

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Categorization of functions and classification of systems

Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique importants pour la sûreté – Catégorisation des fonctions et classement des systèmes



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2020 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 l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

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

About the IEC

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

About IEC publications

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

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

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

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC

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

A propos des publications IEC

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

Recherche de publications IEC -

webstore.iec.ch/advsearchform

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

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Nuclear power plants – Instrumentation, control and electrical power systems
important to safety – Categorization of functions and classification of systems**

**Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-
commande et d'alimentation électrique importants pour la sûreté –
Catégorisation des fonctions et classement des systèmes**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-7973-1

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	8
2 Normative references	9
3 Terms and definitions	10
4 Abbreviated terms	16
5 Categorization scheme	16
5.1 General.....	16
5.2 Background	17
5.3 Description of categories	17
5.3.1 General	17
5.3.2 Category A	19
5.3.3 Category B	19
5.3.4 Category C	19
5.4 Assignment criteria	19
5.4.1 General	19
5.4.2 Category A	20
5.4.3 Category B	20
5.4.4 Category C	20
6 Categorization/classification procedure	21
6.1 General.....	21
6.2 Identification of anticipated operational occurrences (AOO), design basis accidents (DBA) and design extension conditions (DEC).....	22
6.3 Identification and categorization of functions.....	23
6.4 Classification of systems.....	23
6.4.1 Classification of I&C systems.....	23
6.4.2 Classification of electrical power systems	25
7 Assignment of technical requirements to categories and classes	25
Annex A (normative) Assignment of technical requirements to I&C systems.....	28
A.1 General.....	28
A.2 Requirements related to functions.....	28
A.2.1 Basic requirements	28
A.2.2 Specific requirements	28
A.3 Requirements related to systems	29
A.3.1 Basic requirements	29
A.3.2 Specific requirements	30
A.4 Requirements related to equipment qualification	32
A.4.1 Basic requirements	32
A.4.2 Specific requirements	32
A.5 Requirements related to quality aspects.....	33
A.5.1 Basic requirements	33
A.5.2 Specific requirements	34
Annex B (informative) Examples of categories and classes	36
B.1 General.....	36
B.2 Category A/Class 1	36

B.2.1	Typical functions.....	36
B.2.2	Typical I&C systems	36
B.2.3	Typical electrical power systems.....	36
B.3	Category B/Class 2.....	36
B.3.1	Typical functions.....	36
B.3.2	Typical I&C systems	37
B.3.3	Typical electrical power systems.....	37
B.4	Category C/Class 3.....	37
B.4.1	Typical functions.....	37
B.4.2	Typical I&C and electrical power systems	37
	Bibliography.....	39
	Figure 1 – Overall classification scheme	9
	Figure 2 – Method of categorization of functions and classification of I&C systems.....	22
	Figure 3 – Method of classification of electrical power systems.....	25
	Table 1 – Correlation between classes of systems and categories of functions	24
	Table 2 – Tabular correlation between classes and other IEC standards.....	27

IECNORM.COM : Click to view the full PDF of IEC 61226:2020

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**NUCLEAR POWER PLANTS – INSTRUMENTATION, CONTROL
AND ELECTRICAL POWER SYSTEMS IMPORTANT TO SAFETY –
CATEGORIZATION OF FUNCTIONS AND CLASSIFICATION OF SYSTEMS**

FOREWORD

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

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

This fourth edition cancels and replaces the third edition published in 2009. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) to align on IAEA requirements, recommendations and terminology, particularly to take into account the replacement of NS-R-1 by SSR 2/1 and publication of SSG 30;
- b) to extend the scope to electrical power systems;
- c) to move the detailed requirements applying to functions and I&C systems to a normative annex, which will be removed after updating IEC 61513.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
45A/1301/FDIS	45A/1306/RVD

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

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

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

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

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

INTRODUCTION

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

This International Standard responds to an International Atomic Energy Agency (IAEA) requirement¹ to identify and classify nuclear power plants important to safety items on the basis of their functions and safety significance. With the application of the concept of Defence in Depth, which is implemented through the combination of a number of consecutive and sufficiently independent levels of protection, the functions important to safety are distributed over several systems or subsystems. In addition, with programmable digital items now being used for NPP instrumentation and control systems, each system or sub-system often performs many functions. Therefore, it is the intent of this standard to establish the criteria and methods to be used to:

- identify and assign the functions important to safety into categories, depending on their contribution to the prevention and mitigation of postulated initiating events (PIE);
- classify accordingly the I&C and electrical power systems which are necessary to perform these functions.

According to IAEA Safety Standard SSR-2/1 (Requirement 22), the method for classifying the items important to safety shall be based primarily on deterministic methods, complemented where appropriate by probabilistic methods. Several possible approaches for use of probabilistic safety assessment (PSA) for classification are described in IEC TR 61838.

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 that deals with the categorization of functions and classification of I&C and electrical power 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 document

Correct categorization of functions is essential to ensure 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.

This standard establishes the criteria and methods to be used to assign the functions of a NPP accomplished by I&C and electrical power systems to three categories A, B and C, which depend on the importance of the function for safety. Functions with no direct safety role are non categorized (NC).

The category to which a function is assigned determines technical requirements based on providing the appropriate level of assurance that the function will be executed on demand with the required performance and reliability and have the necessary environmental durability and QA. The level of assurance to be shown for each of these aspects shall be consistent with the importance of the function to safety.

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

The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

¹ IAEA SSR-2/1 requirement 22 considering also requirements 4, 18 and 27.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 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 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular, this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA Safety Guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA Safety Guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA Safety Guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A security standards. It builds upon the valid high-level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015, discussions were held in IEC SC 45A to decide how and where general requirements for the design of electrical systems were to be considered. IEC SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 is published, this Note 2 of the introduction of IEC SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS IMPORTANT TO SAFETY – CATEGORIZATION OF FUNCTIONS AND CLASSIFICATION OF SYSTEMS

1 Scope

This document establishes, for nuclear power plants², a method of assignment of the functions specified for the plant into categories according to their importance to safety. Subsequent classification of the I&C and electrical power systems performing or supporting these functions, based on the assigned category, then determines relevant design criteria.

The design criteria, when applied, ensure the achievement of each function in accordance to its importance to safety. In this document, the criteria are those of functionality, reliability, performance, environmental qualification (e.g. seismic) and quality assurance (QA).

This document is applicable to:

- the functions important to safety that are performed by I&C systems and supported by electrical power systems (categorization of I&C functions),
- the I&C systems that enable those functions to be implemented (classification of I&C systems),
- the electrical power systems that support those functions (classification of electrical power systems).

The systems under consideration provide automated protection, closed or open loop control, information to the operating staff, and electrical power supply to systems. These systems 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 and electrical power systems that fulfil these roles safeguard the health and safety of the NPP operators and the public.

This document follows the general principles given in IAEA Safety Requirement SSR-2/1 and Safety Guides SSG-30, SSG-34 and SSG-39, and it defines a structured method of applying the guidance contained in those codes and standards to the I&C and electrical power systems that perform functions important to safety in a NPP. This document is read in association with the IAEA guides together with IEC 61513 and IEC 63046 in implementing the requirements of the IEC 61508 series. The overall classification scheme of structures, systems and components for NPPs can be summarized as follows by Figure 1.

² The scope of this document is consistent with IAEA SSR-2/1 and SSG-30, upon which it is based.

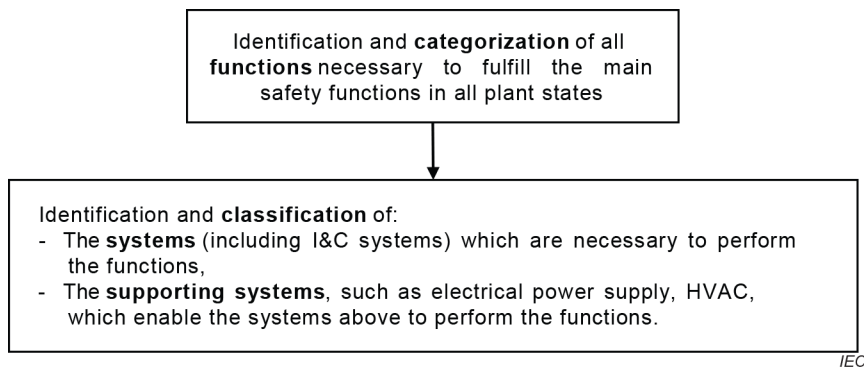


Figure 1 – Overall classification scheme

This 2-phase process is defined for purpose of comprehensiveness; it enables the capture of all the functions and all the systems important to safety, including I&C systems, as well as electrical power systems.

In this scheme, functions are defined and categorized regardless of the physical means that are implemented to fulfill them. In the framework of this document, the functions to be categorized are performed by I&C systems. Accordingly, they are called I&C functions.

This document applies to I&C and electrical power systems for new nuclear power plants as well as for modification and modernization of existing plants.

For existing plants, only a subset of requirements can be applicable, and this subset is identified at the beginning of any project.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

IEC/IEEE 60780-323, *Nuclear facilities – Electrical equipment important to safety – Qualification*

IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*

IEC 60880, *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, *Nuclear power plants – Control rooms – Supplementary control room 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 61500, *Nuclear power plants – Instrumentation and control systems important to safety – Data communication in systems performing category A functions.*

IEC 61513:2011, *Nuclear power plants – Instrumentation and control 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 – Control rooms – Application of visual display units (VDUs)*

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

IEC 62003, *Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*

IEC 62138:2018, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions.*

IEC 62566, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions.*

IEC 62645, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems.*

IEC 62671, *Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality*

IEC 62859, *Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity*

IEC 63046:—³, *Nuclear power plants – Electrical power systems – General requirements*

IAEA GSR Part 2:2016, *Leadership and Management for Safety*

IAEA SSR-2/1 (Rev.1):2016, *Safety of nuclear power plants: Design*

IAEA SSG-30:2014, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants*

3 Terms and definitions

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

³ Under preparation. Stage at the time of publication: IEC CDV 63046:2019.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1

anticipated operational occurrence

AOO

deviation of an operational process from normal operation that 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 or lead to accident conditions

Note 1 to entry: This note applies to the French language only.

[SOURCE: IAEA Safety Glossary, 2018]

3.2

common cause failure

CCF

failures of two or more structures, systems or components due to a single specific event or cause

[SOURCE: IAEA Safety Glossary, 2018]

3.3

controlled state

plant state, following an anticipated operational occurrence or accident conditions, in which fulfilment of the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state

Note 1 to entry: See 4 for the list of fundamental safety functions.

Note 2 to entry: See 3.21 for definition of safe state.

[SOURCE: IAEA Safety Glossary, 2018]

3.4

design basis accident

DBA

postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits

[SOURCE: IAEA Safety Glossary, 2018]

3.5

design extension conditions

DEC

postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits

Note 1 to entry: Design extension conditions comprise conditions in events without significant fuel degradation and conditions in events with melting of the reactor core.

Note 2 to entry: A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.[IAEA SSR-2/1]

[SOURCE: IAEA Safety Glossary, 2018]

3.6

diversity

presence of two or more independent (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

[SOURCE: IAEA Safety Glossary, 2018]

3.7

electrical/electronic/programmable electronic item

E/E/PE item

item based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

[SOURCE: IEC 62138:2018, 3.15]

3.8

electrical power system

system performing electrical power generation, transmission and distribution; performing supply functions to operate plant equipment (pumps, valves, heaters, etc.) and to I&C systems

Note 1 to entry: An electrical system can integrate E/E/PE items to perform its internal electrical control and protection.

[SOURCE: IEC CDV 63046:2019, 3.12]

3.9

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

[SOURCE: IEC 61513:2011, 3.16, modified – The notes to entry have been omitted.]

3.10

function

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

3.11

functionality

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

[SOURCE: IEC 61513:2011, 3.24, modified – The note has been omitted.]

3.12**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

3.13**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

Note 1 to entry: 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.

Note 2 to entry: Items important to safety considered in this standard are I&C and electrical power systems.

[SOURCE: IAEA Safety Glossary, 2018]

3.14**I&C system**

system, based on E/E/PE items, performing I&C functions as well as service and monitoring functions related to the operation of the system itself

[SOURCE: IEC 62138:2018, 3.26, modified – The notes to entry have been omitted.]

3.15**normal operation**

operation within specified operational limits and conditions

Note 1 to entry: For a nuclear power plant, this includes startup, power operation, shutting down, shutdown, maintenance, testing and refuelling.

[SOURCE: IAEA Safety Glossary, 2018]

3.16**performance**

effectiveness with which an intended function is carried out

Note 1 to entry: For example, response time, accuracy, sensitivity to parameter changes.

3.17**periodic testing**

performance of tests at predetermined time points to demonstrate that the functional capabilities of I&C systems and equipment important to safety are retained and that the characteristics relevant to the claims of the safety analysis are satisfied

[SOURCE: IEC 60671:2007, 3.7]

3.18 plant states

Operational states		Accident conditions		
Normal operation	Anticipated operational occurrences	Design basis accidents	Design extension conditions	
			Without significant fuel degradation	With core melting

[SOURCE: IAEA Safety Glossary, 2018]

3.19 postulated initiating event

PIE

postulated event identified in design as capable of leading to anticipated operational occurrences or accident conditions

Note 1 to entry: This note applies to the French language only.

[SOURCE: IAEA Safety Glossary, 2018]

3.20 redundancy

provision of alternative (identical or diverse) structures, systems or components, so that any single structure, system or component can perform the required function regardless of the state of operation or failure of any other

[SOURCE: IAEA Safety Glossary 2018]

3.21 safe state

plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time

Note 1 to entry: See 3.25 for the list of fundamental safety functions.

