IEC 61226

Edition 3.0 2009-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 IEC, Geneva, Switzerland

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

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

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 It also gives information on projects, withdrawn and replaced publications.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 61226

Edition 3.0 2009-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

V

ICS 27.120.20

ISBN 2-8318-1052-1

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

FOREWORD 3
INTRODUCTION 5
1 Scope 8
2 Normative references 8
3 Terms and definitions 9
4 Abbreviations 13
5 Classification scheme 13
5.1 General 13
5.2 Background 14
5.3 Description of categories 14
5.3.1 General 14
5.3.2 Category A 15
5.3.3 Category B 15
5.3.4 Category C 15
5.4 Assignment criteria 16
5.4.1 General 16
5.4.2 Category A 16
5.4.3 Category B 16
5.4.4 Category C 17
6 Classification procedure 17
6.1 General 17
6.2 Identification of design basis 18
6.3 Identification and classification of functions 18
7 Assignment of technical requirements to categories 21
7.1 General requirements 21
7.2 Requirements related to functions 21
7.2.1 Basic requirements 21
7.2.2 Specific requirements 22
7.3 Requirements related to I&C systems 22
7.3.1 Basic requirements 22
7.3.2 Specific requirements 23
7.4 Requirements related to equipment 25
7.4.1 Basic requirements 25
7.4.2 Specific requirements 25
7.5 Requirements related to quality aspects 26
7.5.1 Basic requirements 26
7.5.2 Specific requirements 26
Annex A (informative) Examples of categories 30
Bibliography 32

Figure 1 – Method of classification 20

Table 1 – Tabular correlation between categories and other IEC standards 29

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – CLASSIFICATION OF INSTRUMENTATION AND CONTROL FUNCTIONS

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 61226 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This third edition cancels and replaces the second edition published in 2005 and constitutes a technical revision. The main changes with respect to the previous edition are listed below:

- to introduce a definition for "non-hazardous stable state";
- to clarify limits of categories;
- to clarify requirements related to equipment used for beyond design events.

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

FDIS	Report on voting
45A/745/FDIS	45A/767/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 organisation of the standard

This International Standard responds to an International Atomic Energy Agency (IAEA) requirement[1] to classify nuclear power plants instrumentation and control systems according to their importance to safety. With distributed computer based I&C systems now being used for NPP instrumentation and control systems, the functions important to safety are distributed over several systems or subsystems. Therefore, it is the intent of this standard to

– classify the I&C functions important to safety into categories, depending on their contribution to the prevention and mitigation of postulated initiating events (PIE), and to develop requirements that are consistent with the importance to safety of each of the categories;
– assign specification and design requirements to I&C systems and equipment concerned which perform the classified functions.

According to IAEA recommendation,[2] the methods of classification are primarily based on the deterministic safety analysis, and should be complemented where appropriate by probabilistic methods. Several possible approaches for use of probabilistic safety assessment (PSA) for classification are described in IEC/TR 61838, “Nuclear power plants – Instrumentation and control important to safety – Use of probabilistic safety assessment for the classification of functions”.

This revision of the standard enables quantitative assessment to be partly taken into account.

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

IEC 61226 is directly referenced by IEC 61513 and is the second level SC 45A document tackling the issue of categorization of functions and classification of systems.

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

c) Recommendation and limitation regarding the application of this standard

Correct classification of functions directs the appropriate degree of attention by the plant's designers, operators and regulatory authorities to the specification, design, qualification, quality assurance (QA), manufacturing, installation, maintenance, and testing of the systems that ensure the safety functions.

---

1 IAEA NS-R-1 requirement 5.1.

2 The NS-R-1, section 5.2 requires that the method for classifying the safety significance of a structure, system or component shall be primarily based on deterministic methods complemented where appropriate by probabilistic methods and sound engineering judgment taking into account factors such as

a) the safety function(s) to be performed;

b) the consequences of failure to perform the function;

c) the probability that it (the I&C system) will be required to perform a safety function;

d) the time following a PIE at which, or the period throughout which it (the I&C system) will be called upon to operate.

This standard establishes the criteria and methods to be used to assign the I&C functions of a NPP to three categories A, B and C, which depend on the importance of the function for safety, and an unclassified category for functions with no direct safety role. It outlines generic requirements for each category, and specifies basic technical requirements for matters such as QA, reliability, testing and maintenance.

The category to which a function is assigned determines generic and specific technical requirements. Generic requirements for each function are based on providing the appropriate level of assurance that it will be executed on demand with the required performance and reliability level. This applies to the aspects of functionality, reliability, performance, environmental durability and QA. The level of assurance to be shown for each of these aspects must be consistent with the importance of the function to safety.

i) Assurance of functionality is established by the creation of a complete and comprehensive requirements specification, and the application of appropriate standards and codes.

ii) Assurance of reliability is provided by the selection of appropriate components, structures and levels of redundancy and diversity in association with physical separation and/or barriers, electrical isolation and periodic testing during service.

iii) Assurance of performance is gained by the creation of specifications of the required performance, the application of QA procedures, verification and validation processes during design and manufacture, pre-service testing of the individual and integrated systems and equipment, and testing during service.

iv) Assurance of environmental durability is established by equipment qualification programmes to ensure that ageing effects and environmental conditions that exist when the equipment is required to operate do not degrade its performance below that required.

v) Assurance that the aspects of functionality, performance, environmental durability and reliability have been properly considered at each stage from conception, through design, manufacture, test, installation, commissioning and entry into service is provided by carrying out each stage of the work under the control of an appropriate QA program.

Throughout this standard, the auxiliary "shall" indicates requirements that are mandatory for compliance with the standard, the auxiliary "should" indicates requirements that are not mandatory for compliance with the standard but are strongly recommended and the auxiliary "may" indicates requirements that are optional.

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

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 directly 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 directly 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 directly referenced 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 the technical reports which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety publications of IEC 61508 series 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, as well as to IAEA 50-C-QA (now replaced by IAEA GS-R-3) 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 NS-R-1, establishing safety requirements related to the design of nuclear power plants, and the safety guide NS-G-1.3 dealing with instrumentation and control systems important to safety in nuclear power plants. The terms and definitions used by SC 45A standards are consistent with those used by the IAEA.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – CLASSIFICATION OF INSTRUMENTATION AND CONTROL FUNCTIONS

1 Scope

This International Standard establishes a method of classification of the information and command functions for nuclear power plants, and the I&C systems and equipment that provide those functions, into categories that designate the importance to safety of the function. The resulting classification then determines relevant design criteria.

The design criteria are the measures of quality by which the adequacy of each function in relation to its importance to plant safety is ensured. In this standard, the criteria are those of functionality, reliability, performance, environmental durability (including seismic) and quality assurance (QA).

This standard is applicable to all the information and command functions and the instrumentation and control (I&C) systems and equipment that provide those functions. The functions, systems and equipment under consideration provide automated protection, closed or open loop control and information to the operating staff. They keep the NPP conditions inside the safe operating envelope and provide automatic actions, or enable manual actions, that prevent or mitigate accidents, or that prevent or minimize radioactive releases to the site or wider environment. The I&C functions that fulfil these roles safeguard the health and safety of the NPP operators and the public.

This standard follows the general principles given in IAEA safety code NS-R-1 and safety guide NS-G-1.3, and it defines a structured method of applying the guidance contained in those codes and standards to the I&C systems that perform functions important to safety in a NPP. This standard should be read in association with the IAEA guides and IEC 61513 in implementing the requirements of IEC 61508 series.

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 60671:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 60709, *Nuclear power plants – Instrumentation and control systems important to safety – Separation*

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

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

IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 60964, *Nuclear power plants – Control rooms – Design*

IEC 60965, *Supplementary control points for reactor shutdown without access to the main control room*

IEC 60980, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 60987, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*

IEC 61000-4 (all parts), *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

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

IEC 61771, *Nuclear power plants – Main control room – Verification and validation of design*

IEC 61772, *Nuclear power plants – Main control room – Application of visual display units (VDU)*

IEC 61839, *Nuclear power plants – Design of control rooms – Functional analysis and assignment*

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

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

IAEA GS-R-3:2006, *The management system for facilities and activities* (available in English only)

IAEA NS-G-1.3:2002, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

3 Terms and definitions

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

3.1
anticipated operational occurrence
operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety nor lead to accident conditions

[IAEA Safety Glossary:2007]

3.2
common cause failure
CCF
failure of two or more structures, systems or components due to a single specific event or cause

[IAEA Safety Glossary:2007]

3.3
design basis accident
DBA
accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits

[IAEA Safety Glossary:2007]

3.4
design basis event
DBE
group of design basis accidents and anticipated operational occurrences

NOTE See also 3.13.

3.5
diversity
presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure

[IAEA Safety Glossary:2007]

NOTE The following definition was given in 3.5 of IEC 60880 for the term "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*. It is totally consistent with the IAEA definition given here.

3.6
equipment
one or more parts of a system. An item of equipment is a single definable (and usually removable) element or part of a system

[IEC 61513, 3.17, modified]

3.7
function
specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it

3.8
functionality
attribute of a function which defines the operations which transform input information into output information

[IEC 61513, 3.25]

3.9
human factor engineering programme
programme that describes at least the human factors organisation, role and mission of human factors specialists and team, human factors activities and their integration in the design and validation process, list of deliverables to be provided at each step of the program

3.10
item important to safety
item 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.

Items important to safety include:

a) those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of the site personnel or members of the public;

b) those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions;

c) those features which are provided to mitigate the consequences of malfunction or failure of structures, systems or components.

[IAEA Safety Glossary: 2007]

NOTE Items important to safety considered in this standard are mainly I&C systems important to safety.

3.11
non-hazardous stable state
state of the plant, where stabilisation of any transient has been achieved, the reactor is subcritical, adequate heat removal is ensured and radioactive releases are limited

NOTE A transient is considered to be stabilised when, for all safety significant parameters, the margins (e.g. between the heat removal capacity and heat generation) are either stable or increasing, or sufficient margin remains to cover all expected physical processes.

3.12
performance
effectiveness with which an intended function is carried out (e.g. time response, accuracy, sensitivity to parameter changes)

3.13
plant states

<table>
<tr><td colspan="2">Operational states</td><td colspan="4">Accident conditions</td></tr>
<tr><td rowspan="2">Normal operation</td><td colspan="3">Design basis events</td><td colspan="2" rowspan="2">Beyond design basis accidents</td></tr>
<tr><td>Anticipated operational occurrences</td><td>a)</td><td>Design basis accidents</td></tr>
<tr><td></td><td></td><td></td><td></td><td>b)</td><td>Severe accidents</td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="2">Accident management</td></tr>
</table>

a) Accident conditions which are not explicitly considered design basis accidents but which are encompassed by them.

b) Beyond design basis accidents without significant core degradation.

NOTE This definition is consistent with the one of the IAEA safety glossary. It just indicates the position of the concept of “design basis event” compared to the other concepts.

3.14
postulated initiating event
PIE
event identified during design as capable of leading to anticipated operational occurrences or accident conditions

[IAEA Safety Glossary:2007]

3.15
redundancy
provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other

[IAEA Safety Glossary:2007]

3.16
safety group
assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded

[IAEA Safety Glossary:2007]

3.17
safety related system
a system important to safety that is not part of a safety system

[IAEA Safety Glossary:2007]

3.18
safety system
a system important to safety, provided to ensure the safe shutdown of the reactor and the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accident

[IAEA Safety Glossary:2007]

3.19
single failure
a 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:2007]

3.20
system
set of components which interact according to a design, where an element of a system can be another system, called a subsystem

[IEC 61513, 3.61]

3.21
type test
conformity test made on one or more items representative of the production

[IEV 394-40-02]

3.22
unacceptable consequence
consequence of an operational state or of a PIE, that exceeds specified limits for the corresponding plant states, in terms of releases at the site or to the wider environment

NOTE Additional limits, such as unacceptable fuel damage, or damage to other main components may also be specified on a national basis. This might be either a massive, uncontrolled release caused by events with a frequency that is beyond the NPP's design basis, or events with a frequency that is in the design basis but leading to a magnitude exceeding specified limits. Additional limits, such as unacceptable fuel damage may also be specified. This might be damage to the fuel cladding that leads to an unacceptable increase in the activity of the primary coolant, or structural damage to the fuel that impairs the ability to cool it. Damage to the other barriers may also be considered as unacceptable consequence.

4 Abbreviations

ALARA	As low as reasonably achievable
DBA	Design basis accident
DBE	Design basis event
FAT	Factory acceptance test
FMEA	Failure modes and effects analysis
HMI	Human machine interface
IAEA	International Atomic Energy Agency
I&C	Instrumentation and control
NPP	Nuclear power plant
PIE	Postulated initiating event
PRA	Probabilistic risk assessment
QA	Quality assurance
SAT	Site acceptance test

5 Classification scheme

5.1 General

Functions to be performed by I&C systems shall be assigned to categories according to their importance to safety. The importance to safety of a function shall be identified by means of the consequences in the event of its failure when it is required to be performed and the consequences in the event of a spurious actuation. The category determines the design and quality requirements for I&C systems and equipment. These requirements shall be defined independently from the technology of the equipment to be applied. Subclause 5.2 provides the background to the classification scheme.

Subclause 5.3 describes the three categories that are used to classify functions. The categories are based upon those defined originally in the first edition of IEC 61226 published in 1993.

Subclause 5.4 presents the assignment criteria for each category.

Clause 6 provides guidance on the classification process.

Clause 7 provides the technical requirements for each of the three categories. Most of the requirements apply to the systems and equipment that perform the functions, but some requirements apply only to the functions.

Annex A contains typical examples of the classification of NPP I&C functions. It is only for information because it may depend on the reactor type.

5.2 Background

The principle of defence in depth is firmly established in the safety design basis of nuclear power plants. The fundamental idea is that there should be several layers or echelons of defence in the prevention of unsafe conditions, and that the prevention of unsafe conditions, before mitigation is required, is always to be preferred. Because of the large number of functions that are required to operate and keep safe a NPP, a number that increases with the principle of defence in depth, it is important that the significance to safety of each function is known.

IAEA safety standard series NS-R-1 establishes the idea of classification of NPP systems according to their importance to safety, and gives examples of the classification of the major systems of several types of NPP. All structures, systems and components, including software for instrumentation and control (I&C), that are items important to safety, shall be first identified and then classified on the basis of their function and significance with regard to safety. They shall be designed, constructed and maintained such that their quality and reliability is commensurate with this classification.

The IAEA safety guide NS-G-1.3 gives guidance on the classification of systems according to the importance to safety of the functions they perform. It introduces time factors such as

– the duration that the I&C system is needed once it has been initiated;
– the time for which alternative actions can be taken;
– the timeliness by which hidden faults can be detected and remedied.

This standard extends the classification strategy presented in IAEA Safety Guide NS-G-1.3, and establishes the criteria and methods to be used to assign the I&C functions of a NPP to one of the three categories A, B and C, depending on their importance to safety, or to an unclassified category for functions with no direct safety role. I&C functions falling within the boundary of the safety systems will generally be assigned to category A or B. I&C functions defined as safety related will generally be assigned to categories B or C.

The safety importance of, and the corresponding requirements placed on, parts of the safety systems and safety related I&C systems will differ, so that it is appropriate to assign them to different safety classes. Some I&C systems can have a significant effect on safety and therefore require appropriate attention. Other I&C systems have intermediate, low, or no significance to safety. They have correspondingly less stringent requirements for ensuring system performance and safety justification, and therefore have different technical requirements.

National application of the principles and criteria of this standard may assign differing nomenclature to categories A, B and C. The national application shall be according to the principles, criteria and associated requirements given in this standard. This shall involve establishing and documenting an appropriate correspondence to the categories defined.

5.3 Description of categories

5.3.1 General

I&C systems in NPPs perform functions with different levels of importance to safety. The importance to safety of each I&C function depends upon its role in achieving and maintaining safety, the potential consequence of failure of the function to operate when required, and the probability of these consequences. Therefore, an initial safety analysis of the specific NPP design is required to be completed prior to the classification of the I&C functions. The severity of the potential consequences in the case of a postulated failure of an I&C function, defines the level of assurance that is required for the various attributes of the systems and equipment which deliver the function, most notably that of functionality, performance and reliability.

For the design, assessment and licensing procedures, safety categories A, B and C are defined, with associated sets of technical and quality requirements on the properties of the I&C systems to be applied for the design and implementation of I&C systems and equipment important to safety.

