2, et la CEI 62138;
- revue des exigences existantes et mise à jour des définitions et de la terminologie.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/662/FDIS	45A/666/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.

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

a) Contexte technique, questions importantes et structure de cette norme

Les principes de base de conception de l'instrumentation nucléaire tels que particulièrement appliqués aux systèmes de sûreté des centrales nucléaires de puissance (CNP) furent interprétés dans les normes du secteur nucléaire en référence aux systèmes câblés, en particulier dans le «Guide de sûreté 50-SG-D3» de l'AIEA qui a été remplacé par le guide de l'AIEA NS-G-1.3.

La première édition de la CEI 60987 a été publiée en 1989 pour couvrir les aspects matériels de la conception des systèmes informatisés des systèmes importants pour la sûreté, c'est-à-dire, des systèmes de sûreté et des systèmes liés à la sûreté.

Bien que beaucoup des exigences contenues dans la première édition de la norme restent pertinentes, des facteurs significatifs ont justifié du développement de la révision de la CEI 60987, et en particulier:

– une nouvelle norme est parue qui traite en détail des exigences générales applicables au systèmes nucléaires importants pour la sûreté (la CEI 61513);
– l'utilisation de plateformes système prédéveloppées, plutôt que de développements faits sur commande, a significativement augmentée.

b) Position de la présente norme dans la collection de normes du SC 45A de la CEI

La norme de premier niveau du SC 45A concernant les systèmes informatisés importants pour la sûreté utilisés dans les centrales nucléaires de puissance (CNPs) est la CEI 61513. La CEI 60987 est un document du SC 45A de deuxième niveau qui traite de la question générique de la conception du matériel des systèmes informatisés.

La CEI 60880 et la CEI 62138 sont des normes de second niveau de la collection de normes du SC 45A qui couvrent ensemble les aspects logiciels relatifs aux systèmes informatisés utilisés pour réaliser des fonctions importantes pour la sûreté des CNP. Les CEI 60880 et CEI 62138 font directement référence à la CEI 60987 pour la conception du matériel.

La CEI 60987 fait référence aux exigences de la CEI 60780 en matière de qualification du matériel. Concernant les modules utilisés pour la conception de systèmes particuliers importants pour des applications de sûreté, les retours d'expérience pertinents et qui peuvent faire l'objet d'audits dans le domaine du nucléaire ou pour d'autres applications, peuvent, comme cela est décrit dans la CEI 60780, en combinaison avec l'exécution d'un programme rigoureux d'assurance qualité, constituer une méthode acceptable de qualification.

Pour plus de détails sur la collection de normes du SC 45A de la CEI, voir le point d) de cette introduction.

c) Recommandations et limites relatives à l'application de cette norme

Il est important de noter que cette norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de Classe 1 ou de Classe 2 (voir la CEI 61513 pour ce qui concerne les exigences de classement des systèmes).

Pour assurer la production de systèmes d'une grande fiabilité, cette norme fournit des recommandations particulières pour les aspects suivants:

– une approche générale du développement du matériel informatique;
– une approche générale de la vérification du matériel et des aspects liés au matériel de la validation des systèmes informatisés.

Il est reconnu que la technologie informatique est continuellement en développement et qu'il n'est pas possible pour une norme telle que celle-ci de faire référence aux technologies et techniques de conception modernes. L'accent a été mis sur les questions de principes plutôt que sur celles spécifiques aux technologies liées à la conception du matériel, pour assurer que la norme soit pertinente dans les années à venir. Si de nouvelles techniques de conception sont développées alors il devrait être possible d'évaluer l'aptitude de telles techniques à être employées en adaptant et en appliquant les principes de conception contenus dans cette norme.

Le domaine d'application de cette norme couvre le matériel des systèmes informatisés utilisés par des systèmes de Classe 1 et de Classe 2. Ceci comprend les systèmes multiprocesseurs répartis et les systèmes monoprocesseurs; elle couvre l'évaluation et l'utilisation des éléments commercialement disponibles sur étagère (COTS) et le développement de nouveaux matériels.

d) Description de la structure de la collection des normes du SC 45A de la CEI et relations avec les documents de la CEI, de l'AIEA et de l'ISO

Le document de niveau supérieur de la collection de normes produites par le SC 45A de la CEI est la CEI 61513. Cette norme traite des exigences relatives aux systèmes et équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des CNPs, et structure la collection de normes du SC 45A de la CEI.

La CEI 61513 fait directement référence aux autres normes du SC 45A de la CEI traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, les défaillances de cause commune, les aspects logiciels et les aspects matériels relatifs aux systèmes programmés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la CEI 61513, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de la CEI, qui ne sont généralement pas référencées directement par la CEI 61513, sont relatives à des matériels particuliers, à des méthodes ou à des activités spécifiques. Généralement ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

Un quatrième niveau qui est une extension de la collection de normes du SC 45A de la CEI correspond aux rapports techniques qui ne sont pas des documents normatifs.

La CEI 61513 a adopté une présentation similaire à celle de la CEI 61508, avec un cycle de vie et de sûreté global, un cycle de vie et de sûreté des systèmes, et une interprétation des exigences générales des CEI 61508-1, CEI 61508-2 et CEI 61508-4 pour le secteur nucléaire. La conformité à la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire. Dans ce cadre, la CEI 60880 et la CEI 62138 correspondent à la CEI 61508-3 pour le secteur nucléaire.