[SOURCE: IAEA Safety Glossary, 2018]

3.22 safety categorization

for nuclear power plants, the categorization into a limited number of safety categories of the functions that are required for fulfilling the fundamental safety functions in different plant states, including all modes of normal operation, on the basis of their safety significance

Note 1 to entry: See 3.25 for the list of fundamental safety functions.

[SOURCE: IAEA Safety Glossary, 2018]

3.23 safety classification

for nuclear power plants, the assignment to a limited number of safety classes of systems and components and other items of equipment on the basis of their functions and their safety significance

[SOURCE: IAEA Safety Glossary, 2018]

3.24**safety function**

specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions

Note 1 to entry: Safety functions are required to fulfil the fundamental safety functions that are: (i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store, (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases [IAEA SSR-2/1, Requirement 4].

Note 2 to entry: Safety functions are primarily those that are credited in the safety analysis and include functions performed at all levels of defence in depth.

[SOURCE: IAEA Safety Glossary, 2018]

3.25**safety group**

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

[SOURCE: IAEA Safety Glossary, 2018]

3.26**self-supervision**

automatic testing of system hardware performance and software consistency of a computer based I&C system

[SOURCE: IEC 60671:2007, 3.8]

3.27**single failure**

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

[SOURCE: IAEA Safety Glossary, 2018]

3.28**support system****supporting system**

system that provides services in order to enable another system to perform a function

Note 1 to entry: Services are, for example, electrical power supply, HVAC, cooling, lubrication.

3.29**system**

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

[SOURCE: IEC 61513:2011, 3.56, modified – The notes to entry have been omitted.]

3.30**type test**

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

4 Abbreviated terms

ALARA	as low as reasonably achievable
AOO	anticipated operational occurrence
BWR	boiling water reactor
CCF	common cause failure
DBA	design basis accident
DEC	design extension condition
E/E/PE	electrical/electronic/programmable electronic
FAT	factory acceptance test
FMEA	failure modes and effects analysis
HMI	human machine interface
HVAC	heating, ventilation and air conditioning
IAEA	International Atomic Energy Agency
ISO	International Organization for Standardization
I&C	instrumentation and control
NC	non-categorized
NPP	nuclear power plant
PIE	postulated initiating event
PSA	probabilistic safety assessment
PWR	pressurized water reactor
QA	quality assurance
SAT	site acceptance test
SSC	structures, systems and components

5 Categorization scheme

5.1 General

Safety functions shall be assigned to different categories according to their safety significance. The category determines the class to be assigned to the I&C systems which perform these functions and the class to be assigned to the electrical power systems which support the functions (including those which support the operation of the I&C equipment). Then the class determines the design and quality requirements for these systems.

Subclause 5.2 provides the background to the categorization scheme.

Subclause 5.3 describes the three categories that are used to categorize functions, according to their safety significance. The categories are consistent with those defined in IAEA SSG-30.

Subclause 5.4 presents the assignment criteria for each category.

Clause 6 provides guidance on the categorization process and also provides guidance on the mapping of functional categorization to system classes.

Clause 7 and Annex A address high-level technical requirements for each category (requirements applying to the functions) and each class (requirements applying to the systems that perform the functions). More detailed technical requirements are presented in dedicated IEC standards.

Annex B contains typical examples of the categorization of functions and classification of systems in NPPs. It is only informative since the mentioned functions and systems 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 that there should be several layers or lines of defence in the prevention of unsafe conditions, and that the prevention of unsafe conditions, before mitigation is needed, is always to be preferred. Because of the large number of functions that are required to operate a NPP and sustain its safety, a number that increases with the principle of defence in depth, it is important that the safety significance of each function is known. All the functions performed at the different levels of defence in depth are considered.

IAEA Safety Requirements SSR-2/1 establishes the idea of classification of NPP systems according to their safety significance, and gives examples of the classification of the major systems of several types of NPPs. 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.

IAEA Safety Requirements SSR-2/1, section 5.34 requires that the method for classifying the safety significance of items shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods with account taken of factors such as:

- a) the safety function(s) to be performed by the item;
- b) the consequences of failure to perform a safety function;
- c) the frequency with which the item will be called upon to perform a safety function;
- d) the time following a PIE at which, or the period for which, the item will be called upon to perform a safety function.

The IAEA Safety Guide SSG-30 gives guidance on the categorization of functions and classification of SSCs according to their safety significance.

This document extends the categorization strategy presented in IAEA Safety Guide SSG-30, and establishes the criteria and methods to be used to assign the functions of NPP to one of the three categories A, B and C, depending on their safety significance, or to consider them as “non-categorized” (NC) if they do not have any safety role.

IAEA SSG 39 chapter 5 concerning classification of I&C systems and IAEA SSG 34 chapter 3 concerning classification of electrical power systems directly refer to SSR-2/1 and SSG-30 and are consistent with the principles of this document.

National application of the principles and criteria of this document may assign a different nomenclature to categories A, B and C.

5.3 Description of categories

5.3.1 General

The method for determining the safety significance of a function shall primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment.

The safety significance of a function designed to respond to a PIE shall take account of the following:

- The consequences of failure to perform the function;
- The frequency of occurrence of the postulated initiating event for which the function will be called upon;
- The significance of the contribution of the function in achieving either a controlled state or a safe state.

When assessing the safety significance of a function, the following factors should be considered:

- the role of the function during normal operation (including start-up, refuelling, etc) in preventing the occurrence of PIEs;
- the role of the function in mitigating the consequences of AOO, DBA or DEC;
- the time following a PIE at which, or the period for which it is required to perform the function;
- the consequences in the event of spurious actuation in the different plant states (operational states and accident conditions);
- the role of the function following PIEs such as natural events (e.g. seismic disturbance, flood, extreme wind, lightning), human induced external events (e.g. chemical releases from other plants or industries) and internal hazards (e.g. fire, internal flood, missiles);
- the maintenance, repair and testing strategy.

Therefore, an initial safety analysis of the specific NPP design shall be completed prior to the categorization of the functions. On the basis of this safety analysis, the identification of the functions to be categorized should be performed with a sufficiently detailed granularity, in such a way that one function can be allocated to only one I&C system.

To graduate the consequences of failure to perform the function, SSG-30 defines 3 levels of severity for NPPs keeping in mind that functions implemented to control accidents aim at making the consequences of these accidents acceptable and also as low as practicable. The assessment of the consequences is made under the assumption that the function does not respond when challenged, and without crediting any function that compensates for the failure of the function.

- The severity should be considered 'high' if failure of the function could, at worst lead to a release of radioactive material that exceeds the limits accepted by the regulatory body for design basis accidents; or cause the values of key physical parameters (e.g pressure, temperature, etc) to exceed acceptance criteria for design basis accidents.
- The severity should be considered 'medium' if failure of the function could, at worst lead to a release of radioactive material that exceeds limits established for anticipated operational occurrences; or cause the values of key physical parameters to exceed the design limits for anticipated operational occurrences.
- The severity should be considered 'low' if failure of the function could, at worst lead to doses to workers above authorized limits.

In terms of alignment with IAEA SSG-30 categorization nomenclature, the requirements provided in this document cover the allocation of categories A, B and C to functions that can be implemented by I&C systems and/or supported by electrical power systems. These are equivalent to categories 1, 2 and 3, respectively, from IAEA SSG-30.

5.3.2 Category A

Category A shall be assigned to the functions that play a principal role in the achievement or maintenance of NPP safety to prevent AOO or DBA from leading to consequences of high severity. 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 controlled state ⁴.

Category A also denotes functions whose failure could directly lead to accident conditions which can cause high severity consequences and for which no other category A function exists that prevents such consequences.

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 once the controlled state has been achieved, to prevent AOO or DBA from leading to consequences of high severity, or those which are required to reach the controlled state to prevent AOO or DBA from leading to consequences of medium severity.

Category B functions also denotes functions that are designed to control DEC without significant fuel degradation resulting from or including the postulated failure of a category A function, so that plant or equipment damage or activity release can be avoided or minimised.

Category B also denotes functions whose failure could directly lead to accident conditions which can cause medium severity consequences and for which no other category A or B function exists that prevents such consequences.

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 safety significance, but are not category A or B. They can be part of the total response to AOO or DBA but not be directly involved in avoiding consequences of high severity of the accident, or be functions necessary for other purposes (e.g. mitigate the consequences of DEC or hazards).

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 hereinafter.

If a function does not meet any of these criteria, then it shall be "non-categorized" (NC).

In case of multiple assignments, 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 accordance with the principles outlined in 6.3.

⁴ In order to cope with rapid transients, the plant is controlled during this phase by automatic actions. For slower transients, the controlled state can be obtained using manual actions, provided such actions are considered in accident studies after a consequent grace time. This type of grace time represents a design requirement of the plant corresponding to a delay of diagnosis and action, based on human factors, accessibility considerations and including margins. It does not mean that manual actions are not permitted during that time. In some countries, and for older NPP, the limit between category A and category B may be this grace time, in place of the controlled state.

5.4.2 Category A

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

- a) a function required to reach the controlled state, to prevent an AOO or DBA from leading to consequences of high severity;
- b) a function, the failure or spurious actuation of which during normal operation, would lead to consequences of high severity;
- c) a function required to provide information and control capabilities that allow specified manual actions necessary to reach the controlled state to prevent high-severity consequences.

5.4.3 Category B

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

- a) a function required to reach the controlled state, to prevent an AOO or DBA from leading to consequences of medium severity;
This criterion should apply to plant process control functions if such functions are credited in the safety analysis to prevent an AOO from escalating to DBA.
- b) a function required to reach and maintain a safe state, after the controlled state of an AOO or DBA has been reached, to prevent it from leading to consequences of high severity;
- c) a function required to provide information or control capabilities that allow specified manual actions necessary to reach and maintain a safe state, after the controlled state has been reached, to prevent an AOO or DBA from leading to consequences of high severity;
- d) a function required to control a DEC without significant fuel degradation resulting from or including the postulated failure of a category A function;
- e) a function, the failure or spurious actuation of which during normal operation, would lead to consequences of medium severity and for which no other category A or B function exists that prevents the consequences of medium severity;
- f) a function to reduce considerably the frequency of a DBA as claimed in the safety analysis;

By extension, this criterion should apply to functions, the spurious actuation of which during normal operation, would lead to a DBA.

- g) a function that provides 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 availability⁵.

NOTE Where the monitoring function is the only means of detecting otherwise unrevealed failures, then assigning the monitoring function to category B ensures an appropriate level of quality.

5.4.4 Category C

A 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) a plant process control function operating so that the main plant parameters are maintained within the normal range of operation of the plant;

⁵ Subclause 4.2.6 of IEC 60671:2007 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"

- b) a function actuated in the event of an AOO or DBA and whose failure, when challenged, would result in consequences of low severity;
- c) a function required to reach and maintain for a long time a safe state and whose failure, when challenged, would result in consequences of medium severity;
- d) a function that provides 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 assigned to category B in accordance with 5.4.3g;
- e) a function designed to reduce the actuation frequency of the reactor trip or engineered safety features;

By extension, this criterion should apply to functions, the spurious actuation of which during normal operation, would lead to the actuation of the reactor trip or engineered safety features.

- f) a function to monitor and take mitigating action following internal hazards within the NPP design basis (e.g. fire, flood);
- g) a function the failure or spurious actuation of which during normal operation would lead to consequences of low severity;
- h) a function 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;
- i) a function that provides necessary information to determine the magnitude and dispersion of the radioactive release materials in case of accident;
- j) a function which monitors and/or annunciates the state of the plant so that action can be taken to either prevent an unsafe condition or mitigate the consequences following natural events (e.g. seismic disturbance, flooding, extreme wind, lightning);
- k) a function required to mitigate the consequences of DEC, unless already required to be categorised in safety category B, including information and controls necessary to implement severe accident (i.e. DEC with core melting) management guidelines, and whose failure, when challenged, would result in consequences of high severity;
- l) a function which provides access control for personnel protection;
- m) a function to provide plant staff and off-site emergency services with information that are necessary for the purpose of implementing the emergency response plan.

6 Categorization/classification procedure

6.1 General

An outline of the procedure is shown in Figure 2. It consists in three phases:

- the basic design of the NPP;
- the safety categorization of functions;
- the safety classification of I&C systems⁶.

⁶ The third phase in Figure 2 applies to I&C systems. As for electrical power systems, they inherit their safety class directly from the safety class of the systems they support (whether these systems are I&C systems or systems that directly act on the plant process). See 6.4.2 for more details.