5.3.2 Category A

Category A denotes the functions that play a principal role in the achievement or maintenance of NPP safety to prevent DBE from leading to unacceptable consequences. This role is essential at the beginning of the transient when no alternative actions can be taken, even if hidden faults can be detected. These functions play a principal role in the achievement or maintenance of the non-hazardous stable state[3]. If specified manual actions are provided to reach the non-hazardous stable state, factors such as the availability of redundant, validated, information sources, sufficient duration of the grace time for operator evaluation of alternative sources of information, and whether the manual actions are the only possibility for mitigation of this sequence of events to preserve NPP safety, have to be considered.

Category A also denotes functions whose failure could directly lead to accident conditions which may cause unacceptable consequences if not mitigated by other category A functions. Category A functions have high reliability requirements. Consequently, it may be necessary to limit their functionality and complexity.

5.3.3 Category B

Category B denotes functions that play a complementary role to the category A functions in the achievement or maintenance of NPP safety, especially the functions required to operate after the non-hazardous stable state has been achieved, to prevent design basis events (DBE) from leading to unacceptable consequences, or mitigate the consequences of DBE. The operation of a category B function may avoid the need to initiate a category A function. Category B functions may improve or complement the execution of a category A function in mitigating the consequences of a DBE, so that plant or equipment damage or activity release may be avoided or minimised.

Category B also denotes functions whose failure could initiate a DBE or worsen the severity of a DBE. Because of the presence of a category A function to provide the ultimate prevention of or mitigation of the consequences of a DBE, the safety requirements for the category B function need not be as high as those for the category A function. This allows, if necessary, the category B functions to be of higher functionality than category A functions in their method of detecting a need to act or in their subsequent actions.

5.3.4 Category C

Category C denotes functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety. Category C includes functions that have some safety significance, but are not category A or B. They can be part of the total response to DBA but not be directly involved in mitigating the physical consequences of the accident, or be functions necessary for beyond design basis accidents.

---

[3] In order to cope with rapid transients, the plant is controlled during this phase by automatic actions. For slower transients, stable conditions can be obtained using manual actions, provided such actions are considered after a grace time. This type of grace time represents a design requirement of the plant corresponding to a delay of diagnosis and action, and based on human factors considerations. It does not mean that manual actions are not permitted during that time. In some countries, and for older plants, the limit of category A may be this grace time, in place of the non-hazardous stable state.

5.4 Assignment criteria

5.4.1 General

The criteria that shall be applied for assignment of functions to categories A, B and C are given below.

If a function does not meet any of the criteria given below, then it shall be "non-classified" (NC).

In the case of multiple assignment, the final assignment of a function to a category shall be the highest relevant category.

The final assignment of the function may be modified using probabilistic methods in consistency with the principles outlined in 6.3.

5.4.2 Category A

An I&C function shall be assigned to category A if it meets any of the following criteria:

a) functions required to reach the non-hazardous stable state, to prevent a DBE from leading to unacceptable consequences, or to mitigate its consequences;

b) functions, the failure or spurious actuation of which would lead to unacceptable consequences, and for which no other category A function exists that prevents the unacceptable consequences;

c) functions required to provide information and control capabilities that allow specified manual actions necessary to reach the non-hazardous stable state.

5.4.3 Category B

An I&C function shall be assigned to category B if it meets any of the following criteria and is not otherwise assigned to category A:

a) functions required after the non-hazardous stable state of a DBE has been reached, to prevent it from leading to unacceptable consequences, or to mitigate the consequences;

b) functions required to provide information or control capabilities that allow specified manual actions necessary after the non-hazardous stable state has been reached to prevent a DBE from leading to unacceptable consequences, or mitigate the consequences;

c) functions, the failure of which during normal operation, would require the operation of a category A function to prevent an accident whose study is required;

d) functions to reduce considerably the frequency of a DBE as claimed in the safety analysis;

e) plant process control functions operating so that the main process variables are maintained within the limits assumed in the safety analysis, if these control functions are the only means of control of these variables. If different means are provided, clause 5.4.4 a) may apply;

f) functions used to prevent or mitigate a radioactive release or fuel degradation outside of the limits and conditions of normal operation as defined in the safety analysis;

NOTE 1 This refers to functions that are not already covered by the analysis of DBE leading to category A classification.

g) functions that provide continuous or intermittent tests or monitoring of functions in category A to indicate their continued availability for operation and alert control room staff to their failures, if no alternative means (e.g. periodic tests) are provided to verify their availability[4].

NOTE 2 Where the monitoring function is the only means of detecting otherwise unrevealed failures, then assigning the function to category B ensures that the equipment providing the function is suitably qualified.

5.4.4 Category C

An I&C function shall be assigned to category C if it meets any of the following criteria and is not otherwise assigned to category A or category B:

a) plant process control functions operating so that the main process variables are maintained within the limits assumed in the safety analysis not covered by 5.4.3 e). In case a combination of category C functions is used, a justification of sufficiency shall be provided;

NOTE 1 According to national practices a possible acceptable application of clause 5.4.4 a) is the combination of a regulation function and suitable manual actuation based on independent alarms including a justification of the use of manual action.

b) functions used to prevent or mitigate a minor radioactive release, or minor degradation of fuel, within the NPP design basis;

NOTE 2 A minor release or minor fuel degradation is considered to be that which falls within the normal limits and conditions of operation (e.g. discharge limits).

c) functions that provide continuous or intermittent tests or monitoring of functions in category A and B to indicate their continued availability for operation and alert control room staff to their failures, and are not classified category B according to 5.4.3 g);

d) functions necessary to reach the safety probabilistic goals including those to reduce the expected frequency of a DBE;

e) functions to reduce the demands on a category A function, as claimed in the safety analysis;

f) functions to monitor and take mitigating action following internal hazards within the NPP design basis (e.g. fire, flood);

g) functions to warn personnel or to ensure personnel safety during or following events that involve or result in release of radioactivity in the NPP, or risk of radiation exposure;

h) functions to monitor and take mitigating action following natural events (e.g. seismic disturbance, extreme wind);

i) functions provided for the benefit of the accident management strategy to reach and maintain a safe state for beyond design accidents;

j) functions provided to minimise the consequences of severe accidents;

k) functions which provide access control for the NPP.

6 Classification procedure

6.1 General

An outline of the procedure is shown in Figure 1.

---

4 Subclause 4.2.6 of IEC 60671 provides further guidance on the class of equipment used to implement such functions and in particular notes that where: “test features could interfere in an inappropriate manner with the proper operation of the system or equipment performing the function important to safety, it shall be assigned to the same category”

6.2 Identification of design basis

A main input to the classification process of functions is the nature of the NPP and the reactor type (e.g. PWR (pressurized water reactor), BWR (boiling water reactor) or other reactor type), the associated PIEs, and the major design criteria on redundancy of mechanical and electrical systems and equipment. Another main input is the identification of the major mitigation functions, and their supporting functions, for each PIE.

The assessment of the frequency and consequences of PIEs leads to the identification of DBEs representing the design base of the plant. When considering the design features of the plant the specified ranges of operational states and accident conditions and the defined radiological limits have to be reflected. Individual safety principles that together make up an "integrated overall safety approach" ensure the safety of a NPP. These principles are used in the design by considering the identified DBEs and successive physical barriers to keep radioactive exposure within permitted limits. The DBEs and the major design criteria (redundancy, separation, etc) of the plant, as well as the identification of the prevention and mitigation functions, and their supporting functions are the main input to the classification process.

The importance to safety of each I&C function depends upon the role for achieving and maintaining the NPP safety and the potential consequence of failure of the function to operate when required. Therefore, an initial safety analysis of the specific NPP design is required to be completed prior to the classification of the I&C functions.

6.3 Identification and classification of functions

At an early stage in the design of the NPP, the safety relevant functions shall be identified. The process of identifying these functions and assigning them to the I&C function or to the human operators should be carried out according to IEC 60964. Following this initial identification of a function, a category for each function shall be assigned according to the criteria of Clause 5.

The method for classifying the safety significance of function shall primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment, with account taken of factors such as:

- the safety function(s) to be performed;
- the role of the function in preventing or mitigating postulated initiating events;
- the role of the function during all operating modes (e.g. start-up, normal operation, refuelling, etc);
- the role of the function following PIEs such as natural events (e.g. seismic disturbance, flood, extreme wind, lightning) and internal hazards (e.g. fire, internal flood, missiles, radioactive release from adjacent unit or chemical releases from other plants or industries);
- the consequences of failure of the I&C functions;
- the effects of spurious actuation of the I&C functions;
- the probability that it will be required to perform a function important to safety;
- the time following a DBE at which, or during which it will be required to operate;
- the maintenance, repair and testing strategy.

It will not be possible to identify in detail all the functions at an early stage in the design process, as the characteristics of the NPP will not then have been defined fully. The process of identification and classification of the functions must therefore continue iteratively throughout the design phase. Where an initial assignment of a function to a category is uncertain, then an explanatory note should be added to the categorisation.

Since individual functions may be involved in the implementation of several aspects of the requirements specification, such functions may be assigned to several categories. In that case, the highest category assigned shall be applied.

As the redundancy, diversity and other technical requirements of the functions are determined more exactly, for example after the safety analysis progresses and the operating procedures are developed, the classification list shall be refined and revised, to derive a final list. This list shall be documented and maintained under configuration control since it will be required by plant/I&C designers during the life of the NPP. Also, this list may be required by the regulatory authorities.

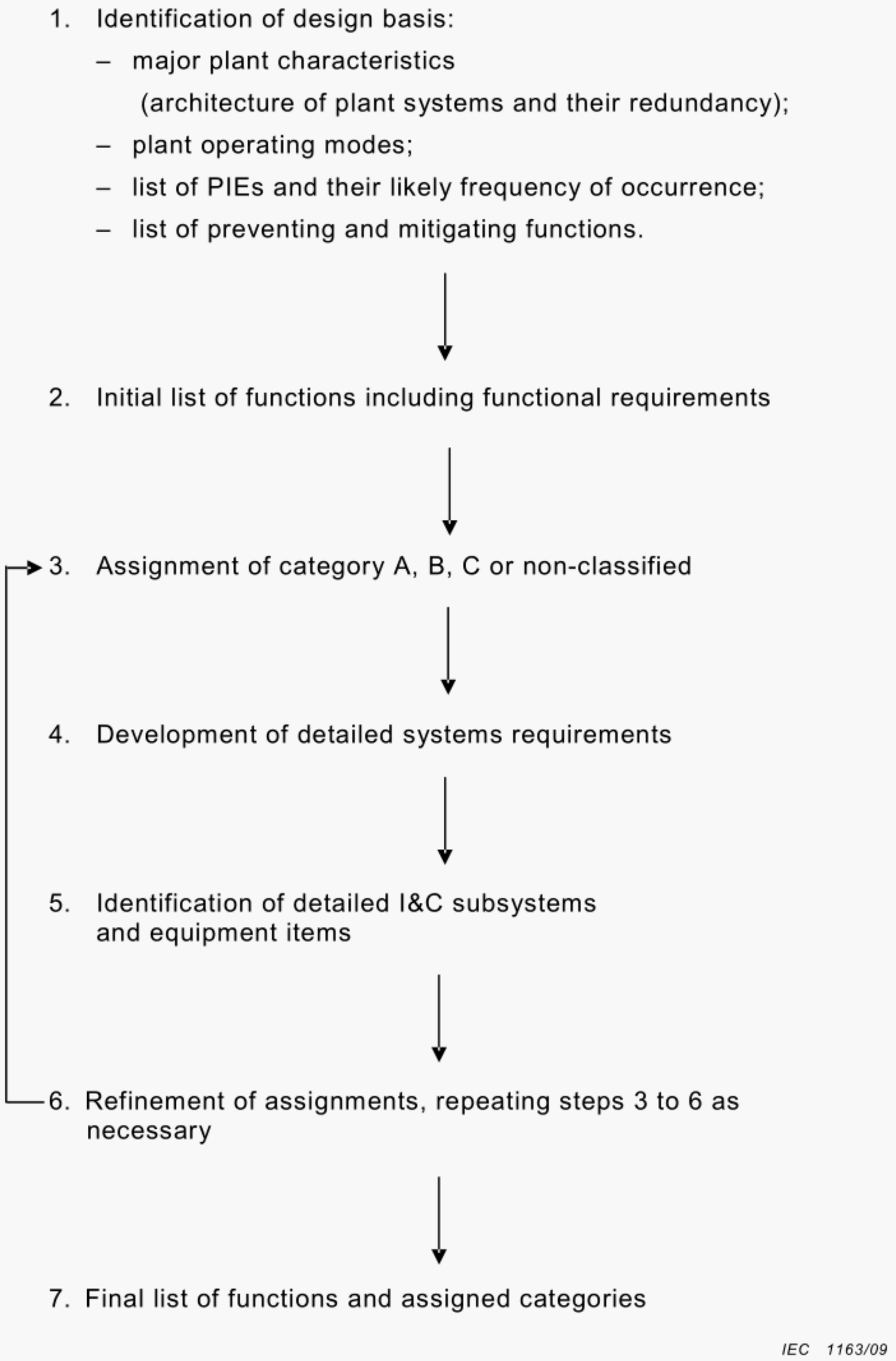

Figure 1 – Method of classification

7 Assignment of technical requirements to categories

7.1 General requirements

Technical requirements for each of the categories A, B and C are given in this clause. The requirements shall be applied to the specification, design, validation, qualification, manufacturing, installation, operation and maintenance phases of the I&C lifecycle as appropriate. The technical requirements constitute four groups:

– requirements that apply to the functions concerning the specification and validation of functionality, performance and reliability;
– requirements that apply to the design of I&C systems related to design characteristics such as redundancy, diversity, testability and separation. These characteristics determine primarily the reliability of the associated functions. The requirements also include HMI requirements;
– requirements concerning the equipment features for the assurance of seismic and environmental durability and electro-magnetic compatibility;
– requirements that are associated with the quality assurance, verification and maintenance which apply to functions, systems and equipment.

In most cases, these requirements are already detailed in appropriate codes and standards. The codes, guides and standards listed in Clause 2 of this standard are normative references and therefore provide the explicit requirements related to the I&C safety categories which are established by this standard. The correlation between the categories and the standards that shall be applied is summarised in Table 1. The detailed requirements from these standards are not repeated in this standard. The same table summarises the main types of requirements for each category. In the text below, some additional details are given.

Wherever possible, equipment with a documented, proven history of reliable operation in nuclear or other industrial applications should be used.

7.2 Requirements related to functions

7.2.1 Basic requirements

The basic requirement for assurance of functionality is the existence of a clear, comprehensive and unambiguous set of functional requirements and design specifications against which the functions shall be checked during design, manufacture, installation, and service, and shall be used as a reference for any in-service modifications.

The reliability required from any function in categories A, B or C should be determined by either a quantitative probabilistic assessment of the NPP, or by qualitative engineering judgement, and included in the specification. The performance required from any function in categories A, B or C shall be determined by appropriate analyses, and included in the specification. These analyses shall be carried out in a structured way following a set of approved procedures, and shall be documented.

Although the reliability requirements of functions in different categories may be the same, the level of assurance that the function will achieve the specified reliability will be different for the three categories, with category A requiring the highest assurance.

There shall be adequate separation between the functions of different categories.

7.2.2 Specific requirements

7.2.2.1 Category A

The design shall be according to the requirements of recognized codes, guides and standards that are appropriate to the high level of assurance of functionality required for category A functions. The design shall aim to ease verification and validation of the final functionality by maintaining simplicity. This should result in the avoidance of unrelated lower category functions being implemented in category A systems (for example, special display calculations and translation of communication protocols should not be carried out by safety system software).

The reliability requirements for category A I&C functions shall be specified as indicated in 7.1. This shall be carried out by establishing the reliability requirements for the functions needed to achieve an acceptably low risk of unacceptable consequences, and then by determining from this the reliability requirements for the I&C functions.

7.2.2.2 Category B

The design process shall be carried out following appropriate recognized codes, guides and standards, or systems and equipment with a documented history of satisfactory operation in a similar application may be used.

7.2.2.3 Category C

The design should be examined to verify that the systems and equipment have been designed or tested to provide the specified functions under the full range of specified operating conditions, including the most adverse anticipated operational conditions or occurrences under which the function is required.