La CEI 61513 fait référence à l'ISO 9001 ainsi qu'au document AIEA 50-C-QA (remplacé depuis par le document AIEA 50-C/SG-Q) pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de la CEI sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des CNPs, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des CNPs et le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle-commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – EXIGENCES APPLICABLES À LA CONCEPTION DU MATÉRIEL DES SYSTÈMES INFORMATISÉS

1 Domaine d'application

1.1 Généralités

La présente Norme internationale est applicable au matériel des systèmes informatisés des CNPs de Classes 1 et 2 (telles que définies dans la CEI 61513).

La structure de cette norme n'a pas évoluée de façon significative depuis la version originale publiée en 1989, néanmoins certaines éléments apparus entre-temps sont maintenant pris en compte par celle-ci (par exemple la CEI 61513 pour la conception de l'architecture des systèmes) et des références aux nouvelles normes sont fournies lorsque cela est pertinent. Le texte de cette norme a aussi évolué pour refléter les développements survenus dans le domaine de la conception du matériel des systèmes informatisés, l'utilisation de matériels prédéveloppés commercialement disponibles sur étagère (par exemple, les COTS) et l'évolution de la terminologie.

Les ensembles de matériel informatique utilisés pour le chargement et la vérification du logiciel ne sont pas considérés comme faisant partie intrinsèque du système important pour la sûreté et comme tel sont hors du domaine d'application de cette norme.

NOTE 1 Le matériel des systèmes informatisés de Classe 3 n'est pas couvert par cette norme et il est recommandé que de tels systèmes soient développés conformément à des normes commerciales.

NOTE 2 En 2006, des discussions ont eu lieu au SC 45A de la CEI pour le développement d'une nouvelle norme concernant les exigences relatives au matériel très complexe. Si cette norme est développée, alors on l'utilisera de préférence à la CEI 60987.

1.2 Utilisation de cette norme pour l'évaluation des matériels pré-développés (par exemple les COTS)

Bien que le but principal de cette norme soit de traiter du sujet du développement du nouveau matériel, le processus défini dans la norme peut aussi servir de guide dans l'évaluation du matériel prédéveloppé tel que COTS. Le texte fournit des recommandations pour interpréter les exigences de la norme lorsque celle-ci est employée pour évaluer de tels composants. En particulier, les exigences d'assurance qualité de 4.3 concernant la gestion de configuration s'appliquent.

Les composants prédéveloppés peuvent contenir des microprogrammes (tels que définis en 3.8) et, lorsque les microprogrammes sont profondément intégrés et que la présence de tels logiciels est effectivement « transparente » pour l'utilisateur, alors il convient d'utiliser la CEI 60987 comme guide pour l'évaluation de tels composants. Un exemple pour lequel cette approche est considérée comme adaptée est l'évaluation des processeurs modernes qui comprennent du microcode. Un tel code fait généralement partie intégrante du matériel, ainsi il est donc acceptable d'évaluer le processeur (comprenant le microcode) en tant que composant matériel intégré en se servant de la présente norme.

Il convient de développer ou d'évaluer le logiciel qui ne peut être considéré comme un microprogramme tel que décrit ci-dessus, conformément aux exigences des normes logiciel applicables (par exemple la CEI 60880 pour les systèmes de Classe 1 ou la CEI 62138 pour les systèmes de Classe 2).

1.3 Application de cette norme au développement des composants logiques programmables

Des composants d'I&C (instrumentation et contrôle-commande) peuvent contenir des composants logiques programmables dont la conception logique applicative particulière est assurée par le concepteur du composant d'I&C, et non par le fabricant de composants électroniques, par exemple les « complex programmable logic devices (CPLD) » et les « field programmable gate arrays (FPGA) ».

Alors que la nature programmable de ces composants confère aux processus de développement utilisés pour ceux-ci, certaines caractéristiques propres aux processus de développement logiciel, les processus de développement utilisés pour de tels composants sont très proches de ceux suivis pour la conception des circuits logiques mettant en œuvre des composants discrets et des circuits intégrés. Ainsi, les processus de conception et de vérification de la conception retenus pour ces dispositifs programmables logiques doivent être conformes aux exigences applicables de la présente norme (par exemple en prenant en compte les caractéristiques particulières des processus de développement de tels dispositifs). Dans la mesure où des outils logiciels sont utilisés en support des processus de conception des composants logiques programmables, il convient que ces outils logiciels suivent les recommandations applicables au développement d'outils logiciels fournies par les normes pertinentes, par exemple la CEI 60880 (systèmes de Classe 1) ou la CEI 62138 (système de Classe 2).

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 60780, *Centrales nucléaires – Equipements électriques de sûreté – Qualification*

CEI 60812, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

CEI 60880, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

CEI 61000 (toutes les parties), *Compatibilité électromagnétique (CEM)*

CEI 61025, *Analyse par arbre de panne (AAP)*

CEI 61513:2001, *Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*

CEI 62138, *Centrales nucléaires – Instrumentation et contrôle commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

ISO 9001, *Système de management de la qualité – Exigences*

AIEA NS-G 1.3, *Systèmes d'instrumentation et de contrôle commande importants pour la sûreté des centrales nucléaires*

AIEA 50-C/SG-Q:1996, *Assurance de la qualité pour la sûreté des centrales nucléaires de puissance et les autres installations nucléaires*

3 Termes et définitions

Pour les besoins de ce document, les termes et définitions de la CEI 61513, ainsi que les suivants, s'appliquent.