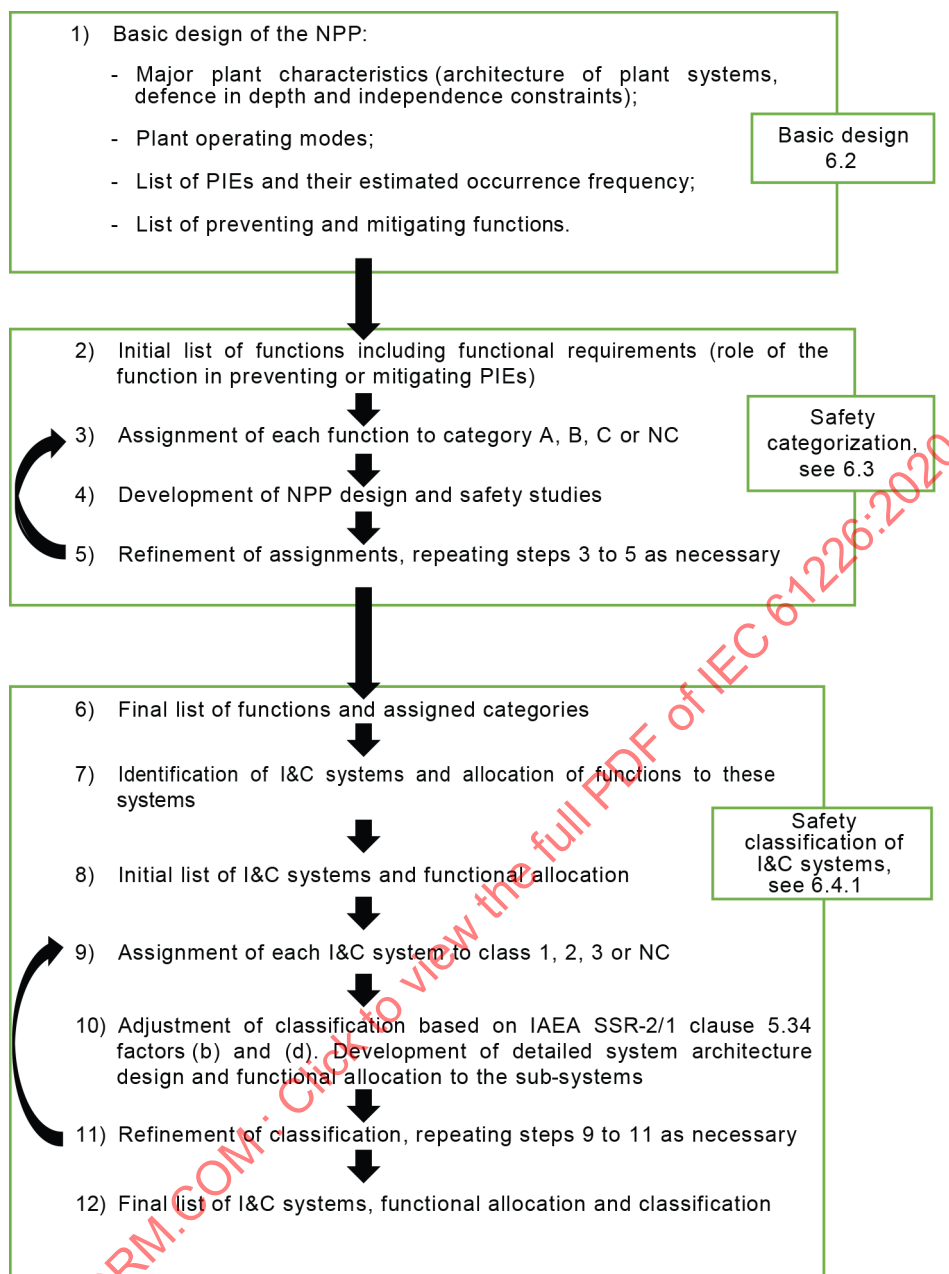


Figure 2 – Method of categorization of functions and classification of I&C systems

6.2 Identification of anticipated operational occurrences (AOO), design basis accidents (DBA) and design extension conditions (DEC)

Main inputs to the categorization process of functions are the nature of the NPP and the reactor type (e.g. PWR (pressurized water reactor), BWR (boiling water reactor) or other reactor type) and the associated PIEs. Another main input is the identification of the major mitigation functions, for each PIE.

The assessment of the frequency and consequences of PIEs leads to the identification of AOOs or DBAs representing the design base of the plant, and of DEC representing other accident conditions to be taken into account in the design. 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 taken into account. 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 AOOs, DBAs and DEC and successive physical barriers to keep radioactive exposure within permitted limits. The AOOs,

DBAs and DECAs, as well as the identification of the prevention and mitigation functions, are the main inputs to the categorization process.

The importance to safety of each function depends upon its role in 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 shall be completed prior to the categorization of the functions.

According to IAEA SSR 2/1 the identification of the design basis and design extension conditions, and therefore the identification and categorization of functions includes all the parts of the plants which could lead to significant radioactive releases, i.e. not only the reactor core, but also spent nuclear fuel, radioactive waste or any other source of radiation at a NPP.

6.3 Identification and categorization 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 an automated function⁷, or to the human operators should be carried out in accordance with IEC 60964. Following this initial identification of a function, a category for each automated or manual function shall be assigned according to the criteria of Clause 5.

It is not possible to identify in detail all the functions at an early stage in the design process, because the characteristics of the NPP are not fully defined. Therefore, the identification and categorization process of the functions shall iteratively continue 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 categorization for later resolution.

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 NPP design is determined more precisely, for example after the safety analysis progresses and the operating procedures are developed, the categorization list shall be refined and revised, to derive a final list of functions and assigned categories. This list shall be documented and maintained under configuration management since it will be required by plant and system designers during the lifetime of the NPP. Also, this list can be required by the regulatory authorities.

6.4 Classification of systems

6.4.1 Classification of I&C systems

Once the safety categorization of the functions is completed, the next step consists in identifying the I&C systems performing or contributing to the functions. All the systems and components that are necessary to perform the functions shall be identified, including not only the systems and components that directly act on the plant process (actuators, valves, etc.), but also the supporting systems, such as HVAC, etc.

By the end of this phase, all the safety categorized functions that need an I&C system to operate are allocated to appropriate I&C systems, taking into account the different levels of defence in depth. Once defined, these systems shall be classified according to their safety significance following a process that takes into account the factors indicated by Requirement 22 in IAEA SSR-2/1 and reproduced hereafter:

⁷ Automated functions addressed here are control functions implemented in I&C systems. The energy conversion or transport function of electrical systems are not addressed.

- a) the safety function(s) to be performed by the system;
- b) the consequences of failure to perform a safety function;
- c) the frequency with which the system will be called upon to perform a safety function;
- d) the time following a PIE at which, or the period for which, the system will be called upon to perform a safety function.

Applying factors (a) and (c) defined in IAEA SSR 2/1, I&C systems that are designed to carry out identified functions shall initially be assigned to the safety class corresponding to the safety category of the functions which they are to perform.

Three safety classes are proposed and correlated with the three categories as shown in Table 1.

Table 1 – Correlation between classes of systems and categories of functions

Categories of functions important to safety			Corresponding classes of systems important to safety
A	(B) ^a	(C) ^a	1
	B	(C) ^a	2
		C	3
^a Use of higher safety class than that required by the category is typically adopted for ancillary functions such as self-supervision, because it avoids the need for a functional isolation.			

The initial classification shall then be amended, as necessary, to take into account factors (b) and (d) defined in IAEA SSR-2/1. For factor (d), consideration of the time following a postulated initiating event before the function is called upon may permit the SSC to be moved into a lower class, provided that its expected reliability can be demonstrated. Such a demonstration may use, for example, time to repair or maintain the SSC, or the possibility of using alternative SSCs within the time window available to perform the required safety function.

Where consideration of the effects of common cause failures shows the required reliability could not be achieved for redundant systems, and leads to implement diversity in independent systems (e.g. as determined by probabilistic criteria), then the refinement of classification may also apply to systems required to manage the effects of common cause failures. In the case of crediting a Class 2 system in the safety analysis to compensate for the postulated failure of a Class 1 system delivering Category A functions, a safety justification shall be established and shall show that the design and qualification requirements applied to the Class 2 system are appropriate and that the reliability targets for the Class 2 system are credible.

For an individual I&C system which is specified and designed in accordance with the highest quality criteria, a figure of the order of 10^{-4} failure/demand can be an appropriate overall limit to place on the reliability that can 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 cause 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.

The granularity of the categorized I&C functions should be sufficiently detailed so that one I&C function should be allocated to only one I&C system.

If an SSC contributes to the performance of several functions of different categories, it shall be assigned to the class corresponding to the highest of these categories (i.e. the one requiring the most conservative engineering design rules).

By applying these considerations, the final list of systems, functional allocation and classifications shall be established. This process shall also take into account other relevant considerations such as the following:

- defence in depth level;
- correlation between classes of systems and category of functions (see Table 1);
- independence requirements;
- allocation of functions designed to provide a back-up of Category A/B functions to a sufficiently separated and diversified system.

6.4.2 Classification of electrical power systems

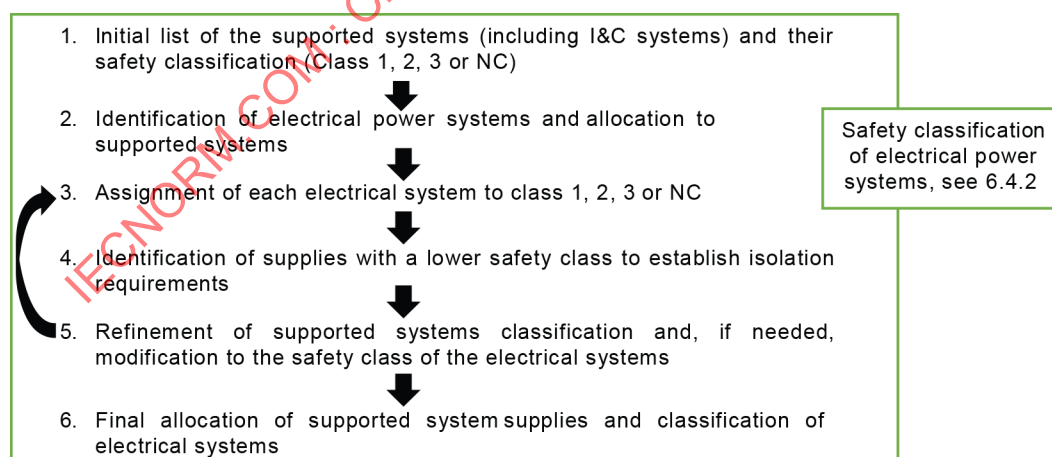
The approach to classification of electrical systems is defined in IEC 63046. This is based on the safety class of the electrical system being consistent with the safety class of the systems important to safety supported by the electrical system. Where an electrical system supplies loads with different safety classes, then the electrical system should be classified in accordance with the highest classified load on that system. Appropriate isolation shall be provided on supplies to loads of lower safety class.

For electrical supplies to I&C systems the supporting electrical system should be classified to be consistent with the safety class of the I&C system. In the event of changes to the safety class of the I&C system (during the refinement of the classification process), then the safety class of the electrical system supporting it should be reviewed accordingly.

Where an I&C system is part of an electrical system (e.g. emergency diesel generators), then the I&C system should be classified to be consistent with the safety class of the electrical system.

Figure 3 below summarizes the method of classification of electrical power systems.

NOTE Electrical power systems that supply power to safety classified systems include both on-site and off-site power systems. As off-site power systems are not part of plant equipment, they are not safety classified (see IAEA Safety Guide SSG-34, Clause 1.6).



IEC

Figure 3 – Method of classification of electrical power systems

7 Assignment of technical requirements to categories and classes

The technical requirements for each of the categories A, B and C and corresponding classes 1, 2, 3 shall be applied to the specification, design, verification, validation, qualification, manufacturing, installation, operation and maintenance phases of the I&C and electrical items lifecycle as appropriate. The technical requirements constitute different groups:

- requirements that apply to the functions concerning the specification and validation of functionality, performance and reliability;
- requirements that apply to the design of 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 qualification and electro-magnetic compatibility;
- requirements that are associated with the quality assurance, verification and maintenance which apply to functions, systems and equipment.

NOTE Requirements associated with cybersecurity are addressed in IEC 62645 and IEC 62859.

In most cases, these requirements are already detailed in appropriate codes and standards. The codes, guides and standards listed in Clause 2 are normative references and therefore provide the mandatory requirements related to the function categories and system classes which are established by this document. The correlation between the classes and the standards that shall be applied is summarised in Table 2. The detailed requirements from these standards are not repeated in this document. Table 2 also summarises the main types of requirements for each class. In the Annex A, some additional details are given for each group of requirements.

IECNORM.COM : Click to view the full PDF of IEC 61226:2020

Table 2 – Tabular correlation between classes and other IEC standards

[illegible]

Annex A

(normative)

Assignment of technical requirements to I&C systems

A.1 General

Note that many requirements of this annex are repeated in IEC 61513. As it is not convenient to repeat the same requirements in different standards (risk of inconsistency when updating one of these standards), the content of this Annex A will be included in IEC 61513 (if not yet already done). Afterwards, this annex will be removed from this document. Where the requirements of this annex are different from those provided in the current issue of IEC 61513, the information of IEC 61513 take precedence.

Requirement to be applied to electrical power systems and components are addressed in IEC 63046.

As an addition to Table 2, this annex aims at giving an overview of the technical requirements that apply to:

- the functions,
- the systems,
- the equipment qualification.

The requirements related to quality assurance are also detailed.

As a general rule, the requirements for systems and components apply to I&C systems and components.

A.2 Requirements related to functions

A.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 shall 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.

A.2.2 Specific requirements

A.2.2.1 Category A

The design shall be performed 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.

If specified manual actions are required to perform category A functions, 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 to preserve NPP safety, should be considered.

Category A functions have high reliability requirements. Consequently, their functionality and complexity should be limited.

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 class 1 systems (for example, special display calculations and translation of communication protocols should not be carried out by class 1 system software).

The reliability requirements for category A functions shall be specified, in order to achieve an acceptably low risk of high severity consequences.

A.2.2.2 Category B

The design shall be performed in accordance with the requirements of recognized codes, guides and standards that are appropriate to the level of assurance of functionality required for category B functions. The design shall aim to ease verification and validation of the final functionality.

The reliability requirements for category B functions shall be specified, in order to achieve an acceptably low risk of high-severity consequences.

The requirements for the category B functions need not be as high as those for the category A functions. 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.

A.2.2.3 Category C

The design shall be examined to verify that the specified functions can be performed under the full range of specified operating conditions, including the most adverse anticipated operational conditions or occurrences under which the function is required.