7.3 Requirements related to I&C systems

7.3.1 Basic requirements

Requirements for the system design shall ensure that the function will achieve the specified reliability. The basic requirements for assuring high reliability concern the provision of appropriate redundancy, diversity and spatial, physical and electrical separation, and effective HMI. For all systems, means of fault detection and repair shall be considered during design and subsequent modifications.

The assessments of reliability and availability shall take into account repair periods, testing and maintenance periods and the potential for both self-revealed and non-self-revealed failure. The assumptions made in the reliability analysis with respect to maintenance, testing, and repair periods shall be verified during operation and corrective action shall be taken if discrepancies are identified.

Specific requirements concerning human factor and HMI shall be included in the design process. These requirements should be the product of a human factor engineering program, implemented from the earliest stages of the design phase.

The design of the system shall allow on-line and/or periodic testing during operation to demonstrate that performance is maintained. Requirements on periodic tests and maintenance activities to ensure the long-term reliability of I&C systems important to safety are defined in 7.5.

Sufficient information and control equipment shall be located, preferably at a single location that is physically and electrically separated from the main control room so that the reactor can be placed and maintained in a safe shutdown state, with essential plant variables monitored when there would be a loss of ability to perform these functions in the main control room.

7.3.2 Specific requirements

7.3.2.1 Category A

An I&C system performing category A functions shall have redundancy. Appropriate separation shall be applied to ensure that any single internal hazard cannot disable redundant parts of the system. A single failure shall not lead to the failure of the intended safety function even during preventive maintenance, periodic testing, inspection or repair. The application of the single failure criterion shall be in accordance with the IAEA Code NS-R-1, 5.34-5.39.

NOTE 1 In consideration of inappropriate actuations of the I&C, only spurious actuations (single or multiple) which can be the result of one single failure in I&C subsystems or support systems are generally considered.

In the case that category A functions have to be performed by operators, purpose designed monitoring and control of systems shall be provided which are separated from other monitoring and control of systems and which are designed to be suitable and adequate for the required reaction time.

The reliability of the I&C systems that perform category A functions shall be assessed and compared to the specification. If discrepancies exist, these shall be resolved. The reliability assessment shall consider the effects of common cause failures, including hardware failures, software failures, and human errors during operation, maintenance, as well as modification and repair activities. The techniques used to assess these effects range from purely qualitative engineering judgement to detailed quantitative analyses, which may themselves depend on qualitative estimates. The type of analysis chosen shall be consistent with the reliability requirement, the higher the reliability requirement, the more rigorous the technique.

Where consideration of the effects of common cause failures shows the required reliability could not be achieved for redundant systems, diversity implemented in independent systems shall be applied (e.g. as determined by probabilistic criteria). The function concerned may then require two or more systems, independent from one another. When a category A function is performed by two or more independent systems, the systems should be class 1 systems. If it is desired to use systems of a lower class, at least one of the systems shall meet the requirements of class 1 systems and a safety justification shall be provided for systems not meeting class 1 system requirements to enable the acceptability of this to be assessed.

NOTE 2 For an individual system which is specified and designed in accordance with the highest quality criteria, a figure of the order of 10^{-4} failure/demand may be an appropriate overall limit to place on the reliability that may be claimed, when all of the potential sources of failure due to the specification, design, manufacture, installation, operating environment, and maintenance practices, are taken into account. This figure includes the risk of common mode failure in the redundant channels of the system, and applies to the whole of the system, from sensors through processing to the outputs to the actuated equipment. Claims for better reliabilities than this are not precluded, but will need special justification, taking into account all of the factors mentioned. Alternatively, the design of independent I&C systems important to safety with an acceptable level of diversity may be applied.

Testing may require suppression of output signals, or the provision of bypass facilities. If bypass facilities are incorporated, their integrity shall be justified to show that they cannot be applied in a way that would prevent the system from achieving its specified safety functions. For example, their use might be physically restricted to a single train of a redundant system at any one time.

For some implementations, additional redundancy may need to be provided to allow routine testing during plant operation. This is necessary, for example, when testing of an active channel cannot be performed at power and tests must be conducted during plant operations to ensure the necessary functional reliability. In such cases, it is not necessary to incorporate additional redundancy for the whole system.

The power supply shall be backed-up by auxiliary power sources.

For category A systems, a formal system failure analysis, for example a failure modes and effects analysis (FMEA), shall be carried out to identify system vulnerability to component

failures and to assess the adequacy of design strategies applied to detect such failures or to mitigate their consequences.

Where a system has built-in self-testing features, and these are claimed as part of the reliability analysis of the function, the failure analysis shall assess these features to find the coverage of the self-tests. Where the failure analysis shows that some failures may not be detected and revealed to the operators by the systems self-testing features, then proof tests shall be developed to reveal such failures. The intervals for the proof test shall be determined from the likely frequency of occurrence of the undetected failure and the reliability required of the function.

Where reliability data is not available, the test interval shall be chosen by comparison with other similar systems. As experience is accumulated, the test interval for the function shall be re-evaluated.

7.3.2.2 Category B

The reliability of systems that perform category B I&C functions shall be assessed and compared to the specification. A function in this category shall be accomplished by redundant and separated means, unless justification is provided. Such justification may be based upon, for example, the ability of the system to achieve its reliability targets without it, the acceptability of the consequences of the function's failure, or the time available to provide alternative responses if the function fails.

The power supply shall be backed-up by auxiliary power sources.

The components employed shall be shown to be of high quality and reliability, and means to ensure that faults can be quickly detected and repaired shall be incorporated.

The principal objectives for the functional design of systems required to provide information or control capabilities in the control room that allow specified manual actions necessary to mitigate the consequences of a DBE are to provide the operator with accurate, complete and timely information regarding the status of plant equipment and systems for all DBE, and to minimise movement required from the operator to monitor and control the plant.

On-line and/or periodic testing of performance shall include confirmation of the functional capacity of subsystems, especially individual testing of redundant trains.

7.3.2.3 Category C

A system in this category does not generally need redundancy or separation This may be provided if it is necessary to achieve the specified reliability of the function. Tolerance to internal and external hazards may be required.

The power supply may be backed-up by auxiliary power sources on a case by case basis.

For systems performing category C functions where redundancy is necessary to achieve the specified reliability, redundancy should be considered as for category B.

Where redundancy is provided, periodic individual testing of the functional capacity of all redundant systems or subsystems shall be included. On-line tests are a means of meeting this requirement.

7.4 Requirements related to equipment

7.4.1 Basic requirements

It is necessary to provide assurance that the equipment will not fail due to the environmental conditions that it may be subjected to during and following a PIE. This assurance may be provided by qualification of the equipment. When qualification is required, this may be achieved using one, or a combination of several different methods: for example, by tests, by analysis, a combination of these two, or possibly by using available data from operational experience. The worst anticipated environment, including earthquake, in which the equipment is required to operate shall be established and stated in the requirements specification.

When functions not originally intended for beyond design basis or severe accidents are expected to play a role in these accidents, the capabilities of their components should be evaluated in order to show that they are able to function in the environmental conditions to be expected.

7.4.2 Specific requirements

7.4.2.1 Category A

The measures taken to provide assurance that category A equipment will continue to operate under all anticipated operating conditions shall include equipment qualification. The results of the tests shall be recorded and retained in the lifetime records of the NPP. Any failures during the qualification tests shall be investigated, and the cause and rectification of the failure shall be documented.

7.4.2.2 Category B

Equipment in category B shall be subject to qualification, to be performed as for category A equipment.

7.4.2.3 Category C

Depending on its function, equipment in category C may require qualification. The design of the equipment should be systematically reviewed against the specification of the worst anticipated environment in which the equipment is required to operate.

Where the equipment is novel, or is required to operate in conditions for which commercial equipment is not normally designed (such as seismic events or extreme environmental conditions), a set of rules shall be established against which the equipment is designed, or an existing design evaluated. These rules shall be based on experience gained from the special design requirements of category A equipment. Equipment provided for the functions classified in application of criteria 5.4.4 i) and j) should be specifically designed for the extreme process and environmental conditions that could arise, as determined from analysis. The appropriateness of adopting equipment produced to commercial standards for the implementation of these functions shall be specifically reviewed.

For other cases, category C equipment may be accepted to normal commercial design standards unless the role of the equipment requires special qualification, for example seismic or fire prevention requirements, or to prevent overvoltages or electrical noise in category C equipment from affecting category A or B functions. Claims for operation in abnormal environmental conditions shall be supported by documentary evidence.

7.5 Requirements related to quality aspects

7.5.1 Basic requirements

The general requirements are related to quality assurance performed during the design, the manufacture, the installation, the commissioning and the operation phases, in order to ensure the correct performance of the relevant systems and equipment.

The objectives of QA are configuration management, change control and traceability. The design shall be documented in sufficient detail to support the manufacture, installation, commissioning and operational phases of the NPP, and the verifications performed at each step. Adequate attention shall be paid to the provision of documentation to permit future modification of the design.

In addition, special QA and testing should be undertaken for developments in proportion to the relative novelty or complexity of the new design or modification. These development activities should be documented as appropriate to the importance to safety of the functions.

A QA plan shall be established according to an appropriate adequate code or standard. This shall require specifications of performance and testing to be defined and verified.

Testing of components, modules, subsystems, and systems shall be carried out according to the QA plan to show satisfactory performance during manufacturing, assembly, and site installation periods, as appropriate to the category of the function.

Tests shall be carried out on components, modules and subsystems to ensure that, with the manufacturing QA, the functions are fulfilled according to the requirements specification. Combined tests of the installed I&C system with the mechanical and fluid systems shall take place at the NPP before operation of the NPP in a mode requiring the availability of the safety functions provided by the system.

The intention of the site tests is the same, regardless of category, but the quality control and documentation requirements vary according to category, as stated hereinafter.

Testing during operation shall be executed to demonstrate that the status of the hardware components of the I&C important to safety is not degraded by faults. I&C systems shall be designed to permit adequate testing and to detect failures within the equipment. Deficiencies identified shall be corrected following a modification control procedure. Suitable records of those corrections shall be kept. Where redundancy is provided, individual checks of the functionality of the redundant channels shall be included. The test interval shall be chosen so that the assessed failure rate or probability of failure to operate on demand meets the requirements of the reliability analysis.

Where computer equipment is used, a software life cycle quality programme appropriate to the category of the function shall be implemented.

7.5.2 Specific requirements

7.5.2.1 Category A

The QA requirements shall be according to IAEA safety standard GS-R-3. The documentation shall enable the history of the items of equipment to be established, including design, manufacturing, and operating aspects. This shall include all equipment down to the module level within the design. The configuration shall be controlled down to the lowest traceable element. Traceability of lot numbers, materials, etc. shall extend throughout the system down to the level of individual modules.

The QA documentation shall allow an investigator to trace backward from a piece of hardware or software to the specification that defines the requirements for it, and to work forwards from any requirement in the specification to the components that implement it.

Type testing shall have been carried out to show that equipment of identical construction to that to be installed at the NPP will function as required by the design when subjected to the anticipated operating environment.

Functional testing of components, modules, subsystems and, whenever practicable, complete systems, shall be carried out. These tests shall be witnessed by the licensee, or his representative.

Functional testing may be performed at the factory or at the site. Tests performed at the factory and at the site shall be co-ordinated to ensure that a full coverage by all tests together is achieved. Where it is not possible to prove that full coverage of all of the specified functions can be achieved, special justification shall be provided.

Site testing shall test, as far as practicable, that all specified safety functions of the installed systems and equipment can be achieved with the required performance. This testing shall take into account variations in operating parameters. This is the site acceptance test (SAT), and shall be witnessed by the licensee, or his representative.

On-line or periodic tests shall demonstrate that the ability to perform all required safety functions including all subsystems necessary to perform these functions is not degraded. Test intervals shall be chosen taking due account of the level of self-monitoring so that the reliability targets for the I&C important to safety are fulfilled taking into account the expected or monitored failure rate of the I&C components.

7.5.2.2 Category B

The QA requirements shall be according to IAEA safety standard GS-R-3. The documentation shall enable the history of the items of equipment to be established, including design, manufacturing, and operating aspects The level of detail to which QA applies to category B functions, systems, or equipment may be lower than that applied to category A functions, systems, or equipment, although the QA programme should be consistent with that for category A.

Type testing shall have been carried out with equipment of similar construction to that to be installed at the NPP provided that analysis has been performed to show that differences in the equipment do not invalidate the test results.

Functional testing shall have been carried out prior to operation to show that each specified function can be achieved by the system using equipment of similar construction to that to be installed at the NPP. Some or all of this testing may be done on site.

SAT testing shall show, as far as is practicable, that all specified safety functions of the installed equipment can be achieved. Tests of control equipment shall show the ability to respond correctly to transients and changes in demand. Testing of display and alarm equipment shall include injection tests of relevant input signals to show satisfactory performance.

7.5.2.3 Category C

Systems and equipment performing category C functions may be accepted at a commercial QA level.

The licensee may accept that the manufacturer's tests are adequate to demonstrate that the specified performance will be achieved. These tests shall be performed on similar equipment.

Specific type and functional testing should be performed when necessary, but is not generally required.

SATs should be carried to show that the system achieves the specified safety related functionality and performance.

Periodic testing of performance may be limited to checks at refuelling outages, or at similar shutdown periods, for functions which are not continuously operating.

Table 1 – Tabular correlation between categories and other IEC standards

Category	Applicable IEC standards		Main requirements for			
	Systems	Equipment	Functions	Design of systems	Equipment features	General
General	IEC 61513 IEC 60964, IEC 60965 IEC 61771, IEC 61772 IEC 61839 IEC 60709	IEC 61000-4 IEC 61000-6-2	Functional specification	Testability HMI specification	Electromagnetic compatibility	QA program Quality control FAT, SAT Periodic testing
A	IEC 60812[5] IEC 60880 IEC 60987	IEC 60780, IEC 60980	Appropriate codes, standards, guides Separation from lower categories High assurance of reliability	Single failure criterion Independence, separation Design to cope with internal common cause failure Diversification case by case FMEA Back-up power supply	Qualification to postulated environment and to seismic conditions	IAEA GS-R-3 Verification on identical equipment Full FAT/SAT Frequent periodic testing
B	IEC 60987 IEC 62138	IEC 60780, IEC 60980	Appropriate codes, standards, guides Separation from lower categories	Single failure criterion, separation both possibly at functional level Back-up power supply	Qualification to environment and seismic conditions that the equipment must withstand	IAEA GS-R-3 Verification on similar equipment Limited SAT and periodic testing
C	IEC 62138			Redundancy and separation case by case	Qualification case by case	Normal industrial practice Periodic test if not used continuously

5 When failure analysis is FMEA.

Annex A
(informative)

Examples of categories

A.1 General

This annex provides examples of assignment of typical functions and typical I&C systems to categories A, B and C. It should be noted, however, that these examples may not necessarily all apply to all reactor types.

A.2 Category A

A.2.1 Typical functions

The I&C functions assigned to category A are necessary for

a) reactor shutdown and maintenance of sub-criticality;

b) isolation of containment;

c) provision of information for essential operator action;

d) decay heat transport to the ultimate heat sink.

A.2.2 Typical I&C systems

Typical I&C systems are as follows:

a) reactor protection system;

b) safety actuation system and safety system support features;

c) key instrumentation and displays to permit pre-planned operator actions that are defined in the NPP operating instructions, and that are required to ensure NPP safety in the short term.

A.3 Category B

A.3.1 Typical functions

The I&C functions assigned to category B are necessary for

a) used fuel pool cooling system;

b) main cooling system isolation;

c) post accident monitoring system;

d) automatic control of the NPP primary and secondary circuit conditions, keeping variables in the limits assumed in the safety analysis, and prevention of events from escalating to accidents;

e) monitoring/controlling the handling of fuel where failure could cause radiation release or fuel degradation outside the limits and conditions of normal operation.

A.3.2 Typical I&C systems

Typical I&C systems are as follows:

a) NPP automatic control system or preventative protection system;

b) part of the decay heat transport to ultimate heat sink not necessary in the short term;
c) instrumentation needed to apply operating procedures for DBE;
d) safety circuits and interlocks of fuel handling systems used when the reactor is shut down.