3.1
ATE
banc d'essai automatique

3.2
COTS
matériel commercialement disponible sur étagère; les COTS forment un sous-ensemble des produits prédéveloppés

3.3
diversité
existence de deux ou plusieurs manières différentes d'atteindre un objectif donné. La diversité est en particulier utilisée comme moyen de défense contre une défaillance de cause commune. Elle peut être réalisée par la mise en œuvre de systèmes physiquement différents les uns des autres, ou par une diversité fonctionnelle dans laquelle des systèmes similaires réalisent l'objectif spécifié de manière différente

[CEI 60880:2006, définition 3.14]

NOTE Cette définition est plus large que celle utilisée dans l'AIEA NS-G-1.3 donnée ci-après: "Présence d'au moins deux systèmes ou composants, pour accomplir une fonction déterminée, lorsque ces différents systèmes ou composants ont des attributs différents de façon à réduire la possibilité de défaillance de mode commun". [CEI 61226:2005, définition 3.5]

3.4
microprogramme
logiciel étroitement dépendant des caractéristiques du matériel sur lequel celui ci est installé. La présence de microprogramme est généralement « transparente » pour l'utilisateur du composant matériel et ainsi il peut être effectivement considéré comme faisant partie intégrante de la conception du matériel (un bon exemple est le microcode d'un processeur). Généralement, le microprogramme ne peut être modifié par un utilisateur qu'en remplaçant le composant matériel (par exemple puce du processeur, carte, EPROM) qui contient ce logiciel par des composants contenant le logiciel modifié, et lorsque c'est le cas, il convient que la gestion de configuration des composants matériels assure la gestion de configuration des microprogrammes. Le microprogramme, tel que considéré dans cette norme, est effectivement du logiciel embarqué sur le matériel

3.5
AMDE
analyse des modes de défaillances et de leurs effets

3.6
AAD
analyse des arbres de défaillances

3.7
CNP
centrale nucléaire de puissance

3.8
prédéveloppé
composant qui existe déjà, qui est un produit commercial ou propriétaire, et qui a été choisi pour être utilise dans un système informatisé

NOTE Cette définition est cohérente avec la définition de logiciel prédéveloppé de la CEI 61513:2001.

3.9
durée de vie qualifiée
période de temps pendant laquelle il a été démontré par essai, analyse ou expérience, qu'une structure, un système ou un composant est capable de fonctionner conformément à ses critères d'acceptation en présence de conditions opérationnelles spécifiques tout en maintenant son aptitude à réaliser ses fonctions de sûreté lors d'accidents de dimensionnement ou de séismes

[Glossaire de sûreté AIEA:2006]

3.10

défaillance matériel détectée
défaillance matériel qui est détectée automatiquement et qui est signalée, par exemple la défaillance d'une carte lorsque le circuit de chien de garde détecte automatiquement la défaillance et émet une alarme.

3.11
système lié à la sûreté
système important pour la sûreté qui ne fait pas partie d'un système de sûreté

[Glossaire de sûreté AIEA:2006]

3.12
système de sûreté
système important pour la sûreté, mis en oeuvre pour garantir un arrêt sûr du réacteur ou l'évacuation de la chaleur résiduelle du cœur, ou pour limiter les conséquences d'un incident prévu d'exploitation ou d'un accident de dimensionnement

[Glossaire de sûreté AIEA:2006]

3.13
défaillance unique
défaillance résultant de la perte de capacité d'un système ou d'un composant, à réaliser sa (ses) fonction(s) prévue(s) et toutes les défaillances consécutives qui en résultent

[Glossaire de sûreté AIEA:2006]

3.14
critère de défaillance unique (CDU)
critère (ou exigence) appliqué à un système pour qu'il soit capable de réaliser sa tâche de sûreté en présence de toute défaillance unique

[Glossaire de sûreté AIEA:2006]

3.15
système important pour la sûreté
système qui fait partie d'un groupe de sûreté et/ou dont le mauvais fonctionnement ou la défaillance peut entraîner l'exposition aux rayonnements du personnel du site ou de membres du public

[Glossaire de sûreté AIEA:2006]

3.16
validation du système
confirmation par examen et apport d'autres éléments justificatifs qu'un système satisfait à la totalité des exigences spécifiées (fonctionnalités, temps de réponse, tolérance aux fautes, robustesse)

[CEI 60880:2006, définition 3.42]

3.17
défaillance matériel non détectée
défaillance matériel qui n'est pas automatiquement détectée par le système et qui peut seulement être mise en évidence lorsqu'on tente d'utiliser une fonction dépendant du matériel défaillant. De telles défaillances peuvent être découvertes par des essais fonctionnels, ou lorsqu'une demande relative à l'exploitation sollicite le système

3.18
vérification
confirmation par examen et apport d'éléments objectifs que les résultats d'une activité sont conformes aux objectifs et exigences établies pour cette activité (ISO 12207)

[CEI 62138:2004, définition 3.35]

4 Structure du projet

4.1 Généralités

Il convient qu'un projet mis en place pour réaliser un système informatisé important pour la sûreté soit divisé en phases. Il convient que chaque phase constitue en quelque sorte une entité, même si celle-ci dépend d'autres phases pour les entrées et qu'elle produise des sorties utilisées par d'autres phases. On considère que les différentes phases du projet forment ensemble un cycle de vie et de sûreté global (voir Article 5 de la CEI 61513 qui fournit les exigences applicables aux cycles de vie des systèmes). La CEI 61513 autorise le déroulement des phases en parallèle tant que l'intégrité du processus de développement n'est pas mis en péril.