A.3 Requirements related to systems

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

The design of the system shall allow self-supervision 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 systems important to safety are defined in Clause A.5.

The design shall recognise the potential for the main control room to be made uninhabitable by hazards. An alternative control location shall be provided containing sufficient information and control equipment to enable the reactor to be placed and maintained in a safe shutdown state, and for essential plant variables to be monitored. The alternative control location shall be demonstrated to not be affected by the same hazards that can render the main control room uninhabitable.

There shall be adequate separation between the systems of different classes. Where the safety class of connecting or interacting systems or sub-systems is not the same (including cases where a system or sub-system in a safety class is connected to a system or sub-system that is not classified), interference between the systems or sub-systems shall be prevented by means of a device, classified in the higher safety class, to ensure that a failure of the system or sub-system in the lower safety class will not induce a failure of the system or sub-system in the higher safety class.

A.3.2 Specific requirements

A.3.2.1 Class 1

A class 1 system shall have redundancy. Appropriate separation shall be applied to ensure that any single internal hazard cannot disable redundant parts of the system. During normal operation modes for which a function performed by a class 1 system is required to be available, a single failure shall not lead to the failure of this function even during preventative maintenance, periodic testing, inspection or repair. The application of the single failure criterion shall be in accordance with the IAEA Requirement SSR-2/1, 5.39-5.40.

NOTE 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.

The reliability of the class 1 systems shall be assessed and compared to the specification. If discrepancies exist, they 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 analyses⁸, 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.

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 shall 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.

⁸ The reliability of software is usually a qualitative measure because there are no generally recognized means to quantify the reliability of software.

The electrical power supply of class 1 I&C systems shall be backed-up by class 1 emergency power sources. The different redundancies of class 1 I&C systems shall be backed-up by different emergency power sources; each of these emergency power sources shall be independent of each other.

For class 1 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 cannot 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 evaluated and revised where applicable.

A.3.2.2 Class 2

A class 2 system needed in case of DBA should have redundancy. Appropriate separation should be applied to ensure that any single internal hazard cannot disable redundant parts of the system. A single failure should not lead to the failure of a category B function that is required after the controlled state of an AOO or DBA to prevent high severity consequences (see 5.4.3, criteria a and b). Any exception to this principle shall be justified by demonstrating that other functions can be credited, to diagnose the situation and to take efficient countermeasures to prevent high severity consequences (consequent grace time, diagnostic, use of alternative category B functions).

A class 2 system needed in case of DEC as a backup of a class 1 system shall be designed and implemented such that a failure of the class 1 system cannot prevent the class 2 system from performing its safety functions.

The reliability of class 2 systems shall be assessed and compared to the specification. A category B function involved in AOO or DBA mitigation 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 redundancy, the acceptability of the consequences of the function's failure, or the time available to provide alternative responses if the function fails. Category B function not involved in AOO or DBA mitigation can also require redundancy to achieve the reliability targets.

The electrical power supply of class 2 I&C systems should be backed-up by class 2 emergency power sources. The different redundancies (if any) of class 2 I&C systems shall be backed-up by different emergency power sources; each of these emergency power sources shall be independent of each other.

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 an AOO or a DBA are to provide the operator with accurate, complete and timely information regarding the status of plant equipment and systems for all plant states, and to minimise movement required from the operator to monitor and control the plant.

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

A.3.2.3 Class 3

A class 3 system does not generally need redundancy or separation. This may be provided if it is necessary to achieve the specified reliability of the function, for instance to provide independence between levels of defence in depth. Tolerance to internal and external hazards can be required.

The electrical power supply of class 3 I&C systems can be without backed-up power sources.

Self-supervision and/or periodic testing of performance shall include confirmation of the functional capacity of class 3 systems or subsystems.

Pre-assembled software used for class 3 I&C systems shall be qualified according to nuclear standards or operationally proven and justified industrial standards (e.g. the IEC 61508 series). The properties required for the application shall be assessed and documented.

A.4 Requirements related to equipment qualification

A.4.1 Basic requirements

It is necessary to provide assurance that the equipment required to mitigate the consequences of a PIE will not fail owing to ageing and to the environmental conditions that it can be subjected to during and following this PIE. This assurance may be provided by qualification of the equipment (see IEC/IEEE 60780-323). 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 DEC, including those with core melting, are expected to play a role in these accidents, the capabilities of their components shall be evaluated in order to show that they are able to operate during the required time frame and in the expected environmental conditions (see IEC/IEEE 60780-323).

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

A.4.2 Specific requirements

A.4.2.1 Class 1

The measures taken to provide assurance that class 1 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.

A.4.2.2 Class 2

Equipment in class 2 shall be subject to equipment qualification to be performed as for class 1 equipment.

A.4.2.3 Class 3

Depending on its function, equipment in class 3 can require qualification. The design of the equipment shall 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 class 1 equipment. Equipment provided for the functions categorised in application of criteria 5.4.4 k) 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, class 3 equipment may be accepted to normal industrial 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 class 3 equipment from affecting class 1 or 2 equipment. Claims for operation in abnormal environmental conditions shall be supported by documentary evidence.

A.5 Requirements related to quality aspects

A.5.1 Basic requirements

The general requirements include 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 in accordance with an appropriate 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 in accordance with 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 and electrical power systems 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 systems.

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

Testing during operation shall be executed to demonstrate that the status of the components of the I&C systems 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 programmable equipment is used, a software life cycle quality programme appropriate to the class of the system shall be implemented.

A.5.2 Specific requirements

A.5.2.1 Class 1

The QA requirements shall be in accordance with the IAEA safety standard GSR Part 2. 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 an item 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 its 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.

Self-supervision or periodic testing 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-supervision so that the reliability targets for the systems important to safety are fulfilled taking into account the expected or monitored failure rate of the components.

A.5.2.2 Class 2

The QA requirements shall be according to IAEA safety standard GSR Part 2. 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 class 2 systems and equipment may be lower than that applied to class 1 systems or equipment, although the QA programme should be consistent with that for class 1.

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.

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-supervision so that the reliability targets for the systems important to safety are fulfilled taking into account the expected or monitored failure rate of the components.

A.5.2.3 Class 3

Class 3 systems and equipment may be accepted at a commercial QA level, taking into account the role of the related functions.

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.

SATs should be carried out 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.

Annex B (informative)

Examples of categories and classes

B.1 General

The categorization of functions and the classification of systems have to be done by application of the processes and criteria given in Clauses 5 and 6. This annex provides examples of assignment of typical functions and typical systems, respectively to categories A, B, C, and to classes 1, 2, 3. It should be noted, however, that these examples may not necessarily all apply to all reactor types.

In addition, IAEA TecDoc 1787 (Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants) provides more technical details and examples for the application of categorization and classification processes.

B.2 Category A/Class 1

B.2.1 Typical functions

The functions assigned to category A are necessary in AOO or DBA to reach the controlled state 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
- e) backup of category A reactor automatic shutdown, if credited in DBA.

B.2.2 Typical I&C systems

Typical I&C systems necessary to reach the controlled state are as follows:

- a) reactor protection system;
- b) safety actuation system;
- 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.

B.2.3 Typical electrical power systems

Typical electrical power systems necessary to reach the controlled state are as follows:

- a) emergency power sources credited in AOO and DBA.

B.3 Category B/Class 2

B.3.1 Typical functions

Typical functions assigned to category B are as follows:

- a) spent fuel pool cooling;
- b) main cooling system isolation;
- c) post accident system (to reach a safe state);

- d) monitoring/controlling the handling of fuel where failure could cause radiation release or fuel degradation outside the limits and conditions of normal operation;
- e) backup of category A reactor automatic shutdown, if credited in DEC;
- f) plant process control functions if credited in the safety analysis to prevent an AOO from escalating to an accident (i.e. to consequences of medium severity).

B.3.2 Typical I&C systems

Typical I&C systems are as follows:

- a) instrumentation needed to apply operating procedures for AOO or DBA;
- b) safety circuits and interlocks of fuel handling systems used when the reactor is shut down.

B.3.3 Typical electrical power systems

Typical electrical power systems are as follows:

- a) alternate power source credited in DEC.

B.4 Category C/Class 3

B.4.1 Typical functions

The functions assigned to category C may include:

- a) plant process control functions (e.g. automatic control of the NPP primary and secondary circuit conditions), keeping variables in the limits and conditions for normal operation (unless credited in the safety analysis to prevent an AOO from escalating to an accident, see B.3.1);
- b) 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;
- c) limiting the consequences of internal hazards;
- d) those whose operating failures or faults could lead to minor radioactive releases, or lead to radioactive hazard to the NPP operating staff;
- e) those necessary to warn of internal or external hazard (fire, flood, explosions, seismic events, etc.);
- f) access control;
- g) warning of significant on- or off-site releases for the purposes of implementing the NPP's emergency plan.

B.4.2 Typical I&C and electrical power systems

Typical I&C and electrical power systems are as follows:

- a) main plant parameters automatic control system (if not credited in the safety analysis to prevent an AOO from escalating to an accident);
- b) alarm system;
- c) radwaste stream monitoring and interlocks, area radiation monitoring;
- d) access control system;
- e) emergency communication systems;
- f) control room data processing system;
- g) fire suppression system;
- h) seismic monitoring system;

- i) NPP site meteorological station;
- j) earthing and lightning protection;
- k) protection against grid open phase.

IECNORM.COM : Click to view the full PDF of IEC 61226:2020

Bibliography

IEC 60050-395, *International Electrotechnical Vocabulary – Part 395: Nuclear instrumentation: Physical phenomena, basic concepts, instruments, systems, equipment and detectors*

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

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*

IEC 62342, *Nuclear power plants – Instrumentation and control systems important to safety – Management of ageing*

ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements.*

ISO/IEC 27002, *Information technology – Security techniques – Codes of practice for information security controls.*

IAEA Safety Glossary:2018, *Terminology used in nuclear safety and radiation protection*

IAEA GSR part 4:2009 *Safety Assessment for Facilities and Activities*

IAEA SF1 *Fundamental Safety Principles*

IAEA TecDoc 1787, *Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants*

IAEA GS-G-3.1:2006, *Application of the Management System for Facilities and Activities.*

IAEA GS-G-3.5:2009, *The Management System for Nuclear Installations.*

IAEA SSG-34:2016, *Design of Electrical Power Systems for Nuclear Power Plants*

IAEA SSG-39:2016, *Design of Instrumentation and Control Systems for Nuclear Power Plants.*

SOMMAIRE

AVANT-PROPOS	42
INTRODUCTION.....	44
1 Domaine d'application	47
2 Références normatives	48
3 Termes et définitions	50
4 Termes abrégés	55
5 Schéma de catégorisation	55
5.1 Généralités	55
5.2 Contexte	56
5.3 Description des catégories	57
5.3.1 Généralités	57
5.3.2 Catégorie A	58
5.3.3 Catégorie B	59
5.3.4 Catégorie C	59
5.4 Critères de répartition dans les différentes catégories	59
5.4.1 Généralités	59
5.4.2 Catégorie A	59
5.4.3 Catégorie B	60
5.4.4 Catégorie C	60
6 Procédure de catégorisation/classement	61
6.1 Généralités	61
6.2 Identification des incidents de fonctionnement prévus (AOO), des accidents de dimensionnement (ADD) et des conditions du domaine de conception étendu (DEC)	62
6.3 Identification et catégorisation des fonctions	63
6.4 Classement des systèmes	64
6.4.1 Classement des systèmes d'I&C	64
6.4.2 Classement des systèmes d'alimentation électrique	65
7 Affectation d'exigences techniques aux catégories et classes	66
Annexe A (normative) Affectation d'exigences techniques aux systèmes d'I&C	68
A.1 Généralités	68
A.2 Exigences concernant les fonctions	68
A.2.1 Exigences de base	68
A.2.2 Exigences spécifiques	69
A.3 Exigences applicables aux systèmes	69
A.3.1 Exigences de base	69
A.3.2 Exigences spécifiques	70
A.4 Exigences liées à la qualification des matériels	73
A.4.1 Exigences de base	73
A.4.2 Exigences spécifiques	73
A.5 Exigences liées aux aspects de qualité (AQ)	74
A.5.1 Exigences de base	74
A.5.2 Exigences spécifiques	75
Annexe B (informative) Exemples de catégories et de classes	77
B.1 Généralités	77
B.2 Catégorie A/Classe 1	77

B.2.1	Fonctions typiques.....	77
B.2.2	Systèmes d'I&C typiques	77
B.2.3	Systèmes d'alimentation électrique typiques.....	77
B.3	Catégorie B/Classe 2.....	77
B.3.1	Fonctions typiques.....	77
B.3.2	Systèmes d'I&C typiques	78
B.3.3	Systèmes d'alimentation électrique typiques.....	78
B.4	Catégorie C/Classe 3.....	78
B.4.1	Fonctions typiques.....	78
B.4.2	Systèmes d'I&C et d'alimentation électrique typiques	78
	Bibliographie.....	80
	Figure 1 – Schéma général de classement.....	48
	Figure 2 – Méthode de catégorisation des fonctions et de classement des systèmes d'I&C..	62
	Figure 3 – Méthode de classement des systèmes d'alimentation électrique.....	66
	Tableau 1 – Corrélation entre classes de systèmes et catégories de fonctions	64
	Tableau 2 – Table de corrélation entre les classes et les autres normes IEC	67

IECNORM.COM : Click to view the full PDF of IEC 61226:2020

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION, DE CONTRÔLE-COMMANDE ET D'ALIMENTATION ÉLECTRIQUE IMPORTANTS POUR LA SÛRETÉ – CATÉGORISATION DES FONCTIONS ET CLASSEMENT DES SYSTÈMES

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61226 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Cette quatrième édition annule et remplace la troisième édition parue en 2009. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- a) l'alignement sur les exigences, les recommandations et la terminologie de l'AIEA, surtout la prise en compte du document SSR 2/1 (ayant remplacé le NS-R-1) et du guide SSG 30;
- b) l'extension du domaine d'application aux systèmes d'alimentation électrique;

- c) le déplacement des exigences détaillées applicables aux fonctions et aux systèmes d'I&C dans une annexe normative, qui sera supprimée à l'issue de la mise à jour de l'IEC 61513.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
45A/1301/FDIS	45A/1306/RVD

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

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

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

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

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

INTRODUCTION

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

La présente Norme internationale satisfait à l'exigence¹ de l'Agence internationale de l'énergie atomique (AIEA) concernant l'identification et le classement des constituants de centrales nucléaires de puissance importants pour la sûreté, sur la base de leurs fonctions et de leur importance pour la sûreté. L'application du concept de défense en profondeur mis en œuvre à travers la combinaison d'un certain nombre de niveaux de protection successifs et suffisamment indépendants entraîne la répartition des fonctions importantes pour la sûreté dans plusieurs systèmes ou sous-systèmes. De plus, l'utilisation actuelle d'éléments numériques programmables pour les systèmes d'instrumentation et de contrôle-commande des centrales nucléaires de puissance permet à chaque système ou sous-système d'assurer souvent plusieurs fonctions. La présente norme a donc pour objet d'établir les critères et méthodes à utiliser pour:

- identifier les fonctions importantes pour la sûreté et les répartir en catégories, selon leur contribution à la prévention et à l'atténuation des conséquences des événements initiateurs postulés;
- classer en conséquence les systèmes d'I&C et d'alimentation électrique qui sont nécessaires pour réaliser ces fonctions.