A.4 Category C

A.4.1 Typical functions

The I&C functions assigned to category C may include

a) monitoring and controlling performance of individual systems and items of equipment during the post-accident phase to gain early warning of the onset of problems, and to keep radioactive releases ALARA;
b) limiting the consequences of internal hazards;
c) those for which operating mistakes could cause minor radioactive releases, or lead to radioactive hazard to the NPP operating staff;
d) those necessary to warn of internal or external hazard (fire, flood, explosions, seismic events, etc.);
e) access control;
f) communication to warn of significant on- or off-site releases for the purposes of implementing the NPP's emergency plan.

A.4.2 Typical I&C systems

Typical I&C systems are as follows:

a) alarm system;
b) radwaste stream monitoring and interlocks, area radiation monitoring;
c) access control system;
d) emergency communication systems;
e) control room data processing system;
f) fire suppression system;
g) seismic monitoring system;
h) NPP site meteorological station.

Bibliography

IEC 60050-394, *International Electrotechnical Vocabulary – Part 394: Nuclear instrumentation – Instruments, systems, equipment and detectors*

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

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC/TR 61838, *Nuclear power plants – Instrumentation and control important to safety – Use of probabilistic safety assessment for the classification of functions*

IAEA Safety Glossary:2007, *Terminology used in nuclear safety and radiation protection*

———

SOMMAIRE

AVANT-PROPOS 35
INTRODUCTION 37
1 Domaine d'application 40
2 Références normatives 40
3 Termes et définitions 42
4 Abréviations 45
5 Schéma de classement 45
5.1 Généralités 45
5.2 Contexte 46
5.3 Description des catégories 47
5.3.1 Généralités 47
5.3.2 Catégorie A 47
5.3.3 Catégorie B 48
5.3.4 Catégorie C 48
5.4 Critères de répartition dans les différentes catégories 48
5.4.1 Généralités 48
5.4.2 Catégorie A 48
5.4.3 Catégorie B 49
5.4.4 Catégorie C 49
6 Procédure de classement 50
6.1 Généralités 50
6.2 Identification de la base de conception 50
6.3 Identification et classement des fonctions 50
7 Affectation des exigences techniques aux catégories 53
7.1 Exigences générales 53
7.2 Exigences concernant les fonctions 53
7.2.1 Exigences de base 53
7.2.2 Exigences spécifiques 54
7.3 Exigences applicables aux systèmes d'I&C 54
7.3.1 Exigences de base 54
7.3.2 Exigences spécifiques 55
7.4 Exigences liées aux matériels 57
7.4.1 Exigences de base 57
7.4.2 Exigences spécifiques 57
7.5 Exigences liées aux aspects de qualité (AQ) 58
7.5.1 Exigences de base 58
7.5.2 Exigences spécifiques 59
Annexe A (informative) Exemples de catégories 62
Bibliographie 64

Figure 1 – Méthode de classement 52

Tableau 1 – Table de corrélation entre les catégories et les autres normes CEI 61

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – CLASSEMENT DES FONCTIONS D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE

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 61226 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 troisième édition annule et remplace la deuxième édition parue en 2005 et constitue une révision technique. Les modifications techniques majeures par rapport à l'édition précédente sont les suivantes:

- introduction d'une définition pour « état contrôlé »;
- clarification des limites des catégories;
- clarification des exigences portant sur les matériels utilisés hors dimensionnement.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/745/FDIS	45A/767/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 la norme

La présente Norme internationale répond à l'exigence[1] de l'Agence Internationale de l'Energie Atomique (AIEA) concernant le classement des systèmes d'instrumentation et de contrôle-commande (I&C) des centrales nucléaires de puissance en fonction de leur importance pour la sûreté. L'utilisation de systèmes d'I&C à base d'informatique répartie dans les systèmes d'instrumentation et de contrôle-commande des centrales nucléaires de puissance entraîne la répartition des fonctions importantes pour la sûreté dans plusieurs systèmes ou sous-systèmes. Ainsi, le but de la présente norme est de:

– classer les fonctions d'I&C importantes pour la sûreté en catégories, dépendant de leur contribution à la prévention et à l'atténuation des évènements initiateurs postulés (EIP), et de développer des exigences qui soient cohérentes avec l'importance pour la sûreté de chacune des catégories;
– assigner aux systèmes d'I&C et aux matériels concernés, réalisant les fonctions classées, les exigences concernant les spécifications et la conception.

Conformément à la recommandation[2] de l'AIEA, les méthodes de classement sont d'abord basées sur une analyse de sûreté déterministe, et il est recommandé de les compléter par des méthodes probabilistes lorsque cela est approprié. Plusieurs approches possibles pour l'utilisation des évaluations probabilistes de sûreté (EPS) sont décrites dans la CEI/TR 61838, «Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Utilisation des évaluations probabilistes de sûreté pour le classement».

La révision de la norme permet de prendre partiellement en compte l'évaluation quantitative.

b) Position du présent document dans la collection de normes du SC 45A

La CEI 61226 est directement référencée par la CEI 61513 et est le document de deuxième niveau du SC 45A traitant de la catégorisation des fonctions et du classement des systèmes.

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

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

Un classement correct des fonctions implique qu'une attention suffisante soit portée par les concepteurs, les exploitants et les autorités de régulation des centrales aux systèmes supports des fonctions de sûreté, dans les domaines des spécifications, de la conception, de la qualification, de l'assurance qualité (AQ), de la fabrication, de l'installation, de la maintenance et des essais.

---

1 Exigence 5.1 du document AIEA NS-R-1.

2 Le Paragraphe 5.2 du document NS-R-1 exige que la méthode de classement de l'importance pour la sûreté des structures, systèmes ou composants soit basée principalement sur des méthodes déterministes complétées où cela est approprié par des méthodes probabilistes et par le jugement de l'ingénieur prenant en compte des facteurs tels que:

a) les fonctions de sûreté à réaliser;

b) les conséquences de l'échec de la réalisation d'une fonction;

c) la probabilité qu'il (le système d'I&C) doive réaliser une fonction de sûreté;

d) le délai suivant un EIP au bout duquel, ou la période pendant laquelle, il (le système d'I&C) sera amener à fonctionner.

Cette norme fixe les critères et méthodes de répartition des fonctions de sûreté d'une centrale nucléaire en trois catégories A, B et C, qui dépendent de l'importance de la fonction pour la sûreté, et en une catégorie non classée, pour les fonctions qui n'ont pas de rôle de sûreté direct. Elle souligne les exigences génériques pour chaque catégorie et spécifie les exigences techniques de base pour les sujets tels que l'AQ, la fiabilité, les essais et la maintenance.

La catégorie attribuée à une fonction détermine des exigences techniques génériques et spécifiques. Les exigences génériques de chaque fonction sont destinées à apporter l'assurance que cette fonction sera réalisée sur demande avec le niveau de performance et de fiabilité requis. Cela s'applique aux aspects de fonctionnalité, de fiabilité, de performance, de résistance aux conditions d'ambiance et d'AQ. Il faut que le niveau de garantie à atteindre pour chacun de ces aspects soit cohérent avec l'importance de la fonction pour la sûreté.

i) L'assurance de la fonctionnalité est établie par la création d'une spécification exhaustive d'exigences, et par l'application des codes et normes appropriés.

ii) L'assurance de fiabilité est fournie par la sélection de composants, de structures et de niveau de redondance et de diversité appropriés, associés aux notions de séparation physique et/ou de barrière, d'isolation électrique et d'essais périodiques en service.

iii) L'assurance de performance est donnée par la création de spécifications des performances requises, l'application des procédures d'AQ, de processus de vérification et de validation pendant la conception et la fabrication, les essais initiaux individuels et d'ensemble des systèmes et matériels, et les essais en service.

iv) L'assurance de la résistance aux conditions d'ambiance est assurée par les programmes de qualification du matériel afin de garantir que les effets du vieillissement et des conditions d'environnement existant au moment où le matériel est appelé à fonctionner ne dégradent pas ses performances au-dessous des valeurs prévues dans l'analyse.

v) L'assurance de la bonne prise en compte à chaque étape, de la conception à la mise en service, en passant par la fabrication, les essais et l'installation, des aspects de fonctionnalité, de performances, de résistance aux conditions d'ambiance de fiabilité, est donnée par la réalisation de chaque étape des travaux sous le contrôle d'un programme approprié d'AQ.

Dans la norme, le verbe «doit» indique que l'exigence doit être obligatoirement satisfaite pour être conforme à la norme, les expressions «il est recommandé que» ou «il convient que» indiquent que la satisfaction de l'exigence n'est pas obligatoire pour être conforme à la norme, mais qu'elle est fortement recommandée, et le verbe «peut» indique que l'exigence est optionnelle.

d) Description de la structure de la collection des normes du SC 45A 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 publiées 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 centrales nucléaires, 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 pas référencées directement par la CEI 61513, sont relatives à des matériels particuliers, à des méthodes techniques 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 série de publications fondamentales de sécurité 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 Partie 3 de la CEI 61508 pour le secteur nucléaire.

La CEI 61513 fait référence aux normes ISO, ainsi qu'au document AIEA 50-C-QA (remplacé depuis par le document AIEA GS-R-3) pour ce qui concerne l'assurance qualité.

Les normes publiées 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 centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle-commande importants pour la sûreté des centrales nucléaires. Les termes et définitions utilisés dans les normes publiées par le SC 45A sont conformes à ceux utilisés par l'AIEA.

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – CLASSEMENT DES FONCTIONS D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE

1 Domaine d'application

La présente Norme internationale établit une méthode de classement des fonctions d'information et de commande des centrales nucléaires de puissance et des systèmes d'I&C et matériels qui assurent ces fonctions en catégories indiquant l'importance pour la sûreté de la fonction. Le classement qui en résulte permet alors de déterminer les critères de conception appropriés.

Les critères de conception sont les mesures de qualité garantissant que l'adéquation de chaque fonction par rapport à son importance pour la sûreté de l'installation est assurée. Dans la présente norme les critères retenus concernent la fonctionnalité, la fiabilité, les performances, la résistance aux conditions d'ambiance (incluant les séismes) et l'assurance qualité (AQ).

La présente norme est applicable à toutes les fonctions d'information et de commande, à tous les systèmes d'I&C et les matériels supports de ces fonctions. Les fonctions, systèmes et matériels considérés, assurent la protection automatique, les régulations en boucles ouvertes et fermées et l'information des opérateurs. Elles permettent de maintenir les paramètres d'exploitation de la centrale à l'intérieur du domaine opérationnel sûr et elles assurent les actions automatiques, ou permettent les actions manuelles qui préviennent ou gèrent les accidents ou qui préviennent ou minimisent les rejets radioactifs sur le site ou dans l'environnement en général. Les fonctions d'I&C qui remplissent ces rôles protègent la santé et la sécurité des opérateurs et du public.

La présente norme est conforme aux principes généraux donnés dans le code NS-R-1 et dans le guide de sûreté NS-G-1.3 de l'AIEA, et elle définit une méthode structurée d'application des directives contenues dans ces codes et normes pour les systèmes d'I&C qui assurent des fonctions importantes pour la sûreté dans les centrales nucléaires de puissance. Il convient de lire la présente norme avec les guides de l'AIEA et la CEI 61513 dans la mise en œuvre des exigences de la série CEI 61508.

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 60671:2007, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

CEI 60709, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Séparation*

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 60880:2006, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

CEI 60964, *Centrales nucléaires de puissance – Salles de commande – Conception*

CEI 60965, *Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)*

CEI 60980, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

CEI 60987, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés*

CEI 61000-4 (toutes les parties), *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure*

CEI 61000-6-2, *Compatibilité électromagnétique (CEM) – Partie 6-2: Normes génériques – Immunité pour les environnements industriels*

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

CEI 61771, *Centrales nucléaires de puissance – Salle de commande principale – Vérification et validation de la conception*

CEI 61772, *Centrales nucléaires de puissance – Salles de commande principale – Utilisation des unités de visualisation*

CEI 61839, *Centrales nucléaires de puissance – Conception des salles de commande – Analyse fonctionnelle et affectation des fonctions*

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*

AIEA NS-R-1:2005, *Sûreté des centrales nucléaires: Conception*

AIEA GS-R-3:2006, *The management system for facilities and activities* (disponible en anglais seulement)

AIEA NS-G-1.3: 2005, *Systèmes d'instrumentation et de contrôle commande importants pour la sûreté des centrales nucléaires*

3 Termes et définitions

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

3.1
incident de fonctionnement prévu
écart de fonctionnement par rapport au fonctionnement normal que l'on s'attend à voir survenir au moins une fois pendant la durée de vie utile de l'installation mais qui, grâce aux dispositions appropriées prises lors de la conception, ne cause pas de dommage significatif à des constituants importants pour la sûreté et ne dégénère pas en conditions accidentelles

[Glossaire de sûreté de l'AIEA:2007]

3.2
défaillance de cause commune
DCC
défaillance de deux ou de plusieurs structures, systèmes ou composants due à un événement ou à une cause spécifique unique

[Glossaire de sûreté de l'AIEA:2007]

3.3
accident de dimensionnement
ADD
conditions accidentelles auxquelles une installation nucléaire est conçue pour résister conformément à des critères de conception spécifiés et dans lesquelles l'endommagement du combustible et les rejets de matières radioactives sont maintenus en dessous des limites autorisées

[Glossaire de sûreté de l'AIEA:2007]

3.4
événements de dimensionnement
EDD
ensemble des accidents de dimensionnement et des incidents de fonctionnement prévus

NOTE Voir aussi 3.13.

3.5
diversité
présence de deux ou plusieurs systèmes ou composants redondants pour l'accomplissement d'une fonction déterminée, lorsque ces différents systèmes ou composants possèdent des attributs différents afin de réduire le risque de défaillance de cause commune, y compris la défaillance de mode commun

[Glossaire de sûreté de l'AIEA:2007]

NOTE La définition suivante du terme « diversité » est donnée dans le 3.5 de la CEI 60880: *existence d'au moins deux différents moyens ou façons d'atteindre un objectif spécifié. La diversité est un moyen spécifique de défense contre les défaillances de cause commune. Elle peut être réalisée en installant des systèmes qui sont physiquement différents les uns des autres ou par la diversité fonctionnelle, lorsque des systèmes identiques atteignent un objectif spécifié de différentes façons*. Celle-ci est totalement cohérente avec la définition de l'AIEA donnée ici.

3.6
matériel
une ou plusieurs parties d'un système. Un matériel est un élément unique, identifiable (et généralement amovible) ou une partie d'un système

[CEI 61513, 3.17, modifiée]

3.7
fonction

but précis ou objectif devant être accompli, qui peut être spécifié ou décrit sans référence aux moyens physiques nécessaires pour son atteinte

3.8
fonctionnalité
attribut d'une fonction définissant les opérations de transformation des informations d'entrée en informations de sortie

[CEI 61513, 3.25]

3.9
programme d'ergonomie
programme décrivant au minimum l'organisation relative à l'ergonomie, les missions et les rôles individuels et collectifs des ergonomes, leurs activités et l'intégration de celles-ci dans les processus de conception et de validation, la liste des éléments à produire à chaque étape du programme

3.10
constituant important pour la sûreté
constituant faisant partie d'un groupe de sûreté et/ou dont le mauvais fonctionnement ou la défaillance pourrait entraîner une exposition à des rayonnements du personnel du site ou de personnes du public.

Les constituants importants pour la sûreté comprennent:

a) les structures, systèmes et composants dont le mauvais fonctionnement ou la défaillance pourraient entraîner une exposition indue à des rayonnements du personnel du site ou de personnes du public;
b) les structures, systèmes et composants qui empêchent les incidents de fonctionnement prévus d'aboutir à des conditions accidentelles;
c) les dispositifs fournis pour atténuer les conséquences d'un mauvais fonctionnement ou d'une défaillance de structures, systèmes ou composants

[Glossaire de sûreté de l'AIEA:2007]

NOTE Les constituants importants pour la sûreté considérés dans la présente norme sont principalement des systèmes d'I&C importants pour la sûreté.

3.11
état contrôlé
état de la centrale, pour lequel la stabilisation de tous les transitoires est atteinte, le réacteur est sous-critique, une évacuation appropriée de la chaleur résiduelle est assurée et les rejets radioactifs sont limités

NOTE On considère qu'un transitoire est stabilisé lorsque, pour tous les paramètres significatifs de sûreté, les marges (par exemple entre les capacités de production et d'évacuation de chaleur) sont ou stables, ou en augmentation ou bien lorsqu'il existe une marge suffisante pour faire face à tous les processus physiques prévus.