Un plan d'assurance qualité doit être mis en œuvre dans le cadre du processus de développement du matériel.

4.2 Subdivision du projet

Les exigences générales suivantes définissent les exigences applicables au cycle de vie de développement du matériel des systèmes informatisés dans le cadre du domaine de cette norme.

a) Le cycle de vie de développement du matériel doit être compatible avec le cycle de vie global du système (Annexe A).

b) Chaque sous-phase du cycle de vie du développement du matériel doit être constituée d'activités bien définies et bien documentées.

c) Les composants matériel prédéveloppés (par exemple COTS) devant être intégrés lors de la conception doivent être vérifiés et testés de façon appropriée avant d'être utilisés.

d) Des moyens adaptés (par exemple lots de rechange, appareil d'essai et de maintenance, etc.) des locaux (par exemple laboratoires, ateliers, espace, etc.) doivent être prévus pour réaliser les tâches associées à chaque phase de développement.

e) Chaque phase de développement doit comprendre la production d'une documentation adaptée.

f) Chaque phase de développement doit se terminer en réalisant la vérification (voir Article 7).

g) A chaque activité de vérification on doit produire un rapport, susceptible d'être audité, indiquant les résultats obtenus et toutes les modifications de conception, conséquence de la vérification réalisée.

h) Chacun des travaux s'inscrivant dans le cadre des activités doit être programmé pour garantir que le temps nécessaire est prévu pour réaliser les activités suivantes:

   1) résolution de tous les problèmes d'interaction entre les phases de développement logiciel et matériel, nécessaire pour garantir la compatibilité logiciel/matériel du système;

2) production de la documentation et réalisation des activités de test, vérification et d'assurance qualité.

4.3 Assurance qualité

Le processus de conception et de développement doit satisfaire aux exigences applicables du guide AIEA 50-C/SG-Q (la conformité à l'ISO 9001 est une méthode acceptable pour satisfaire ces exigences). Un programme d'assurance qualité doit exister ou bien comme document(s) séparé(s) ou bien en tant que partie d'un document décrivant un programme d'assurance qualité global. Ce programme doit traiter de l'utilisation de matériel existant et du développement de matériel autant que nécessaire. Il convient d'inclure dans le plan d'assurance qualité toutes les activités qualité liées au matériel qui sont du ressort de l'exploitant de la tranche, du propriétaire, des contractants et des sous-contractants prenant part au processus de développement du matériel.

4.3.1 Le programme doit couvrir les phases suivantes, lorsque celles-ci sont pertinentes pour un système ou un développement:

a) conception et développement;

b) approvisionnement;

c) fabrication;

d) installation et mise en service;

e) exploitation et maintenance.

4.3.2 Le fait de s'intéresser à toutes les phases listées ci-dessus avant que le processus de conception ne commence ne constitue pas une exigence, par contre lorsque chaque phase débute un programme établissant les exigences applicables à cette phase doit être en place.

4.3.3 Il convient que le ou les programmes d'assurance qualité décrivent l'organisation, la gestion et la réalisation des activités liées à la qualité, ceci comprenant

a) la gestion de configuration de la documentation;

b) le processus de conception;

c) le processus d'approvisionnement des biens et des services;

d) la gestion de configuration des instructions de montage, des procédures, des schémas,

e) la gestion de configuration des matériaux et des composants utilisés pour fabriquer le matériel du système;

f) les activités de contrôle de la qualité, par exemple des inspections formelles;

g) le contrôle des matériels d'essai;

h) le contrôle de l'envoi, du stockage et de la manutention du matériel;

i) le processus d'essai;

j) la gestion des non-conformités détectées et la mise en oeuvre des actions correctives;

k) la procédure d'archivage des rapports d'assurance qualité;

l) les procédures d'audit interne.

5 Exigences applicables au matériel

5.1 Généralités

5.1.1 Les exigences applicables au matériel doivent être cohérentes avec les exigences relatives au système et former une partie des spécifications du système informatisé (voir Article 6 de la CEI 61513:2001). Les spécifications du système informatisé sont une description commune logiciel/matériel du système et définissent les objectifs de conception du système et des fonctions devant être réalisées par le système informatisé (des systèmes peuvent être développés pour une application particulière ou faire l'objet d'un développement

générique, par exemple le développement d'une plate-forme basé sur des exigences génériques qui ont été déclinées).

5.1.2 Les exigences relatives au matériel doivent être spécifiées dans les spécifications d'exigences matériel du système ou dans un document *ad hoc*.

5.1.3 La présentation des exigences matériel doit être conforme à des techniques ou à des méthodes dont le format n'altère pas leur lisibilité, par exemple il convient que les exigence matériel ne soient pas difficiles à comprendre.

5.1.4 Les exigences matériel fonctionnelles doivent être non ambiguës, testables et/ou vérifiables et pouvoir être satisfaites.