Selon la norme de sûreté SSR-2/1 (Exigence 22) de l'AIEA, le classement des constituants importants pour la sûreté doit être d'abord basé sur des méthodes déterministes, complétées par des méthodes probabilistes lorsque cela est approprié. Plusieurs approches possibles pour l'utilisation des évaluations probabilistes de sûreté (EPS) sont décrites dans l'IEC TR 61838.

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

L'IEC 61226 est directement référencée par l'IEC 61513 et est le document de deuxième niveau du SC 45A qui traite de la catégorisation des fonctions et du classement des systèmes d'I&C et d'alimentation électrique.

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

c) Recommandations et limites relatives à l'application du présent document

Une catégorisation correcte des fonctions est indispensable pour assurer qu'une attention suffisante soit portée par les concepteurs, les exploitants et les autorités de régulation des centrales aux systèmes assurant les 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.

La présente norme fixe les critères et méthodes de répartition des fonctions d'une centrale nucléaire de puissance réalisées par les systèmes d'I&C et d'alimentation électrique en trois catégories A, B et C, qui dépendent de l'importance de la fonction pour la sûreté. Les fonctions qui n'ont pas de rôle de sûreté direct sont non catégorisées (NC).

La catégorie attribuée à une fonction détermine des exigences techniques destinées à donner l'assurance que cette fonction est réalisée sur demande avec le niveau de performance et de fiabilité exigé et qu'elle satisfait aux exigences de résistance aux conditions environnementales et d'AQ. Le niveau d'assurance à atteindre pour chacun de ces aspects doit être cohérent avec l'importance de la fonction pour la sûreté.

d) Description de la structure de la collection des normes du SC 45A de l'IEC et relations avec d'autres documents de l'IEC, et d'autres organisations (AIEA, ISO)

Les documents de niveau supérieur de la collection de normes produites par le SC 45A de l'IEC sont l'IEC 61513 et l'IEC 63046. L'IEC 61513 traite des exigences générales 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 de puissance. L'IEC 63046 traite des exigences générales relatives

¹ L'exigence 22 de l'AIEA SSR-2/1 en prenant également en compte les exigences 4, 18 et 27.

aux systèmes d'alimentation électrique des centrales nucléaires de puissance; elle couvre les systèmes d'alimentation électrique y compris les alimentations des systèmes d'I&C. L'IEC 61513 et l'IEC 63046 doivent être considérées ensemble et au même niveau. L'IEC 61513 et l'IEC 63046 structurent la collection de normes du SC 45A de l'IEC et forment un cadre complet établissant les exigences générales relatives aux systèmes d'I&C et d'alimentation électrique des centrales nucléaires de puissance.

L'IEC 61513 et l'IEC 63046 font directement référence aux autres normes du SC 45A de l'IEC traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation, la défense contre les défaillances de cause commune, la conception des salles de commande, la compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes numériques programmables, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes, de second niveau, forment, avec l'IEC 61513 et l'IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont pas référencées directement par l'IEC 61513 ou l'IEC 63046, 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 l'IEC correspond aux Rapports techniques qui ne sont pas des documents normatifs.

Les normes de la collection produite par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes et aspects fondamentaux de sûreté établis par les normes de sûreté de l'AIEA pertinentes pour les centrales nucléaires, ainsi qu'avec les documents pertinents de la collection de l'AIEA pour la sécurité nucléaire (NSS), en particulier avec le document d'exigences SSR-2/1 qui établit des exigences de sûreté relatives à la conception des centrales nucléaires de puissance, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires de puissance, avec le guide de sûreté SSG-39 qui traite de la conception des systèmes d'instrumentation et de contrôle-commande des centrales nucléaires de puissance, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires de puissance, et avec le guide de mise en œuvre NSS 17 traitant de la sécurité informatique pour les installations nucléaires. La terminologie et les définitions utilisées pour la sûreté et la sécurité dans les normes produites par le SC 45A sont cohérentes avec celles utilisées par l'AIEA.

Les normes IEC 61513 et IEC 63046 ont adopté une présentation similaire à celle de la publication fondamentale de sécurité IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau de la sûreté nucléaire, les normes IEC 61513 et IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, de l'IEC 61508-2 et de l'IEC 61508-4 pour le secteur nucléaire. Dans ce cadre, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à l'IEC 61508-3 pour le secteur nucléaire. Les normes IEC 61513 et IEC 63046 font référence aux normes ISO ainsi qu'aux documents AIEA GS-R partie 2 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au deuxième niveau, la norme IEC 62645 est le document chapeau des normes du SC 45A de l'IEC portant sur la sécurité nucléaire. Elle est élaborée à partir des principes pertinents de haut niveau et des concepts principaux des normes génériques de sécurité, en particulier l'ISO/IEC 27001 et l'ISO/IEC 27002; elle les adapte et les complète pour les rendre applicables au secteur nucléaire; elle est coordonnée étroitement avec la série IEC 62443. Au deuxième niveau, la norme IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et l'IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

NOTE 1 Il est défini par hypothèse que pour la conception des systèmes d'I&C qui assurent des fonctions de sûreté conventionnelle des centrales nucléaires de puissance (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les dangers chimiques et la prévention contre les dangers liés à l'énergie du procédé), des normes nationales ou internationales sont appliquées.

NOTE 2 Le domaine de l'IEC SC 45A a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015, des discussions ont eu lieu au sein de l'IEC SC 45A pour décider de la façon et de l'endroit pour établir les exigences générales portant sur la conception des systèmes électriques. Les experts de l'IEC SC 45A ont recommandé que pour établir des exigences générales pour les systèmes électriques une norme indépendante soit développée au même niveau que l'IEC 61513. Le projet IEC 63046 est lancé pour atteindre cet objectif. Lorsque la norme IEC 63046 sera publiée, la présente Note 2 de l'introduction sera supprimée.

IECNORM.COM : Click to view the full PDF of IEC 61226:2020

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION, DE CONTRÔLE-COMMANDE ET D'ALIMENTATION ÉLECTRIQUE IMPORTANTS POUR LA SÛRETÉ – CATÉGORISATION DES FONCTIONS ET CLASSEMENT DES SYSTÈMES

1 Domaine d'application

Le présent document établit, pour les centrales nucléaires de puissance², une méthode d'affectation en catégories des fonctions spécifiées pour la centrale, sur la base de leur importance pour la sûreté. Le classement, sur la base de la catégorie attribuée, des systèmes d'I&C et d'alimentation électrique assurant ou contribuant à la réalisation de ces fonctions détermine alors les critères de conception appropriés.

Les critères de conception, dès lors qu'ils sont appliqués, garantissent que chaque fonction est réalisée selon son importance pour la sûreté. Les critères retenus dans le présent document concernent la fonctionnalité, la fiabilité, les performances, la qualification aux conditions environnementales (par exemple, la qualification sismique) et l'assurance qualité (AQ).

Le présent document est applicable aux:

- fonctions importantes pour la sûreté dont la réalisation est assurée par des systèmes d'I&C avec l'appui de systèmes d'alimentation électrique (catégorisation des fonctions d'I&C),
- systèmes d'I&C qui permettent la mise en œuvre de ces fonctions (classement des systèmes d'I&C),
- systèmes d'alimentation électrique qui contribuent à ces fonctions (classement des systèmes d'alimentation électrique).

Les systèmes à l'étude assurent la protection automatique, les régulations en boucles ouvertes et fermées, l'information des opérateurs et l'alimentation électrique des systèmes. Ces systèmes permettent de maintenir les paramètres d'exploitation de la centrale nucléaire de puissance à l'intérieur du domaine de sûreté d'exploitation et assurent les actions automatiques, ou permettent les actions manuelles qui préviennent ou limitent les conséquences des accidents, ou qui empêchent ou réduisent le plus possible les rejets radioactifs sur le site ou dans l'environnement en général. Les systèmes d'I&C et d'alimentation électrique qui remplissent ces rôles protègent la santé et assurent la sécurité des opérateurs de centrales nucléaires de puissance ainsi que du public.

Le présent document est conforme aux principes généraux donnés dans la norme d'exigences de sûreté SSR-2/1 et dans les guides de sûreté SSG-30, SSG-34 et SSG-39 de l'AIEA, et il définit une méthode structurée d'application des recommandations contenues dans ces codes et normes pour les systèmes d'I&C et d'alimentation électrique qui assurent des fonctions importantes pour la sûreté dans les centrales nucléaires de puissance. Le présent document est utilisé ensemble avec les guides de l'AIEA, l'IEC 61513 et l'IEC 63046 dans la mise en œuvre des exigences de la série IEC 61508. Le schéma général de classement des structures, systèmes et composants des centrales nucléaires de puissance peut être résumé tel que représenté à la Figure 1.

² Le domaine d'application du présent document est cohérent avec celui des documents SSR-2/1 et SSG-30 de l'AIEA, sur lesquels il se fonde.

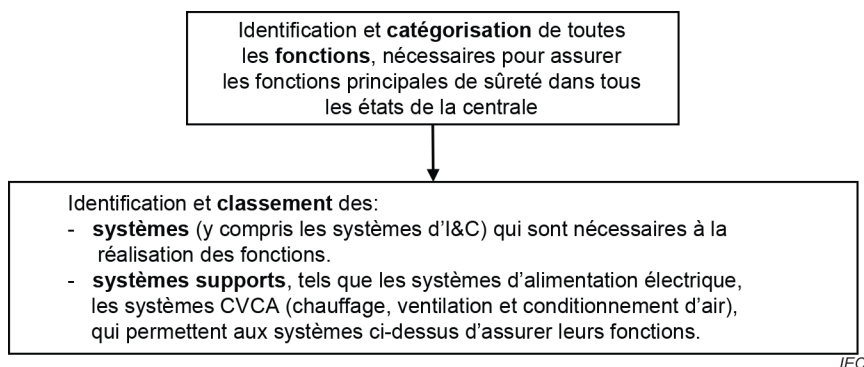


Figure 1 – Schéma général de classement

Ce processus à 2 phases est défini dans un but d'exhaustivité. Il permet la prise en compte de toutes les fonctions et de tous les systèmes importants pour la sûreté, y compris les systèmes d'I&C, ainsi que les systèmes d'alimentation électrique.

Les fonctions contenues dans ce schéma sont définies et catégorisées indépendamment des moyens physiques mis en œuvre pour les assurer. Dans le cadre du présent document, les fonctions à catégoriser sont assurées par les systèmes d'I&C. Elles sont par conséquent appelées fonctions d'I&C.

Le présent document s'applique aux systèmes d'I&C et d'alimentation électrique pour les nouvelles centrales nucléaires de puissance, ainsi que pour la modification et la modernisation des centrales existantes.

Pour les centrales existantes, seul un sous-ensemble d'exigences peut être appliqué et ce sous-ensemble est identifié au début de tout projet.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

IEC/IEEE 60780-323, *Installations nucléaires – Équipements électriques importants pour la sûreté – Qualification*

IEC 60812, *Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC)*

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

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

IEC 60965, *Centrales nucléaires de puissance – Salles de commande – Salle de commande supplémentaire pour l'arrêt des réacteurs sans accès à la salle de commande principale*

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

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

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

IEC 61500, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Communications de données dans les systèmes réalisant des fonctions de catégorie A*

IEC 61513:2011, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

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

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

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

IEC 62003, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences relatives aux essais de compatibilité électromagnétique*

IEC 62138:2018, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

IEC 62566, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie A*

IEC 62645, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences relatives aux programmes de sécurité applicables aux systèmes programmés*

IEC 62671, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils numériques à fonctionnalités limitées*

IEC 62859, *Centrales nucléaires de puissance – Systèmes d'instrumentation et contrôle-commande – Exigences pour coordonner sûreté et cybersécurité*

IEC 63046:—³, *Centrales nucléaires de puissance – Système d'alimentation électrique – Exigences générales*

IAEA GSR Part 2:2016, *Direction et gestion pour la sûreté*

IAEA SSR-2/1 (Rev.1):2016, *Sûreté des centrales nucléaires: conception*

³ En cours d'élaboration. Stade au moment de la publication: IEC CDV 63046:2019.