3.12
performance
efficacité avec laquelle une fonction prévue est exécutée (par exemple temps de réponse, précision, sensibilité aux variations de paramètres)

3.13
états de la centrale

<table>
<tr><td colspan="2">Etats opérationnels</td><td colspan="3">Conditions accidentelles</td></tr>
<tr><td rowspan="2">Exploitation normale</td><td colspan="2">Evénements de dimensionnement</td><td colspan="2">Accidents hors dimensionnement</td></tr>
<tr><td>Incidents de fonctionnement prévus</td><td>a)</td><td>Accidents de dimensionnement</td><td>b)</td><td>Accidents graves</td></tr>
<tr><td colspan="5">Gestion accidentelle</td></tr>
</table>

a) Conditions accidentelles qui ne sont pas explicitement prises en considération comme accidents de dimensionnement mais qui sont couvertes par celles-ci.

b) Accidents hors dimensionnement sans dégradation significative du cœur.

NOTE Cette définition est compatible avec celle du glossaire de sûreté de l'AIEA. Elle indique juste la position du concept d' « évènement de dimensionnement » par rapport aux autres concepts.

3.14
événement initiateur postulé
EIP
évènement dont on détermine au stade de la conception qu'il peut entraîner des incidents de fonctionnement prévus ou des conditions accidentelles

[Glossaire de sûreté de l'AIEA:2007]

3.15
redondance
mise en place de structures, systèmes ou composants (identiques ou différents) supplémentaires, afin qu'un élément quelconque puisse remplir la fonction requise indépendamment de l'état de fonctionnement ou de défaillance d'un autre élément

[Glossaire de sûreté de l'AIEA:2007]

3.16
groupe de sûreté
ensemble d'équipements prévus pour accomplir toutes les actions requises si un événement initiateur postulé particulier se produit afin que les limites spécifiées dans la base de conception pour les incidents de fonctionnement prévus et les accidents de dimensionnement ne soient pas dépassées

[Glossaire de sûreté de l'AIEA:2007]

3.17
système lié à la sûreté
système important pour la sûreté qui ne fait pas partie d'un système de sûreté

[Glossaire de sûreté de l'AIEA:2007]

3.18
système de sûreté
système important pour la sûreté destiné à garantir la mise à l'arrêt sûre du réacteur ou l'évacuation de la chaleur résiduelle du cœur, ou à limiter les conséquences des incidents de fonctionnement prévus et des accidents de dimensionnement

[Glossaire de sûreté de l'AIEA:2007]

3.19
défaillance unique
défaillance qui rend un système ou un composant impropre à remplir sa (ses) fonction(s) de sûreté prévue(s) et toute autre défaillance qui peut en résulter

[Glossaire de sûreté de l'AIEA:2007]

3.20
système
ensemble de composants qui interagissent conformément à une conception donnée, où un élément du système peut être un autre système appelé sous-système

[CEI 61513, 3.61]

3.21
essai de type
essai de conformité effectué sur une ou plusieurs entités représentatives de la production

[VEI 394-40-02]

3.22
conséquence inacceptable
conséquence d'un état de fonctionnement ou d'un EIP, dépassant les limites spécifiées pour les états de la centrale correspondants, en terme de rejets sur le site ou dans l'environnement

NOTE Des limites complémentaires, telles qu'un endommagement inacceptable du combustible ou l'endommagement d'autres composants principaux peuvent aussi être spécifiées au niveau national. Il peut s'agir d'un rejet massif et incontrôlé dont la fréquence se situe hors des bases de conception de la centrale, ou d'un évènement dont la fréquence est comprise dans les bases de conception, mais qui entraîne un dépassement d'ampleur des limites spécifiées. Des limites complémentaires, telles qu'un endommagement inacceptable du combustible peuvent également être prescrites. Il peut s'agir d'endommagements des gaines entraînant un accroissement inacceptable de l'activité du fluide primaire, ou de dommages structurels entraînant l'impossibilité de refroidir le combustible. L'endommagement des autres barrières peut aussi être considéré comme une conséquence inacceptable.

4 Abréviations

ALARA	Aussi faible qu'il soit raisonnablement possible de réaliser
ADD	Accidents de dimensionnement
EDD	Evénement de dimensionnement
RU	Recette usine
AMDE	Analyse des modes de défaillance et de leurs effets
IHM	Interface homme machine
AIEA	Agence Internationale de l'Energie Atomique
I&C	Instrumentation et contrôle-commande
NPP	Centrale nucléaire de puissance
EIP	Evénement initiateur postulé
EPS	Evaluation probabiliste de sûreté
AQ	Assurance qualité
RS	Recette site

5 Schéma de classement

5.1 Généralités

Les fonctions assurées par les systèmes d'I&C doivent être affectées à des catégories suivant leur importance pour la sûreté. L'importance pour la sûreté d'une fonction doit être déterminée par les conséquences de son échec lorsque son exécution est nécessaire et les conséquences de son activation intempestive. La catégorie détermine les exigences de

conception et de qualité portant sur les systèmes et les matériels d'I&C. Ces exigences doivent être définies indépendamment de la technologie employée par le matériel. Le Paragraphe 5.2 traite du contexte du schéma de classement.

Le Paragraphe 5.3 décrit les trois catégories qui sont utilisées pour classer les fonctions. Les catégories sont basées sur celles définies originellement dans la première édition de la CEI 61226 publiée en 1993.

Le Paragraphe 5.4 présente les critères d'affectation pour chaque catégorie.

L'Article 6 donne des lignes directrices sur le processus de classement.

L'Article 7 fournit des exigences techniques pour chacune des trois catégories. La plupart des exigences s'appliquent aux systèmes et matériels qui réalisent les fonctions, mais certaines exigences s'appliquent seulement aux fonctions.

L'Annexe A contient des exemples caractéristiques de classement de fonctions d'I&C de centrales nucléaires. Elle n'est donnée que pour information car cela dépend du type du réacteur considéré.

5.2 Contexte

Le principe de défense en profondeur est très fermement établi dans la conception de base de sécurité des centrales nucléaires de puissance. L'idée fondamentale est qu'il convient de prévoir plusieurs couches ou échelons de défense pour prévenir les conditions dangereuses avant que la mise en œuvre de mesures d'atténuation ne soit nécessaire, ce qui est toujours préférable. En raison de la nécessité de mettre en œuvre un grand nombre de fonctions pour que la sûreté de la centrale en fonctionnement soit garantie, et que ce nombre augmente du fait du principe de défense en profondeur, il est important que l'importance pour la sûreté de chacune de ces fonctions soit connue.

La série de normes de sûreté de l'AIEA NS-R-1 définit l'idée de classement des systèmes des centrales nucléaires selon l'importance pour la sûreté, et donne des exemples de classement des systèmes principaux de plusieurs types de centrales. Toutes les structures, systèmes et composants, y compris les logiciels pour l'instrumentation et le contrôle-commande (I&C) qui sont importants pour la sûreté doivent être d'abord identifiés puis classés sur la base de leurs fonctions et de leur importance pour la sûreté. Ils doivent être conçus, fabriqués et maintenus de telle façon que leur qualité et leur fiabilité soient cohérentes avec ce classement.

Le guide de sûreté NS-G-1.3 donne des indications sur le classement des systèmes en fonction de l'importance pour la sûreté des fonctions qui sont assurées. Il introduit des facteurs temporels tels que

– la durée de fonctionnement nécessaire du système d'I&C une fois qu'il a démarré;
– le temps pendant lequel des actions alternatives peuvent être réalisées;
– les délais de détection et de correction des défaillances cachées.

La présente norme étend la stratégie de classement présentée dans le guide de sûreté de l'AIEA NS-G-1.3, et définit les critères et méthodes à utiliser pour affecter les fonctions d'I&C des centrales nucléaires à une des trois catégories A, B et C en fonction de leur importance pour la sûreté, ou à la catégorie non classée pour les fonctions sans rôle de sûreté direct. Les fonctions d'I&C situées dans le domaine des systèmes de sûreté seront généralement affectées aux catégories A ou B. Les fonctions d'I&C définies comme liées à la sûreté seront généralement affectées aux catégories B ou C.

L'importance pour la sûreté des parties de systèmes de sûreté et de systèmes d'I&C liés à la sûreté, ainsi que les exigences correspondantes dont ils sont l'objet, différeront de telle manière qu'il est approprié de les affecter à des classes de sûreté différentes. Certains

systèmes d'I&C peuvent avoir un impact important sur la sûreté et donc nécessiter une attention particulière. D'autres systèmes d'I&C auront une importance moyenne, faible ou nulle pour la sûreté. Ils feront donc l'objet d'exigences moins rigoureuses concernant la garantie des performances système et les justifications de sûreté, et ils feront l'objet d'exigences techniques différentes.

L'application nationale des critères et des principes de la présente norme peut imposer une nomenclature différente des catégories A, B et C. Les applications nationales doivent être faites en accord avec les principes, les critères et les exigences associées donnés dans cette norme. Cela doit comprendre la détermination et la documentation d'une correspondance appropriée des catégories définies.

5.3 Description des catégories

5.3.1 Généralités

Dans les centrales nucléaires, les systèmes d'I&C assurent des fonctions à différents niveaux de sûreté. L'importance pour la sûreté de chacune de ces fonctions d'I&C dépend de son rôle dans l'obtention et le maintien de la sûreté, des conséquences potentielles de la défaillance opérationnelle de la fonction lorsque celle-ci est requise, et de la probabilité associée à ces conséquences. Ainsi, une analyse de sûreté initiale de la conception spécifique à la centrale doit être réalisée avant le classement des fonctions d'I&C. La gravité des conséquences potentielles liées à la défaillance hypothétique d'une fonction d'I&C définit le niveau d'assurance requis pour les différents attributs du système et du matériel support de la fonction, et plus particulièrement pour les domaines des fonctionnalités, des performances et de la fiabilité.

Concernant les procédures de conception, d'évaluation et d'autorisation, les catégories de sûreté A, B et C sont définies, avec des ensembles associés d'exigences techniques et de qualité relatifs aux propriétés des systèmes d'I&C, devant être appliquées lors de la conception et de la mise en œuvre des systèmes d'I&C et des matériels importants pour la sûreté.

5.3.2 Catégorie A

La catégorie A est utilisée pour désigner les fonctions qui tiennent un rôle principal dans l'obtention ou le maintien de la sûreté de la centrale nucléaire pour empêcher que les évènements de dimensionnement (EDD) ne conduisent à des conséquences inacceptables. Ce rôle est essentiel en début de transitoire lorsque aucune autre action n'est possible, et cela même si une erreur cachée peut être détectée. Ces fonctions jouent un rôle majeur dans l'atteinte ou le maintien de l'état contrôlé stable[3]. Si des actions manuelles spécifiées sont nécessaires pour atteindre l'état contrôlé, on doit prendre en compte des facteurs tels que la disponibilité de sources d'information redondantes et validées, les délais suffisants pour permettre aux opérateurs d'évaluer les sources alternatives d'information et si ces actions manuelles sont les seuls moyens d'atténuation de cette séquence événementielle pour préserver la sûreté de la centrale nucléaire.

La catégorie A est aussi utilisée pour désigner les fonctions dont la défaillance pourrait conduire directement à des conditions accidentelles qui pourraient entraîner des conséquences inacceptables, si elles n'étaient pas atténuées par d'autres fonctions de catégorie A. Une grande fiabilité est exigée pour les fonctions de catégorie A. Ainsi il peut être nécessaire de limiter leur fonctionnalité et leur complexité.

---

[3] Pour faire face aux transitoires rapides, durant cette phase la tranche est contrôlée par des actions automatiques. Pour des transitoires plus lents, l'état contrôlé peut être atteint à l'aide d'actions manuelles, à condition que de telles actions se déroulent après le «délai de grâce». Ce type de délai de grâce représente une exigence de la conception de la centrale correspondant à un laps de temps dû au diagnostique et aux actions, et est basé sur des considérations liées aux facteurs humains. Cela ne veut pas dire que les actions manuelles sont interdites durant cette période. Dans certain pays, et pour des installations plus anciennes, la limite associée à la catégorie A peut être ce délai de grâce, en lieu et place de l'état contrôlé.

5.3.3 Catégorie B

La catégorie B est utilisée pour désigner les fonctions qui tiennent un rôle complémentaire par rapport au fonctions de catégorie A dans l'obtention et le maintien de la sûreté de la centrale nucléaire, spécialement les fonctions nécessaires à l'exploitation après l'atteinte de l'état contrôlé, pour empêcher que les EDD ne conduisent à des conséquences inacceptables ou pour gérer les conséquences des EDD. La mise en œuvre d'une fonction de catégorie B peut éviter le déclenchement d'une fonction de catégorie A. Les fonctions de catégorie B peuvent améliorer ou compléter l'exécution d'une fonction de catégorie A dans l'atténuation des conséquences d'un EDD, pour que des dommages portant sur la centrale ou sur des matériels ou des rejets radioactifs puissent être évités ou minimisés.

La catégorie B est aussi utilisée pour désigner les fonctions dont la défaillance pourrait initier ou aggraver un EDD. Le niveau des exigences de sûreté des fonctions de catégorie B n'a pas à être aussi élevé que celui des fonctions de catégorie A, du fait de la présence de ces fonctions de catégorie A pour assurer l'ultime prévention ou atténuation des conséquences des EDD. Cela permet, lorsque nécessaire, aux fonctions de catégorie B d'avoir une fonctionnalité supérieure à celle des fonctions de catégorie A au niveau de la méthode de détection de la nécessité d'agir ou dans leurs actions ultérieures.

5.3.4 Catégorie C

La catégorie C est utilisée pour désigner les fonctions qui tiennent un rôle auxiliaire ou indirect dans l'obtention et le maintien de la sûreté de la centrale nucléaire. La catégorie C recouvre toutes les fonctions qui ont une importance pour la sûreté et qui ne sont ni en catégorie A ni en catégorie B. Celles-ci peuvent faire partie de la réponse globale à un ADD sans être directement impliquées dans l'atténuation des conséquences physiques de l'accident ou être nécessaires pour un accident hors dimensionnement.

5.4 Critères de répartition dans les différentes catégories

5.4.1 Généralités

Les critères qui doivent être appliqués pour la répartition des fonctions dans les catégories A, B et C sont donnés ci-dessous.

Si une fonction ne satisfait à aucun des critères donnés ci-dessous, elle doit être considérée comme «non classée» (NC).

Dans le cas où la répartition est possible dans plusieurs catégories, au final, la fonction doit être affectée à la catégorie la plus haute possible.

L'affectation finale des fonctions peut être modifiée en utilisant des méthodes probabilistiques en cohérence avec les principes présentés en 6.3.

5.4.2 Catégorie A

Une fonction d'I&C doit être affectée à la catégorie A si elle remplit un des critères suivants:

a) fonctions nécessaires pour atteindre l'état contrôlé, pour empêcher qu'un EDD ne conduise à des conséquences inacceptables, ou pour gérer ses conséquences;

b) fonctions dont la défaillance ou la mise en oeuvre intempestive entraînerait des conséquences inacceptables et pour lesquelles il n'existe pas d'autre fonction de catégorie A pour parer à ces conséquences inacceptables;

c) fonctions nécessaires pour fournir de l'information et des moyens de commande qui permettent de réaliser les actions manuelles spécifiées nécessaires pour atteindre l'état contrôlé.