5.1.5 Il convient que les spécifications d'exigences du matériel fournissent une vue d'ensemble des exigences matériel, identifient les fonctions matériel importantes pour la sûreté nucléaire (néanmoins, si celles-ci sont assurées en combinaison avec le logiciel du système, il convient qu'elles soient définies dans les spécifications d'exigences du système), identifient les exigences de conception matériel, les exigences de fiabilité matériel et définissent les exigences de résistance du matériel à l'environnement d'ambiance.

5.1.6 Les exigences matériel relatives au système informatisé peuvent comprendre des exigences applicables au matériel en général aussi bien que des exigences particulières au matériel du système informatisé en question, par exemple le câblage, la préparation de la surface des locaux d'installation.

5.1.7 En général, il convient que les exigences fonctionnelles matériel décrivent ce qui doit être fait et non comment cela doit être fait. Cependant l'utilisation de composants/plateformes préexistants peut avoir à un certain niveau pour résultat une conception matériel ascendante, de bas en haut. Avant que de tels composants préexistants ne soient sélectionnés pour être utilisés, on doit réaliser une évaluation pour confirmer que les caractéristiques des performances du matériel (par exemple les modes de défaillance) sont cohérentes avec les exigences systèmes. Si des anomalies sont détectées alors elles doivent être traitées, ou en modifiant la conception matériel ou la conception système (tout en s'assurant que les exigences liées à la sûreté nucléaire ne sont pas remises en question).

5.2 Exigences fonctionnelles et de performances

5.2.1 Les exigences matériel fonctionnelles et de performance doivent être cohérentes avec les exigences fonctionnelles et de performances du système important pour la sûreté.

5.2.2 Les exigences matériel fonctionnelles et de performances, combinées aux exigences logiciel (autant que nécessaire pour couvrir toutes les exigences matériel) doivent être vérifiées par rapport aux exigences système.

5.2.3 Toutes les parties du système qui contiennent du logiciel doivent être évaluées conformément au 1.2 de cette norme.

a) Les exigences matériel fonctionnelles doivent au minimum comprendre, les définitions pour

   1) les objectifs assignés à l'ensemble du matériel du système informatisé et à chaque sous-système matériel;

   2) les nombres et les types de capteurs et d'actionneurs qui doivent être connectés sur le système informatisé;

   3) les nombres et les types d'appareils relatifs à l'interface homme/machine tels que les afficheurs, les imprimantes et les claviers.

b) Il convient que chaque composant ou sous-système livré par un fournisseur, qui doit être intégré dans le système, soit accompagné de ses spécifications de performances relatives

aux aspects liés à la sûreté. Si de telles spécifications ne sont pas fournies alors une analyse doit être réalisée pour déterminer les caractéristiques de conception matériel du composant de façon à pouvoir confirmer son aptitude à être employé.

c) Les exigences de performances matériel doivent contenir (cela est applicable à toute application particulière):

1) le taux d'acquisition de données demandé;
2) la capacité de traitement de données demandée;
3) la puissance de calcul demandée;
4) la fiabilité et la disponibilité demandées;
5) les interfaces de communication demandées (protocoles, vitesse de transmission);
6) les précisions demandées sur les conversions et les calculs;
7) la capacité d'élimination du bruit pour les signaux demandée;
8) les temps de réponse demandés;
9) les limitations concernant les dimensions physiques;
10) les contraintes spatiales (par exemple les longueurs des lignes de transmission de données);
11) les capacités en terme de pièces de rechange (le cas échéant);
12) les exigences relatives à qualification environnementale;
13) les exigences concernant l'alimentation électrique.

d) Toutes les contraintes imposées sur la conception matériel par les conceptions logiciel ou système doivent être notées.

5.3 Exigences de fiabilité/disponibilité

5.3.1 Les exigences de fiabilité/disponibilité matériel doivent être cohérentes avec les exigences de fiabilité globale du système. Elles doivent comprendre une description de tous les types de défaillances qui doivent être tolérées sans perte ou avec une dégradation définie de fonction. Il convient de donner des objectifs de fiabilité matériel.

NOTE La fiabilité matériel dans ce contexte s'intéressant aux défaillances matérielles aléatoires exclut toutes défaillances dues à des erreurs logiques de conception.

5.3.2 Le critère de défaillance unique du document AIEA NS-G-1.3 doit être satisfait par l'architecture d'ensemble du système d'IC de la centrale nucléaire, indépendamment des exigences de fiabilité/disponibilité (voir 3.6).

5.3.3 Il convient que les exigences matériel donnent des objectifs chiffrés pour les paramètres de fiabilité matériel (tels que le temps moyen entre défaillances (détectées), le temps moyens entre défaillances (non détectées), le temps moyen de réparation pour les défaillances détectées)). Il convient d'indiquer toutes les exigences de fiabilité devant être basées sur des analyses détaillées de la conception matériel (par exemple des analyses au niveau composants, cartes ou sous-unité) qui doivent être prises en compte pour étayer les résultats obtenus et annoncés en terme de fiabilité.