IAEA SSG-30:2014, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants* (disponible en anglais seulement)

3 Termes et définitions

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

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

- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <http://www.iso.org/obp>

3.1

incident de fonctionnement prévu

AOO

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 ou ne dégénère pas en conditions accidentelles

Note 1 à l'article: Le terme abrégé "AOO" est dérivé du terme anglais développé correspondant "anticipated operational occurrence".

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.2

défaillance de cause commune

DCC

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

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.3

état contrôlé

état de la centrale, après un incident de fonctionnement prévu ou des conditions accidentelles, dans lequel les fonctions fondamentales de sûreté peuvent être assurées et qui peut être maintenu pendant une durée suffisante pour mettre en œuvre les dispositions permettant d'atteindre un état sûr

Note 1 à l'article: Se référer à liste des fonctions fondamentales de sûreté en 3.254.

Note 2 à l'article: Voir la définition de l'état sûr en 3.21.

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.4

accident de dimensionnement

ADD

accident postulé conduisant à l'apparition de conditions accidentelles par rapport auxquelles une installation nucléaire est conçue pour résister conformément à des critères de conception spécifiés et à une méthodologie conservative, et pour lesquelles les rejets de matières radioactives restent dans des limites acceptables

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.5

conditions du domaine de conception étendu

DEC

conditions accidentelles postulées qui ne sont pas prises en compte dans les accidents de dimensionnement mais qui le sont dans le processus de conception de l'installation selon des méthodes de type "hypothèse la plus probable", et dans lesquelles les rejets de matières radioactives sont maintenus dans des limites acceptables

Note 1 à l'article: Les conditions du domaine de conception étendu comprennent les conditions correspondant aux événements sans dégradation significative du combustible et les conditions correspondant aux événements avec fusion du cœur.

Note 2 à l'article: Un ensemble de conditions du domaine de conception étendu doit être établi à partir du jugement de l'ingénieur, d'évaluations déterministes et d'évaluations probabilistes en vue d'améliorer encore la sûreté de la centrale nucléaire en renforçant les capacités de cette dernière à résister, sans conséquences radiologiques inacceptables, à des accidents qui sont plus sévères que les accidents de dimensionnement ou qui incluent des défaillances supplémentaires. Ces conditions du domaine de conception étendu doivent être utilisées pour déterminer les scénarios d'accidents supplémentaires à prendre en considération dans la conception et pour prévoir les dispositions pratiques à adopter pour la prévention de ces accidents ou l'atténuation de leurs conséquences. [AIEA SSR-2/1]

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.6

diversité

présence de deux ou plusieurs systèmes ou composants indépendants (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 une défaillance de mode commun

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.7

élément électrique/électronique/électronique programmable

élément E/E/PE

élément réalisé à base de technologie électrique (E) et/ou électronique (E) et/ou électronique programmable (PE)

[SOURCE: IEC 62138:2018, 3.15]

3.8

système d'alimentation électrique

système assurant la production, le transport et la distribution de l'énergie électrique, ainsi que l'alimentation des matériels de la centrale (pompes, robinets, éléments chauffants) et des systèmes d'I&C

Note 1 à l'article: Un système d'alimentation électrique peut intégrer des éléments E/E/PE pour ses fonctions de contrôle et de protection électrique internes.

[SOURCE: IEC CDV 63046:2019, 3.12]

3.9

matériel

une ou plusieurs parties d'un système; un équipement est une partie déterminée et définissable (et généralement amovible) d'un système

[SOURCE: IEC 61513:2011, 3.16, modifié – Les notes à l'article ont été omises.]

3.10

fonction

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

3.11

fonctionnalité

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

[SOURCE: IEC 61513: 2011, 3.24, modifié – La note a été omise.]

3.12

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

3.13

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

Note 1 à l'article: Les constituants importants pour la sûreté comprennent:

- a) les structures, systèmes et composants dont le mauvais fonctionnement ou la défaillance pourraient entraîner une exposition induite 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 conçus pour atténuer les conséquences d'un mauvais fonctionnement ou d'une défaillance de structures, systèmes ou composants

Note 2 à l'article: Les constituants importants pour la sûreté pris en compte dans la présente norme sont les systèmes d'I&C et les systèmes d'alimentation électrique.

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.14

système d'I&C

système réalisé sur la base d'éléments E/E/PE, exécutant des fonctions d'I&C ainsi que des fonctions de service et d'affichage liées au fonctionnement du système lui-même

[SOURCE: IEC 62138:2018, 3.26, modifié – Les notes à l'article ont été omises.]

3.15

fonctionnement normal

fonctionnement dans des limites et conditions d'exploitation spécifiées

Note 1 à l'article: Pour une centrale nucléaire, cela comprend le démarrage, le fonctionnement en puissance, la mise à l'arrêt, l'arrêt, la maintenance, les essais et le rechargement en combustible.

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.16

performance

efficacité avec laquelle une fonction prévue est exécutée

Note 1 à l'article: Par exemple, temps de réponse, exactitude, sensibilité aux variations de paramètres.

3.17**essais périodiques**

réalisation d'essais à des instants prédéfinis permettant de démontrer que les capacités fonctionnelles des systèmes et des matériels d'I&C importants pour la sûreté sont assurées et de confirmer que les caractéristiques importantes pour satisfaire aux exigences de l'analyse de sûreté sont satisfaites

[SOURCE: IEC 60671:2007, 3.7]

3.18**états de la centrale**

Conditions de fonctionnement attendues		Conditions accidentelles	
Fonctionnement normal	Incidents de fonctionnement prévus	Accidents de dimensionnement	Accidents du domaine de conception étendu
			Sans endommagement significatif du combustible Avec fusion du cœur

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.19**événement initiateur postulé****PIE**

événement postulé dont il est déterminé au stade de la conception qu'il peut entraîner des incidents de fonctionnement prévus ou des conditions accidentelles

Note 1 à l'article: Le terme abrégé "PIE" est dérivé du terme anglais développé correspondant "postulated initiating event".

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.20**redondance**

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

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.21**état sûr**

état de la centrale, après un incident de fonctionnement prévu ou des conditions accidentelles, dans lequel le réacteur est sous-critique et les fonctions fondamentales de sûreté peuvent être assurées et maintenues stables pendant une longue période

Note 1 à l'article: Se référer à liste des fonctions fondamentales de sûreté en 3.25.

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.22**catégorisation de sûreté**

pour les centrales nucléaires de puissance, répartition en un nombre limité de catégories de sûreté, sur la base de leur importance pour la sûreté, des fonctions requises pour assurer les fonctions fondamentales de sûreté dans les différents états de la centrale, y compris tous les modes de fonctionnement normal

Note 1 à l'article: Se référer à liste des fonctions fondamentales de sûreté en 3.25.

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.23

classement de sûreté

pour les centrales nucléaires de puissance, répartition en un nombre limité de classes de sûreté des systèmes, composants et autres matériels, sur la base de leurs fonctions et de leur importance pour la sûreté

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.24

fonction de sûreté

objectif spécifique devant être réalisé pour la sûreté d'une installation nucléaire ou d'une activité afin de prévenir ou atténuer les conséquences radiologiques du fonctionnement normal, des incidents de fonctionnement prévus et des conditions accidentelles

Note 1 à l'article: Les fonctions de sûreté sont nécessaires pour 'assurer les fonctions fondamentales de sûreté qui sont: (i) la maîtrise de la réactivité, (ii) l'évacuation de la chaleur provenant du réacteur et de l'installation d'entreposage du combustible, (iii) le confinement des matières radioactives, la protection contre les rayonnements et la maîtrise des rejets radioactifs programmés, ainsi que la limitation des rejets radioactifs accidentels [AIEA SSR-2/1, Exigence 4]

Note 2 à l'article: Les fonctions de sûreté sont principalement celles mentionnées dans l'analyse de sûreté et comprennent les fonctions réalisées à tous les niveaux de défense en profondeur.

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.25

groupe de sûreté

ensemble d'équipements prévus pour accomplir toutes les actions exigées si un événement initiateur 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

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.26

autosurveillance

test automatique des performances matérielles et de la cohérence logicielle d'un système d'I&C informatisé

[SOURCE: IEC 60671:2007, 3.8]

3.27

défaillance unique

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

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.28

système support

système qui fournit des services pour permettre à un autre système de remplir une fonction

Note 1 à l'article: Ces services comprennent, par exemple, l'alimentation électrique, le CVCA, le refroidissement, la lubrification.

3.29**système**

ensemble de composants qui interagissent conformément à une conception donnée, un élément d'un système pouvant être un autre système, appelé sous-système

[SOURCE: IEC 61513:2011, 3.56, modifié – Les notes à l'article ont été omises.]

3.30**essai de type**

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

4 Termes abrégés

ALARA	aussi faible qu'il soit raisonnablement possible de réaliser
AOO	anticipated operational occurrence (incident de fonctionnement prévu)
BWR	boiling water reactor (réacteur à eau bouillante)
DCC	défaillance de cause commune
ADD	accidents de dimensionnement
DEC	design extension condition (conditions du domaine de conception étendu)
E/E/PE	élément électrique/électronique/électronique programmable (élément E/E/PE)
FAT	factory acceptance test (essai de recette usine)
AMDE	analyse des modes de défaillance et de leurs effets
IHM	interface homme-machine
CVCA	chauffage, ventilation et conditionnement d'air
AIEA	Agence internationale de l'énergie atomique
ISO	International Organization for Standardization (Organisation Internationale de normalisation)
I&C	instrumentation et contrôle-commande
NC	non catégorisé
CNP	centrale nucléaire de puissance
EPS	évaluation probabiliste de sûreté
PIE	postulated initiating event (événement initiateur postulé)
PWR	pressurized water reactor (réacteur à eau pressurisée)
AQ	assurance qualité
SAT	site acceptance test (recette site)
SSC	structures, systèmes et composants

5 Schéma de catégorisation**5.1 Généralités**

Les fonctions de sûreté doivent être affectées à différentes catégories selon leur importance pour la sûreté. La catégorie détermine la classe à attribuer aux systèmes d'I&C qui réalisent ces fonctions et la classe à attribuer aux systèmes d'alimentation électrique qui permettent l'accomplissement de ces fonctions (y compris ceux qui alimentent les matériels d'I&C). La classe détermine ensuite les exigences de conception et de qualité applicables à ces systèmes.

Le 5.2 traite du contexte de la démarche de catégorisation.

Le 5.3 décrit les trois catégories qui sont utilisées pour catégoriser les fonctions, selon leur importance pour la sûreté. Les catégories sont cohérentes avec celles définies dans l'AIEA SSG-30.

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

L'Article 6 donne des recommandations relatives au processus de catégorisation ainsi que des recommandations relatives à la relation entre la catégorisation fonctionnelle et les classes des systèmes.

L'Article 7 et l'Annexe A traitent des exigences techniques de haut niveau pour chaque catégorie (exigences s'appliquant aux fonctions) et chaque classe (exigences s'appliquant aux systèmes qui réalisent les fonctions). Des exigences techniques plus détaillées sont présentées dans des normes IEC spécialisées.

L'Annexe B contient des exemples caractéristiques de catégorisation des fonctions et de classement des systèmes de centrales nucléaires de puissance. Elle est uniquement informative puisque les fonctions et systèmes mentionnés peuvent dépendre du type de réacteur concerné.

5.2 Contexte

Le principe de défense en profondeur est très fermement établi dans la conception de base de sûreté des centrales nucléaires de puissance. L'idée fondamentale à privilégier est qu'il convient de prévoir plusieurs niveaux ou lignes de défense pour prévenir les conditions dangereuses avant que la mise en œuvre de mesures d'atténuation ne soit nécessaire. En raison du grand nombre de fonctions exigées pour assurer le fonctionnement de la centrale nucléaire de puissance et garantir sa sûreté, nombre qui augmente du fait du principe de défense en profondeur, il est essentiel que l'importance pour la sûreté de chacune de ces fonctions soit connue. Toutes les fonctions réalisées aux différents niveaux de défense en profondeur sont prises en considération.

La norme de sûreté de l'AIEA SSR-2/1 définit le principe de classement des systèmes de centrales nucléaires de puissance selon leur importance pour la sûreté, et donne des exemples de classement des systèmes principaux de plusieurs types de centrales nucléaires de puissance. 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 entretenus de telle façon que leur qualité et leur fiabilité soient cohérentes avec ce classement.

Conformément aux exigences du 5.34 de la norme de sûreté SSR-2/1 de l'AIEA, la détermination de l'importance pour la sûreté des constituants doit reposer principalement sur des méthodes déterministes complétées, s'il y a lieu, par des méthodes probabilistes, en tenant compte de facteurs tels que:

- a) la ou les fonctions de sûreté destinées à être assurées par le constituant;
- b) les conséquences liées au non-accomplissement d'une fonction de sûreté;
- c) la fréquence avec laquelle le constituant sera appelé à assurer une fonction de sûreté;
- d) le moment auquel, après un PIE, le constituant sera appelé à assurer une fonction de sûreté ou la durée pendant laquelle il sera appelé à l'assurer.

Le guide de sûreté de l'AIEA SSG-30 donne des recommandations sur la catégorisation des fonctions et le classement des SSC selon leur importance pour la sûreté.

Le présent document étend la stratégie de catégorisation présentée dans le guide de sûreté de l'AIEA SSG-30, et définit les critères et méthodes à utiliser pour affecter les fonctions des centrales nucléaires de puissance à une des trois catégories A, B et C en fonction de leur importance pour la sûreté, ou pour les considérer comme "non catégorisées" (NC) si elles ne jouent aucun rôle de sûreté.

Le chapitre 5 de l'AIEA SSG 39 traitant du classement des systèmes d'I&C et le chapitre 3 de l'AIEA SSG 34 traitant du classement des systèmes d'alimentation électrique font directement référence aux SSR-2/1 et SSG-30 et sont cohérents avec les principes du présent document.

L'application nationale des critères et des principes du présent document peut imposer une nomenclature différente des catégories A, B et C.

5.3 Description des catégories

5.3.1 Généralités

La détermination de l'importance pour la sûreté d'une fonction doit tout d'abord reposer sur des méthodes déterministes, complétées le cas échéant par des méthodes probabilistes et le jugement de l'ingénieur.

La détermination de l'importance pour la sûreté d'une fonction destinée à satisfaire à un événement initiateur postulé (PIE) doit tenir compte des aspects suivants:

- Les conséquences de l'échec de la réalisation de la fonction.
- La fréquence d'occurrence du PIE pour lequel la fonction sera sollicitée.
- L'importance de la contribution de la fonction à l'atteinte d'un état contrôlé ou d'un état sûr.

Lors de l'évaluation de l'importance pour la sûreté d'une fonction il convient de prendre en compte les facteurs suivants:

- le rôle de la fonction dans la prévention des PIE pendant le fonctionnement normal (y compris pendant le démarrage, le rechargement, etc.);
- le rôle de la fonction dans l'atténuation des conséquences des AOO, des ADD ou des DEC;
- le moment auquel, après un PIE, la fonction doit être assurée ou la durée pendant laquelle elle doit être réalisée;
- les conséquences en cas d'activation intempestive, pour les différents états de la centrale (conditions de fonctionnement attendues et conditions accidentelles);
- le rôle de la fonction après des PIE tels que des phénomènes naturels (par exemple: séisme, inondation, vent extrême, foudre), des phénomènes externes d'origine humaine (par exemple: rejets chimiques d'autres usines et d'autres industries) et des agressions internes (par exemple: incendie, inondation interne, missiles);
- la stratégie d'essai, de maintenance et de réparation.

Ainsi, une analyse de sûreté initiale de la conception spécifique à la centrale nucléaire de puissance doit être réalisée avant la catégorisation des fonctions. Il convient d'identifier, sur la base de cette analyse de sûreté, les fonctions à catégoriser avec une granularité suffisamment détaillée, de telle sorte qu'une fonction donnée puisse être affectée à un seul système d'I&C.

Pour évaluer les conséquences de l'échec de la réalisation de la fonction, le guide SSG-30 définit pour les centrales nucléaires de puissance trois niveaux de gravité, en gardant à l'esprit que les fonctions mises en œuvre pour contrôler les accidents ont pour objectif de rendre les conséquences de ces accidents acceptables et également aussi faibles que possible. L'évaluation de ces conséquences est faite en prenant comme hypothèse la non-réponse de la fonction sollicitée, sans valoriser le secours possible de cette fonction par une autre fonction:

- Il convient de considérer la gravité comme "élevée" lorsque la défaillance de la fonction peut, dans le cas le plus défavorable, entraîner un rejet de matières radioactives supérieur aux limites admises par l'autorité de régulation pour les accidents de dimensionnement. Il convient également de la considérer ainsi lorsqu'une telle défaillance peut amener les valeurs des paramètres physiques clés (par exemple: pression, température, etc.) à dépasser les critères d'acceptation des accidents de dimensionnement.
- Il convient de considérer la gravité comme "moyenne" lorsque la défaillance de la fonction peut, dans le cas le plus défavorable, entraîner un rejet de matières radioactives supérieur aux limites définies pour les incidents de fonctionnement prévus. Il convient également de la considérer ainsi lorsqu'une telle défaillance peut amener les valeurs des paramètres physiques clés à dépasser les limites de conception des incidents de fonctionnement prévus.
- Il convient de considérer la gravité comme "faible" lorsque la défaillance de la fonction peut, dans le cas le plus défavorable, conduire à exposer les travailleurs à des doses dépassant les limites autorisées.

Vis-à-vis de la nomenclature de catégorisation du document SSG-30 de l'AIEA, les exigences fournies par le présent document couvrent l'allocation aux catégories A, B et C des fonctions qui peuvent être mises en œuvre par des systèmes d'I&C et/ou supportées par des systèmes d'alimentation électrique. Elles correspondent respectivement aux catégories 1, 2 et 3 du guide SSG-30 de l'AIEA.

5.3.2 Catégorie A

La catégorie A doit être attribuée aux fonctions qui jouent un rôle principal dans l'obtention ou le maintien de la sûreté de la centrale nucléaire de puissance pour empêcher que les incidents de fonctionnement prévus (AOO) ou les accidents de dimensionnement (ADD) ne conduisent à des conséquences de gravité élevée. Ce rôle est essentiel en début de transitoire lorsqu'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 ⁴.

La catégorie A s'applique aussi aux fonctions dont la défaillance peut conduire directement à des conditions accidentelles qui peuvent entraîner des conséquences de gravité élevée, et pour lesquelles il n'existe pas d'autres fonctions de catégorie A empêchant de telles conséquences.

⁴ Pour faire face aux transitoires rapides, la centrale est contrôlée durant cette phase 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 soient prises en compte dans les études d'accident après un "délai de grâce" approprié. Ce type de délai de grâce représente une exigence de conception de la centrale correspondant à un délai nécessaire au diagnostic et aux actions, prenant en compte avec des marges suffisantes les aspects liés au facteur humain et à l'accessibilité. Cela ne signifie pas que les actions manuelles sont interdites durant cette période. Dans certains pays, et pour des centrales nucléaires de puissance plus anciennes, la limite entre la catégorie A et la catégorie B peut être ce délai de grâce, en lieu et place de l'état contrôlé.

5.3.3 Catégorie B

La catégorie B est attribuée aux fonctions qui jouent un rôle complémentaire par rapport aux fonctions de catégorie A dans l'obtention et le maintien de la sûreté de la centrale nucléaire de puissance, spécialement les fonctions dont la réalisation est exigée après l'atteinte de l'état contrôlé pour empêcher que des AOO ou des ADD ne conduisent à des conséquences de gravité élevée, ou celles qui sont requises pour l'atteinte de l'état contrôlé pour empêcher que des AOO ou des ADD ne conduisent à des conséquences de gravité moyenne.

La catégorie B est aussi attribuée aux fonctions conçues pour contrôler les DEC sans dégradation du combustible résultant ou comprenant la défaillance hypothétique d'une fonction de catégorie A, afin que les dommages pour la centrale ou ses matériels ou les rejets radioactifs puissent être évités ou minimisés.

La catégorie B est aussi attribuée aux fonctions dont la défaillance peut conduire directement à des conditions accidentelles qui peuvent entraîner des conséquences de gravité moyenne, et pour lesquelles il n'existe pas d'autres fonctions de catégorie A ou B empêchant de telles conséquences.

5.3.4 Catégorie C

La catégorie C est attribuée aux fonctions qui jouent un rôle auxiliaire ou indirect dans l'obtention et le maintien de la sûreté de la centrale nucléaire de puissance. 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 AOO ou ADD sans être directement impliquées pour éviter des conséquences de gravité élevée, ou être nécessaires pour d'autres raisons (par exemple, pour atténuer les conséquences des DEC ou des agressions).

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-après.

Si une fonction ne satisfait à aucun de ces critères, elle doit être considérée comme "non catégorisée" (NC).

Si la répartition est possible dans plusieurs catégories, la fonction doit être affectée, finalement, à la catégorie la plus haute possible.

L'affectation finale des fonctions peut être modifiée en utilisant des méthodes probabilistes, conformément aux principes présentés en 6.3.

5.4.2 Catégorie A

Une fonction doit être affectée à la catégorie A si elle satisfait à un des critères suivants:

- a) une fonction requise pour atteindre l'état contrôlé, afin d'empêcher qu'un AOO ou ADD ne conduise à des conséquences de gravité élevée;
- b) une fonction dont la défaillance ou l'activation intempestive en fonctionnement normal entraînerait des conséquences de gravité élevée;
- c) une fonction requise pour fournir de l'information et des moyens de commande qui permettent de réaliser les actions manuelles spécifiées nécessaires pour atteindre l'état contrôlé afin d'éviter des conséquences de gravité élevée.

5.4.3 Catégorie B

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

- a) une fonction requise pour atteindre l'état contrôlé, pour empêcher qu'un AOO ou ADD ne conduise à des conséquences de gravité moyenne.
Il convient d'appliquer ce critère aux fonctions de régulation des paramètres du procédé de la centrale si ces fonctions sont prises en compte dans l'analyse de sûreté pour empêcher un AOO de se dégrader en ADD.
- b) une fonction requise pour atteindre et maintenir l'état sûr, après atteinte de l'état contrôlé associé à un AOO ou ADD, afin d'empêcher que cet AOO ou ADD ne conduise à des conséquences de gravité élevée;
- c) une fonction requise pour fournir de l'information et des moyens de commande permettant de réaliser les actions manuelles spécifiées nécessaires pour atteindre et maintenir l'état sûr, après atteinte de l'état contrôlé pour empêcher qu'un AOO ou ADD ne conduise à des conséquences de gravité élevée;
- d) une fonction requise pour le contrôle d'une condition DEC sans dégradation significative du combustible résultant de ou comprenant la défaillance hypothétique d'une fonction de catégorie A;
- e) une fonction dont la défaillance ou l'activation intempestive en fonctionnement normal entraînerait des conséquences de gravité moyenne, et pour laquelle il n'existe pas d'autres fonctions de catégorie A ou B empêchant des conséquences de gravité moyenne;
- f) une fonction requise dans l'analyse de sûreté pour réduire de façon importante la fréquence d'un ADD;

Par extension il convient d'appliquer ce critère aux fonctions dont l'activation intempestive en fonctionnement normal pourrait conduire à un ADD.

- g) une fonction qui assure des essais, de façon continue ou intermittente, ou une surveillance de fonctions de catégorie A, pour garantir la continuité de leur disponibilité opérationnelle et pour prévenir le personnel de la salle de commande de leurs défaillances, lorsqu'aucun autre moyen (par exemple, essais périodiques) n'est mis en œuvre pour vérifier leurs disponibilités⁵.

NOTE Lorsque la fonction de surveillance est le seul moyen de détection des défaillances qui sinon seraient cachées, l'affectation de la fonction de surveillance à la catégorie B garantit un niveau de qualité approprié.

5.4.4 Catégorie C

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

- a) une fonction de commande du procédé de la centrale assurant le maintien des paramètres de la centrale dans les limites de la plage de fonctionnement normal.
- b) une fonction sollicitée en cas d'un AOO ou ADD et dont la défaillance, si elle se produisait, entraînerait des conséquences de gravité faible;
- c) une fonction permettant d'atteindre et de maintenir pendant une longue durée un état sûr et dont la défaillance, si elle se produisait, entraînerait des conséquences de gravité moyenne;
- d) une fonction qui assure des essais, 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 affectées à la catégorie B conformément à 5.4.3g;

⁵ Le 4.2.6 de l'IEC 60671:2007 fournit des recommandations supplémentaires sur le classement des matériels utilisés pour mettre en œuvre 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".

- e) une fonction destinée à réduire la fréquence d'arrêt automatique du réacteur ou de mise en service des dispositifs de sauvegarde;
Par extension, il convient d'appliquer ce critère aux fonctions dont l'activation intempestive en fonctionnement normal pourrait conduire à l'arrêt automatique du réacteur ou à la mise en service des dispositifs de sauvegarde.
- f) une fonction de surveillance et de limitation des conséquences en cas d'agression interne prise en compte dans le dimensionnement de la centrale nucléaire de puissance (exemple: incendie, inondation);
- g) une fonction dont la défaillance ou l'activation intempestive en fonctionnement normal entraînerait des conséquences de gravité faible;
- h) une fonction d'alerte du personnel ou assurant sa sécurité, pendant ou après des événements comprenant ou ayant entraîné des rejets radioactifs dans la centrale nucléaire de puissance ou un risque d'exposition aux rayonnements;
- i) une fonction fournissant les informations nécessaires pour déterminer l'ampleur et la dispersion des rejets de matières radioactives en cas d'accident;
- j) une fonction qui surveille et/ou annonce un état de la centrale afin que des actions puissent être lancées, soit pour éviter une situation non sûre, soit pour en atténuer les conséquences après des phénomènes naturels (par exemple séisme, inondation, vent extrême, foudre);
- k) une fonction permettant d'atténuer les conséquences d'une condition DEC, sauf si elle doit déjà être affectée à la catégorie de sûreté B, y compris les informations et commandes nécessaires à la mise en œuvre des recommandations de gestion des situations d'accident grave (c'est-à-dire des DEC avec fusion du cœur), et dont la défaillance, si elle se produisait, entraînerait des conséquences de gravité élevée;
- l) une fonction de contrôle d'accès pour la protection du personnel;
- m) une fonction permettant de fournir au personnel de la centrale et aux services d'urgence hors site les informations nécessaires à la mise en œuvre du plan d'urgence.

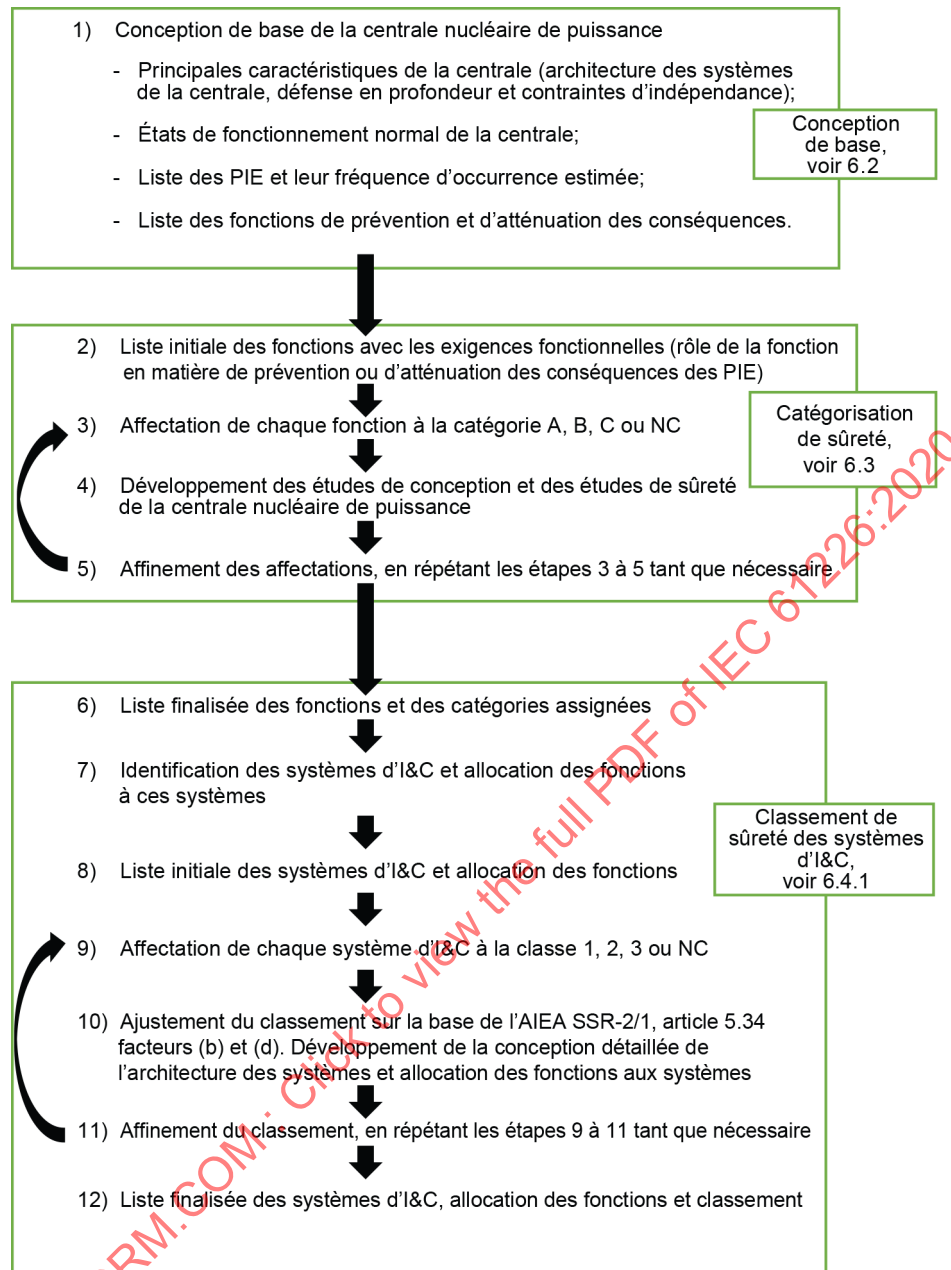
6 Procédure de catégorisation/classement

6.1 Généralités

Un diagramme de la procédure est donné à la Figure 2. Il comprend trois phases:

- la conception de base de la centrale nucléaire de puissance;
- la catégorisation de sûreté des fonctions;
- le classement de sûreté des systèmes d'I&C⁶.

⁶ La troisième phase représentée à la Figure 2 s'applique aux systèmes d'I&C. La classe de sûreté des systèmes d'alimentation électrique découle directement de la classe de sûreté des systèmes qu'ils alimentent (qu'il s'agisse de systèmes d'I&C ou de systèmes qui agissent directement sur le procédé de la centrale). Voir le 6.4.2 pour plus de détails.



IEC

Figure 2 – Méthode de catégorisation des fonctions et de classement des systèmes d'I&C

6.2 Identification des incidents de fonctionnement prévus (AOO), des accidents de dimensionnement (ADD) et des conditions du domaine de conception étendu (DEC)

La nature de la centrale nucléaire de puissance et le type de réacteur (par exemple, PWR (réacteur à eau pressurisée), BWR (réacteur à eau bouillante) ou autres types de réacteur) et les PIE associés sont les principales données d'entrée du processus de catégorisation. Une autre donnée d'entrée essentielle est l'identification des fonctions principales d'atténuation des conséquences pour chaque PIE.

L'évaluation de la fréquence et des conséquences des PIE conduit à l'identification des AOO ou ADD représentant la base de conception de la centrale, et des DEC représentant d'autres conditions accidentelles à prendre en compte lors de la conception. Lors de l'étude des dispositions de conception de la centrale, l'ensemble des conditions de fonctionnement prévues et des conditions accidentelles, ainsi que les limites radiologiques définies, doivent être prises en compte. Les principes de sûreté élémentaires qui ensemble forment une "approche globale intégrée de sûreté" garantissent la sûreté de la centrale nucléaire de puissance. Ces principes sont utilisés lors de la conception en prenant en considération les AOO, ADD et DEC identifiés et les barrières physiques successives permettant de maintenir les expositions aux rayonnements dans les limites autorisées. Les AOO, ADD et DEC ainsi que l'identification des fonctions de prévention et d'atténuation des conséquences sont les données d'entrée essentielles du processus de catégorisation.

L'importance pour la sûreté de chacune des fonctions dépend de son rôle dans l'obtention et le maintien de la sûreté de la centrale nucléaire de puissance et des conséquences potentielles de l'échec de la réalisation de la fonction lorsque celle-ci est appelée. Ainsi, une analyse de sûreté initiale de la conception spécifique à la centrale doit être réalisée avant la catégorisation des fonctions.

Selon l'AIEA SSR 2/1, l'identification du dimensionnement de base et du domaine de conception étendu, et donc l'identification et la catégorisation des fonctions, concernent toutes les parties des centrales pouvant entraîner des rejets importants de matières radioactives, c'est-à-dire non seulement le cœur du réacteur, mais aussi le combustible nucléaire usé, les déchets radioactifs ou toute autre source de rayonnement dans une centrale nucléaire de puissance.

6.3 Identification et catégorisation des fonctions

Dès le début de la conception de la centrale nucléaire de puissance, les fonctions relevant de la sûreté doivent être identifiées. Il convient d'identifier ces fonctions et de les affecter à une fonction automatisée⁷ ou aux opérateurs conformément aux exigences de l'IEC 60964. À l'issue de cette identification initiale des fonctions, chaque fonction automatique ou manuelle doit être affectée à une catégorie selon les critères de l'Article 5.

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 de puissance ne sont pas complètement définies. Par conséquent, le processus d'identification et de catégorisation des fonctions doit se poursuivre 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 pour une décision ultérieure.

Étant donné qu'une même fonction élémentaire peut être utilisée pour répondre à plusieurs spécifications distinctes, 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 catégorisation doit être affinée et revue pour converger vers une liste finalisée des fonctions et des catégories assignées, dès que la conception de la centrale nucléaire de puissance est connue plus précisément, par exemple lorsque la progression de l'analyse de sûreté est suffisamment avancée et après le développement des procédures de conduite. Cette liste doit être documentée et tenue à jour par gestion de configuration car elle sera exigée par les concepteurs de la centrale et des systèmes pendant toute la durée de vie de la centrale nucléaire de puissance. Cette liste peut aussi être exigée par les autorités de régulation.

⁷ Les fonctions automatisées traitées ici sont les fonctions de contrôle-commande mises en œuvre dans les systèmes d'I&C. La conversion d'énergie ou la fonction de transport d'énergie des systèmes électriques n'est pas concernée.

6.4 Classement des systèmes

6.4.1 Classement des systèmes d'I&C

La prochaine étape après celle de la catégorisation de sûreté des fonctions consiste à identifier les systèmes d'I&C qui réalisent ou qui contribuent à la réalisation des fonctions. Tous les systèmes et composants nécessaires à l'exécution des fonctions doivent être identifiés, c'est à dire non seulement les systèmes et composants qui agissent directement sur le procédé de la centrale (actionneurs, vannes, etc.), mais également les systèmes supports tels que les systèmes CVCA, etc.

À la fin de cette phase, toutes les fonctions de sûreté catégorisées et qui nécessitent un système d'I&C pour fonctionner sont allouées aux systèmes d'I&C appropriés, en tenant compte des différents niveaux de défense en profondeur. À l'issue de la définition de ces systèmes, ces derniers doivent être classés en fonction de leur importance pour la sûreté, selon un processus qui tient compte des facteurs indiqués dans l'exigence 22 de l'AIEA SSR 2/1 et reproduits ci-après:

- a) la ou les fonctions de sûreté destinées à être assurées par le système;
- b) les conséquences résultant du non-accomplissement d'une fonction de sûreté;
- c) la fréquence avec laquelle le système sera appelé à assurer une fonction de sûreté;
- d) le moment auquel, après un PIE, le système sera appelé à assurer une fonction de sûreté ou la durée pendant laquelle il sera appelé à l'assurer.

En application des facteurs (a) et (c) définis dans l'AIEA SSR 2/1 les systèmes d'I&C destinés à exécuter les fonctions identifiées, doivent d'abord être affectés à la classe de sûreté correspondant à la catégorie de sûreté des fonctions qu'ils réalisent.

Trois classes de sûreté sont proposées et corrélées avec les trois catégories comme présentées dans le Tableau 1.

Tableau 1 – Corrélation entre classes de systèmes et catégories de fonctions

Catégories des fonctions importantes pour la sûreté			Classes correspondantes des systèmes importants pour la sûreté
A	(B) ^a	(C) ^a	1
	B	(C) ^a	2
		C	3
^a Une classe de sûreté supérieure à celle exigée par la catégorie est généralement adoptée pour les fonctions auxiliaires telles que l'autosurveillance, puisque cela évite la nécessité d'un isolement fonctionnel.			

Le classement initial doit être ensuite modifié, si nécessaire, pour tenir compte des facteurs (b) et (d) définis dans l'AIEA SSR 2/1. Pour le facteur (d), la prise en considération du délai entre l'occurrence du PIE et la sollicitation de la fonction peut permettre d'assigner une classe inférieure aux structures, systèmes et composants (SSC), à condition que la fiabilité attendue puisse être démontrée. Une telle démonstration peut prendre en compte, par exemple, le temps de réparation ou d'entretien des SSC, ou la possibilité d'utiliser d'autres SSC dans les délais impartis pour exécuter la fonction de sûreté exigée.

Lorsque la prise en compte des effets des défaillances de cause commune montre que la fiabilité requise ne pourra pas être satisfaite par des systèmes redondants et conduit à mettre en œuvre une diversification par des systèmes indépendants (par exemple, pour respecter des critères probabilistes), alors l'affinement du classement peut également s'appliquer aux systèmes permettant de gérer les effets des défaillances de cause commune. Dans le cas de la prise en compte d'un système de Classe 2 dans l'analyse de sûreté pour compenser la défaillance hypothétique d'un système de Classe 1 qui assure des fonctions de Catégorie A, une justification de sûreté doit alors être établie et prouver que les exigences de conception

et de qualification appliquées au système de Classe 2 sont appropriées et que les objectifs de fiabilité pour le système de Classe 2 sont crédibles.

Pour un système d'I&C 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, dès lors 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 diversité.

Il convient de détailler suffisamment la granularité des fonctions d'I&C, catégorisées pour qu'une fonction d'I&C ne soit attribuée qu'à un seul système d'I&C.

Une SSC qui contribue aux performances de plusieurs fonctions de différentes catégories doit être affectée à la classe correspondant à la catégorie la plus élevée (c'est-à-dire celle correspondant aux règles de conception techniques les plus exigeantes).

La liste finalisée des systèmes, des allocations de fonctions et des classements doit être établie en appliquant ces considérations. Ce processus doit également prendre en compte d'autres considérations pertinentes telles que:

- le niveau de défense en profondeur;
- la corrélation entre classes de systèmes et catégories de fonctions (voir Tableau 1 ci-dessus);
- les exigences d'indépendance;
- l'allocation des fonctions destinées à secourir les fonctions de Catégorie A ou B à un système suffisamment séparé et diversifié.

6.4.2 Classement des systèmes d'alimentation électrique

L'IEC 63046 définit l'approche de classement des systèmes d'alimentation électrique. Cette approche repose sur la cohérence entre la classe de sûreté du système électrique et la classe de sûreté des systèmes importants pour la sûreté alimentés par le système électrique. Lorsqu'un système électrique alimente des utilisateurs ayant différentes classes de sûreté, il convient de classer ledit système électrique en cohérence avec la classe la plus élevée des utilisateurs de ce système. Un isolement approprié doit être assuré pour les alimentations des utilisateurs de classe de sûreté inférieure.

Il convient de classer le système électrique alimentant un système d'I&C en cohérence avec la classe de sûreté du système d'I&C. En cas de modification de la classe de sûreté du système d'I&C (lors de l'affinement du processus de classement), il convient de modifier en conséquence la classe de sûreté du système électrique qui supporte ce système d'I&C.

Lorsqu'un système d'I&C fait partie intégrante d'un système électrique (par exemple, les générateurs diesel de secours), il convient de classer le système d'I&C en cohérence avec la classe de sûreté du système électrique.

La Figure 3 ci-dessous résume la méthode de classement des systèmes d'alimentation électrique.