5.4.3 Catégorie B

Une fonction d'I&C doit être affectée à la catégorie B si elle satisfait un des critères suivants et si elle n'a pas, par ailleurs, été affectée à la catégorie A:

a) fonctions nécessaires, après atteinte de l'état contrôlé associé à un EDD, pour empêcher que cet EDD n'ait des conséquences inacceptables ou pour en atténuer les conséquences;

b) fonctions nécessaires pour fournir de l'information et des moyens de commande permettant de réaliser les actions manuelles spécifiées nécessaires après atteinte de l'état contrôlé pour empêcher qu'un EDD n'ait des conséquences inacceptables ou pour en atténuer les conséquences;

c) fonctions dont les défaillances en exploitation normale entraîneraient l'activation d'une fonction de catégorie A pour éviter un accident dont l'étude est requise;

d) fonctions requises au niveau de l'analyse de sûreté pour réduire de façon importante la fréquence d'EDD;

e) fonctions de commande du procédé maintenant dans les limites imposées par l'analyse de sûreté, des variables principales du procédé; ces fonctions étant les seuls moyens de commande de ces variables. Si plusieurs moyens peuvent être utilisés alors le 5.4.4 a) peut s'appliquer;

f) fonction utilisée pour empêcher ou limiter les rejets radioactifs ou l'endommagement du combustible au-delà des limites et des conditions de fonctionnement normal telles que définies dans l'analyse de sûreté;

NOTE 1 Ceci correspondant aux fonctions qui ne sont pas couvertes par l'analyse des EDD entraînant un classement en catégorie A.

g) fonctions qui assurent des tests, de façon continue ou intermittente, ou une surveillance de fonctions de catégorie A, pour garantir la continuité de leurs disponibilités opérationnelles et pour prévenir le personnel de la salle de commande de leurs défaillances, lorsque aucun autre moyen (par exemple tests périodiques) n'est mis en oeuvre pour vérifier leurs disponibilités[4].

NOTE 2 Lorsque la fonction de surveillance est le seul moyen de détection des défaillances qui sinon seraient cachées, le classement de la fonction en catégorie B garantit que le matériel qui assure la fonction est qualifié de façon appropriée.

5.4.4 Catégorie C

Une fonction d'I&C doit être affectée à la catégorie C si elle satisfait un des critères suivants et si elle n'a, par ailleurs, été affectée ni à la catégorie A ni à la catégorie B:

a) fonctions de commande du procédé maintenant dans les limites imposées par l'analyse de sûreté, des variables principales du procédé non couvertes par 5.4.3 e). Lorsque on utilise une combinaison de fonctions de catégorie C on doit justifier que cela est suffisant;

NOTE 1 Suivant la pratique nationale une application possible du paragraphe 5.4.4 a) est la combinaison de fonctions de régulation et d'actions manuelles appropriées reposant sur des alarmes indépendantes, ceci comprenant une justification de l'utilisation des actions manuelles.

b) fonctions utilisées pour prévenir ou atténuer des rejets radioactifs mineurs ou des dégradations mineures du combustible, dans les limites de dimensionnement de la centrale;

NOTE 2 Des rejets ou des endommagements de combustible sont considérés comme mineurs lorsqu'ils restent dans les limites et les conditions de fonctionnement normal (par exemple les limites de rejet).

---

[4] Le 4.2.6 de la CEI 60671 fournit des recommandations supplémentaires sur le classement des matériels utilisés pour mettre en oeuvre de telles fonctions et en particulier il est noté que lorsque «des caractéristiques d'essai pourraient interférer de façon inappropriée avec le bon fonctionnement du système ou du matériel réalisant la fonction importante pour la sûreté, ils doivent être affectés à la même catégorie».

c) fonctions qui assurent des tests, de façon continue ou intermittente, ou une surveillance de fonctions de catégories A et B, pour garantir la continuité de leurs disponibilités opérationnelles et pour prévenir le personnel de la salle de commande de leurs défaillances, et qui ne sont pas classées en catégorie B conformément à l'article 5.4.3 g);

d) fonctions nécessaires pour atteindre des objectifs probabilistes de sûreté, ceux-ci comprenant ceux de réduction de la fréquence prévue d'EDD;

e) fonctions permettant de réduire la sollicitation de fonction de catégorie A, comme requis dans l'analyse de sûreté;

f) fonctions de surveillance et d'atténuation relatives aux risques internes de la centrale couvertes par le dimensionnement de la centrale (exemple: incendie, inondation);

g) fonctions d'alerte du personnel ou assurant sa sûreté, pendant ou après des événements comprenant ou ayant entraîné des rejets radioactifs dans la centrale ou un risque d'exposition aux rayonnements;

h) fonctions permettant de surveiller et de décider d'actions d'atténuation suite à des phénomènes naturels (exemple: séisme, tempête);

i) fonctions prévues au titre de la stratégie de gestion accidentelle pour atteindre et maintenir l'état sûr lors des accidents hors dimensionnement;

j) fonctions installées pour minimiser les conséquences des accidents graves;

k) fonctions permettant de contrôler les accès à la centrale nucléaire.

6 Procédure de classement

6.1 Généralités

Un diagramme de la procédure est donné à la Figure 1.

6.2 Identification de la base de conception

La nature de la centrale et le type de réacteur (par exemple REP (réacteur à eau pressurisée), REB (réacteur à eau bouillante) ou autres types de réacteur), les EIP associés, et les principaux critères de conception sur la redondance des systèmes mécaniques et électriques et des matériels sont les principales données d'entrée du processus de classement. Une autre donnée d'entrée essentielle est la liste des fonctions de limitation principales des conséquences pour chaque EIP et de leurs fonctions supports.

L'évaluation de la fréquence et des conséquences des EIP conduit à l'identification des EDD représentant la base de conception de la centrale. Lors de l'étude des caractéristiques de conception de la centrale, la gamme des états de fonctionnement opérationnels et des conditions accidentelles spécifiées et des limites radiologiques prescrites doivent être retraduites. Les principes de sûreté individuels qui ensemble forment une «approche d'ensemble intégrée de sûreté» garantissent la sûreté de la centrale. Ces principes sont utilisés lors de la conception lorsqu'on considère les EDD identifiés et les barrières physiques successives permettant de maintenir les expositions aux rayonnements dans les limites permises. Les EDD et les principaux critères de conception de la centrale (redondance, séparation, etc.), ainsi que l'identification des fonctions de prévention et d'atténuation et leurs fonctions supports sont les données d'entrée essentielles du processus de classement.

L'importance pour la sûreté de chacune des fonctions d'I&C dépend de son rôle dans l'obtention et le maintien de la sûreté de la tranche et des conséquences potentielles d'une défaillance de celle-ci à fonctionner lorsque nécessaire. Ainsi, l'analyse initiale de sûreté spécifique à la tranche doit être complétée avant de classer les fonctions d'I&C.

6.3 Identification et classement des fonctions

Dès le début de la conception de la centrale, les fonctions relevant de la sûreté doivent être identifiées. Il est recommandé d'identifier ces fonctions et de les affecter à l'I&C ou aux

opérateurs, conformément aux exigences de la CEI 60964. Suite à cette identification initiale des fonctions, chaque fonction doit être affectée à une catégorie suivant les critères de l'Article 5.

La méthode de classement de l'importance pour la sûreté d'une fonction doit tout d'abord reposer sur des méthodes déterministes, complétées lorsque nécessaire par des méthodes probabilistes et le jugement de l'ingénieur, en prenant en compte des facteurs tels que:

- la ou les fonctions de sûreté à assurer;
- le rôle de la fonction dans la prévention ou l'atténuation des EIP;
- le rôle de la fonction durant tout les états opérationnels (par exemple: le démarrage, le fonctionnement normal, les rechargements, etc.);
- le rôle de la fonction après des EIP tels que les phénomènes naturels (par exemple: séisme, inondations, tempête, foudre) et les agressions internes (par exemple: incendie, inondation interne, missiles, rejet radioactifs d'une unité voisine, rejets chimiques d'autres usines et d'autres industries);
- les conséquences de la défaillance des fonctions d'I&C;
- les effets d'activations intempestives des fonctions d'I&C;
- la probabilité de la nécessité d'avoir recours à une fonction importante pour la sûreté;
- le temps après l'EDD pendant lequel ou auquel la fonction devra intervenir;
- la stratégie d'essai, de maintenance et de réparation.

Au début du processus de conception, il n'est pas possible d'identifier en détail toutes les fonctions, tant que toutes les caractéristiques de la centrale nucléaire n'ont pas été complètement définies. Il faut donc que le processus d'identification et de classement des fonctions se poursuive de façon itérative durant la phase de conception. Lorsque l'affectation initiale d'une fonction à une catégorie est incertaine, il convient d'ajouter à cette catégorisation un document explicatif.

Considérant que les fonctions individuelles peuvent être utilisées pour réaliser plusieurs aspects des exigences de spécifications, de telles fonctions peuvent être affectées à plusieurs catégories. Dans ce cas, le principe d'affectation à la catégorie la plus haute doit être appliqué.

La liste de classement doit être affinée et revue pour converger vers une liste finalisée, dès que la redondance, la diversité et les autres exigences techniques relatives aux fonctions sont fixées plus précisément, par exemple suite aux progrès faits dans l'analyse de sûreté et au développement des procédures de conduite. Cette liste doit être documentée et maintenue par contrôle de configuration car elle sera nécessaire aux concepteurs de la centrale et de l'I&C durant la vie de la centrale. Cette liste peut aussi être demandée par les autorités de sûreté.

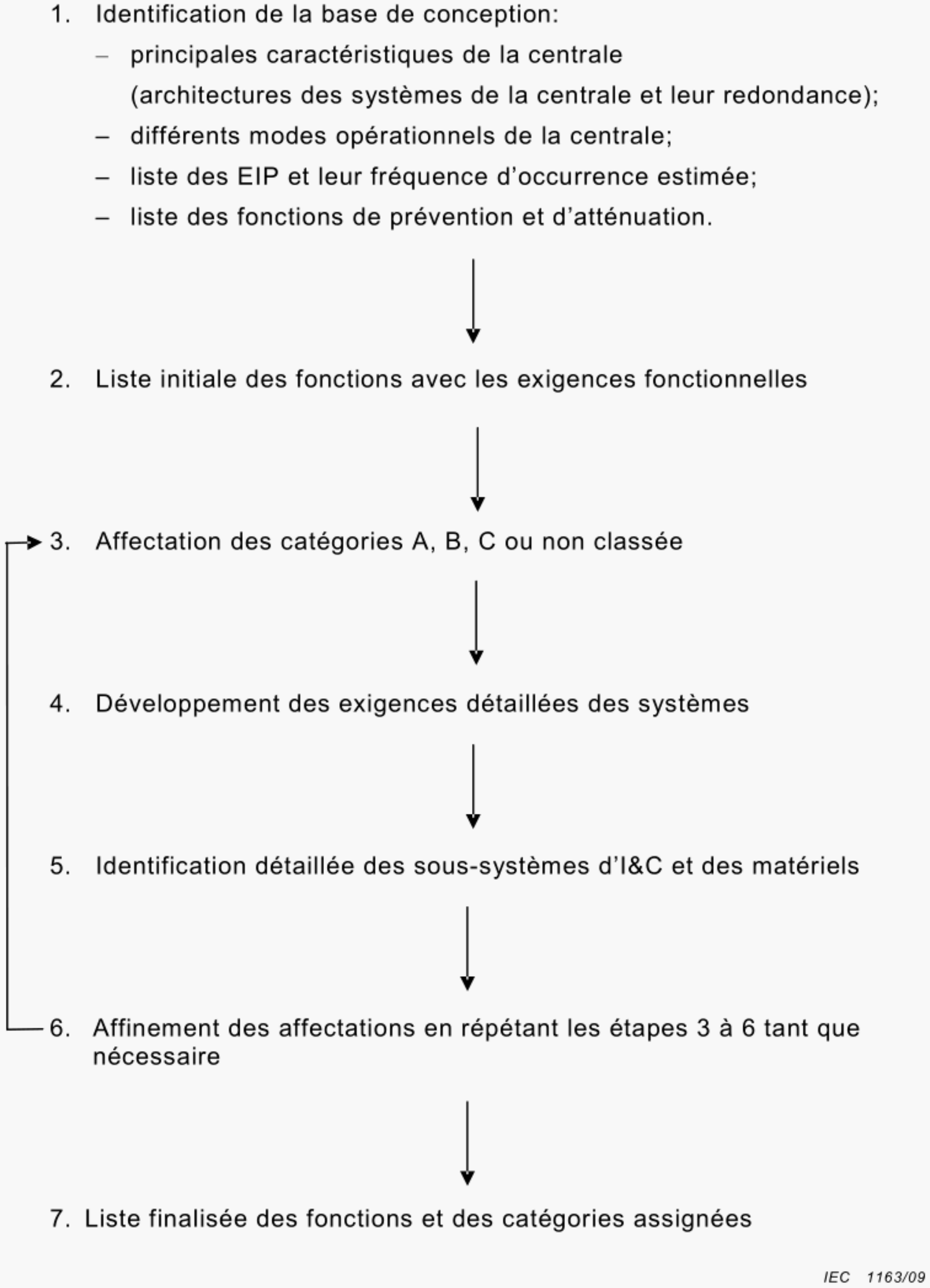

Figure 1 – Méthode de classement

7 Affectation des exigences techniques aux catégories

7.1 Exigences générales

Des exigences générales pour chaque catégorie A, B et C sont données dans ce paragraphe. Les exigences doivent être appliquées de façon appropriée durant les phases de spécifications, de conception, de validation, de qualification, de fabrication, d'installation, d'exploitation et de maintenance du cycle de vie de l'I&C. Les exigences techniques sont réparties en quatre groupes:

- exigences qui s'appliquent aux fonctions concernant les spécifications et la validation des fonctionnalités, des performances et de la fiabilité;
- exigences qui s'appliquent à la conception des systèmes d'I&C liées aux caractéristiques de conception telles que la redondance, la diversité, la testabilité et la séparation. Ces caractéristiques déterminent principalement la fiabilité des fonctions associées. Les exigences couvrent aussi les exigences liées à 'interface homme machine;
- exigences concernant les caractéristiques de tenue des matériels aux séismes, aux conditions d'ambiance et à la compatibilité électromagnétique;
- exigences associées à l'assurance qualité, à la vérification et à la maintenance, s'appliquant aux fonctions, aux systèmes et aux matériels.

Dans la plupart des cas, ces exigences sont déjà détaillées dans les codes et normes pertinents. Les codes, guides et normes listés à l'Article 2 de la présente norme sont des références normatives et donc fournissent les exigences explicites liées aux catégories de sûreté de l'I&C qui sont définies par la présente norme. La corrélation entre les catégories et les normes qui doit être appliquée est résumée au Tableau 1. Les exigences détaillées de ces normes ne sont pas répétées dans la présente norme. Ce tableau résume aussi les principaux types d'exigences concernant chaque catégorie. Dans le texte ci-dessous, quelques détails complémentaires sont fournis.

Il convient d'utiliser, quand que cela est possible, des matériels possédant un retour d'expérience avéré et documenté dans le domaine du nucléaire ou d'autres applications industrielles.

7.2 Exigences concernant les fonctions

7.2.1 Exigences de base

L'exigence de base concernant l'assurance de la fonctionnalité est l'existence d'un ensemble d'exigences fonctionnelles et de spécifications de conception claires, complètes et non ambiguës, par rapport auquel la fonction doit être vérifiée durant la conception, la fabrication, l'installation et le temps de service, et qui doit être utilisé comme référence pour toutes modifications en service.

Il est recommandé que les exigences de fiabilité portant sur toute fonction de catégories A, B ou C soient déterminées soit par une évaluation probabiliste quantitative de la centrale, soit par un jugement qualitatif de l'ingénieur, et qu'elles soient intégrées aux spécifications. On doit déterminer par des analyses appropriées, d'une façon structurée et en suivant un ensemble de procédures approuvées, les exigences de performances portant sur toutes les fonctions de catégories A, B ou C, et on doit les documenter.

Bien que les exigences de fiabilité portant sur les fonctions de différentes catégories puissent être les mêmes, le niveau d'assurance de l'atteinte du niveau de fiabilité requis par une fonction sera différent pour les trois catégories, la catégorie A demandant le plus haut niveau de confiance.

Il doit y avoir une séparation appropriée entre les fonctions de différentes catégories.

7.2.2 Exigences spécifiques

7.2.2.1 Catégorie A

La conception doit être conforme aux exigences des codes, guides et normes dont on a reconnu la pertinence, considérant le niveau élevé d'assurance de fonctionnalité exigé pour les fonctions de catégorie A. La conception doit veiller à faciliter la vérification et la validation de la fonctionnalité finale en maintenant la simplicité. Cela devrait permettre d'éviter de mettre en œuvre des fonctions de catégories inférieures dans des systèmes de catégorie A (par exemple, il convient que les affichages spéciaux pour les calculs et les traducteurs de protocoles de communication ne soient pas assurés par des systèmes numériques de sûreté).

Les exigences de fiabilité pour les fonctions d'I&C de catégorie A doivent être spécifiées comme indiqué en 7.1. Cela doit être fait en établissant les exigences de fiabilité pour les fonctions permettant d'atteindre un niveau faible de risques ayant des conséquences inacceptables, et déterminer ainsi à partir celles-ci les exigences de fiabilité pour les fonctions d'I&C.