5.3.4 Les méthodes qui peuvent être utilisées pour analyser la fiabilité et les effets des défaillances sur le matériel du système comprennent

– les AAD, qui prennent en compte l'identification et l'analyse des facteurs qui ont eu pour conséquence ou qui ont contribué à l'apparition de l'événement indésirable défini (voir la CEI 61025 pour les recommandations concernant cette technique);
– les AMDE, qui identifient les défaillances qui ont des conséquences significatives ayant un impact sur les performances du système, par exemple la fiabilité, la sûreté, la disponibilité (voir la CEI 60812 pour les recommandations concernant cette technique).

Si nécessaire, une technique d'analyse adaptée doit être appliquée au matériel des systèmes de Classe 1 et de Classe 2 afin d'assurer qu'aucune défaillance matériel possible ne produise des effets inacceptables au niveau de la sûreté nucléaire.

5.3.5 On peut utiliser une technique telle que les AAD en la combinant avec des données connues de défaillance des composants pour calculer les valeurs caractérisant la fiabilité du matériel du système. On doit utiliser une telle approche pour analyser le matériel des systèmes de Classe 1 (voir la CEI 61513) à moins qu'un retour d'expérience suffisant ne soit disponible pour avoir l'assurance que les objectifs de fiabilité matériel seront atteints. Il convient aussi d'employer de telles techniques pour des systèmes de Classe 2, ou procédant d'une autre manière, une justification de la fiabilité requise peut être obtenue en se basant sur un raisonnement qualitatif (par exemple, qualité des composants, redondance matériel, retour d'expérience en exploitation, proportion des défaillances matériel détectées par rapport aux défaillances matériel non détectées, etc.) et ceci tout particulièrement si les exigences de fiabilité matériel ne sont pas très exigeantes.

5.3.6 On doit définir les stratégies et les dispositions à mettre en oeuvre qui permettent de garantir la fiabilité et la disponibilité du système informatisé sur l'ensemble de sa durée de vie. Ces mesures doivent apparaître dans la documentation en tant qu'exigences de maintenance. Ceci doit comprendre des exigences permettant de garantir que les activités de maintenance n'introduisent pas de défaut qui puissent conduire à des défaillances de cause commune. Les activités de maintenance sur les systèmes à voies multiples sont généralement considérées comme le moyen le plus susceptible d'introduire de tels défauts et donc ces systèmes doivent être conçus pour minimiser ces activités autant que faire se peut. Lorsque des activités de maintenance, pouvant introduire des défaillances de cause commune, sont nécessaires, les exigences de conception doivent spécifier comment le risque associé à de telles défaillances est minimisé.

5.3.7 Il convient que les exigences de maintenance couvrent (cela est applicable à chaque système particulier)

a) les exigences pour l'exploitation du système durant les activités de maintenance;

b) le remplacement des éléments consommables, par exemple filtre à air;

c) toutes les exigences relatives au remplacement de routine des sous-systèmes, des modules et/ou des composants;

d) le domaine de la revalidation matériel (par exemple les essais) nécessaires suite aux activités de maintenance matériel.

5.3.8 Cependant, étant donné qu'il convient que les spécifications d'exigences définissent le « quoi » plutot que le « comment », il peut ne pas être facile de définir les exigences de maintenance en détail lors de la phase de spécifications d'exigences du projet; dans ce cas il convient de terminer la définition de ces exigences lors d'une phase ultérieure du processus de développement.

5.4 Exigences relatives à la résistance aux conditions d'environnement

5.4.1 Les exigences relatives à la résistance du matériel aux conditions d'environnement doivent traiter des contraintes physiques, climatiques, sismiques, chimiques, électriques et des conditions radiologiques telles qu'elles peuvent survenir. Il convient d'y inclure toutes exigences particulières liées l'installation et la mise en service.

5.4.2 Le degré d'immunité aux interférences électromagnétiques doit être spécifié en fonction de l'environnement d'exploitation et testé conformément aux normes applicables, par exemple la CEI 61000. Potentiellement, l'environnement électromagnétique peut dépendre d'un grand nombre de sources d'interférences électriques, par exemple les contacteurs, les téléphones mobiles, les relais, les talkies-walkies, les décharges électrostatiques, la foudre, les défauts de terre.

5.4.3 Il convient de spécifier les niveaux de qualification électromagnétique par rapport à des estimations réalistes des conditions d'exploitation en prenant en compte les circonstances crédibles les plus pénalisantes.

5.4.4 Les exigences matériel doivent identifier tous les matériaux de construction interdits et toutes les exigences pour les matériaux et les types de processus de production particuliers à utiliser.

5.4.5 Si un processus de qualification matériel particulier est demandé alors il convient de le documenter dans les exigences matériel.

5.5 Exigences documentaires

Les exigences documentaires pour le matériel doivent faire partie des exigences documentaires du système informatisé (voir la CEI 61513). Il convient que la documentation produite comprenne (si nécessaire)

a) les documents de conception (composants matériel système, conception matériel des interfaces, etc.);

b) manuels opérateur;

c) manuels de maintenance.

6 Conception et développement

6.1 Généralités

Cet article est applicable au niveau conception et développement matériel système, sous-système et module.

6.1.1 Il convient que le processus de conception et de développement pour le nouveau matériel prenne en compte en entrée les spécifications d'exigences matériel. Il convient que le processus de développement comprenne plusieurs étapes de conception qui au final permettent de produire un matériel satisfaisant aux spécifications d'exigences matériel.