7.2.2.2 Catégorie B

Le processus de conception doit se dérouler conformément aux codes, guides et normes pertinents sur le sujet, ou on peut aussi utiliser des systèmes et des matériels ayant un retour d'expérience en exploitation documenté et satisfaisant pour des applications similaires.

7.2.2.3 Catégorie C

Il convient de procéder à l'examen de la conception des systèmes et des matériels pour vérifier que ceux-ci ont été conçus ou testés pour assurer les fonctions spécifiées dans toute la gamme des états opérationnels, ceux-là comprenant les incidents ou les conditions de fonctionnement prévus les plus sévères dans lesquels la fonction est appelée à opérer.

7.3 Exigences applicables aux systèmes d'I&C

7.3.1 Exigences de base

Les exigences de conception des systèmes doivent garantir que la fonction aura la fiabilité spécifiée. Les exigences de base pour atteindre un haut niveau de fiabilité concernent les clauses applicables à la redondance, la diversité, l'espacement, la séparation physique et électrique et une IHM efficace. Durant la conception et au cours des modifications ultérieures, on doit prévoir pour tous les systèmes des moyens de détection et de réparation des défauts.

L'évaluation de la fiabilité et de la disponibilité doit prendre en compte les périodes de réparation, d'essai, de maintenance et la possibilité d'avoir des défauts cachés ou non. Les hypothèses faites dans l'analyse de fiabilité, concernant les périodes de maintenance, d'essai et de réparation doivent être vérifiées en exploitation et des mesures correctives doivent être prises si des différences avec celles-ci apparaissent.

Le processus de conception doit comprendre des exigences spécifiques concernant les facteurs humains et l'IHM. Il est recommandé que ces exigences soient le résultat d'un programme d'ergonomie, mis en œuvre dès les premières étapes de la phase de conception.

En exploitation, la conception du système doit permettre des essais en ligne et/ou périodiques, pour démontrer que les performances sont maintenues. Les exigences portant sur les essais périodiques et les activités de maintenance pour assurer la fiabilité à long terme des systèmes d'I&C importants pour la sûreté sont définies en 7.5.

Un ensemble suffisant d'équipements d'information et de commande doit être installé de préférence dans un local unique, séparé physiquement et électriquement de la salle de commande principale, pour pouvoir mettre et maintenir le réacteur en arrêt sûr, avec la

possibilité de surveiller les variables principales de la centrale pour le cas où il y aurait perte de la possibilité de réaliser ces fonctions dans la salle de commande principale.

7.3.2 Exigences spécifiques

7.3.2.1 Catégorie A

Un système d'I&C assurant des fonctions de catégorie A doit être redondant. Pour garantir que ces parties de système redondantes ne puissent être rendues non opérationnelles par un risque interne unique, celles-ci doivent être séparées de façon appropriée. Une défaillance unique ne doit pas entraîner la défaillance de la fonction de sûreté cible, et cela même durant la maintenance préventive, les essais périodiques, l'inspection ou les réparations. L'application du critère de défaillance unique doit se faire conformément au code AIEA NS-R-1, 5.34-5.39.

NOTE 1 Considérant les actions inappropriées des systèmes d'I&C, seules les actions intempestives (uniques ou multiples) qui peuvent être le résultat d'une défaillance unique dans les sous-systèmes d'I&C ou dans les systèmes supports sont généralement prises en compte.

Lorsque des fonctions de catégorie A doivent être réalisées par des opérateurs, des systèmes de surveillance et de commande conçus expressément pour cela doivent être fournis et isolés des autres systèmes de surveillance et de commande qui eux sont conçus de façon appropriée pour les temps de réaction requis.

La fiabilité des systèmes d'I&C qui réalisent les fonctions de catégories A doit être évaluée et comparée à celle spécifiée. Si des différences existent, elles doivent être résolues. L'estimation de la fiabilité doit considérer les conséquences des défaillances de cause commune, y compris les défaillances matérielles, les défaillances logicielles et les erreurs humaines durant l'exploitation, la maintenance, ainsi que les activités de modification et de réparation. Les techniques utilisées pour l'évaluation vont du jugement de l'ingénieur purement qualitatif à des analyses quantitatives détaillées, qui peuvent elles même dépendre d'estimations qualitatives. Le type d'analyse choisi doit être cohérent avec les exigences de fiabilité; plus le niveau de fiabilité requis est élevé, plus la technique doit être rigoureuse.

Lorsque les conséquences des défaillances de cause commune montrent que les objectifs de fiabilité des systèmes redondants ne peuvent être atteints, le principe de la diversité mise en œuvre dans des systèmes indépendants doit être appliqué (par exemple sur des critères probabilistes). La fonction concernée peut alors exiger l'emploi de deux ou plusieurs systèmes, indépendants les uns des autres. Lorsqu'une fonction de catégorie A est réalisée par deux systèmes indépendants ou plus, il convient que les systèmes soient de classe 1. Si on souhaite utiliser des systèmes de classe inférieure, au moins un des deux systèmes doit satisfaire aux exigences des systèmes de classe 1 et des justifications de sûreté doivent être fournies pour les systèmes ne satisfaisant pas les exigences des systèmes de classe 1 pour permettre de juger de leur acceptabilité.

NOTE 2 Pour un système individuel, spécifié et conçu en conformité avec les critères du plus haut niveau de qualité, une probabilité de l'ordre de 10^{-4} échec/demande peut être revendiquée comme une limite de fiabilité globale légitime, considérant que toutes les sources potentielles de défaillances dues aux spécifications, à la conception, à la fabrication, à l'installation, à l'environnement d'exploitation et aux pratiques de maintenance sont prises en compte. Ce chiffre comprend le risque de défaillance de cause commune dans les voies redondantes d'un système, et concerne l'ensemble du système, des capteurs en passant par les unités de traitement, jusqu'aux sorties vers les actionneurs. La possibilité de prétendre atteindre un niveau de fiabilité supérieur n'est pas exclue, mais cela demande des justifications spéciales, prenant en compte tous les facteurs déjà mentionnés. Une autre solution peut être d'utiliser des systèmes d'I&C importants pour la sûreté conçus de manière indépendante avec un niveau acceptable de diversification.

Les essais peuvent nécessiter l'inhibition des signaux de sortie, ou la mise en place de possibilités d'évitement. Si des possibilités d'évitement sont intégrées, leur intégrité doit faire l'objet de justifications et on doit montrer qu'elles ne peuvent être mises en œuvre d'une façon qui pourrait empêcher le système d'assurer ses fonctions de sûreté spécifiées. Par exemple, à un instant quelconque, leur utilisation pourrait physiquement réduire à une voie unique la redondance d'un système.

Pour certaines réalisations, il peut être nécessaire de mettre en place un niveau de redondance supplémentaire pour permettre le déroulement d'essais de routine, tranche en exploitation. Cela est nécessaire par exemple lorsque l'essai d'une voie active ne peut être réalisé en puissance et qu'il faut que les essais soient réalisés durant l'exploitation de la tranche pour assurer la fiabilité fonctionnelle requise. Dans de tels cas, il n'est pas nécessaire de prévoir un niveau de redondance supplémentaire pour tout le système.

Les sources d'énergie doivent être secourues.

Pour les systèmes de catégorie A, on doit réaliser une analyse formelle des défaillances des systèmes, par exemple une analyse des modes de défaillances et de leurs effets (AMDE), pour identifier la vulnérabilité des systèmes aux défaillances de composants et pour évaluer la pertinence des stratégies de conception appliquées pour détecter de telles défaillances ou pour en atténuer leurs conséquences.

Lorsqu'un système intègre des mécanismes de diagnostic interne des défaillances et que ceux-ci sont pris en considération dans l'analyse de fiabilité de la fonction, l'analyse des défaillances doit les évaluer et estimer la couverture de ces tests internes. Si l'analyse des défaillances montre que certaines défaillances peuvent ne pas être détectées et signalées aux opérateurs par le système de diagnostic interne, alors des essais de preuve doivent être développés pour mettre à jour de telles défaillances. La durée de l'intervalle entre ces essais de preuve doit être calculée à partir de la fréquence probable de l'occurrence de la défaillance non détectée et de la fiabilité requise de la fonction.

Lorsque les données relatives à la fiabilité ne sont pas disponibles, l'intervalle de test doit être choisi par comparaison à d'autres systèmes similaires. Lorsque le retour d'expérience est constitué, l'intervalle de test de la fonction doit être réévalué.

7.3.2.2 Catégorie B

La fiabilité du système qui assure des fonctions d'I&C de catégorie B doit être évaluée et comparée à l'objectif de fiabilité spécifié pour les fonctions. Une fonction de cette catégorie doit être assurée à l'aide de moyens redondants et séparés, à moins qu'une justification ne soit fournie. Une telle justification peut reposer par exemple sur la capacité du système à atteindre ses objectifs de fiabilité sans redondance ni séparation, sur l'acceptabilité des conséquences de la défaillance de la fonction, ou sur le temps disponible pour fournir une autre solution si la fonction fait défaut.

Les sources d'énergie doivent être secourues.

Il doit être démontré que les composants employés ont un haut niveau de qualité et de fiabilité, et les moyens de garantir que les fautes peuvent être rapidement détectées et réparées doivent être intégrés.

Les principaux objectifs de la conception fonctionnelle des systèmes requis pour offrir les moyens d'information et de commande qui permettent de réaliser les actions manuelles nécessaires pour limiter les conséquence des EDD à dans la salle de commande sont de fournir à temps aux opérateurs l'information complète et précise relative à l'état des matériels et des systèmes de tranche pour tous les EDD et de minimiser les déplacements nécessaires de l'opérateur pour surveiller et commander l'installation.

Les essais périodiques et/ou en ligne des performances doivent permettre aussi de confirmer la capacité fonctionnelle des sous-systèmes, en particulier les essais individuels des voies redondantes.

7.3.2.3 Catégorie C

Un système de cette catégorie ne doit généralement pas être redondant, ni faire l'objet de mesures de séparation. Ce peut être le cas si cela est nécessaire pour atteindre le niveau de fiabilité spécifié pour la fonction. La tolérance aux risques internes et externes peut être requise.

Des sources d'énergie auxiliaires peuvent être utilisées, sur la base du cas par cas.

Lorsque pour atteindre un niveau de fiabilité spécifié, la redondance est requise pour les systèmes réalisant des fonctions de catégorie C, il convient de considérer la redondance de la même façon que pour la catégorie B.

Lorsqu'il y a redondance, on doit intégrer des essais périodiques individuels de la capacité fonctionnelle de tous les systèmes ou sous-systèmes redondants. Les essais en ligne sont un moyen de satisfaire à cette exigence.

7.4 Exigences liées aux matériels

7.4.1 Exigences de base

Il est nécessaire de garantir que les matériels n'auront pas de défaillances dues aux conditions d'ambiance résultant des EIP et auxquelles ils peuvent être soumis pendant et après ceux-ci. Cette garantie peut être apportée par une qualification des matériels. Lorsque la qualification est requise, celle-ci peut être réalisée en utilisant une ou plusieurs méthodes: par exemple par essais, par analyse, par une combinaison de ces deux dernières ou aussi en utilisant les données disponibles sur le retour d'expérience. On doit déterminer et indiquer dans les spécifications d'exigences les conditions d'ambiance les pires dans lesquelles le matériel doit fonctionner, y compris celles concernant les séismes.

Lorsque que l'on demande à des fonctions qui ne sont pas conçues à l'origine pour faire face aux accidents graves ou hors dimensionnement de jouer un rôle lors de ces accidents, il convient d'évaluer les capacités de leurs composants de façon à montrer qu'elles sont capables d'opérer dans les conditions d'ambiance prévues.

7.4.2 Exigences spécifiques

7.4.2.1 Catégorie A

Les mesures prises pour fournir l'assurance que les matériels de catégorie A continueront de fonctionner dans toutes les conditions opérationnelles prévues doivent inclure une qualification matérielle. Les résultats des essais doivent être enregistrés et conservés durant la durée de vie de la centrale. Toute défaillance durant les essais de qualification doit faire l'objet d'investigations, et les causes et les modifications de la défaillance doivent être documentées.

7.4.2.2 Catégorie B

Les matériels de catégorie B doivent faire l'objet d'une qualification réalisée comme celle des matériels de catégorie A.

7.4.2.3 Catégorie C

Suivant la fonction supportée, les matériels de catégorie C peuvent nécessiter une qualification. Il convient de comparer systématiquement la conception des matériels aux spécifications d'exigences des conditions d'ambiance les pires dans lesquelles le matériel doit fonctionner.

Lorsque le matériel est nouveau, ou lorsqu'il doit fonctionner dans des conditions pour lesquelles le matériel commercial n'a pas été normalement conçu (telles que les séismes ou les conditions d'ambiance extrêmes), on doit établir un ensemble de règles par rapport auxquelles on réalise la conception ou par rapport auxquelles la conception du matériel existant est évaluée. Ces règles doivent reposer sur l'expérience acquise au niveau des exigences de conception spéciales des matériels de catégorie A. Il convient que les matériels mis en œuvre dans le cadre des fonctions classées en appliquant les critères 5.4.4 i) et j) soient spécifiquement conçus en fonction des conditions d'ambiance et de procédé extrêmes qui pourraient survenir et telles que déterminées par l'analyse. L'adéquation d'un matériel produit suivant des normes commerciales à être utilisé pour la réalisation de ces fonctions doit faire l'objet d'une révision particulière.

Pour les autres cas, les matériels de catégorie C peuvent être acceptés sur la base des normes de conception commerciales courantes à moins que le rôle du matériel ne nécessite une qualification spéciale, par exemple des exigences sismiques ou de prévention des incendies, pour la prévention des survoltages ou des perturbations électriques produites par les matériels de la catégorie C et pouvant affecter les fonctions de catégorie A ou B. Le fait de prétendre pouvoir fonctionner dans des conditions d'ambiance anormales doit être justifié par des preuves documentées.

7.5 Exigences liées aux aspects de qualité (AQ)

7.5.1 Exigences de base

Les exigences générales sont liées à l'assurance qualité réalisée pendant les phases de conception, de fabrication, d'installation, de mise en service et d'exploitation, de façon à garantir des performances correctes pour les systèmes et les matériels concernés.

Les objectifs d'AQ sont la gestion de configuration, le contrôle des modifications et la traçabilité. La conception doit être documentée de façon suffisamment détaillée pour servir de support durant les périodes de fabrication, d'installation, de mise en service et d'exploitation de la tranche, ainsi que pour les vérifications réalisées à chaque étape. On doit faire tout particulièrement attention aux précautions documentaires qui permettront des modifications ultérieures de conception.

De plus, il convient de prévoir pour les développements, proportionnellement au caractère novateur ou complexe des nouvelles conceptions ou des modifications, une AQ et des essais spéciaux. Il convient de documenter ces activités de développement en fonction de l'importance pour la sûreté des fonctions.

Un plan d'AQ conforme à une norme ou un code pertinents doit être mis en place. Il doit imposer la définition et la vérification des spécifications des performances et des essais.

L'essai de composants, modules, sous-systèmes et systèmes doit être fait conformément à un plan d'AQ pour démontrer, en tenant compte de la catégorie de la fonction, le déroulement satisfaisant des phases de fabrication, d'assemblage et d'installation sur le site.

Les essais doivent être réalisés sur des composants, des modules et des sous-systèmes afin de garantir qu'avec l'AQ de fabrication, les fonctions satisfont aux spécifications d'exigences. Des essais combinés du système d'I&C installé avec les systèmes hydrauliques et mécaniques, dans un mode nécessitant la disponibilité des fonctions de sûreté assurées par le système, doivent être réalisés sur la tranche avant l'exploitation.

L'objectif des essais sur site est le même pour toutes les catégories, mais le contrôle qualité et les exigences de documentation diffèrent suivant la catégorie, comme précisé ci-après.

Des essais doivent être faits en exploitation pour démontrer que l'état des composants matériels de l'I&C importants pour la sûreté n'est pas dégradé par les défaillances. Les systèmes d'I&C doivent être conçus pour permettre de faire des essais appropriés et détecter

les défaillances dans les matériels. Les défauts identifiés doivent être corrigés en respectant une procédure de contrôle des modifications. L'enregistrement adapté de ces corrections doit être conservé. Lorsqu'il y a redondance, les vérifications individuelles de la fonctionnalité des canaux redondants doivent faire partie des essais. L'intervalle entre les essais doit être choisi pour que le taux de défaillance évalué ou la probabilité d'échec de fonctionnement sur demande satisfasse aux exigences de l'analyse de fiabilité.