6.1.2 Le niveau d'activité de conception le plus général peut être appelé conception « préliminaire », cela comprend l'analyse des différentes solutions de conception de façon à définir l'architecture système en terme de sous-systèmes et de modules.

6.1.3 La conception préliminaire est généralement suivie d'une ou plusieurs étapes de conception détaillée. Les activités de conception détaillée doivent développer la conception préliminaire pour couvrir la conception détaillée des sous-systèmes, des modules et des composants de façon que la description de la conception matériel soit suffisamment aboutie pour pouvoir être mise en œuvre.

6.1.4 Des prototypes du matériel peuvent être réalisés, non seulement pour montrer le bon fonctionnement des modules matériel entre eux, mais aussi pour vérifier la compatibilité du matériel et du logiciel.

6.1.5 Des composants pré-développés (par exemple des COTS) peuvent être utilisés comme système matériel ou comme sous-ensemble de composants matériel. Les paragraphes de 6.2 à 6.7 traitent principalement du cas où un développement de matériel dédié est nécessaire; cependant, lorsque cela est justifié, des recommandations expliquant comment les exigences de ces paragraphes peuvent s'appliquer dans le cas de l'utilisation de prédéveloppés composants sont données.

6.2 Activités de conception

6.2.1 Les caractéristiques de performances du système dépendantes des performances du matériel doivent être prises en compte lors de la conception matériel, et il faut prouver ou par analyse ou par essai que la conception matériel satisfait ses exigences. De telles exigences peuvent concerner la précision de calcul, le temps de réponse, les exigences portant sur les capacités de résistance du matériel aux conditions d'environnement et sur l'alimentation électrique (pour les composants pré-existants les spécifications composant matériel doivent être vérifiées par rapport aux exigences matériel système pour garantir que les composants préexistants satisfassent aux exigences spécifiées ou aux performances matériel qui doivent être vérifiées par essai).

6.2.2 Toute non-conformité aux exigences matériel doit être traitée, ou en changeant la conception ou en modifiant les exigences (l'impact de toute modification doit être complètement évalué et documenté).

6.2.3 Les concepteurs matériel doivent identifier les essais qui sont nécessaires pour montrer que les performances requises sont atteintes. De tels essais peuvent être réalisés sur le matériel seul, ou bien réalisés lorsque le matériel est intégré avec le logiciel, par exemple comme une partie de la phase d'essai lors de l'intégration système.

6.2.4 Les concepteurs matériel doivent spécifier toutes les activités de maintenance nécessaires pour garantir que les exigences de fiabilité et de performances sont satisfaites tout au cours de la vie opérationnelle du matériel. Ceci peut comprendre des procédures d'essai opérationnel, d'étalonnage, de réparation, de remplacement périodique et de maintenance. Il convient de réaliser ces activités pour qu'on ait une confiance suffisante dans le bon fonctionnement du matériel et ainsi réduire au minimum les occurrences d'intervention humaine ou de réalisation de travaux sur le système, diminuant ainsi la probabilité de défauts (tels que de potentielles défaillances de cause commune) introduits par des activités de maintenance

6.2.5 Lorsque des objectifs de durée de vie qualifiée sont indiqués des justifications doivent montrer que ces objectifs sont réalistes et peuvent être atteints.

6.3 Fiabilité

6.3.1 Il convient de spécifier les exigences de fiabilité dans la documentation des exigences matériel (voir 5.3).

6.3.2 Lorsqu'elle est nécessaire pour appuyer l'analyse de sûreté de niveau système, une analyse des défaillances matériel potentielles doit être réalisée lors de la conception. Lorsque des systèmes à voies multiples ou de multiples systèmes (sur chacun desquels on peut avoir un ou des voies matériel) sont utilisés pour réaliser une fonction de sûreté nucléaire alors on doit prendre en compte dans cette analyse les défaillances de cause commune matériel potentielles. Les causes possibles d'introduction de défaillances de cause commune liées au matériel sont les suivantes:

– activités de maintenance réalisées simultanément ou séquentiellement sur des voies multiples d'un matériel (particulièrement lorsque ces activités peuvent introduire des pannes matériel);

– essais périodiques;

– défaillances matériel aléatoires non détectées simultanées sur des voies multiples d'un matériel qui affectent la ou les mêmes fonctions de sûreté nucléaire;

– erreur de conception cachée touchant des voies multiples de matériel et qui ne sont pas détectées par le processus de conception.

6.3.3 Les méthodes qui peuvent être utilisées pour analyser la fiabilité et les effets des défaillances sur le matériel du système comprennent les AAD et les AMDE (voir 5.3.4).

6.3.4 Il convient que la conception matériel minimise l'impact potentiel des facteurs suivants sur la sûreté nucléaire:

– activités de maintenance;
– défaillance de système due à une défaillance aléatoire matériel;
– défaillance matériel due à des conditions d'environnement.

6.3.5 Si on considère que la fiabilité matériel estimée n'est pas suffisante pour remplir un rôle particulier alors on doit prendre des mesures compensatrices. Ceci peut prendre la forme d'améliorations de conception ou de modifications liées à l'exploitation (telles que l'augmentation de la fréquence des essais opérationnels). Cependant, il convient de faire attention lorsqu'on choisit l'option d'augmenter les essais opérationnels, car toutes les activités intrusives sur l'installation en exploitation comporte un risque intrinsèque d'introduction directe ou indirecte d'erreur (par exemple l'effet d'ensemble réseau d'essais d'exploitation peut avoir un impact négatif sur la sûreté. De façon idéale, il convient de réaliser les essais lorsque les défauts potentiels du processus d'essai ne peuvent avoir d'impact sur la sûreté nucléaire, par exemple durant les arrêts de l'installation ou lorsque les matériels à essayer sont isolés de l'installation en fonctionnement.

6.3.6 Lorsqu'on réalise des évaluations probabilistes de sûreté en appui du rapport de sûreté de la CNP, les valeurs probabilistes évaluées de la fiabilité matériel (par exemple celles résultant d'une AAD) peuvent être utilisées dans l'analyse de la centrale et ainsi contribuer à la précision des calculs de fiabilité de l'installation dans son ensemble.

6.4 Maintenance

La conception matériel doit traiter de toutes les exigences spécifiques de maintenance provenant des spécifications d'exigences matériel. De plus, dans la mesure du possible, il convient que la conception intègre des dispositions pour réduire le risque d'introduction de panne durant les activités de maintenance, des exemples de disposition sont les suivants:

– il convient que les composants qui sont susceptibles d'être remplacés suite à une défaillance soient facilement accessibles;
– il convient que les composants remplaçables soit clairement identifiée pour que le personnel de maintenance puisse facilement vérifier que les composants utilisés sont les bons;
– il convient de prévoir un espacement suffisant des bornes;
– il convient de prévoir la mise à disposition de borniers d'essai pour réaliser les activités d'étalonnage ou d'essai (de façon que le câblage d'exploitation n'ait pas à être débranché pour faciliter la réalisation de ces activités);
– il convient que la conception matériel adopte un modèle structuré avec un étiquetage clair pour réduire le risque d'erreurs de maintenance.

6.5 Interfaces

Le paragraphe 6.1.1.2.1 de la CEI 61513:2001 fournit des exigences pour les interfaces du système qui vise à prévenir la propagation des défaillances par celles-ci.

6.6 Modifications

Conformément aux spécifications d'exigences matériel, le matériel doit pouvoir être modifié (voir Article 12).

6.7 Perte d'alimentation électrique

Conformément aux spécifications d'exigences matériel, le système informatisé doit être conçu pour être insensible aux conséquences des pertes d'alimentation électriques de courtes durée et aux variations de tension de l'alimentation électrique (tension/fréquence). Des dispositions système doivent être prises pour avertir les opérateurs et le personnel de maintenance de

telles fluctuations d'alimentation (ce rôle peut ne pas être assigné au matériel et ainsi se trouver hors du domaine de cette norme).

6.8 Sélection des composants

Lorsqu'on utilise des composants préexistants la conception de ceux-ci doit être compatible avec le rôle qu'ils doivent jouer dans le matériel du système.

6.9 Documentation de conception

6.9.1 La documentation de conception matériel doit décrire la conception matériel et les moyens par lesquels les exigences matériel ont été satisfaites. L'emploi d'un format standard pour la documentation de conception ainsi que d'outils de conception matériel automatique est recommandé.

6.9.2 Il convient de mettre en place une hiérarchie de documents de conception traitant du matériel du système informatisé constituée d'un certain nombre de « niveaux » documentaires. Il convient de spécifier pour chaque niveau de la documentation de conception les aspects de conception pertinents pour ce niveau et de définir les exigences matériel pour les niveaux inférieurs. Durant le processus de conception, on doit produire des documents pour la fabrication/assemblage, les recettes usine, l'installation, la mise en service, la maintenance et l'exploitation (lorsqu'ils sont nécessaires).

6.9.3 On peut produire une description préliminaire de la conception matériel définissant l'architecture matériel, par exemple la structure et les relations entre les différentes parties du système. Il convient d'y intégrer une représentation globale du matériel à l'aide de schémas de principe représentant les sous-systèmes et les modules de niveaux inférieurs. Il convient aussi d'y intégrer les exigences matériel pour la conception détaillée, telles que:

– le nombre et le type de processeurs principaux ou autres;
– les exigences matériel relatives à la mémoire informatique;
– le nombre et le type des interfaces;
– le nombre et le type de bus et de liaisons de données.

6.9.4 Au terme de la conception et du développement du matériel, la documentation doit être produite et comprendre une description complète finale qui contient les détails de la conception jusqu'au plus bas niveau, et qui couvre les fonctionnalités, les limitations et les autres caractéristiques du matériel.

6.9.5 Cette description finale contenue dans la documentation doit contenir les informations suivantes:

a) description générale de la conception;
b) références croisées relatives aux documents de conception;
c) une description de la structure du matériel en terme de sous-système matériel, chaque sous-système devant être décrit en terme de composants et modules principaux;
d) chaque sous-système en terme de modules et de composants principaux (sous forme de schéma de principe et de schéma filaire);
e) une description des interfaces matériel des sous-systèmes. Les interfaces doivent être décrites de façon appropriée logiquement, physiquement, électriquement ou en d'autres termes;
f) une description des interfaces du matériel du système informatisé. Les interfaces avec tous les autres systèmes qu'ils soient dans ou dehors de la centrale, doivent être identifiées et les exigences liées au matériel et spécifiques aux interface doivent être indiquées;
g) un plan physique. Une description à base de diagrammes de la configuration physique du matériel doit être fournie;