Lorsque du matériel informatique est utilisé, on doit mettre en place un programme qualité pour le cycle de vie logiciel pertinent pour la catégorie de la fonction.

7.5.2 Exigences spécifiques

7.5.2.1 Catégorie A

Les exigences d'AQ doivent être conformes à la norme de sûreté AIEA GS-R-3. La documentation doit permettre de retracer l'historique d'un matériel et couvrir la conception, la fabrication et les aspects opérationnels. Cela comprend, pour la conception, tous les matériels jusqu'au niveau module. La configuration doit être contrôlée jusqu'au plus petit élément traçable. La traçabilité des numéros de lot, des matériaux, etc. doit être étendue à tout le système jusqu'au niveau module individuel.

La documentation d'AQ doit permettre, lors d'investigations, de remonter d'un élément matériel ou logiciel jusqu'aux spécifications qui définissent les exigences pour celui-ci, et de descendre de n'importe quelle exigence des spécifications jusqu'aux composants qui la satisfont.

Les essais de type doivent être réalisés pour montrer qu'un matériel de fabrication identique à celui installé sur la tranche fonctionnera comme demandé lors de la conception en présence de l'environnement opérationnel prévu.

Les essais fonctionnels doivent être réalisés sur les composants, modules, sous-systèmes et, lorsque c'est possible, sur les systèmes entiers. L'exploitant ou ses représentants doivent être témoins des essais.

Les essais fonctionnels peuvent être réalisés dans l'usine ou sur le site. Les essais réalisés à l'usine et sur le site doivent être coordonnés pour garantir que la couverture des essais est totale. Lorsqu'il n'est pas possible de prouver que toutes les fonctions spécifiées peuvent être réalisées, en garantissant la couverture totale, des justifications spéciales doivent être fournies.

Les essais de site doivent démontrer, autant que possible, que les fonctions de sûreté spécifiées, supportées par les systèmes et les matériels installés, atteignent leurs objectifs avec les performances désirées. Ces essais doivent prendre en compte les variations de paramètres opérationnels. On parle alors d'essai de recette site (RS), et l'exploitant ou ses représentants doivent en être témoins.

Les essais en ligne ou périodiques doivent montrer que l'aptitude du système à assurer toutes les fonctions de sûreté requises n'a pas été détériorée; ceux-ci couvrent les sous-systèmes nécessaires pour réaliser ces fonctions. Les intervalles de temps entre essais doivent être choisis en fonction du niveau d'auto-surveillance, de façon à atteindre les objectifs de fiabilité des systèmes d'I&C importants pour la sûreté, en prenant en compte les taux de défaillance des composants d'I&C prévus ou observés.

7.5.2.2 Catégorie B

Les exigences d'AQ doivent être conformes à la norme de sûreté AIEA GS-R-3. La documentation doit permettre de retracer l'histoire d'un matériel et de couvrir la conception, la fabrication et les aspects opérationnels. Le niveau de détail de l'AQ applicable aux fonctions, systèmes et matériels de la catégorie B peut être plus bas que celui applicable aux fonctions,

systèmes et matériels de la catégorie A, bien qu'il soit recommandé que le programme d'AQ soit cohérent avec celui de la catégorie A.

Les essais de type doivent être réalisés avec un matériel de fabrication similaire à celui installé sur la tranche, à condition qu'une analyse ait été réalisée pour montrer que les différences de matériels n'invalident pas les résultats des essais.

Des essais fonctionnels doivent être réalisés avant la mise en exploitation pour montrer que chaque fonction spécifiée peut être assurée par le système formé de matériels d'une fabrication similaire de ceux installés sur la tranche. Certains de ces essais peuvent être faits sur site.

Les essais recette site (RS) doivent montrer, autant que possible, que toutes les fonctions de sûreté spécifiées du matériel installé peuvent être assurées. Les essais du matériel de commande doivent montrer son aptitude à répondre correctement aux transitoires et aux demandes de changements. Les essais d'affichage et d'équipements d'alarme doivent comprendre des essais d'injection de signaux d'entrée pertinents pour mettre en évidence leurs performances satisfaisantes.

7.5.2.3 Catégorie C

Les matériels et systèmes réalisant des fonctions de catégorie C peuvent être acceptés sur la base d'une AQ de niveau commercial.

L'exploitant peut accepter les essais constructeur et juger qu'ils sont adaptés pour démontrer que les performances spécifiées seront atteintes. Ces essais doivent être réalisés sur des matériels similaires. Il convient de réaliser les essais spécifiques de type et les essais fonctionnels qui sont nécessaires, mais généralement ceux-ci ne sont pas requis.

Il convient de réaliser les essais recette site pour montrer que le système assure les fonctionnalités et performances liées à la sûreté qui ont été spécifiées.

Les essais périodiques des performances peuvent être limités à des vérifications ayant lieu durant les arrêts pour rechargement ou les périodes d'arrêt similaires, pour les fonctions qui ne sont pas continuellement en service.

Tableau 1 – Table de corrélation entre les catégories et les autres normes CEI

Catégorie	Normes CEI applicables		Exigences principales pour			
	Systèmes	Matériel	Fonctions	Conception système	Spécificités matérielles	Généralités
Toutes catégories	CEI 61513 CEI 60964, CEI 60965 CEI 61771, CEI 61772 CEI 61839 CEI 60709	CEI 61000-4 CEI 61000-6-2	Spécification fonctionnelle	Testabilité Spécification IHM	Compatibilité électromagnétique	Programme AQ Contrôle qualité RU, RS Essais périodiques
A	CEI 60812[5] CEI 60880 CEI 60987	CEI 60780, CEI 60980	Codes, normes, guides pertinents Séparation des catégories inférieures Haut niveau d'assurance de la fiabilité	Critère de défaillance unique Indépendance, séparation Conception prenant en compte les DCC internes Diversification au cas par cas AMDE Secours sources électriques	Qualification aux conditions d'ambiance prévues et aux séismes	AIEA GS-R-3 Vérification sur matériel identique RU/RS complètes Essais périodiques fréquents
B	CEI 60987 CEI 62138	CEI 60780, CEI 60980	Codes, normes, guides pertinents Séparation des catégories inférieures	Critère de défaillance unique, séparation possible au niveau fonctionnel Secours sources électriques	Qualification aux conditions d'ambiance prévues et aux séismes, auxquels le matériel doit résister	AIEA GS-R-3 Vérification sur matériel similaire RS limitée et essais périodiques
C	CEI 62138			Redondance et séparation au cas par cas	Qualification au cas par cas	Pratique industrielle courante Essais périodiques si pas d'utilisation en service continu

5 Lorsque l'analyse de défaillance est une AMDE.

Annexe A
(informative)

Exemples de catégories

A.1 Généralités

La présente annexe fournit des exemples d'affectation de fonctions et de systèmes de contrôle-commande typiques aux catégories A, B et C. Il convient de noter cependant que ces exemples ne sont pas pertinents pour tous les types de réacteurs.

A.2 Catégorie A

A.2.1 Fonctions typiques

Les fonctions d'I&C affectées à la catégorie A sont nécessaires pour

a) l'arrêt du réacteur et son maintien en état sous-critique;

b) l'isolement de l'enceinte;

c) les moyens d'information opérateur concernant les actions essentielles;

d) évacuation de la chaleur résiduelle vers la source froide d'ultime secours.

A.2.2 Systèmes d'I&C typiques

Les systèmes d'I&C typiques sont les suivants:

a) système de protection réacteur;

b) système des actionneurs de sûreté et systèmes de sûreté supports;

c) l'instrumentation et l'affichage clé permettant la réalisation des actions opérateurs préalablement planifiées dans les instructions opérationnelles de la tranche et nécessaires pour garantir la sûreté de celle-ci dans le court terme.

A.3 Catégorie B

A.3.1 Fonctions typiques

Les fonctions d'I&C affectées à la catégorie B sont nécessaires pour

a) le système de refroidissement de la piscine contenant le combustible usagé;

b) l'isolement du système de refroidissement principal;

c) le système de surveillance post accidentel;

d) les commandes automatiques des conditions de circuit du primaire et du secondaire de la tranche, permettant de conserver les variables principales dans les limites définies par l'analyse de sûreté et pour éviter que les événements ne dégénèrent en accident;

e) la surveillance/contrôle lors de la manipulation du combustible où une défaillance pourrait entraîner un rejet radioactif ou un endommagement du combustible sortant des conditions et des limites du fonctionnement normal.

A.3.2 Systèmes d'I&C typiques

Les systèmes d'I&C typiques sont les suivants:

Annexe A
(informative)

Exemples de catégories

A.1 Généralités

La présente annexe fournit des exemples d'affectation de fonctions et de systèmes de contrôle-commande typiques aux catégories A, B et C. Il convient de noter cependant que ces exemples ne sont pas pertinents pour tous les types de réacteurs.

A.2 Catégorie A

A.2.1 Fonctions typiques

Les fonctions d'I&C affectées à la catégorie A sont nécessaires pour

a) l'arrêt du réacteur et son maintien en état sous-critique;

b) l'isolement de l'enceinte;

c) les moyens d'information opérateur concernant les actions essentielles;

d) évacuation de la chaleur résiduelle vers la source froide d'ultime secours.

A.2.2 Systèmes d'I&C typiques

Les systèmes d'I&C typiques sont les suivants:

a) système de protection réacteur;

b) système des actionneurs de sûreté et systèmes de sûreté supports;

c) l'instrumentation et l'affichage clé permettant la réalisation des actions opérateurs préalablement planifiées dans les instructions opérationnelles de la tranche et nécessaires pour garantir la sûreté de celle-ci dans le court terme.

A.3 Catégorie B

A.3.1 Fonctions typiques

Les fonctions d'I&C affectées à la catégorie B sont nécessaires pour

a) le système de refroidissement de la piscine contenant le combustible usagé;

b) l'isolement du système de refroidissement principal;

c) le système de surveillance post accidentel;

d) les commandes automatiques des conditions de circuit du primaire et du secondaire de la tranche, permettant de conserver les variables principales dans les limites définies par l'analyse de sûreté et pour éviter que les événements ne dégénèrent en accident;

e) la surveillance/contrôle lors de la manipulation du combustible où une défaillance pourrait entraîner un rejet radioactif ou un endommagement du combustible sortant des conditions et des limites du fonctionnement normal.

A.3.2 Systèmes d'I&C typiques

Les systèmes d'I&C typiques sont les suivants:

Annexe A
(informative)

Exemples de catégories

A.1 Généralités

La présente annexe fournit des exemples d'affectation de fonctions et de systèmes de contrôle-commande typiques aux catégories A, B et C. Il convient de noter cependant que ces exemples ne sont pas pertinents pour tous les types de réacteurs.

A.2 Catégorie A

A.2.1 Fonctions typiques

Les fonctions d'I&C affectées à la catégorie A sont nécessaires pour

a) l'arrêt du réacteur et son maintien en état sous-critique;

b) l'isolement de l'enceinte;

c) les moyens d'information opérateur concernant les actions essentielles;

d) évacuation de la chaleur résiduelle vers la source froide d'ultime secours.

A.2.2 Systèmes d'I&C typiques

Les systèmes d'I&C typiques sont les suivants:

a) système de protection réacteur;

b) système des actionneurs de sûreté et systèmes de sûreté supports;

c) l'instrumentation et l'affichage clé permettant la réalisation des actions opérateurs préalablement planifiées dans les instructions opérationnelles de la tranche et nécessaires pour garantir la sûreté de celle-ci dans le court terme.

A.3 Catégorie B

A.3.1 Fonctions typiques

Les fonctions d'I&C affectées à la catégorie B sont nécessaires pour

a) le système de refroidissement de la piscine contenant le combustible usagé;

b) l'isolement du système de refroidissement principal;

c) le système de surveillance post accidentel;

d) les commandes automatiques des conditions de circuit du primaire et du secondaire de la tranche, permettant de conserver les variables principales dans les limites définies par l'analyse de sûreté et pour éviter que les événements ne dégénèrent en accident;

e) la surveillance/contrôle lors de la manipulation du combustible où une défaillance pourrait entraîner un rejet radioactif ou un endommagement du combustible sortant des conditions et des limites du fonctionnement normal.

A.3.2 Systèmes d'I&C typiques

Les systèmes d'I&C typiques sont les suivants:

Annexe A
(informative)

Exemples de catégories

A.1 Généralités

La présente annexe fournit des exemples d'affectation de fonctions et de systèmes de contrôle-commande typiques aux catégories A, B et C. Il convient de noter cependant que ces exemples ne sont pas pertinents pour tous les types de réacteurs.

A.2 Catégorie A

A.2.1 Fonctions typiques

Les fonctions d'I&C affectées à la catégorie A sont nécessaires pour

a) l'arrêt du réacteur et son maintien en état sous-critique;

b) l'isolement de l'enceinte;

c) les moyens d'information opérateur concernant les actions essentielles;

d) évacuation de la chaleur résiduelle vers la source froide d'ultime secours.

A.2.2 Systèmes d'I&C typiques

Les systèmes d'I&C typiques sont les suivants:

a) système de protection réacteur;

b) système des actionneurs de sûreté et systèmes de sûreté supports;

c) l'instrumentation et l'affichage clé permettant la réalisation des actions opérateurs préalablement planifiées dans les instructions opérationnelles de la tranche et nécessaires pour garantir la sûreté de celle-ci dans le court terme.

A.3 Catégorie B

A.3.1 Fonctions typiques

Les fonctions d'I&C affectées à la catégorie B sont nécessaires pour

a) le système de refroidissement de la piscine contenant le combustible usagé;

b) l'isolement du système de refroidissement principal;

c) le système de surveillance post accidentel;

d) les commandes automatiques des conditions de circuit du primaire et du secondaire de la tranche, permettant de conserver les variables principales dans les limites définies par l'analyse de sûreté et pour éviter que les événements ne dégénèrent en accident;

e) la surveillance/contrôle lors de la manipulation du combustible où une défaillance pourrait entraîner un rejet radioactif ou un endommagement du combustible sortant des conditions et des limites du fonctionnement normal.

A.3.2 Systèmes d'I&C typiques

Les systèmes d'I&C typiques sont les suivants:

Annexe A
(informative)

Exemples de catégories

A.1 Généralités

La présente annexe fournit des exemples d'affectation de fonctions et de systèmes de contrôle-commande typiques aux catégories A, B et C. Il convient de noter cependant que ces exemples ne sont pas pertinents pour tous les types de réacteurs.

A.2 Catégorie A

A.2.1 Fonctions typiques

Les fonctions d'I&C affectées à la catégorie A sont nécessaires pour

a) l'arrêt du réacteur et son maintien en état sous-critique;

b) l'isolement de l'enceinte;

c) les moyens d'information opérateur concernant les actions essentielles;

d) évacuation de la chaleur résiduelle vers la source froide d'ultime secours.

A.2.2 Systèmes d'I&C typiques

Les systèmes d'I&C typiques sont les suivants:

a) système de protection réacteur;

b) système des actionneurs de sûreté et systèmes de sûreté supports;

c) l'instrumentation et l'affichage clé permettant la réalisation des actions opérateurs préalablement planifiées dans les instructions opérationnelles de la tranche et nécessaires pour garantir la sûreté de celle-ci dans le court terme.

A.3 Catégorie B

A.3.1 Fonctions typiques

Les fonctions d'I&C affectées à la catégorie B sont nécessaires pour

a) le système de refroidissement de la piscine contenant le combustible usagé;

b) l'isolement du système de refroidissement principal;

c) le système de surveillance post accidentel;

d) les commandes automatiques des conditions de circuit du primaire et du secondaire de la tranche, permettant de conserver les variables principales dans les limites définies par l'analyse de sûreté et pour éviter que les événements ne dégénèrent en accident;

e) la surveillance/contrôle lors de la manipulation du combustible où une défaillance pourrait entraîner un rejet radioactif ou un endommagement du combustible sortant des conditions et des limites du fonctionnement normal.

A.3.2 Systèmes d'I&C typiques

Les systèmes d'I&C typiques sont les suivants: