IEC/TR 61838

Edition 2.0 2009-12

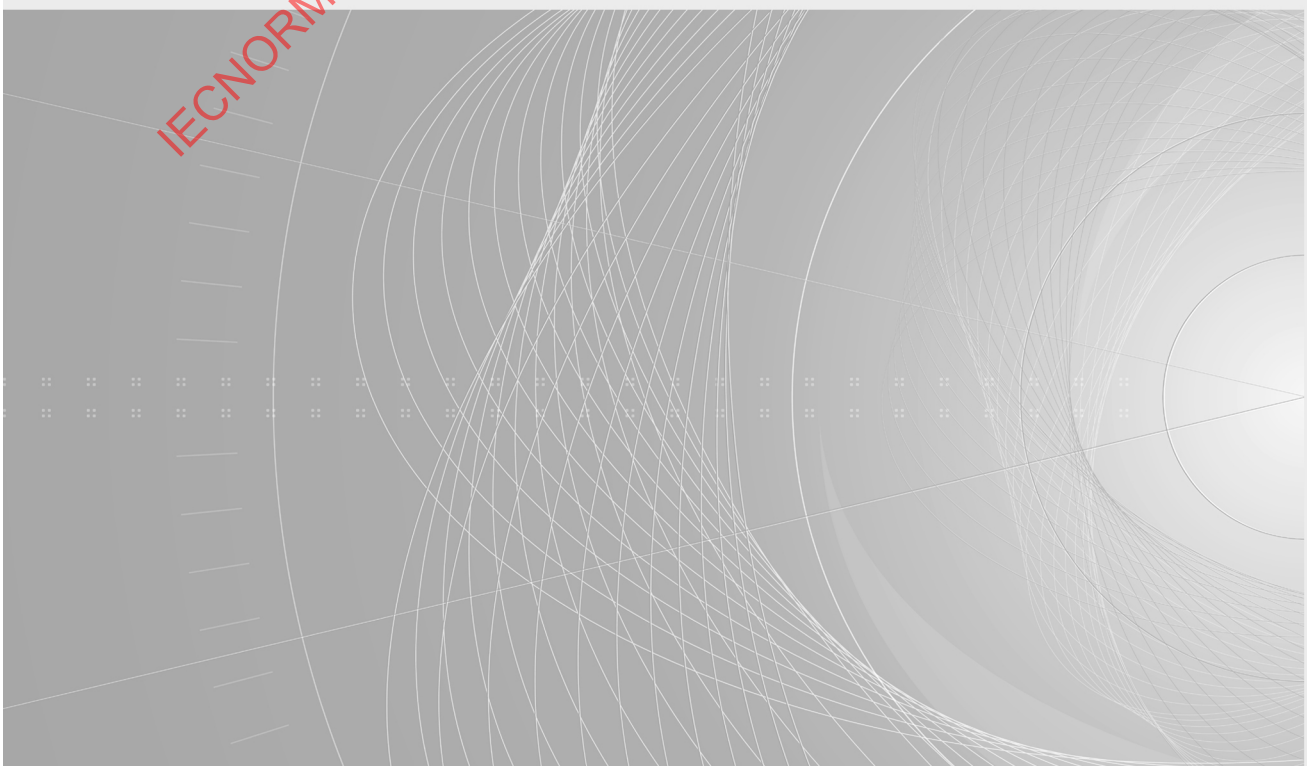
TECHNICAL REPORT

RAPPORT TECHNIQUE

colour inside

Nuclear power plants – Instrumentation and control important to safety – Use of probabilistic safety assessment for the classification of functions

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Utilisation des évaluations probabilistes de sûreté pour le classement des fonctions



IEC/TR 61838:2009

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

About the IEC

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

About IEC publications

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

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

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

A propos des publications CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TR 61838

Edition 2.0 2009-12

TECHNICAL REPORT

RAPPORT TECHNIQUE

colour inside

Nuclear power plants – Instrumentation and control important to safety – Use of probabilistic safety assessment for the classification of functions

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Utilisation des évaluations probabilistes de sûreté pour le classement des fonctions

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 27.120.20

ISBN 978-2-88910-575-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – USE OF PROBABILISTIC SAFETY ASSESSMENT FOR THE CLASSIFICATION OF FUNCTIONS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC 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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 61838, which is a technical report, has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 2001.

The main technical changes with regard to the previous edition are as follows:

– to update references taking into account standards published since issue 1;
– to update the terminology;

– to take into account the progress done concerning the use of PSA for classification since issue 1.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
45A/766/DTR	45A/779A/RVC

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

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

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

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

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 Technical Report

IEC 61226 "Nuclear power plants – Instrumentation and control systems important for safety – Classification" was published in 1993, and revised in 2005 and 2009. The need to classify instrumentation and control functions on nuclear power plants now originates from an International Atomic Energy Agency (IAEA) requirement stated in Standard NS-R-1, clause 5.2. IEC 61226 emphasizes that it is the **functions**, which must be classified early in the design phase so that the degree of importance to safety of each function is determined. At the design stage, I&C functions are allocated to specific instrumentation and control systems each of which will normally comprise of several types of equipment. These systems and equipment are usually assigned to classes according to the safety significance of the functions assigned to each system (as per IEC 61513), but it is the functions which determine the fundamental categorization. IAEA guide NS-G-1.14 (currently in draft form) extends the concept of categorising functions to assigning the resultant category to all structures, systems and components (SCCs) that implement the function.

In order to cater for this association of systems and equipment with functions, the concept of an FSE was introduced in IEC 61226. An FSE is defined as:

> Functions, and the associated systems and equipment. Functions are carried out for a purpose or to achieve a goal. The associated systems and equipment are the collection of components and the components themselves that are employed to achieve the functions.

IEC 61226 provides a categorization method for FSE based upon qualitative, role-based criteria. Many of the criteria are well understood in the nuclear industry since they recognize that the single and most important nuclear safety function is to prevent accidents and mitigate against fission product releases. Consequently, the classification of FSE in IEC 61226, Edition 3 is a deterministic process and takes little account of quantitative risk assessment techniques.

During the last ten years, risk assessment methods, particularly applied to nuclear power plants, have matured although their use in NPP design (and licensing) varies greatly throughout the world. In some countries, a probabilistic risk assessment is seen as an essential element of the design process and of the final safety case; this is not the case in other countries.

The release in 2000 of IAEA NS-R-1 and in 2002 of NS-G-1.3 has highlighted the requirement to factor engineering judgement and probabilistic criteria into the process of categorisation. For several years, how a risk based classification scheme could be incorporated into IEC 61226 to meet this requirement has been the topic of discussion. As indicated above, there are significant differences in the use of risk assessments throughout the world, which leads to several questions when drafting an International Standard, namely:

1) Should a risk-based classification scheme be acceptable in place of the deterministic approach? If so, what are the requirements (especially regarding the standard of modelling and the validity of data) that must be applied?
2) If a risk-based classification leads to different classifications of FSE compared to the deterministic approach, which should take precedence?
3) Should the two approaches be used together in order to gain the maximum benefit? The deterministic approach is based on sound, well-proven nuclear safety principles, which people are comfortable with. Risk assessment results could lead to the classification of specific I&C functions being upgraded or downgraded (because of plant-specific design features). Should this upgrading or downgrading be limited in some way?
4) Should the use of risk assessments be mandated when considering the effectiveness of plant and I&C modifications throughout the plant lifetime? Similarly, should requirements be included for the use of risk assessments in making decisions about preventive maintenance?

5) How should classification be applied to novel plant designs which do not fit the current role-based classification scheme in IEC 61226, and how could classification based on power plants be extended to other nuclear power plants, nuclear facilities such as low power reactors used for research or isotope production, facilities handling high-level radio-isotopes, nuclear fuel fabrication, and nuclear fuel reprocessing facilities?

This technical report now has been revised in the light of the publication of IAEA NS-R-1 and NS-G-1.3, which require that classification be based upon deterministic methods complemented where appropriate by engineering judgement and risk-related considerations. Both the precise wording of NS-R-1 clause 5.2 and the list of criteria to consider (expanded in clause 2.38 of NS-G-1.3) emphasize the importance of the latter criteria. It is eminently clear that it is a requirement to consider engineering judgment and the cited risk-related criteria, except where it can be shown to not be appropriate. This conclusion is also supported by clause 3.4 of NS-R-1, which requires that design management "*shall take account of the results of the deterministic and complementary probabilistic safety analyses*", and now further emphasized by IAEA NS-G-1.14 (draft currently in the review stage) which advocates a balanced approach between probabilistic and deterministic methods.

This requirement to include risk-related consideration in the process of classification (unless shown to be inappropriate) is of such paramount importance to the adoption of a method of classification that the relevant clauses are reproduced below from NS-G-1.3 (note that clause 2.37 of NS-G-1.3 is a verbatim citation of clause 5.2 of NS-R-1[1]):

> 2.37. In particular, the Requirements for Design require (Ref. [NS-R-1], para. 5.2) that the method for classifying the safety significance of a structure, system or component be based primarily on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgement, and that account be taken of factors such as:
>
> - The safety function(s) to be performed;
> - The consequences of the I&C system's failure;
> - The probability that the I&C system will be called upon to perform a safety function; and
> - Following a PIE, the time at which or the period for which the I&C system will be called upon to operate.
>
> 2.38. In the method of classification, in addition to considering the aforementioned factors, as required in [NS-R-1], the following factors should also be taken into account in determining the class of the I&C system. The criteria, as set out in the following factors for illustrative purposes, should be chosen so as to provide a quantitative and/or qualitative indication of the relative importance to safety of the I&C system being classified:
>
> - The probability of PIEs and the potential severity of their consequences if the I&C system provided fails (e.g. high, medium or low probability, with high, medium or low consequences (e.g. radiological consequences));
> - The potential of the I&C system itself to cause a PIE (i.e. the I&C system's failure modes), the provisions made in the safety systems or in other I&C systems covered by this Safety Guide for such a PIE (i.e. provisions for detection of I&C system failure), and the combination of probability and consequences of such a PIE (i.e. frequency of failure and radiological consequences);
> - The length of time for which the I&C system is required once the safety function is initiated (e.g. up to 12 hours, beyond 12 hours);
> - The timeliness and reliability with which alternative actions can be

1 Reproduced with the permission of IAEA.

taken (e.g. immediate/low reliability, beyond 30 minutes/high reliability); and

- The timeliness (e.g. up to 12 hours, beyond 12 hours) and reliability with which any failure in the I&C system can be detected and remedied.

The goal of this report is then to help the community reach some consensus on a blended approach to classification. Such an approach could possibly incorporate a framework where the fundamental safety functions of last resort would be identified largely deterministically (and presumably fall into Category A) while the primary continuously-operating functions that maintain the plant at normal full-power would likely fall into Category C. Subsequently, all plant functions, particularly those falling into Category B, would be classified using a blend of methodologies that are appropriate to the plant design concept and the national licensing approach in the member nation.

It was recognized by 2001 that an amendment to IEC 61226 would be very difficult. In order to advance the debate, however, the first edition of this Technical Report presented a number of different approaches to the application of risk-based and time-based criteria in the classification of FSE. Since then, the increased use of PSA techniques and in particular the release of IAEA NS-R-1 and now the current work on NS-G-1.14 indicate the need to revise this Technical Report. Accordingly, this report examines both the issue of balancing the qualitative and quantitative risk-based approaches, and the details of possible quantitative methodologies.

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

IEC 61838 as a technical report is a fourth level IEC SC 45A document.

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

c) Recommendations and limitations regarding the application of the Technical Report

It is important to note that a technical report is entirely informative in nature. It gathers data collected from different origins and it establishes no requirements.

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

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

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

A fourth level extending the IEC SC 45A standard series, corresponds to the Technical Reports which are not normative.

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

IEC 61513 refers to ISO as well as to IAEA 50-C-QA (now replaced by IAEA GS-R-3) for topics related to quality assurance (QA).

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

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – USE OF PROBABILISTIC SAFETY ASSESSMENT FOR THE CLASSIFICATION OF FUNCTIONS

1 Scope

This Technical Report provides a survey of some of the methods by which probabilistic risk assessment results can be used to establish "risk-based" classification criteria, so as to allow FSEs to be placed within the four categories established within IEC 61226.

The application of risk-based classification (categorisation) techniques, in conjunction with the role-based deterministic approach to classification given in IEC 61226 Edition 3, will continue to be decided by the utility and/or regulator within the National Regulatory frameworks. However, these approaches would be expected to take due account of internationally agreed approaches such as expressed in IAEA standards and guides. However, those are essentially high level and for instrumentation and control systems IAEA have left it to IEC TC45 SC 45A to determine the detailed approaches available and to express them in standards. There is an increasing level of consensus on the topic of classification; however there is some way to go yet. Edition 1 of this technical report published in 2001 assisted in the revision of IEC 61226 published in 2005. The scope of this revision to IEC 61838 is to stimulate debate on this subject and encourage the convergence of views so that further revision to IEC 61226 can be agreed to bring it into line with the latest IAEA guidance, i.e. to explicitly include consideration of aspects such as risk and time lines of response.

The safety principles and the usefulness of a risk-based approach to classification are discussed and a description of four different approaches is presented. Two of these approaches are applied to a practical example and the results compared as a means to evaluate the robustness and generality of the risk-based approach.

In other respects, references are given in this report to IEC and IAEA documents, which relate directly to the topic.

This report also discusses the limitations associated with the use of either a risk-based approach or a role-based approach on its own, either of which would be inconsistent with the guidance soon to be released in IAEA NS-G-1.14.

2 Normative references

The following documents are referenced in 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 60709:2004, *Nuclear power plants – Instrumentation and control systems important to safety – Separation*

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

IEC 61226:2009, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

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

IEC 62138:2004, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IAEA NS-R-1:2000, *Requirements: Safety of Nuclear Power Plants Design, Safety Requirements*

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

IAEA NS-G-1.14, *Safety Guide: Safety Classification of Structures, Systems and Components Important to Safety Important to Safety in Nuclear Power Plants (draft)*

INSAG-10: 1996, *Defense in depth in nuclear safety*

INSAG-12, *Basic safety principles for nuclear power plants 75-INSAG-3, Rev. 1*

IAEA Safety glossary, 2007 edition

3 Terms and definitions

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

3.1
diversity
presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure

[IAEA Safety Glossary, 2007 edition]

3.2
equipment
one or more parts of a system. An item of equipment is a single definable (and usually removable) element or part of a system

[IEC 61513]

3.3
function
specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it

[IEC 61226]

3.4
functionality
attribute of a function which defines the operations which transfer input information into output information

[IEC 61513]

3.5
I&C FSE: functions, and the associated systems and equipment
functions are carried out for a purpose or to achieve a goal. The associated systems and equipment are the collection of components and the components themselves that are employed to achieve the functions

[IEC 61513]

3.6
item important to safety
item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public.

Items important to safety include:

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

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

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

[IAEA Safety Glossary, 2007 edition]

NOTE 1 In this technical report the items considered will be mainly I&C FSE.

NOTE 2 The above definition of "important to safety" refers to both systems or functions that are designed explicitly for their safety function (items b and c) and the systems whose failure could require other functions to act (item a). This is in contrast with the definition in IEC 61508 where "safety related" applies only to systems and functions designed explicitly to provide a safety function (items b and c).

3.7
nuclear safety
achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards

[IAEA Safety Glossary, 2007 edition]

3.8
performance
effectiveness with which an intended function is carried out (e.g. time response, accuracy, sensitivity to parameter changes)

[IEC 61226]

3.9
postulated initiating event (PIE)
event identified during design as capable of leading to anticipated operational occurrences or accident conditions

[IAEA Safety Glossary, 2007 edition]

3.10
redundancy
provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other

[IAEA Safety Glossary, 2007 edition]

3.11
risk-based categorisation
the approach to categorisation based on the significance with regard to safety of the function being categorized (i.e. degree of risk eliminated by the function).

NOTE This approach requires analyzing both the consequence eliminated or reduced by the function and the reliability that the plant safety analysis requires for this function. The term "probabilistic categorisation" is often imprecisely used for this approach. One limitation of this approach is that it imposes an analysis burden before one may complete the categorisation.

3.12
role-based categorisation
the deterministic approach to categorisation based purely on the function (i.e. role) performed by a function being categorized. This usually involves selecting the most appropriate role from a list of roles associated with each category, such as in clause 5.4 of IEC 61226, Edition 3. The list of roles associated with each category is deterministically selected, based on non-quantitative criteria related to the safety significance of the function.

NOTE One limitation of this approach is that it does not provide a systematic approach for functions that do not exactly fit the list provided.

3.13
safety function
specific purpose that must be accomplished for safety

[IAEA Safety Glossary, 2007 edition]

3.14
safety system
system important to safety, provided to ensure the safe shutdown of the reactor and the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents

[IAEA Safety Glossary, 2007 edition]

3.15
significant sequence
credible series or set of events that would result in unacceptable consequences such as:

- unacceptable radioactive release at the site or to the wider environment. This might be either a massive, uncontrolled release at a frequency that is outside the NPP's design basis, or releases at a frequency that is within the design basis but exceed specified magnitude and/or frequency limits;
- unacceptable fuel damage. This might be damage to the fuel clad that leads to an unacceptable increase in the activity of the primary coolant, or structural damage to the fuel that impairs the ability to cool it

3.16
single failure criterion (SFC)
criterion (or requirement) applied to a system such that it must be capable of performing its safety task in the presence of any single failure

[IAEA Safety Glossary, 2007 edition]

3.17
system
set of components which interact according to a design, where an element of a system can be another system, called a subsystem

[IEC 61513]

3.18
unavailability
fraction of time that a system or component is not capable of supporting its function

NOTE Unavailability may occur as a result of the item being repaired or a malfunction being detected, or the item being tested, or it may occur as a result of undetected malfunctions.

4 Abbreviations

ALARP	As Low as Reasonably Practicable
CCF	Common Cause Failure
DBC	Design Basis Conditions
DEC	Design Extension Conditions
EQ	Environmental Qualification
FSE	Function(s) and the associated systems and equipment that implement it (them)
FMEA	Failure Modes And Effects Analysis
I&C	Instrumentation And Control
IAEA	International Atomic Energy Agency
NPP	Nuclear Power Plant
PIE	Postulated Initiating Event
PSA	Probabilistic Safety Assessment
QA	Quality Assurance
SFC	Single Failure Criterion
SQ	Seismic Qualification
V&V	Verification and Validation
/ry	per reactor year
/y	per year

5 Limitations regarding the use of individual approaches alone

5.1 General

Clause 5.2 of IAEA NS-R-1 is clear in its requirement to use a balance of deterministic methods and risk-based (or probabilistic) methods and the draft guide NS-G-1.14 further emphasizes the importance of a balanced methodology. To explore this concept, this clause considers the limitations of trying to approach the question of categorisation on the basis of either a purely deterministic role-based or a purely risk-based approach

5.2 Limitations regarding the use of a PSA-related approach alone

The use of probabilistic safety assessment technology enables information to be obtained which can lead to improved risk-informed decisions and to more cost effective and efficient use of resources to improve the safety of NPPs. Reaching consensus within an international standard on the use of PSA techniques in the design and in-service support of NPPs has been limited by several factors, including:

- The development and use of probabilistic safety assessment techniques continues to evolve within member nations and its level of acceptance and the extent of its application are not consistent.
- The application of probabilistic safety assessment techniques as a classification tool in the design of a NPP requires a PSA to be carried out early in the design phase. The performance of such a detailed assessment at this point in time is not common practice, partly due to the changing plant design and partly due to the lack of quantitative data at this first stage.

Indeed, even when the PSA is applied to an existing design, there are often technical limitations in the analysis that prevent the design review being performed exclusively using probabilistic data as its basis. This is because the PSA might not be sufficiently accurate and exhaustive. These limitations include:

- the difficulties related to modelling and quantifying common cause failures, software errors, and human errors,
- the lack or the unavailability of plant specific information,
- the scope limitations of the level of the PSA performed,
- the exclusion of some potential initiating events (e.g. fire, flood, earthquake),
- the completeness of the uncertainty analysis.

In light of these factors, care shall be taken in making design decisions, such as whether to add a new safety-related function to the plant design and in defining the reliability requirements for safety and safety-related functions. These factors are slightly less critical to the process of categorisation because the category should be sensitive only to the order of magnitude of the required reliability, not its precise value. This is because the category does not set functional, qualification (seismic or environmental) or reliability requirements, rather it determines only the rigour of the design process and other life cycle stages, the purpose of which is to provide the appropriate level of assurance that the specific functional and other requirements will be met. Nevertheless appropriate conservatism should be applied.

For these reasons, (and of course the requirement in IAEA NS-R-1 to also use deterministic methods), the use of PSA, as the sole basis for the development of the design and classification of its I&C safety functions cannot be achieved. Despite these limitations, PSA is clearly valuable when used in conjunction with the qualitative approach based upon the defence-in-depth principle that has been firmly established in the safety design basis of NPPs (see IAEA NS-R-1, clauses 4.1 and 4.2). When PSA is used during the design phase for future NPPs as well as during the review of existing designs, it should be used along with and as a complement to the qualitative method.

5.3 Limitations regarding the use of the deterministic role-based approach alone

The use of a deterministic role-based classification scheme carries with it the built-in limitation of any menu: it can cover only what safety functions pertain to designs within the knowledge base of those preparing the menu list, and is unlikely to encompass all features of novel plant designs or even of existing plants. This is clearly identified in clause 2.4 of draft NS-G-1.14. For example, consider the factors of time, consequences, and risk reduction:

- A safety function may fit Category B according to the criteria listed in IEC 61226, 5.4.2, but if under some circumstances it shall either act, or be manually supported in case of its failure within a very short time frame, then operator action cannot be credited and the function should be upgraded to Category A.
- For a passively-safe reactor, the safety shutdown system, which would be Category A per IEC 61226, 5.4.1, might involve negligible consequences of failure, which is certainly at odds with the current definition of Category A.
- In plant designs where the required reliability (to meet PSA targets) affects the category, some functions which would be Category C per criteria e) or f) in 5.4.3 of IEC 61226 (Edition 3) may require much higher reliabilities than is consistent with Category C. The Stepback function (criterion e) that is implemented in a number of designs is an example (see the worked example in 9.1).
- The roles that can be (or have been) assigned in a role-based scheme and based on experience with existing designs cannot be assured to be appropriate for a new reactor design. This has been identified in the draft of IAEA NS-G-1.14 (in clause 2.4)

This consideration complies with the list of considerations that clause 5.2 of NS-R-1 requires designers to consider. This list, particularly as amplified by clause 2.38 of IAEA NS-G-1.3, is simply too long, and requires plant-specific details to fit any practical role-based schema: engineering judgement and a fault-tree like approach are needed to complete the classification.

6 Open issues regarding categorisation

6.1 General

Unanimity among the international community in several areas is not yet possible, although considerable progress is being made. This clause is intended to highlight these areas of continuing debate, and to foster eventual convergence of views. This clause addresses the following questions:

a) Why Categorize: To determine requirements, or do requirements determine the category?

b) To what degree are risk or probabilistic methods already used implicitly?

c) How precise do PSA results need to be?

6.2 Why categorize: To determine requirements, or do requirements determine the category?

A review of the ways in which categorisation is performed in several member states reveals divergent philosophies about categorisation, causing one to pose the question:

> Does categorisation determine the requirements or do the requirements determine the category?

IAEA NS-R-1 requires the 'classification'[2] of structures, systems[2] and components, but the guidance as to why is open to interpretation. Clause 5.1 of this standard states:

> 5.1. 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.

This wording suggests that:

– the functional requirements and degree of risk elimination/reduction (i.e. safety significance) determine the category or classification, and then

– the category should determine the level of quality assurance and design assurance that would be required to ensure that the structure, system, or component would be designed to meet its functional requirements (including robustness in the presence of accident conditions). The higher the category, the higher shall be the assurance that the functional requirements are met.

It would be entirely consistent with the above to interpret the second sentence from NS-R-1 above to also mean that additional functional assurance requirements should be applied as appropriate to the category. (Functional assurance requirements are additional requirements that apply to the implementation of a function that reduce its susceptibility to systematic (design) failures and/or random hardware failures. Examples include redundancy, software self-checks, and use of a hardware watchdog in programmable systems.)

This seems to be where Clause 7 of IEC 61226 steps into the design process, although it does not distinguish basic functional requirements from functional assurance requirements. In Clause 7 of IEC 61226, the category is assumed selected and then the category serves to assign a required reliability and in some cases specific functional assurance requirements

[2] IEC 61226 and IEC 61513 clarify the use of "category" and "class" (and the respective verbs) and their proper application, respectively, to functions and systems. One categorizes functions, which are then implemented in systems which shall be of sufficient class for the functions they host. See particularly IEC 61513, 5.3.1.1.

such as power supply redundancy (category determines requirements). This does not matter in practice, provided that the category was first determined on the basis of the fundamental factors required by IAEA NS-R-1 (see clause 5.2):

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

b) the consequences of failure of the items to perform its function;

c) the probability that the items will be called upon to perform a safety function;

d) the time when, or the period throughout which, the items will be called upon to operate.

Here for example, the reliability required of a function may determine its category to be A, and this required reliability will also dictate redundancy and independence of its power supplies.

Undoubtedly, quality assurance influences reliability, just as required reliability clearly influences the quality assurance procedures applied in the design, operation, and maintenance of the function. Additionally, in practice, it is impractical to design a large number of functions and systems to a continuum of functional, functional assurance, and quality requirements, which is why the continuum is discretized into 3 categories. It is both practical and conducive to safety to standardize functional assurance requirements such as inter-channel and inter-category independence, redundancy, single-failure criterion, and other attributes on the basis of category. Indeed this is common practice and is seen in various standards.

Hence there is a large room for debate as to whether requirements determine the category or the category determines the requirements. Part of this debate revolves around the lack of clear distinction between functional and functional assurance requirements.

This suggests the following interpretation:

a) Basic functional requirements (i.e. those applied in the safety analysis) determine the category.

b) The category determines functional assurance requirements.

While the above is a widespread interpretation, it is not certain that it is unanimously accepted.

In the light of the above, the participants in the preparation of IEC 61838 discussed this interpretation and the reasons for performing categorisation, and ranked these reasons in (rough descending) order of importance, as given below. The first item in the list was unanimously agreed to, and thereafter there was a general agreement that there was little difference in their ranking.

- To provide the appropriate level of assurance that the requirements (functional, reliability, EQ, SQ) are met, based on the importance to safety of the functions. This implies the appropriate level of QA, V&V independence, and functional assurance requirements, etc.
- To preserve the original design properties over the life of the plant, and through design changes and maintenance, and eventual replacement by equipment of equal capability.
- To understand the importance to safety of the function and the selection of equipment of the function (this statement is also true in the reverse).
- To identify the equipment for which the operators and maintainers shall follow suitable procedures that are more detailed than for lower category systems.
- To allow planning for the long-term: to provide guidance for maintenance so that the original design properties are preserved.
- To maximize cost-effectiveness (so that money and effort can be spent on the most safety-important functions).
- To establish requirements for appropriate record keeping.
- To facilitate designing the layers of defence.

- To meet the legal requirement to demonstrate ALARP (in the U.K.).

6.3 To what degree are risk-based and probabilistic methods already used implicitly?

While categorisation is performed on a risk-based or probabilistic basis in a few member states (notably Canada and the United Kingdom), categorisation is performed nominally deterministically, following Clause 5 of IEC 61226 in most member states.

Nevertheless, Clause 5 of IEC 61226 includes some explicitly probabilistic considerations, and even the claimed deterministically based methods involve probabilistic considerations at some point, as illustrated by the following 3 items.

IEC 61226, 5.4.2 – Category B

a) Functions to reduce considerably the frequency of a DBE as claimed in the safety analysis.

IEC 61226, 5.4.3 – Category C

b) Functions necessary to reach the safety probabilistic goals including those to reduce the expected frequency of a DBE.

c) Functions to reduce the demands on a category A function, as claimed in the safety analysis.

Probabilistic considerations in deterministic methods

Even in member states where a purely deterministic methodology is claimed, there are elements of probability and risk factored in at some stage of design confirmation. For example, in one such methodology, if a PSA shows some event sequence to be an unacceptable contributor to the overall risk of core damage, a new function may be added to the plant. In such cases, this new function can be category C if the event sequence involves 2 or more failures, but will likely be category A if only one failure is already recognized. This implicitly recognizes that the frequency at which the new function may be demanded to function affects its category.

6.4 How precise do PSA results need to be?

One of the concerns cited about the use of a risk-based approach is the sensitivity of PSA results to errors and uncertainties in failure rate data. This section provides some of the insights offered by delegates from member states where PSA results are used in categorisation.

Note that in determining the category of a new function probabilistically, based on PSA results, by definition the new function is left out of the event sequence in order to reveal its required reliability.

- The first consideration is that even in a dominantly risk-based methodology, the reliability spectrum is in effect discretized in powers of 10 from one category to the next. Thus precise results from the PSA are neither trusted nor needed.
- Secondly, sensitivity studies are usually conducted for results near the boundaries between categories. If these studies reflect a high degree of sensitivity in the PSA results, then the design of the existing systems is re-examined since they should be designed to be relatively insensitive to failure rates of components.
- Thirdly, a basic conservatism is applied whereby none of the existing systems accounted for in the PSA is credited with unrestricted values. For example, a fault tree analysis of a reactor protection system (RPS) might show that for the event sequence being studied, the P_{FD} of the RPS is ~10^{-4}. Despite this, the categorisation methodology usually limits the credit for any one system or function to 10^{-3} of category A functions (and lower for other categories). This has two conservative effects:

- it generally reinforces Defence-in-Depth, and
- it increases the required category of the new function.

7 Current practices in some member states

7.1 General

This clause provides a brief summary of the current degree of application of risk-based or probabilistically influenced categorisation in some member countries. This clause presents the points considered significant in the context of the international discussion as well as overviews contributed by several national committees after the meetings.

7.2 Brief summaries

This subclause summarises the main points made during the discussions about the current level of risk-related categorisation. These points serve to update all member committees on current practices in many member states (in some cases, flagged by *, national committees later submitted more extensive summaries of the practices in their states, and these are reported in 7.3).

Canada * PSAs are done for a large number of events (~ 50), and are an integral part of licensing, since the regulator requires both deterministic and probabilistic analyses. Categorisation is performed primarily on the basis of a function's required reliability (either λ_D for process (continuously running) systems or P_{FD} for safety (poised) systems. In some cases, where a function is also credited in the deterministic analysis, the category may be set accordingly (higher than the probabilistically-based category).

France * PSAs are done for a large number of possible events. To address sequences leading to core damage at frequencies exceeding 10^{-7}/y, new functions may be added to the plant, or an existing system may be assigned a new function. Where these cases involve two independent failures, the new function can be Category C. If only one failure is involved, the new function might have to be category A.

PSAs are updated every 10 years.

Germany * According to German regulations, the reactor protection system shall be designed such that it is not the determining factor in the unavailability of the safety system. The common interpretation of this requirement is that the I&C contribution to the overall failure rate of a safety-related system is limited to 10 % of that due to mechanical components.

PSAs are updated every 10 years.

Japan	Safety classification is based on the deterministic approach. However, PSAs are done for a large number of events and the utilization of risk information in addition to the traditional deterministic approach is currently a developing issue. Considering there is as yet little experience in Japan in this area, it is expected it will take some years to change directly the safety classification guide relating to design using risks. The utilization of risk information in Japan is going to start with the operation / inspection area and seismic aspects. The latest situation and detailed information of introduction of Risk Informed Regulation (RIR) in Japan has been added to the website of Japan's Nuclear Safety Commission (NSC). （http://www.nsc.go.jp）
Korea	PSAs are performed for all operating plants as well as plants under construction. PSAs covered large number of possible events. A simple, clear classification into 4 categories is used. Up to now, PSAs have not affected classification, but there are several cases of PSA results being used to extend the allowable outage time and the surveillance test interval of safety system.
Sweden	PSAs are used extensively on all plants. They are not directly used for categorisation, but to identify systems requiring special consideration. They are an everyday tool at Ringals. The regulator requires both deterministic and probabilistic reports. Software is seen as difficult to model in PSAs.
Switzerland	With the new regulatory guideline A06 (PSA application) that is in force since June 2008, PSA is systematically introduced into the reactor oversight (concerning the assessment of the safety, plant modifications - including technical specifications - and event analysis) as an additional element in decision making. Furthermore, the guideline A06 describes the identification of components, which are important from the PSA point of view. A modification of these components requires approval from the regulatory body.
United Kingdom *	PSAs include models of dangerous failure rate (λ_D) for control systems and P_{FD} for safety systems. The Level 3 PSAs usually demonstrate that I&C components are not dominant contributors.

7.3 More detailed explanations

Several national committees contributed descriptions of current national practice regarding the application of risk-based tools in their states. These are presented below (in alphabetical order):

- Canada
- France
- Germany
- Korea
- United Kingdom

A concise summary is provided for the longer descriptions.

Canada

Licensing in Canada is based on meeting both deterministic and probabilistic requirements. Categorisation is primarily probabilistic, with some deterministic adjustments. Currently operating plants use the categorisation methodology explained in 8.4. Future plants (now under consideration) will use the NS-R-1 compliant methodology described in 8.5.

The deterministic licensing requirements are twofold: the so-called single accident case (in which all safety systems are postulated to work as per design) and the so-called dual-accident case (in which for each PIE, each safety system in turn is postulated to fail). It is recognized that the probability of the dual accident case is considerably lower than the single-failure case, and therefore larger releases are permitted.

Meeting the probabilistic targets is demonstrated by PSAs. A typical PSA consists of more than 50 cases, such as loss of plant control computers, loss of Class IV[3] power, various breaks in various places of various size, etc.

Both the deterministic and PSA methods are used in plant design review, and either may result in the addition of new mitigating systems.

Categorisation is performed using the risk-based methods as described in Clause 8. In certain cases, where new mitigating systems are added to a plant design, a new safety-related function may be categorised as Category B due to its role in the deterministic analysis even though its category as dictated by the risk-based method might be Category C.

France

Summary:

Safety of French nuclear facilities is based primarily on deterministic concepts and Defence in Depth, thus categorisation in the basic design is purely deterministic. The deterministic design is reviewed using PSAs. PSAs are performed during the original plant design, and revised periodically during plant life. If an accident sequence appears to contribute a core-melting probability greater than 10^{-7}/y, then either an existing function is upgraded in category, or a new function is added to the plant. Under some circumstances (described in 8.2.1.3) the category of this new function may be determined based on its required reliability, but otherwise categorisation is deterministically based.

Full statement:

Safety of French nuclear facilities (NPPs, research reactors, facilities for enrichment, etc.) is based primarily on deterministic concepts and Defence in Depth (INSAG-10). The first step of categorisation is thus purely deterministic (8.2.1.1).

During design of new fission NPPs, probabilistic methods are applied as additional methods for identifying sequences with multiple contributors leading to severe accidents, whose contribution can be considered as non negligible in regard of severe accident probability. The overall probabilistic goal for the risk of core melting, taking into account hazards and uncertainties and all reactor states, is 10^{-5}/y, so sequences with probability greater than 10^{-7}/y are systematically taken into account in this list. To address these sequences, there are two possibilities: upgrading the category of an already existing function or adding a new safety function. In the latter case, the category of the function shall be selected to facilitate showing that the required reliability is achieved (8.2.1.3). The allocation of the function to a system depends obviously on other constraints, such as class of the system (regarding IEC 61513), independence requirements between systems and functions, keeping a low enough level of complexity for safety classified systems, etc.

3 In CANDU plants, Class IV power supplies the main coolant pumps.

For existing plants, a PSA is performed every ten years, to confirm that the plant still adequately meets the relevant safety requirements. During this phase, assumptions used for former PSAs have to be verified, in regard with experience gained on plants of the same type, and the validity of some of these could be reassessed. If the probability of a severe accident, taking into account hazards and uncertainties and all reactor states, is judged to be greater than 10^{-5}/y, design changes have to be decided to achieve this probabilistic goal.

In the case of introducing a new I&C equipment or group of equipment a probabilistic analysis is performed, complementary to verification of adequateness of the new solution with applicable design requirements, to confirm that the renovated part presents as good as or better properties than the replaced part. Reliability is seen as one of these properties. Validation of model and of assumptions used in this case is a key point of the demonstration of this property. The choice of the model has to be appropriate for with the complexity of the internal behaviour of the equipment or equipment group.

The following key points have to be underlined:

a) PSAs cannot be used to reduce the category of an existing function. They are used to identify weak points and to improve design (eventually by upgrading categorisation of functions or by adding complementary defence lines),

b) PSAs may, in certain cases, lead to re-examining maintenance intervals but they cannot be used without complementary justification to reduce the frequency of maintenance of qualified equipment, which have to resist special conditions (e.g. LOCA and post-LOCA severe accident conditions, etc.).

This method remains applicable for all nuclear facilities (research reactors, facilities for enrichment etc.). Nevertheless, it has to be adapted due to the fact that definition of severe accident and definition of acceptance level, in terms of impact, can change for these facilities. The probability goal of 10^{-5}/y for severe accidents can be changed with regard to impact of severe accidents for these applications (that could be very different from the core melt scenario taken into account for fission reactors).

Germany

According to German regulations, the licensing procedures for safety related decisions for NPPs in Germany are based on deterministic principles.

Probabilistic methods are applied as additional methods for supporting arguments, such as:

- A PSA is performed for each plant every ten years, to confirm that the plant still adequately meets the relevant safety requirements.
- In the case of introducing a new I&C technology a probabilistic analysis is performed to confirm the adequateness of the hardware design in comparison to a proven/former technology and to confirm the intended time interval for surveillance testing.

For the overall safety design, PSA methodology is applied for identifying weaknesses and to ensure a balanced safety concept by supporting licensing decisions that are based on the fulfilment of deterministic requirements.

Korea

PSA methods are not applied to any system classification or any functional categorization in nuclear I&C systems and/or functions.

PSA methods have been used to extend surveillance test intervals for reactor protection systems and engineered safety features actuation systems.

PSA methods are used to increase the allowable outage time for equipment in safety related systems.

United Kingdom

Summary:

The licensing procedures for safety related decisions for NPPs in the United Kingdom are based on risk principles. Risk shall be reduced to as low as reasonably practicable, as demonstrated by PSAs. IEC 61508 is an important standard used for guidance.

Full statement:

Within the UK the NPP operators (licensee) are required to reduce the risk to workers and members of the public so far as is reasonably practicable. A key element of the operators' response to this requirement is the demonstration that plant risks are as low as reasonably practicable. This demonstration includes a probabilistic safety assessment which includes figures for the contribution of the I&C systems to the plant risk targets. Typically the I&C systems provide a contribution to the initiating frequency of postulated events (i.e. through the probability of dangerous failures per year - PDFY) and/or risk reduction (i.e. probability of failure on demand - PFD). Hence probabilistic targets are assigned to the various I&C systems and a demonstration is required that appropriate standards have been met. An example of a standard which provides guidance on graded reliability targets/safety integrity levels (PFD/PDFY bands) that has been used in the UK is IEC 61508.

Functions are categorised on their importance to safety using appropriate standards such as IEC 61226. Note that IEC 61508 provides guidance on E/E/PES systems generically for class requirements (e.g. a Cat A function with a 10^{-4} PFD integrity requirement would be implemented using equipment (SIL capable) meeting the requirements of IEC 61508 SIL 4 consistent with a limit of 10^{-4} PFD placed on PES in nuclear applications in the UK); however, the preference would be to follow nuclear context standards such as IEC 61513 again with the limit placed on the performance claim that can be accepted).

8 A survey of risk-related techniques of categorisation

8.1 General

As discussed in Clause 5, quantitative risk assessment can be used to supplement the deterministic approach to classification of I&C functions. It is recognized that the development and use of risk assessment techniques (often termed probabilistic risk assessment or probabilistic safety assessment) are well advanced within some nations but have not reached a consistent level of acceptance across all member nations.

The information obtained from the use of PSA techniques can lead to the improvement of risk-effective decision making and a more focused and efficient use of resources particularly when deciding where limited financial resources can be best invested to yield the highest benefit. It is recommended that PSA be used on existing NPPs to determine those parts of the I&C system which should be modified or enhanced in order to improve the safety, design and operation of the plant and the I&C system. This is particularly appropriate to the safety reviews of existing plants.

The application of PSA-related methods and technology for categorisation should be used to complement the deterministic role-based approach in assigning the category of a function , especially where PSA methods are well-established and data is available; this is often true for determining upgrades but unfortunately not for new designs. Nevertheless, for the most effective results, PSA should be used during the design phase of the NPP and its I&C system to inform the classification of the required I&C functions.

Once the iterative blend of deterministic and PSA-based plant design has converged upon a feasible design (as described in IEC 61513, 5.1.2.2), the reliability requirements and the functional requirements for the safety-related functions are defined. Categorisation can then be finalized.

This report presents six different approaches to the use of PSA techniques. This list of approaches is not claimed to be comprehensive; indeed, there will be many ways in which probabilistic techniques can improve the decision making during the design of a NPP. This report is intended to stimulate debate on the best use of probabilistic techniques during the design phase of the instrumentation and control systems of a NPP.

The six approaches are as follows:

Approach 1, see 8.2 – Time and reactor states based approach

This has been introduced in the European Utility Requirements document to be used for future NPP to decide how I&C functions should be classified.

Approach 2, see 8.3 – Quantitative importance based approach

This approach is based on a full probabilistic technique to determine the contribution of each I&C function to plant fault sequences. In this way, the importance of each I&C function can be quantitatively calculated. The technique has been used in the USA as the basis for on-line plant risk monitoring.

Approach 3, see 8.4 – Consequence – mitigation based approach

This approach has been used in Canada for the design of existing CANDU NPPs. Note that a different approach will be used for the new build projects in Canada.

Approach 4, see 8.5 – Combined deterministic-probabilistic approach based on NS-R-1

This approach is now being used in Canada for the design of new CANDU NPPs. It defines reactor states as per NS-R-1 by assigning acceptable consequence and frequency for each state, then uses an approach based closely on the existing IEC 61226 methodology.

Approach 5, see 8.6 – Application of risk methodologies in U.S.A. nuclear regulation

This approach describes the trial applications of recently released United States Nuclear Regulatory Commission Regulatory Guide 1.201 “Guidelines for Categorizing Structures, Systems, and Components (SSC) in Nuclear Power Plants According to Their Safety Significance.” In the classification method endorsed by this Regulatory Guide, the safety significance of SSCs is determined using an integrated decision-making process, which incorporates both risk and traditional engineering insights.

Approach 6, see Annex B – Defence in depth based approach

This approach was described in 6.5 in Edition 1, and has been retained in Annex B because it is referenced for comparative purposes.

This approach is aimed at the use of probabilistic techniques to modify I&C classifications that have been determined by the accepted qualitative method. It considers whether the probabilistic techniques should not be permitted to change the classifications by more than one level in order to minimize the risk of over reliance on probabilistic data which may be based on generic component reliability data.

The approach has not yet been applied to a classification of functions of NPPs.

8.2 Approach 1: Time and reactor states based approach

8.2.1 Categorisation of FSE during the design phase

8.2.1.1 Step one – Deterministic approach

Safety of French nuclear facilities (NPPs, research reactors, facilities for enrichment, etc.) is based primarily on deterministic concepts and Defence in Depth (INSAG-10).

The design provisions in French PWR NPPs are justified by a limited number of conventional operating conditions (initiating events of incident and accident sequences are used to define the capabilities of buildings, systems and equipment needed for safety functions) arising from simple initiators and by the application of deterministic rules and criteria that include margins and conservatisms. The results of these studies shall respect the criteria aimed at limiting the consequences of the evaluated events.

The operating situations are classified into 4 sets (Plant Condition Categories - PCCs) based on frequency ranges and consequences[4]. The occurrence of an event in any such set is related to a maximum allowed level of releases or radiation exposure. Consequences exceeding these levels are considered unacceptable, and prevention and/or mitigation functions shall be added. These functions are categorised as per IEC 61226.

The consequences of failure of I&C equipment shall be covered by these cases. In effect, failures of I&C equipment shall be limited by design so that consequential failures cannot lead to consequences more serious than allowed for the 4th (and most serious) set (PCC-4). Failures of I&C equipment belonging to non-classified or class 3 systems is limited by design so that consequential failures cannot lead to consequences more serious than allowed for the 2nd set (PCC-2).

The consequences of an external or internal hazard are analysed under the assumption of the most penalizing combination of failure of all equipment not designed for the initiating event and by demonstrating that all of the equipment qualified for the event together with the equipment which is not affected by the event by virtue of separation features designed for such events (fire, flood) are sufficient to prevent unacceptable consequences.

This first step provides the basis for categorizing functions according to IEC 61226 Ed. 3 as follows:

– Category A: 5.4.1
– Category B: 5.4.2- items a), b), c), e)
– Category C: 5.4.3- items b), c), f), j), k), l).

The categorisation is based on the distinction between the non-hazardous stable state and the final "safe state" according to the definitions given in IEC 61226.

Category A corresponds to short-term actions that prevent unacceptable consequences and lead the plant to the non-hazardous stable state. Category B corresponds to functions leading to reaching the assured shutdown state where the time frame of the processes is longer and any failures can be compensated by independent complementary measures so that the non-hazardous stable state is maintained.

From the perspective of safety, the non-hazardous stable state shall be maintained indefinitely. Nevertheless, it is reasonable to accept some relaxation of requirements for the long-term rejection of decay heat in PWRs. This suggests a relaxation of requirements for maintaining guaranteed shutdown after 24 h and the acceptance of non-classified functions

[4] The PCCs are numbered PCC-1 to PCC-4, with PCC-4 having the lowest frequencey and the highest consequences.

after 72 h on the assumption that there exist complementary means of assuring these functions within delays that preclude unacceptable consequences.

Table 1 illustrates these allowances:

Table 1 – Classification of I&C FSE

	I&C FSE to be used in the safety analysis			
State of reactor	**Initiating event**	**Non-hazardous stable state**	**Safe shutdown state**	
Time scale		24 h		72 h
DBC	Category A	Category B	Category C	Non classified
DEC	Category C			Non classified
Internal hazards	Category C			Non classified

The independence required (as described above) between Category C functions (as defined by IEC 61226), participating in successive defence-in-depth levels, is achieved by allocating them to independent systems (as defined by IEC 61513). The following points have to be carefully considered through the design process of I&C architecture:

- The requirement for independence between successive lines of defence for any given scenario.
- The requirement for independence between levels of defence in depth. Table 2 relates the criteria given in IEC 61226, 5.4.3 and levels of defence in depth:

Table 2 – Correspondence between IEC 61226 and INSAG-10

Category C criteria (IEC 61226, Ed. 3, 5.4.3)	**Corresponding level of defence in depth (INSAG-10)**
Criteria a/, c/, f/	First level of defence in depth
Criteria b/, g/, h/	Second level of defence in depth
Criteria, d/ e/	Third level of defence in depth
Criteria i/, j/, g/	Fourth level of defence in depth

- The necessity for ensuring emergency power supply and the requirements of electrical separation between important for safety, safety-related and non-classified systems (see IEC 60709 requirements on this subject).

8.2.1.2 Step two: Level 1 PSA and determination of individual sequences of significant contribution to core damage frequency

The categorisation process is completed using PSAs. For that purpose, the goal of PSAs is to show that the intended probabilistic target for serious accidents, that is accidents whose consequences can exceed the limits assumed in plant design, is reached.

The probabilistic target is currently set for each reactor type according to accident consequences. For new French PWRs the probabilistic target for individual sequences leading to core damage is generally set at a frequency below 10^{-7}/y. The overall probabilistic goal for the core damage frequency, taking into account hazards and uncertainties and all reactor states, is below 10^{-5}/ry (INSAG-12). General rules for French PSAs are given in the basic safety regulation “Development and Utilization of PSAs” adopted in 2002 by the French Safety Authority[5].

5 This document is available on the Autorité de sureté nucléaire (ASN) website (www.asn.fr).

A Level 1 PSA aims at determining the multiple failure scenarios with significant contributions to the core damage frequency. These scenarios include at least two independent causal events (initiators). On the other hand, consequences arising from a common initiator are treated deterministically (using the approach described above in Step One) except where the maximum frequency of the initiator is demonstrably negligible in terms of the 10^{-7}/y objective, below which events are excluded. In practice, every initiator associated with a control failure is treated deterministically.

Examples of complex sequences currently part of the reference Level 1 PSA are:

- ATWS (Anticipated Transient Without SCRAM);
- total loss of steam generator feedwater;
- small break loss of coolant accident and loss of medium head safety injection;
- small break loss of coolant accident and loss of low head safety injection;
- station black out;
- total loss of the cooling chain.

8.2.1.3 Selecting the category of functions required by the PSA

In some areas, the PSA may indicate that the probabilistic target is not reached. To address each family of multiple failure scenarios, identified and considered significant relative to the 10^{-7}/ry objective, there are two possible cases:

– Either an un-classified function exists which can prevent the scenario and reduce its consequences to acceptable levels (case 1), or

– There is no such function (case 2).

In the first case, the function is assigned to a safety class so that it may be credited in the PSA. If the existing function is of Category A or B, this classification is preserved.

In the second case, a new function of class A, B or C is added. This function is assigned to Category A if it provides functions described in 5.4.1 of IEC 61226.

In other cases, the reliability of the function required to adequately mitigate the scenarios shall be claimed. It should be demonstrated that spurious actuation of the function does not initiate a failure sequence that increases the risk of core damage.

Finally, it should be ensured that the allocation of the function to a system (per IEC 61513) makes sure that failure of I&C equipment (whether classified or not) can neither initiate a multiple failure scenario nor cause a failure of the function to mitigate the consequences of this same scenario.

The category of the function shall be selected to facilitate showing that the claimed reliability is achieved.

Demonstrating a probability of failure on demand below 10^{-3} for the set composed of data acquisition (including the sensor), logic solver and voting components, is extremely difficult for software developed following only Category C requirements. It is appropriate therefore to assign such functions to Category A. In cases where this function is required to mitigate a failure of another Category A function, it is essential to ensure the independence of these functions. Several approaches can be foreseen, the simplest being to assign these two functions to two independent Class 1 systems.

Demonstrating a probability of failure on demand better than 10^{-2} for the signal acquisition, logic solver and voting hardware components following Category C processes for software development is conceivably achievable, but requires sufficient reliability data.

8.2.1.4 Minimum requirements by category

Some requirements are dictated by the selected category, while others are related to the class of the equipment or system, but all depend upon the assumptions of independence used in the accident analysis.

The list of requirements is perhaps open-ended, but includes as a minimum (see Table 3):

Table 3 – Minimum requirements by level of function

Category		A	B	C
Single failure criterion		YES	YES	NO, except if this requirement helps to demonstrate functional reliability or ability to perform function in case of internal hazard (fire, flooding, etc.)
Emergency electrical supply		YES	YES	NOT ALWAYS, it could be required in case for example of considering this function after earthquake, off-site power loss, etc.
Physical separation	Between redundant paths	YES (physical and electrical)		NO
	Between systems of different classes	Between classified and non-classified systems Between class 1 and 2 systems and others systems that could interfere with them		
Automatic actuation		Required if action before 30 min	Required if action before 30 min	Required if action before x min (x depends of impact analysis, it is >30 min for preventive actions and always >20 min for the actuation of mitigation means)

Additional independence requirements are imposed to ensure:

- that no function of a lower category can impair a function of higher category,
- that no failure of I&C equipment can impair successive lines of defence,
- that there is no common cause source of multiple failures that can impair a function added specifically to address these multiple failures.

These independence requirements are subject to the constraint that undue complexity is not introduced in systems of class 1 or 2.

Traceability of requirements for software is required in accordance with IEC 60880 for class 1 systems and IEC 62138 for class 2 and class 3 systems.

Table 4 lists other requirements on equipment:

Table 4 – Equipment requirements

Category	A	B	C
Design and construction code for electrical and I&C systems (e.g. RCC-E)	YES	YES	YES
Quality assurance	YES	YES	YES
Periodic tests	YES	YES	YES
Component reliability database and component reliability modelling	YES	YES	According to requirements derived from PSA
Qualification for operating conditions (see IEC 60780 for details)	YES	YES	IF APPLICABLE (e.g. if credited during or after a pipe rupture, etc.)
Minimal reliability requirements	YES at acquisition and logic level	YES at acquisition and logic level	YES at acquisition and logic level

8.2.2 Impact of safety reviews on categorisation

During the life of a plant, a Level 1 PSA is performed as part of the periodic safety review. The PSA uses operational experience feedback that may involve updating reliability data, assumptions regarding failure mechanisms and sequences, and the frequency of some PIEs.

Such PSA is intended to improve the plant design throughout its life and to be used in the decision-making process:

- by presenting evidence of the need to upgrade some sub-systems,
- by identifying equipment that requires better maintenance procedures,
- by revealing possibilities of multiple failures that could be significant,
- by feeding back operational experience to improve the data used for similar plants.

The PSA is required to show that the overall core damage frequency remains below the initial target of 10^{-5}/ry.

IMPORTANT: PSAs cannot be used alone to reduce the category of an existing function.

On the other hand, PSAs may lead to re-examining maintenance intervals, the category of existing functions, or the addition of new functions or refurbishment of parts of the plant. However, the PSA results cannot be used without complementary justification to increase maintenance intervals associated with qualified equipment. The age of the equipment shall be factored into the justification of such a change to show that there is no impact on its credited capabilities under both normal and accident conditions.

8.3 Approach 2: Quantitative importance based approach

8.3.1 General

Instrumentation and control functions can be assessed for their importance to safety by considering the consequences of their malfunction, such as failure to operate when required to do so, or spurious operation. PIEs within the NPP's design basis can be used as the starting point for the assessment. This assessment should include the analysis of all significant sequences of events, in order to identify the important functions required to be performed by the I&C.

This consideration of functions performed by the I&C functions, systems and equipment can be used to assign each of the FSE to one of the categories defined in IEC 61226, that is category A, B, C or unclassified. An unclassified assignment is made if the FSE is not significant to safety.

I&C FSE falling within the boundary of the safety system as defined in IAEA Safety Guide 50-SG-D8 [Note: this document has been replaced by NS-G-1.3.] are generally to be assigned to category A. I&C FSE defined as safety related in that guide are generally assigned to category B or C (and occasionally category A).

8.3.2 Quantitative assignment criteria

In order to be able to establish the safety significance of every I&C function, a set of criteria shall be determined. An example of these criteria is given below, based on work that has been carried out in the USA. The technique is based on a quantitative analysis of the contribution to risk using the cut set theory to give a consistent mathematical approach. In some cases, a function may be assigned to more than one category due to its contribution in several event sequences. In this case, the final assignment of such functions should be to the highest applicable category.

8.3.3 Quantitative criteria

8.3.3.1 Quantitative risk expressions for NPPs

When a quantitative risk assessment is performed on a NPP one or more of the following risk expressions may be developed depending upon the level of the PSA performed:

- Core melt (or core damage) frequency (level 1 PSA);
- Radiological release frequency and associated source terms (level 2 PSA);
- Health effects measured in terms of latent and/or fatalities (level 3 PSA).

In general, as a minimum for a level 1 PSA, a Boolean expression for core damage is generated in terms of the Boolean union of all the accident sequences on the event trees leading to core damage[6]. This expression is usually constructed for the Boolean union of all the minimum cut sets which contribute beyond some minimal level to one or more significant accident sequences. In other words, core damage can be expressed in terms of the frequency of occurrences of all the PIEs. The probabilities of each of the potential sequences resulting from an individual PIE or core damage frequency C(t) is the sum of the frequencies at which initiating events cause damage to the core.

$$C(t) = \sum_{i=1}^{n_i} \Pr\left\{\begin{matrix}\text{FSE are in a critical state} \\ \text{when the initiating event occurs}\end{matrix}\right\} C_{f,i}(t)$$

$$C(t) = \sum_{i=1}^{n_i} \Pr\{U_i E_{i,k}\} C_{f,i}(t) \qquad (1)$$

where

$\Pr$ is the probability;

$E_{i,k}$ is the event that minimal cut set “k” containing PIE “i” recurs;

U_i is the Boolean union of the minimal cut sets containing PIE “i”;

---

6 Core damage frequency is chosen as the example risk measure for which importance to safety contributions can be determined for the FSE. However, the importance approach to safety evaluation is a general one and can be employed in a similar fashion for any top event occurrence frequency (such as release frequencies and health effect which can be expressed as a Boolean union of underlying minimal cut sets).

n_i is the number of PIEs;

$C_{f,i}(t)$ is the failure frequency of PIE "i".

The above expression can be evaluated provided that

- the FSEs are reasonably reliable (i.e. the probability of two or more minimal cut sets occurring simultaneously is small);
- the individual events making up the cut sets (i.e. basic events) can be considered to be independent;
- the conditional probability of failure per unit time "λ" is a satisfactorily accurate approximation for the failure frequency.

In this case, expression (1) becomes:

$$C(t) = \sum_{i=1}^{n_i} \left\{ \sum_{\substack{j \\ i \in k_i}} \prod_{\substack{l \in K_j \\ i \in K_j \\ i=1}} q_i \right\} \lambda_i \qquad (2)$$

where

j is the domain of index for the minimal cut sets;

K_j is the jth minimal cut set;

$\in$ means "belongs to";

q is the event probability;

l is the domain of index of PIE;

$\lambda_i \cong C_{f,i}(t)$;

i is the domain of index for PIEs;

n_i is the number of PIEs in all of the minimal cut sets.

NOTE That the parenthetical term in expression (2) is a first order approximation for the critical state unavailability of the FSEs associated with PIE "i". This term is the sum of the minimal cut set probabilities containing the PIE "i". Expression (2) is generally accurate enough for most risk calculation and can therefore be used for establishing the importance of minimal cut set contribution to the overall frequency of core damage.

8.3.3.2 Importance to safety evaluation

If the above approach is employed, then the importance to safety of FSEs can be determined in terms of weighting functions which assess the contribution of each of the basic events (and thereby the postulated failure conditions of the corresponding FSEs of which they are constructed) to the overall frequency of core damage. The development of an importance expression for a function, and/or the associated systems and items of equipment by which it is implemented, involves three steps:

a) the formation of a new core damage top event that is the Boolean union of the minimal cut sets containing either the PIE or enabling event;

b) the use of expression (1) to compute the frequency of occurrence of this new top event (for PIE importance expressions, only one event can function as an initiating event for the new top event);

c) divide the resulting frequency of occurrence by the core damage frequency.

Stated mathematically, the importance to safety for basic events (or the FSEs of which they are constructed) as weighted to the core damage frequency is:

$$ICD = \frac{\text{Frequency of the Boolean union of the minimal cut sets containing the events of interest}}{\text{Top event occurrence frequency, C(t)}}$$

Therefore the importance to safety is simply given by the fractional contribution of the minimal cut sets (containing either the PIE or the enabling event) to the total core damage frequency. In many cases, in a risk assessment, C(t) can be taken to be a constant to the degree of accuracy necessary to establish reasonable importance rankings. In this ranking scheme, it should be noted that the numerator is a linear function of the failure frequency for PIEs. For enabling events, the numerator is a linear function of the enabling event unavailability. Conceptually, enabling (or pivotal) event importance is a contributing measure of importance since enabling events do not cause the occurrence of the top event (in this case core damage).

8.3.4 Category assignment

Based upon the importances derived from the above analysis, instrumentation and control FSE can be assigned to classification categories in accordance to a scale of importance. A logarithmic scale has been found to be most appropriate (although other scales could be used). For example,

- an I&C FSE should be assigned to category A if its calculated importance is $1{,}0 > I \geq 0{,}01$;
- an I&C FSE should be assigned to category B if its calculated importance is $0{,}01 > I \geq 0{,}001$;
- an I&C FSE should be assigned to category C if its calculated importance is $0{,}001 > I \geq 0{,}0001$.

8.3.5 Classification procedure

8.3.5.1 General

Using the method described in the preceding subclauses of 8.3, I&C functions can be classified according to their importance. Most NPP design phases contain iterative cycles while plant design options are studied. During these cycles, the I&C requirements are progressively refined and individual functions become more or less important to safety. This procedure is described below.

8.3.5.2 Identification of design basis

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

The assignment of FSE to categories depends upon their role in preventing or mitigating PIEs. The categorization process requires consideration of the role of the FSE in preventing and mitigating PIEs in all operating modes and plant conditions (e.g. start-up, normal operation, refuelling), as an FSE may have a significant role in some operating modes only, and also following PIEs such as natural events (e.g. seismic disturbance, flood, extreme wind, lightening) and hazards (e.g. fire, internal flood, missiles, radioactive release from adjacent NPP).

8.3.5.3 Identification and categorization of FSE

At an early stage in the design of the NPP, functions with a safety role shall be identified. The process of identifying these functions and assigning them to the I&C FSE or to the human operators should be performed according to IEC 60964. Following this initial identification of FSE, a category should be assigned for each FSE.

It will not be possible to identify in detail all the FSE at an early stage in the design process, as the characteristics of the NPP will not then have been defined fully. The process of identification and categorization of the FSE shall therefore continue iteratively throughout the design phase. Where an initial assignment of a FSE to a category is uncertain, then an explanatory note should be added to the categorization. The functions performed by each I&C system should be reviewed, to identify the sub-FSE within the FSE and to assign the appropriate category to each sub-FSE.

Since individual FSE may be involved in the implementation of several aspects of the requirements specification, the assignment process may result in some FSE being assigned to several categories. In the case of multiple assignment, the final assignment of each FSE and all sub-FSE should be to the highest applicable category.

As the redundancy, diversity and other technical requirements of the FSE are determined more exactly, for example as the safety analysis progresses and the operating procedures are developed, the categorization list is refined and revised, to derive a final list. This list should be included in the documentation that is required to obtain and maintain the NPP operating license.

8.3.6 Determination of requirements

The specific technical and quality requirements for FSEs that have been assigned to categories A, B, and C using the probabilistic approach presented above are given in IEC 61226.

8.4 Approach 3: Consequence – mitigation based approach

8.4.1 History: A dual licensing requirement leading to the probabilistic approach

Licensing in Canada has been (and continues to be) based on a dual deterministic and probabilistic basis, where requirements under both regimes shall be met.

The probabilistic requirements evolved gradually out of the deterministic licensing requirements for two deterministic scenarios, called “single accidents” and “dual accidents”. A “single accident” is a failure of a process system, while a “dual accident” is a failure of a process system combined with a failure of any one of the special safety systems (these correspond to Category A functions). The release limits are determined separately for these so-called single and dual accident cases. Because of the complete independence of the special safety systems from each other and from the process systems, these dual accident events are of much lower frequency than single accident events and are therefore accorded higher release limits (i.e. comparable risk, where risk is defined as probability * consequence).

The risk target for the earliest CANDU plants was expressed as a frequency of less than 10^{-5} events per year for a serious accident. This target was met by a combination of low frequency of serious process failures (events requiring a special safety system to act) combined with low unavailability of the special safety systems. The total failure rate for serious process failures due to all causes has been required to be less than one in three years assumed for failure of normally operating systems designed to normal industrial standards at that time. The major mitigating systems that prevented release from the fuel (shutdown, emergency core cooling) and those which contained the fission products (containment), were each required to have an unavailability of 3×10^{-3}.

8.4.2 Current probabilistic targets

The considerations outlined above became the basis for the current reliability requirements of 1×10^{-3} for the unavailability of each of the major mitigating systems (defined as the two independent shutdown systems, the emergency core cooling system, and the containment system). This means that the frequency of a major release would be about 10^{-6} events per year (i.e. frequency of serious process failure (3×10^{-1}) together with two mitigating systems

having an unavailability of 10^{-3} each). This is the basis for the current probabilistic safety assessment target, with a further analysis margin applied, of 10^{-7} events per year for loss of safety related systems leading to a release exceeding the regulatory dose targets, for individual events.

For the frequency range from 10^{-1} to 10^{-6} events per year, a number of regulatory dose limits are applied to characterize the consequence, with the limit becoming larger as the frequency of the event becomes smaller. It should be noted that the regulatory dose limits are associated with initiating events within a particular estimated frequency range, and not directly to the frequency range.

8.4.3 Classification of safety-related systems

Because of the requirement to meet both the deterministic and the probabilistic or risk-based criteria for releases, reliability requirements are imposed on systems which play a role with respect to an accident sequence leading to a release, whether this role is that of initiator or terminator or mitigator.

Traditionally, this classification allowed for 3 categories of systems in decreasing order of safety significance as follows:

- Special safety systems, having an unavailability target of 1×10^{-3}:
  - Both independent emergency shutdown (reactor trip) systems
  - Emergency core cooling
  - Containment
- Safety support systems, having an unavailability target derived from that above, generally 10^{-2},
  - Emergency backup power systems
  - Long-term cooling pumps, etc.
- Normal process control systems whose failures could theoretically initiate an accident sequence, having a target probability of failure per year < 10^{-1}.
  - Reactor regulating system
  - Heat transport system pumps, etc.

The increasing use of PSAs has in the past identified the need to add new mitigating functions that did not fall neatly under these three umbrellas, but the general methodology used for categorisation has successfully assigned a suitable category in every case. One example is presented in Clause 9 in order to allow comparison of various categorisation methodologies.

8.4.4 Application of design requirements

In the past, it was felt that standardized sets of design requirements could be developed based on the safety importance of a safety related system, and that the reliability target set for the system could be used to select the appropriate set of design requirements. However, this has so far been found to be impractical for CANDU plants, except in a very few isolated cases. Instead, design requirements for each safety related system are developed based on the general safety significance of types of systems (described above), the judgement and experience of the designers and safety analysts, and the results of safety analysis and PSA. The PSA reliability targets (i.e. unavailability) are used to develop specific requirements for redundancy, diversity, and protection from common cause events.

Since the mid-1990s, however, probabilistic criteria in the selection of design requirements have been used for computer software design. More recently, this has been extended in some parts of the Canadian industry to the complete computer-based system.

The risk-based approach is applied on the basis of the consequence of failure of the system (function) being categorized. This is done by associating the safety function with its required reliability within the accident event sequence.

8.4.5 Purpose of categorisation

Categorisation is required by NS-R-1 (clause 5.1) for the purpose of ensuring that the quality assurance in all aspects of a computer-based safety related system from design to operation and maintenance are appropriate to the importance to safety of the system.

Unquestionably the quality assurance requirements influence the resulting or achieved reliability of a system, but it is the required reliability that determines the category. One should also observe that in general, the higher the required reliability, the more demanding are other requirements such as provisions for back-ups, defences against common mode failures (by requirements such as channel separation, seismic or environmental qualification, etc.), but these requirements arise from the accident analysis or PSA, and not from the category.

8.4.6 Categorisation principles

The fundamental principles applied in the risk-based approach to categorisation are:

a) The concept arises from deterministic roots similar in principle to application of the single failure criterion, whereby both single and dual accidents shall be analysed (and is effectively calibrated against this basis).

b) Multiple layers of protection are needed (defence in depth):

   (For example, no computer-based or hardwired system can be credited with unavailability better than 10^{-3}: this forces the use of multiple independent defensive functions or systems).

c) Every layer is either assigned a required reliability, or its required reliability is determined from the initiating event frequency and the reliability of all other functions involved in the event sequence (this determines the allowable unavailability for poised functions or the allowable failure frequency for continuous functions). PSAs often serve as a source of data in this regard.

d) In general, the most stringent reliability requirements are associated with the most significant safety functions (i.e. those whose failure would lead to the gravest consequences).

e) Some safety functions and roles have been assigned reliability requirements to ensure that certain event sequences meet specific targets:

   - Frequency of loss of reactor reactivity control (LORC) < 10^{-1} per year (this criterion is to be tightened for future reactors)
   - Total demand frequency on Category A functions, requiring response within a very short time, due to all causes < 3×10^{-1} per year
   - Category A function unavailability shall be < 10^{-3}, but is generally not credited as better than 10^{-3} for purposes of categorising other functions or systems.

f) Common software is treated as a common cause of failure in multi-channel systems, so that while channelisation may allow credit for random hardware failures, no credit can be taken for redundancy if the software is common to the redundant channels.

g) Failure to function per design in all possible roles of a safety-related function are considered (preventative/mitigative, process control, monitoring, and testing), and the most demanding category is assigned.

h) Failure of a mitigating system such that it acts spuriously and deleteriously, either initiating an accident event sequence or interfering with another plant function is also considered. (Note that this consideration was added to comply with IEC 61226 Editions 2 and 3 and IAEA NS-G-1.3 clause 2.38.)

i) Partial failures are also considered, since they may in some cases be limiting.

j) Where the function being categorized is credited by virtue of safety action by the operator, the overall function (including sensors, alarms and displays, and final elements) is categorised as if it were automatic.

k) The category determines only the quality assurance aspects of development and maintenance of the computer-based system; it does not define the required reliability, qualification, or any functional or performance requirements. In other words, the category reflects the safety requirements, and does not set them.

NOTE It is assumed that the rigour of the quality assurance applied to the design process influences the realized reliability: this is why categorisation is performed:- to ensure the correct level of rigour is identified and enforced.

8.4.7 Categorisation methodology

For purposes of categorisation, the spectrum of required reliability for all safety-related functions is discretized and the term “safety significance” describes the segment of the discretized spectrum a system function may be required to meet. The following Table 5 illustrates the “safety significance” in terms of the applicable reliability metric:

Table 5 – Safety significance

Safety significance	Examples	Poised systems	Continuous systems
		Required unavailability	Required failure rate (f/y)
High	Emergency reactor shutdown Emergency core cooling	$\leq 10^{-3}$	$\leq 10^{-3}$
Medium		10^{-2} ....10^{-3}	10^{-2} ....10^{-3}
Low	Normal production control systems	$> 10^{-2}$	$> 10^{-2}$ [a]
[a] Note that the sum of frequencies of failures of such systems that require a Category A system to act is limited to less than 3×10^{-1}/y.			

It is important to keep in mind that the “safety significance” reflects the consequences of failure of the safety function, as discussed above in 8.4.3.

Because of the complexity of computer-based systems, the nature of the failure has also to be considered. There are some partial failures of safety-related systems that can be more deleterious than outright or complete failures because they may mask a problem and delay action by an alternate system, or their failure may impact another system. For these and other reasons, categorisation takes into account these partial failures by classifying them into three “failure types” as illustrated in Table 6. In all cases, the impact of the failure that is most demanding determines the category.

Table 6 – Failure impact type

Failure impact type	Failure impact description
Type I	Complete failure of the safety function or any failure which prevents the safety function from meeting the performance criteria assumed in the safety analysis
Type II	Partial failure of the safety function which may reduce the safety function’s speed or depth or internal redundancy, but which does not prevent it from achieving the minimal performance assumed in the safety analysis (e.g. one of several redundant components may fail, but the effect is within the tolerance assumed in the analysis).
Type III	Partial failure which does not impact the performance of the safety function assumed in the safety analysis (e.g. a status indicator may fail, but the safety function is still completely operable)

The final stage of the categorisation process is illustrated in Table 7 where the safety significance and the failure impact type are combined to determine the category.

Table 7 – Category determination

Category		Failure impact type		
		Type I	Type II[a]	Type III
Safety significance	High	A	B	Unclassified
	Medium	B	C	Unclassified
	Low	C	Unclassified	Unclassified
[a] Assuming the partial failure does not affect any other plant function.				

The categorization process usually proceeds as follows:

a) The safety function(s) of the system for which the software is required is (are) defined from the deterministic or probabilistic safety analysis.

b) The safety analysis and PSAs are reviewed to determine the required unavailability or reliability for the software-based system, and then this is used to assign the reliability metric called *"*safety significance*"* of the system as per Table 5.

c) Various kinds of failure modes are considered, as described above, and the failure impact type is selected from Table 6. This is an extension of the classic approach that considers only complete failures, and in some cases discloses more limiting event sequences.

d) Table 7 is used to select one of four different levels of software category.

If the software performs more than one function, then the process is repeated for every functional role, and the most demanding category is used.

8.5 Approach 4: Combined deterministic-probabilistic approach Bbased on NS-R-1

8.5.1 General

The development of a probabilistic safety classification methodology that has been applied to an advanced plant is described below. It includes the criteria used to determine the safety importance of a function and the structures, systems, and components that perform that function. A major feature of this approach is that is covers structures and systems, not just I&C functions.

For the advanced CANDU reactor, it was decided to develop a safety classification method, based on both probabilistic and deterministic principles, that would be applicable to all components that are important to safety, and that fully satisfies the requirements of IAEA NS-R-1, in which clause 5.2 states:

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

The safety function(s) to be performed by the item;

The consequences of failure to perform its function;

The probability that the item will be called upon to perform a safety function;

The time following a PIE at which, or the period throughout which, it will be called upon to operate".

A key consideration in the above IAEA NS-R-1 clause is the requirement to 'complement deterministic requirements with probabilistic methods and engineering judgment'. Based on

this requirement, it was further decided to develop a safety classification method that would be fully compatible with probabilistic methods – that is, addressing most of the systems and components credited in Probabilistic Safety Assessments - while retaining the deterministic classification criteria. This includes the consideration of the probability and consequence of the release of radioactive materials, as well as other materials that would harm the environment. It would also apply to all structures, systems, and components in the plant that perform a safety function.

8.5.2 Basis for the historical approach

It is noted that CANDU plants, since the 1960s, have applied probabilistic or risk based criteria to systems and components that perform important preventative and mitigating safety functions. The criteria were initially defined as the single and dual failure approach, where a "serious process failure" was assumed to have a certain frequency of occurrence and a dose criterion was defined with all of the "Special Safety Systems" remaining functional (single failure), and a second dose criterion was defined with one of the "Special Safety Systems failed (dual failure). An unavailability requirement was defined for each of the "Special Safety Systems, which effectively established the frequency requirement for releases to satisfy the dose criteria. This effectively established three distinct "plant states" (normal operation, single failure, and dual failure) having defined frequencies and radiation dose criteria (see Figure 1).

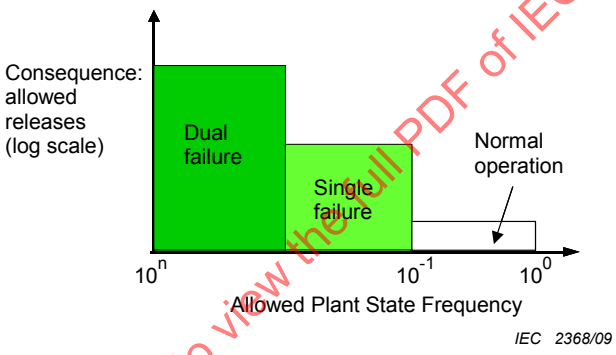


Figure 1 – Historical plant states and allowed releases

System reliability targets and other safety requirements were established based on their function in each of these "plant states", in terms of defined system types (Special Safety Systems, Safety support Systems, and other safety related systems). These requirements were mainly based on their mitigating functions for accident conditions, with some requirements also directed at preventing the accidents. As documented in 5.4 of this report, this formed the basis for a consistent categorisation methodology for safety-related I&C systems.The goal was to expand the concept, consistent with NS-R-1, to all structures, components and systems.

8.5.3 Plant state basis

It was decided to adopt the IAEA NS-R-1 concept of plant states (Clause 3.4:"…plant states be identified and grouped into a limited number of categories according to their probability of occurrence…") to define the probabilistic criteria (i.e. frequency and consequence of a release). Consistent with NS-R-1, the Plant States are identified as:

- Normal Operation (NO),
- Anticipated Operational Occurrences (AOO),
- Design Basis Accidents (DBA), and
- Beyond Design Basis Accidents (BDBA).

For each of these states, the allowed frequency of operation and the allowed releases are defined (see Figure 2).

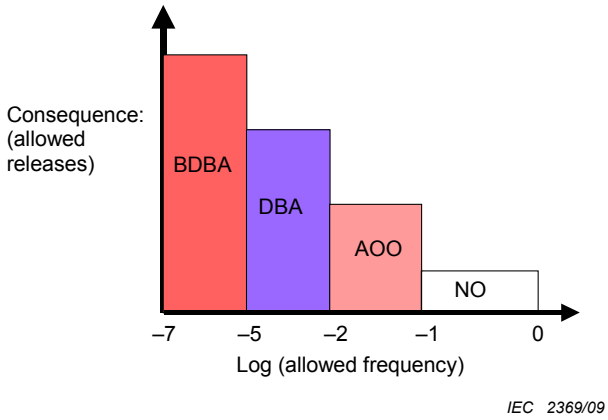


Figure 2 – Plant states and allowed releases

Postulated Initiating Events (PIEs) cause the plant to transit from one state to another. For example, an external PIE (xPIE) such as a Design Basis Earthquake puts the plant into the DBA plant state, as does an internal PIE (iPIE) such as a large loss of coolant. In general, PIEs are assigned to the plant states based on their impact and frequency of occurrence, which are determined by a combination of probabilistic techniques, safety analysis, and engineering judgment.

Safety functions are provided to act as barriers to prevent transitions from one state to the next. When equipment failures cause the acceptance criteria (frequency and consequence) for a Plant State to be exceeded, the event sequence proceeds to another Plant State. For example, if the equipment provided to deal with an event that puts the plant in the AOO state fails to provide the required safety function for that plant state, the event becomes an initiating event in the DBA plant state.

The safety requirements applied to the equipment during each plant state include the required reliability (defined for each PIE, and shown as summed across all PIEs in Figure 3), thus ensuring compliance with the acceptance criteria for each plant state. This establishes the probabilistic basis for the plant, covering the spectrum from low consequence and high probability events (i.e. Normal Operation and Anticipated Operational Occurrences, which together are identified as the “operational states”) through to low probability and high consequence events (Beyond Design Basis Accidents), and possibly the improbable state where large releases are considered.

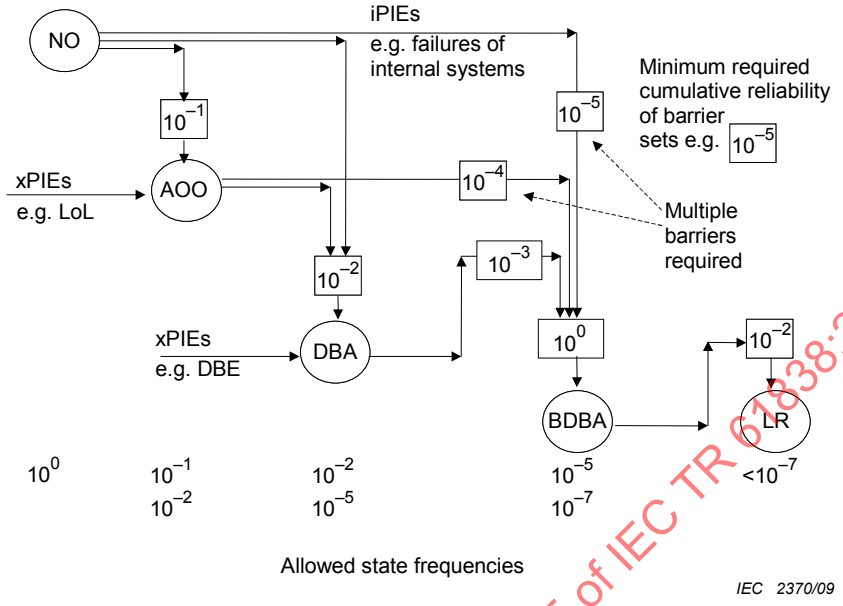


Figure 3 – Reliability requirements for state transition barriers

8.5.4 Defence in depth considerations

Transitions from one plant state to another are caused by the combination of a postulated initiating event (PIE) and the failure of equipment designed to perform the safety functions to stay in that plant state. The PIE may be an external PIE (xPIE), such as an earthquake or loss of grid, or an internal PIE, such as the failure of a plant component (iPIE) such as a process vessel or pipe or control function. Together with the expected frequency of these PIEs, the allowed frequency for each plant state defines the reliability requirements or risk reduction ratios to be placed on the internal barriers against transitions (i.e. structures or equipment). This will be expressed in terms of failure rate from the NO state or probability of failure on demand from other states. These are shown in the Figure 3 in terms of the frequencies summed across all PIEs (therefore showing cumulative risk reduction factors). For individual events and safety functions, these reliability requirements may be up to 2 orders of magnitude lower.

In some cases, the risk reduction ratios exceed the performance commonly demonstrated in operating plants (10^{-3}) for even category A functions, so these cases clearly demand multiple layers of defence (defence in depth, or system redundancy). A risk reduction factor of 10^{-5} could be achieved by two independent functions of whose probabilities of failure compound to less than 10^{-5} (e.g. 10^{-2} and 10^{-3}).

A deterministic element is overlaid at this point: at least one of these systems would be required to be of the category demanded by the categorisation, as shown in Figure 4.

8.5.5 Basis for classification – Based on IEC 61226

For safety classification, the key deterministic consideration is the order of importance of performing the safety functions during each plant state to maintain the plant in that state (i.e. to act as barriers to transit to a more serious state). The most important are considered to be the functions performed during the DBA plant state, as failure would put the plant in the BDBA state and result in a significant release (i.e. the consequence defined for the BDBA plant state, which includes the release associated with severe core damage) at a relatively high frequency. The next most important are considered to be the functions performed during the

AOO plant state due to the frequency of their failure and the consequence of failure, which would be that of the DBA plant state. The failure of functions during the NO plant state (small release, but high probability), and the failure of functions during the BDBA plant state (large release, but very low probability) are considered to be equal in terms of importance. Figure 4 illustrates these states and the classification of the barrier functions to prevent transition to a more serious state.

After a review of various types of safety classification methodologies (including those based on classification of pressure boundary components), the deterministic methodology included in IEC 61226 was selected as it was most compatible with the probabilistic basis defined by the Plant States, with its safety categorization of safety functions roughly based on the consequence of their failure, with a separate definition of safety requirements (i.e. Safety Classes in IEC 61513). It also has clearly defined deterministic criteria to establish the safety categories that can be applied to a wide range of items, unlike the pressure boundary classification methods which are usually quite specific to pressure boundary components.

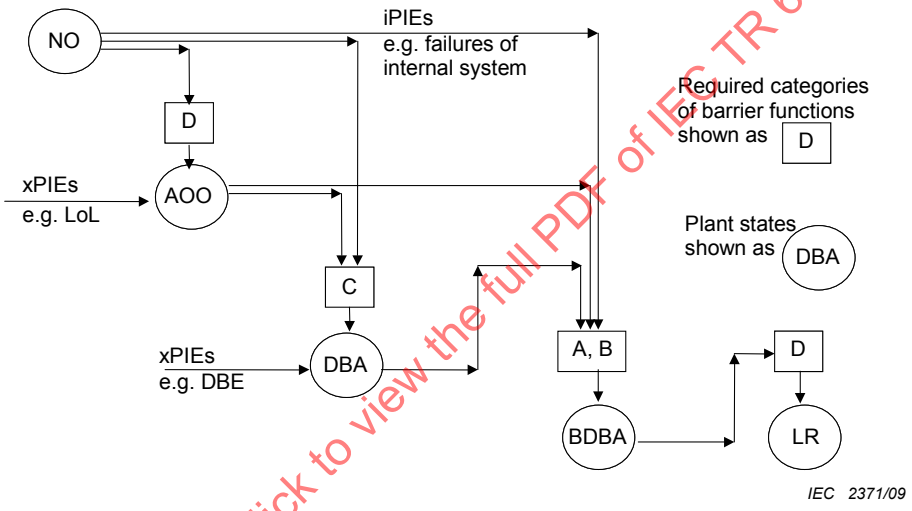


Figure 4 – Categories required to maintain plant states

8.5.6 Application of IEC 61226

However, the deterministic criteria and safety categories of IEC 61226 (Ed. 3, 2009) are not fully compatible with the probabilistic criteria defined for the four Plant States. For example, Category B and C include a mixture of criteria that apply to the NO plant state (e.g. 5.4.2 (e)), the AOO plant state (e.g. 5.4.3 (a) and (b)), the DBA plant state (e.g. 5.4.3 (d)), and the BDBA plant state (e.g. 5.4.3 (i) and (j)).

In order to adapt the IEC 61226 deterministic methodology to be compatible with the probabilistic criteria associated with the Plant States, it was necessary to make the following changes:

a) A new category (Category D) was created to make the deterministic criteria more compatible with the probabilistic criteria defined by the plant states, and to enable the assignment of appropriate requirements to equipment performing the functions in the NO and BDBA plant states. In general, Categories A and B are used for the Design Basis Accident plant state, Category C is used for the AOO plant state, and Category D is used for both the NO and the BDBA plant state. Although the categories are associated with these plant states for most situations, the criteria (i.e. consequence of failure) may apply to other plant states for certain situations, so the categories are not absolutely restricted to one plant state (e.g. certain failures of a reactor coolant system component during the NO or AOO plant state may have the same large consequence, as its failure during the DBA plant state, so the category should be the same).

b) The term “category” was redefined to be “Safety Function Category”, to emphasize that the safety importance is based on the safety function, and not on a system type, or system requirements, and to clearly distinguish it from other types of categorization used in a nuclear plant (e.g. seismic category).

c) The deterministic criteria were redefined for each category to more closely reflect the probability and consequence of failure of the function.

d) The requirements to be applied to the equipment that perform the functions are called “Safety Classes” and are directly associated with the Safety Function Categories, but can be changed if the required reliability of the function can still be achieved with a different Safety Class. The change of the Safety Class is justified by a probabilistic analysis.

The above changes to the IEC 61226 methodology make the determination of safety importance and the application of requirements simple and easily understood, while allowing flexibility in the application of requirements. Although the overall classification concept is the same as that described in 5.4 of this report, the application is very much simplified due to the use of plant states to define the risk aspects.

In terms of meeting the IAEA criteria, the following considerations apply:

- The safety function(s) to be performed by the item;

  The safety functions are developed from the fundamental safety functions in IAEA NS-R-1, and apply during each plant state, but the performance requirements will be different for each plant state based on the frequency and consequence criteria. The specific safety functions for systems and equipment during each plant state are identified by the probabilistic safety assessment.

- The consequences of failure to perform its function;

  The assignment of the Safety Function Category (A, B, C, or D) is based on the consequences that would occur if the safety function was not performed in that plant state (i.e. both the frequency of the release and the size of the release). If equipment is provided in a higher plant state to perform the function, it is credited in considering the consequence of failure. The consequences are considered only in a qualitative sense, in terms of the acceptance criteria of the higher plant state. That is, in conjunction with an initiating event, failure of a Category A function will result in a BDBA, which is termed an “unacceptable consequence”; failure of a Category B function will credit the operation of the Category A functions, and therefore the consequence is limited to the DBA acceptance criteria; failure of a Category C function will credit the Category B and A functions, so the consequence will be limited to the DBA acceptance criteria; and if a Category D function for the NO plant state fails, the Category C equipment will be credited and the consequence will be limited to the AOO acceptance criteria. The failure of the functions needed to mitigate a BDBA (i.e. to prevent a large release) are of high consequence, but very low frequency, and are treated the same as the high frequency/low consequence functions for the NO plant state (Category D).

- The probability that the item will be called upon to perform a safety function;

  The probability that an item will be called upon to operate is related to the plant state for which it performs a function.

- The time following a PIE at which, or the period throughout which, it will be called upon to operate.
  This is a consideration mainly for Category A, where the immediate requirement to perform the function to prevent a significant consequence means that the equipment shall be highly reliable, having specific requirements imposed to satisfy this high reliability. For Categories B, C, and D, the consequence of the timing is not so critical, and alternatives can be provided to increase the reliability of the function (redundant or diverse equipment).

8.5.7 Safety classification methodology

The application of the above changes to the safety classification methodology for advanced CANDU reactors is shown in the following Table 8, where the usual classification is indicated

by the larger bolded characters (in the shaded boxes). These indicate the importance of the safety function performed during that plant state, which also indicates the requirements applicable to the systems or equipment performing the function (Safety Class). The characters in brackets indicate that in certain (infrequent) cases, components performing a function in a lower plant state may have failure modes that satisfy the assignment criteria for that Safety Function Category, but have no mitigating systems or components in a higher category since the failure rate is very low (e.g. in the BDBA range for Safety Function Categories A and B). For these components, the higher Safety Function Category reflects the importance of the function in preventing a large consequence, and also results in the higher level of requirements (Safety Class) to provide confidence that the failure rate remains low. The alternative would be to provide additional equipment in the next plant states to mitigate such a failure mode.

Table 8 – Application of the changes to the safety classification methodology

Safety importance	**Safety function identification based on plant state**				**System or component requirement**
Safety function category	**Normal operation (NO)**	**Anticipated operational occurrences (AOO)**	**Design basis accidents (DBA)**	**Beyond design basis accidents (BDBA)**	**Safety class**
A	(A)	(A)	**A**	--	**1**
B	(B)	(B)	**B**	--	**2**
C	(C)	**C**	C	--	**3**
D	**D**	N/A	D (Non-rad)	**D**	**4**
Frequency range	Operational states 10^{0} to 10^{-2}		10^{-2} to 10^{-5}	**10^{-5} to 10^{-7}**	

8.5.8 Deterministic criteria for safety function categories

The safety importance of a function is based on the following criteria for the assignment of Safety Function Categories:

a) **SF Category A**: Failure of the function results immediately (in the short term) in an accident with unacceptable consequences in the absence of further protective action. Functions of the following types are included in this safety function category:

- Functions whose failure would cause an immediate loss of integrity of fuel or reactor coolant pressure boundary,
- Functions that shall be performed immediately following initiation of a DBA to stabilize the associated transient and to bring the plant to a controlled state, failure of which would cause unacceptable consequences.

b) **SF Category B**: Failure of the function results in unacceptable consequences in the longer term, after stabilization of the initial transient, or the consequence of failure is less than that of Category A. These functions are complementary to those of Category A. Functions of the following types are included in this safety function category:

- Functions that provide support services (power, air, water, lubrication) or complement the proper operation of Category A SSCs during and following a Design Basis Accident (these SSCs may perform functions during normal plant operation or anticipated operational occurrences as well).

- Functions that monitor parameters or equipment during and following a DBA that are needed for credited manual actions in the post accident scenario.
- Functions that maintain a confinement boundary for radioactive materials outside the reactor without further levels of defence and whose failure would cause a radioactive release beyond regulatory limits for DBA.

c) **SF Category C**: Failure of the function results in a DBA that is mitigated by a higher category system, or in a release of radioactive material that exceeds the AOO reference dose limits, or in the loss of the backup for an SSC in a higher category, or in the potential impairment of an SSC in a higher category. Functions of the following types are included in this safety function category:

- Functions performed during AOOs and required to:

  Control reactor power,

  Shutdown the reactor,

  Remove decay heat from the fuel,

  Maintain a confinement boundary for radioactive materials whose failure would result in a minor release of radioactive materials or where a higher category protective safety function is provided.
- Functions to monitor or test systems performing higher category functions during normal plant operation.
- Failure causes loss of an SSC that has a backup function for a higher category.
- Functions that prevent criticality of fuel outside the reactor core.

d) **SF Category D**: Functions not included in the previous Safety Function Categories that are required to satisfy the safety goals for core damage frequency (small release and large release). Functions of the following types are included in this safety function category:

- Functions to mitigate the consequences of Beyond Design Basis Accidents and Severe Accidents.
- Functions to maintain the plant in a normal operating condition, where failure is mitigated by a Category C system.
- Systems with functions for protecting the environment and non-human biota from the release of non-radiological hazardous substances.

8.5.9 Other classification considerations

The purpose of safety classification is ultimately to provide consistency in the assignment of requirements, and to provide the proper measure of assurance that the functions will be performed in accordance with their acceptance criteria.

In the above safety classification methodology, four categories are considered to result in the most suitable assignment of requirements to the different types of equipment. The use of four Safety Function Categories is because in past plant designs (and it is believed to be the same for other reactor types), four distinctly different types of systems, with different requirements, were used to perform the safety function, as follows:

a) Special Safety Systems, consisting of two fast acting shutdown systems, an emergency core cooling system, and the containment system (usually called Engineered Safety Features on other reactor types). These systems are required to act very quickly and with high reliability. To ensure the reliability aspect, they are independent of the normally operating systems as much as practical, and generally avoid unnecessary complexity. A common characteristic of these systems is that they must respond immediately to the most severe initiating events to avoid a major release. These systems are normally standby systems. Because of the large consequence of failure of these systems, they are subject to a very stringent set of requirements.

b) Safety Support Systems, needed to support the longer-term functions of the Special Safety Systems. These systems generally have a higher level of complexity in their design

and are normally redundant or diverse in design and therefore did not require such high reliability requirements for the individual systems or equipment. Since the Special Safety Systems had already operated when these systems were required, the consequence of failure of these systems was not as significant as for the Special Safety Systems. These systems may also perform functions for the normal operation of the plant.

c) Other safety related systems, used to provide any other mitigation functions to maintain the plant in a safe state in the long term for a design basis accident. Because of their functions during an accident, a higher level of requirements was applied than for the systems that maintain the plant in a normal operating state.

d) Systems that perform safety functions during normal plant operation, the failure of which would cause an accident condition. In the past, these systems were usually designated as non-safety related, or unclassified. For beyond design basis accidents, where the above systems may have failed, they could be credited to mitigate the situation. However, they are included in the safety classification methodology because they are addressed in the Probabilistic Safety Assessment, and their reliability (i.e. failure frequency) establishes the reliability requirements for the accident mitigation systems.

8.5.10 Worked example

The following is an example of the application of the above safety function categorization methodology to the fuel cooling systems.

All modern designs feature numerous heat removal systems. In this case, the systems include the main feedwater system, the auxiliary feedwater system, the emergency feedwater system, the reserve water system, the moderator heat removal system and finally the vault cooling water system.

During full power operation, the fuel is cooled by the steam generators using feedwater from the main feedwater system, so this safety function is required for the NO plant state, and is Safety Function Category D (the only failure mode takes the plant from the NO state to the AOO state). In the past, these types of systems were not included in the safety classification (usually designated as non-safety related or unclassified), as it was not considered necessary to impose additional requirements on them. However, in a probabilistic method, it is important to identify the safety function they perform since the assigned failure rate determines the reliability requirements for the mitigating systems.

If the main feedwater supply fails, the plant enters the AOO plant state, and an auxiliary feedwater supply (startup feedwater) is provided to the steam generators after the reactor is shutdown. A failure of this system would take the plant to the DBA state, so this function is Safety Function Category C.

If the auxiliary feedwater supply fails, then the plant enters the DBA plant state, and the emergency feedwater system is actuated to perform the heat removal function. This function is not needed immediately, since there is time available before the steam generator inventory is exhausted, so it is Category B (if this were not the case, this function would have been Safety Function Category A). There is also an additional steam generator feedwater supply available by gravity flow from the reserve water system, and if this is needed to meet the acceptance criteria for the DBA plant state it would be Safety Function Category B, and if it is needed just to supply additional margin after the DBA criteria are satisfied, it would be Safety Function Category C.

If the emergency feedwater system fails, then the plant enters the BDBA plant state, where the moderator cooling system will remove heat from the fuel as the pressure tubes heat up and sag into contact with the moderator tubes, so the moderator heat removal system is Category D. Note that this same system also performs a heat removal function during normal operation (but with much less heat load), which would also be Safety Function Category D. However, for its BDBA function, it is designed for the increased heat removal capability and for the environmental conditions to perform its required function. If this system fails, a vault

cooling water system is designed to cool the calandria vessel as the core is displaced to the bottom of the vessel, which would also be Safety Function Category D.

In each case above, the frequency and the release criterion for each plant state would have to be satisfied. Note that this criterion needs to be satisfied for many different sequences, so for individual sequences the target criteria would be lower than that shown for each plant state. In terms of the requirements for the equipment performing the functions, a reliability (unavailability) target would be defined, based on the number of systems and the plant state requirements, and a Safety Class would be applied. For Safety Function Category A, Safety Class 1 requirements would be applied (e.g. as defined in IEC 61513), and so on for the other categories. Based on the specific reliability requirements identified for individual systems, the Safety Class could be reduced accordingly, but a case would have to be made to show that this is acceptable.

8.5.11 Conclusion

The above safety classification methodology is based on four Safety Function Categories to define the importance of the function and the equipment that performs the function, four Safety Classes to define sets of requirements, and four Plant States to define the probabilistic criteria. It has been applied to an advanced plant, where it is easily understood and applied by designers and others. It supports the implementation of the different levels of defence while providing flexibility to designers to use equipment with different levels of requirements and reliability. These factors and the changes to the IEC 61226 methodology described above are considered to be essential in the implementation of a safety classification methodology that makes full use of modern probabilistic or risk informed principles, as required by IAEA NS-R-1.

8.6 Approach 5: Application of risk methodologies in U.S.A. nuclear regulation

NOTE Annex B captures the United States' contribution from Edition 1.

In 2006, the United States Nuclear Regulatory Commission issued Regulatory Guide 1.201 "Guidelines for Categorizing Structures, Systems, and Components (SSC) in Nuclear Power Plants According to Their Safety Significance." This trial use framework combines classical binary deterministic classification (safety versus non-safety) with risk informed evaluation of SSC roles in maintaining plant safety. It implements an acceptable approach to the regulation stated in 10 CFR 50.69[7] The risk evaluations may include PRA as well as other non-PRA evaluations such as Fire Induced Vulnerability Evaluation, and Seismic Margins Analysis. It is based on original work done by the Nuclear Energy Institute (NEI).

In the classification method endorsed by this Regulatory Guide, the safety significance of SSCs is determined using an integrated decision-making process, which incorporates both risk and traditional engineering insights. The safety functions of SSCs include both the design-basis functions (derived from the safety-related definition) and functions credited for preventing and/or mitigating severe accidents. Treatment requirements are then commensurately applied for the categorized SSCs to maintain their functionality.

Figure 5 provides a conceptual understanding of the new risk-informed SSC categorization scheme. The figure depicts the current safety-related[8] versus nonsafety-related SSC categorization scheme with an overlay of the new safety-significance categorization. In the traditional deterministic approach, SSCs were generally categorized as either "safety-related" (as defined in 10 CFR 50.2) or "nonsafety-related." This division is shown by the vertical line in the figure. Risk insights, including consideration of severe accidents, can be used to identify SSCs as being either safety-significant or low-safety-significant as shown by the

---

7 Title 10 of the U.S. Code of Federal Regulations, Part 50 "Domestic Licensing of Production and Utilization Facilities."

8 Note that in U.S. regulatory practice, the use of the term "safety-related" differs from its use in the IAEA guides. It is essentially equivalent to the IAEA term "safety systems."

horizontal line in the figure. This results in SSCs being grouped into one of four categories, as represented by the four boxes in Figure 5.

RISC-1 SSCs are safety-related SSCs that the risk-informed categorization process determines to be significant contributors to plant safety. Licensees shall continue to ensure that RISC-1 SSCs perform their safety-significant functions consistent with the categorization process, including those safety-significant functions that go beyond the functions defined as safety-related for which credit is taken in the categorization process.

RISC-2 SSCs are those that are defined as nonsafety-related, although the risk-informed categorization process determines that they are significant contributors to plant safety on an individual basis. The NRC staff recognizes that some RISC-2 SSCs may not have existing special treatment requirements. As a result, the focus for RISC-2 SSCs is on the safety-significant functions for which credit is taken in the categorization process.

RISC-3 SSCs are those that are defined as safety-related, although the risk-informed categorization process determines that they are not significant contributors to plant safety. Special treatment requirements are removed for RISC-3 SSCs and replaced with high-level requirements. These high-level requirements are intended to provide sufficient regulatory treatment, such that these SSCs are still expected to perform their safety-related functions under design-basis conditions, albeit at a reduced level of assurance compared to the current special treatment requirements. However, 10 CFR 50.69 does not allow these RISC-3 SSCs to lose their functional capability or be removed from the facility.

Finally, RISC-4 SSCs are those that are defined as nonsafety-related, and that the risk-informed categorization process determines are not significant contributors to plant safety. 10 CFR 50.69 does not impose alternative treatment requirements for these RISC-4 SSCs. However, as with the RISC-3 SSCs, changes to the design bases of RISC-4 SSCs shall be made in accordance with current applicable design change control requirements (if any), such as those set forth in 10 CFR 50.59.

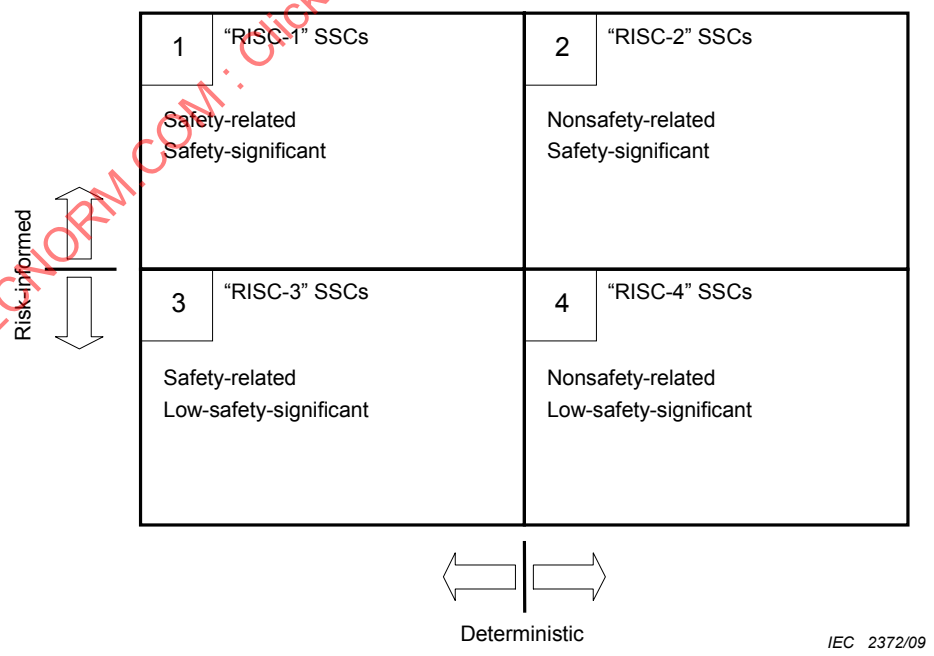


Figure 5 – RISC Categories

The categorization approached described in Regulatory Guide 1.201 has not been practically applied in the area of instrumentation and control systems. Classification has followed the

traditional approach of Class 1E and Non-class 1E. However, there traditionally has been a degree of distinction made within these categories. The major NSSS control systems are described in the Safety Analysis Report even though they are nonsafety-related. The NRC staff accepts that special systems provided for mitigation of anticipated transient without scram (ATWS) may be considered nonsafety-related while they do receive staff scrutiny. The same is true for more recent Diverse Actuation Systems that are provided to mitigate the effects of Common Cause Failures of the primary safety system. Applying the Regulatory Guide 1.201 process to these cases would provide a more systematic treatment.

In Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," the NRC endorses IEEE Standard 1012-1998 as an acceptable method for complying with the regulations for promoting high functional reliability and design quality in software used in safety systems. While the scope of the Regulatory Guide is limited to safety systems, this standard presents a graded approach based on a defined four-level "Software Integrity Levels" method of quantifying software criticality. The Regulatory Guide states that the software used in nuclear power plant safety systems should be assigned integrity level 4 or equivalent, as demonstrated by a mapping between the applicant or licensee approach and integrity level 4 as defined in IEEE Standard 1012-1998. In a more recent revision of this standard (2004), not yet addressed by the NRC, the definitions of the Software Integrity Levels are made to be more consistent with the SIL levels defined in IEC 61508. This introduces the potential for a more rational basis of classification using risk informed methods. The relationship of IEC 61508 to the nuclear specific standards produced by IEC is discussed in Annex D of IEC 61513.

9 Comparison of risk-related categorisation results

This Clause presents comparisons between various methodologies where such comparisons are possible, given the differences between the plant technologies associated with the methodologies surveyed in the previous clauses. At this stage of preparation, only one comparison has been compiled.

9.1 CANDU plant stepback function

9.1.1 Problem statement

Consider the classic loss of reactivity control (LORC) accident, in which the reactor regulating system (RRS) suffers a fault that causes it to drive all reactivity mechanisms in the direction that adds reactivity to the core. Unless this event is terminated, the fuel will overheat, potentially fail and then challenge other barriers[9].

The plant design is such that one set of these mechanisms can either be driven in or out by RRS, or independently dropped by a poised mitigation function called stepback (STP). When each rod is dropped (by de-energizing an electro-magnet), the drive is disconnected from the rod and it falls into the core regardless of the action of RRS. When dropped, the reactivity influence of the four rods overcomes the sum of all RRS-induced reactivity insertions, thus STP is capable of overcoming any failure in RRS, and safely terminating the event sequence. STP may be considered independent of RRS by the rules expressed in IEC 61513, 5.3.1.5. Additionally, the computer hardware and electromagnetic clutches that perform the STP function can be (and are) tested periodically during normal reactor operation.

In addition to STP, there are two safety shutdown systems (SDS) that can independently terminate the transient. In the deterministic safety analysis, STP is not credited and only the later of these two systems to detect the accident and act is credited. Similarly, one generally credits only one shutdown system for purposes of categorisation, although both are credited in the full plant PSAs.

---

9 Note that the example cited has been simplified to better illustrate the principles.

For historical reasons, RRS is required to meet a reliability requirement of no more than one LORC event per 10 years. Both shutdown systems are special safety systems, and therefore shall be designed to meet an unavailability of 10^{-3} or better.

What is the category of the STP function?

9.1.2 Solution using approach 3

a) Identify the event sequence and layers of protection that provide the defence in depth against this accident, as shown in Figure 6 below.

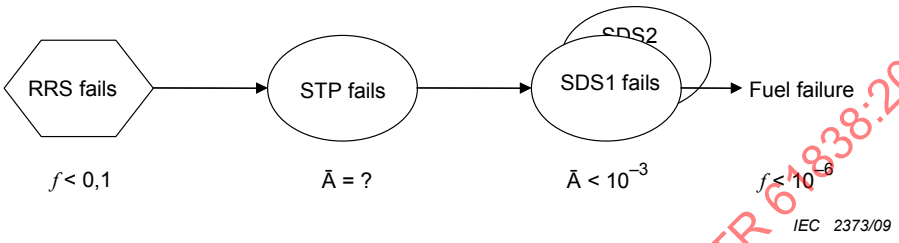


Figure 6 – Event sequence and layer protection identification

Fuel failures may occur only if all the functions shown fail. (Note that this simplified example omits the further barriers to a release of radioactivity, such as the fuel sheath, the primary heat transport system, emergency core cooling, and containment.)

The design requirement is:

$$f_{LORC} \times \bar{A}_{STP} \times \bar{A}_{SDS} \leq 1 \times 10^{-6} \quad \text{(where only one SDS is credited)}$$

This requires:

$$\bar{A}_{STP} \leq 1 \times 10^{-2}$$

The above value for the required unavailability of STP is based on the more conservative of the target values and the realized values for the other systems forming the safety group. For example, even though in practice the shutdown systems demonstrate unavailability well below 10^{-3}, credit better than 10^{-3} is normally not given.

b) Determine the safety significance using the required unavailability of STP.

From Table 5 in 8.4.7, the safety significance of STP is medium.

c) Determine the limiting case failure impact type.

To do this, we assess the partial failures to determine which would be the limiting case; a partial failure or a complete failure. A partial failure could range from failure-to-drop of from 1 to 3 rods, or a delay in the drop of a number or all of the rods. All of these partial failures are equivalent in terms of safety analysis to a complete failure of STP (failure to drop any rods). Thus the limiting case failure impact is complete failure.

d) Determine the category from the safety significance (medium) and failure impact type (complete failure). Table 7 gives us:

Category B.

9.1.3 Comparisons with other methods

Some insight into the robustness of this approach can be obtained by comparing the category obtained using this risk-based approach with that which would be obtained by other methods. One should expect similar but not necessarily identical results, since none of these other approaches was designed with the CANDU design in mind. Two comparisons are made below:

a) To the role-based method of IEC 61226, and

b) To the Role-Reliability-Timeframe method of IEC/TR 61838 (entitled “Defence in Depth” method in Edition 1 of 61838, and reproduced in Annex B).

The rules-based method in clause 5 of IEC 61226 (2nd Edition) suggests that RRS would be Category C and STP would be Category B, since a failure of RRS does not immediately and automatically require operation of a Category A function. This is consistent with the criteria 5.4.2e) and 5.4.3a).

It is instructive to examine why the same category should result from such apparently diverse approaches. The goal of both approaches is to reduce to an acceptable level the risk of release to the public, and to do so using layers of protection (defence in depth). In both approaches, the integrity-related requirements of the protective function (e.g. reliability, redundancy, seismic or environmental qualification, quality assurance) are applied more rigorously to the final layers of defence. The real difference is simply that the reliability is quantified in the risk-based approach, where the reliability requirements for each category have been graded by consideration of all the classic PIEs (loss of reactivity control, loss of coolant, etc.) so that the final safety objective is met. The advantage of the risk-based approach is that it can be generalized to other reactor designs and mitigative functions not predicted in the role-based rules.

The **role-reliability-timeframe method** (as described in Appendix B) also provides a basis for comparison. Under this approach, the role of STP could be either “preventative” or “terminative”, so both are evaluated, and the more demanding category assigned. For either role, the reliability target lies on the boundary between “low” and “moderate”,

Using Table B.1 for the “preventative” group, the time element, being very short, dictates that one select the “response to a fault” row of the table. The reliability target may be taken to be in the “moderate” range. This role therefore yields a category of B.

Similarly, considering STP as a mitigative function and using Table B.3 yields category B.

Using Table B.2 for the “terminative” group, the “automatic action” row of the table applies, and the reliability target lies on the boundary between “low” and “moderate” columns. This yields either Category A or B, depending on the application of the reliability target. It should be noted that in practice RRS has demonstrated a failure rate of less than 10^{-1}, and both of the shutdown systems have demonstrated an in-service unavailability of between 10^{-4} and 3×10^{-3}. (Note that 10^{-3} is the licensing requirement and design target, but the real unavailability is that which is determined during operational surveillance testing.) Even without regard to the non-probabilistic requirement to credit only one of the two shutdown systems, this suggests that the boundary case issue be resolved in favour of assigning a reliability target of “low”. This yields category B for the terminative role.

9.2 Conclusions arising from the use of various approaches

Both of the probabilistic or risk-based methodologies yield similar results (category B in the CANDU STP case), despite the fact that they were developed to suit different reactor technologies. This result also agrees with the deterministic role-based category.

This suggests that that a well-constructed risk-based approach may be robust and potentially generally applicable to a wide variety of reactor designs, including designs for which the methodology was not specifically designed.

The above conclusions are related in that they both stem from the risk-based methodologies having been calibrated against deterministic criteria associated with Category A functions. These methods are both reasonable implementations of the recommendation in NS-G-1.14 to use a balanced method for categorisation.

Annex A
(informative)

The use of PSA: methods and results

NOTE 1 This annex (formerly Clause 5 in Edition 1) provides some information on the use of PSA in plant design, but it should be noted that this is not the same as risk-based, or PSA-informed classification. PSA methods (help to) determine the required reliability of the various functions in the plant, and also identify where new functions need to be added and what their required reliability would be. In contrast, the risk-based classification methods seek to use this required reliability (largely obtained from the PSA as the major input) to determine the appropriate quality assurance level.

NOTE 2 Precise values from the PSA analysis are not essential to the risk-based categorisation process, since the required unavailability is discretized into ranges bordered by powers of 10. If there is a concern about the conservatism or accuracy of the required unavailability of the function being categorized, then an appropriate correction should be applied.

A.1 General

The design of an NPP is principally based upon stringent deterministic requirements and on the well-understood and well-proven defence-in-depth principles. Even with a completely new design, the basic safety functions (particularly the Category A functions) and the responses to all PIEs are generally well laid out before the PSA work begins. However, probabilistic studies can be carried out to determine, in a quantitative format, the relative importance of the instrumentation and control functions in the overall safety of the NPP, and can determine where additional safety-related functions are required to meet PSA safety targets.

In fact, probabilistic safety assessments may be used in two areas:

- To support the design process of new NPPs in order to determine the correct classification of the I&C functions, especially to avoid down or upgrading of classification;
- To verify the design and identify improvements to the I&C systems which will be most effective. This use of probabilistic techniques is particularly appropriate to the safety reviews of existing NPPs.

In this way, probabilistic safety assessments can be used to improve the design of NPPs and focus resources on the provision of I&C functions that have the greatest safety significance.

However, we have to note that the use of PSA continues to evolve within member nations and its level of acceptance is not consistent, even if PSA are used in some countries as part of the licensing process.

A.2 Use of PSA in the design of future NPPs

A.2.1 Overall scope

PSA may be used in the design phase with the following purposes:

- to identify the reliability of equipment and systems required to cope with safety targets;
- to complement the qualitative approach in assessing the frequency of initiating events;
- to identify the complex failure sequences to be considered in the design;
- to support the definition of technical specifications and emergency procedures;
- to achieve a balanced design.

Typically, PSA covers the assessment of the core damage frequency, the evaluation of the containment response and the estimation of release frequencies and magnitudes.

Simplified PSA methods for I&C assessment are normally used during the early stages of the design process, in particular to examine the adequacy of redundancy provisions and the need for safeguards against common cause failure of simple redundant systems and to guard against the impact of human errors. Moreover, it is usually important to know the uncertainties and take them into account in the safety assessment and in the subsequent classification. Therefore, particular attention must be given to the following points:

- sensitivity studies and the evaluation of the uncertainties in the modelling;
- the quality of the reliability databases that are used to provide reference data.

A.2.2 Methods

A.2.2.1 Probabilistic safety targets

Probabilistic safety targets for the I&C functions should be consistent with those set for the overall NPP. An example of such targets is provided in IAEA INSAG 12 document as follows:

- core damage cumulative frequency shall be lower than 10^{-5} per reactor year;
- cumulative frequency of exceeding the limiting release shall be lower than 10^{-6} per reactor year;
- sequences involving very large releases with gross failure of containment shall have a cumulative frequency well below the previous target of 10^{-6} per reactor year.

A.2.2.2 Initiating events

The initiating events that will be considered in the probabilistic studies are principally the events used to justify the design of a specific plant system or of a specific I&C function.

Accordingly, the designer speaks about a family of events. A family of events is in fact a group of elementary events that lead to the same main event. This arrangement of elementary events in families of events may differ from plant to plant but the arrangement selected should be clearly defined at the beginning of the design.

A.2.2.3 Reliability data

During the design phase, it is usual for a generic reliability database to be used because little or no plant specific data is available. Such data should be used with caution since it may not be valid for the application in the environment of the NPP. Better data can often be obtained from operating plants where similar equipment has been in service.

Point values may be used, in which case sensitivity studies should be carried out to evaluate the influence on the design of the critical assumptions and base data.

A.2.2.4 Common cause failure (CCF)

I&C equipment is subject to common cause failures through the use of identical components and techniques. These common cause failures can be caused by error in design, manufacturing, operation and maintenance processes as well as common environmental stresses.

For the case of equipment that consists of components whose freedom from failures caused by design/manufacturing errors and environmental stresses can be reasonably determined through test, experience or analysis; the probability of common cause failure should be quantified according to the β factor model or another appropriate technique.

For the case of equipment that consists of components whose freedom from failures caused by design/manufacturing errors and environmental stresses cannot be reasonably determined through test, experience or analysis, the β factor model is not applicable.

A.2.2.5 Human reliability

Human reliability or the probability of occurrence of human error is an important design consideration. Therefore, the assessment of the probability of human error should be included in the PSA. On the human error assessment both time independent (e.g. latent errors) and time dependent (e.g. diagnosis errors) should be considered.

A.2.3 Plant analysis and modelling I&C in PSA

The plant model should consist of

- a set of initiating events;
- event trees that describe the accident sequences in terms of progression from an initiating event to a final state including the successes or failures of systems and operator actions;
- fault trees or the equivalent mathematical functions that describe the system failures as combinations of basic events (component failures, human errors, etc.).

Event trees and fault trees can be combined in order to identify the basic event combinations specific to each accident sequence.

A.3 Benefits of the use of PSA for existing NPPs

For existing NPPs, PSA is widely used during the periodic safety reviews in order to

- highlight and place the dominant sequences in a hierarchy;
- help decide whether to implement modifications to the safety and safety-related I&C systems and equipment;
- evaluate the global safety level of the plants.

The possible improvements can be prioritized according to the reduction of risk (probability and consequences). Also the PSA allows attention to be paid to sequences that can lead to

- high pressure core melt;
- containment by-pass;
- other dominant sequences, such as those including human errors or equipment failures.

PSA is a very useful tool to evaluate the importance of I&C functions and assess the benefit of potential modifications. So, the designer can use the results of PSA along with other deterministic studies in order to decide which improvements will give the greatest safety improvement. This allows cost-benefit arguments to take place based upon sound engineering information and analysis.

Annex B
(informative)

Approach 6: Role-Reliability-Timeframe based approach

(formerly called the “Defence in depth approach”)

NOTE This Annex (formerly subclause 6.5 “Defence in depth approach” in Edition 1) provides some information on an approach that had been developed in The United States, but which has not been used as yet. While this clause has been replaced with an updated contribution in 8.6, the original clause has been preserved in this annex because it is used as a basis of comparison between two risk-based approaches in Cause 9.

B.1 General

The purpose of an effective classification scheme is to allow general requirements to be established for FSE. These requirements then contribute to the assurance that the given FSE will be available to perform its specified function for a specified period of time before, during or after a PIE. IEC 61226 only considers the function performed without regard to the required reliability of that function or the potential existence of other functions to offset the loss of a given function. A classification scheme that considers quantitative factors will allow the FSE to be more correctly placed in its relative place of importance to safety.

The classification scheme presented in this clause considers three factors, namely defence in depth, reliability and time.

Defence-in-depth: defence-in-depth has a basis in IAEA safety philosophy. While the IAEA concept of defence-in-depth has five echelons, only three echelons are considered for the I&C equipment, the others being associated with evacuation plans, etc. The echelons that will be used here are “prevention, termination and mitigation”.

Reliability: it is possible to establish a reliability target for every FSE. In doing this, the consequences of the loss of the function should be taken into consideration. Also, consideration of the existence of other features which may mitigate the loss of the function may reduce the reliability target for a given FSE. The target might be assigned as a result of a PSA study. For some functions, it may not be practical to determine a specific target number. Therefore, the targets are divided into three ranges. The boundaries between these ranges should be determined by the system designer and may vary from country to country, or even between nuclear power plants within a country. The following are given as an example and may be used for guidance.

High $<10^{-4}$ probability of failure on demand

Moderate 10^{-4} to 10^{-2} probability of failure on demand

Low $>10^{-2}$ probability of failure on demand

For continuous functions, failure on demand should be replaced by failures per unit of time. Furthermore, for certain safety functions, it is necessary to have very high reliability, in the order of 10^{-6} failures per demand. To achieve such very high reliability, it is generally considered necessary to provide multiple, diverse functions. Each of these functions would be placed in the high reliability target, and the independence between them evaluated to assure that the very high reliability goal is met. Reliability includes not only the quantitative elements such as redundancy, failure rate and test interval, but also the qualitative elements that give assurance to the quantitative number evaluated. Such qualitative elements include the independence and depth of the design verification, the qualification of the personnel involved in the design and maintenance of the FSE, the thoroughness of the quality assurance programmes of the organizations involved in the FSE, etc.

Time: time is also an important factor in the assurance of a function. For short action times, where human intervention is not possible, a higher degree of assurance for the automatic functions is necessary. For moderate action times, where the human operator, if provided with adequate means, may take preplanned actions from normal control stations, a lower dependence on the automatic functions can be taken. Finally, long action times, which allow for the planning and execution of alternative actions should the preplanned actions prove to be unavailable or ineffective will place the minimum reliance on any given FSE. Time is not necessarily measured from the beginning of the event. For instance, a precisely timed action may be required some hours or days after the initiating event. However, when that action is needed, there is no chance to recover from its failure. This may put the required action time in the shorter range.

B.2 The classification scheme

To perform this quantitative classification, the designer must first determine the defence-in-depth role for each FSE. Based on this role, one of the three groups, prevention, termination or mitigation can be selected, each of which is detailed in Tables B.1, B.2 and B.3 respectively.

Next, the reliability target should be determined to be in the high, moderate or low range. This target will be used for the horizontal axis of the selected grid.

Finally the time element required for action is determined for the vertical axis. Time elements are interpreted differently depending on the selected grid, as is explained below.

The intersection of the reliability target and time element in the selected grid will determine the safety category, i.e. A, B, C or NS, for that FSE.

a) Prevention group

FSE that prevent postulated initiating events include safety related interlocks and limitation functions. Also, control functions for normal operations whose failure would constitute a PIE are included. Functions which must respond to an upset in other equipment are assigned to the short action time group. Examples of such short times include the power reduction required following partial loss of normal feedwater. Control functions that normally regulate principal plant parameters are placed in the intermediate action time group. Finally, FSE whose purpose is to monitor the conditions of the plant to ensure that they are within the boundaries of the safety analysis assumptions are in the long action time group.

Presumably, if these monitoring functions were to fail, the operator would have a considerable length of time to re-establish the desired conditions. The grid for the prevention group of FSE follows in Table B.1.

Table B.1 – Prevention

Time element	Reliability target		
	High	Moderate	Low
Response to fault	A	B	C
Control failure	B	C	NS
Maintain pre-event conditions	C	NS	NS

b) Termination group

The termination group is the most familiar. It includes most of the classical safety system functions such as automatic reactor shutdown (scram), initiation of auxiliary feedwater and isolation of faulted lines. This grid has only two time element groups. For actions that must be carried out immediately on the detection of the PIE, the short action group is selected. Manual actions, if available to backup the automatic functions, will be in the longer action time group. The temporal dividing point between these groups is subject to the regulations of various countries. Many countries consider that operator action may not be taken for 30 min following an event. Note that given the uncertainty in establishing the reliability of human actions, no manual FSE are found in the high reliability target group.

Table B.2 – Termination

Time element	Reliability target		
	High	Moderate	Low
Automatic action	A	A	B
Human action	–	A	C

c) Mitigation group

Mitigation functions generally provide for the safety of the public for extended periods after a PIE. For FSE in this group, the short action times are for automatic functions or actions which must be precisely timed in relation to plant status or events. Intermediate action times are for those operator actions that can be conducted with the resources readily available. Longer action times reflect the possibility of planning and procuring the necessary resources to accomplish the function. These long actions may include the support of external organizations, such as the town fire brigade supplying additional water. The dividing point between intermediate and long term actions should be agreed with the country's regulatory authority. A value of 10 h is taken here as an indicative number. The grid for mitigate FSE is presented in Table B.3.

Table B.3 – Mitigation

Time element	Reliability target		
	High	Moderate	Low
Automatic action	A	B	C
Short term human action <10 h	–	B	NS
Long term human action >10 h	–	C	NS

B.3 Combining the results

A given function may play multiple roles in the defence in depth. For instance, it may prevent one postulated initiating event, but be required to terminate a different event. In such cases, the reliability and action time target ranges may be different for each role. The category should be determined for the various roles of the function, and then the highest category assigned to the function.

Once all functions have been assigned a category, they are collected into groups, and associated systems and equipment are allocated to perform the functions. The associated systems and equipment inherit the highest category of the functions that they perform. It may be possible for a given component within a system to have a lower category than the overall system, provided it can be demonstrated that sufficient independence is maintained so that failure of that component will not degrade the portions of the system that carry out the higher category functions. For example, communications equipment that reports the status of the reactor shutdown systems to the operator may be of a lower category than the reactor

shutdown systems themselves if adequate isolation is provided in the interface between the communications equipment and the safety system channels.

Bibliography

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

IEC 60812:2006, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

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

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

IEC 60987:2007, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*

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

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – UTILISATION DES ÉVALUATIONS PROBABILISTES DE SÛRETÉ POUR LE CLASSEMENT DES FONCTIONS

AVANT-PROPOS

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

La tâche principale des comités d'études de la CEI est l'élaboration des Normes internationales. Toutefois, un comité d'études peut proposer la publication d'un rapport technique lorsqu'il a réuni des données de nature différente de celles qui sont normalement publiées comme Normes internationales, cela pouvant comprendre, par exemple, des informations sur l'état de la technique.

La CEI 61838, qui est un rapport technique, a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Cette seconde édition annule et remplace la première édition parue en 2001.

Les principales modifications techniques par rapport à l'édition précédente sont les suivantes:

- Mettre à jour les références en prenant en compte les normes publiées depuis la sortie de la première édition.
- Mettre à jour la terminologie.
- Prendre en compte les progrès réalisés au niveau de l'utilisation des études probabilistes de sûreté depuis la première publication.

Le texte de ce rapport technique est issu des documents suivants:

Projet d'enquête	Rapport de vote
45A/766/DTR	45A/779A/RVC

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

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

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

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

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 du présent rapport technique

La CEI 61226 «Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – classification» – a été publiée en 1993 et révisée en 2005 et en 2009. La nécessité de classer les fonctions d'instrumentation et de contrôle-commande concernant des centrales nucléaires découle actuellement de l'exigence de l'Agence Internationale de l'Energie Atomique (AIEA) se trouvant dans le paragraphe 5.2 de la norme NS-R-1. La CEI 61226 insiste sur le fait que ce sont les fonctions qu'il faut classer à un stade précoce de la phase de conception afin que le degré d'importance au niveau de la sûreté de chaque fonction soit précisé. Au stade de la conception, les fonctions de contrôle-commande (I&C) sont allouées à des systèmes d'instrumentation et de contrôle-commande particuliers, et chacun de ces systèmes comprend normalement plusieurs types de matériels. Ces systèmes et matériels sont généralement attribués à des classes prenant en compte l'importance de sûreté associée aux fonctions attribuées à chaque système (conformément à la CEI 61513), mais ce sont les fonctions qui restent déterminantes pour la catégorisation. Le guide AIEA NS-G-1.14, en préparation, étend le concept de la catégorisation d'une fonction et attribue cette catégorie à toutes structures, systèmes ou composants (SCCs) qui supportent la fonction.

Afin de pouvoir associer les systèmes et les matériels aux fonctions, le concept de FSE a été introduit dans la CEI 61226. Les FSE sont définis comme:

> Les fonctions et les systèmes et matériels associés. Les fonctions sont des actions qui sont effectuées dans un but ou pour atteindre un objectif. Les systèmes et matériels associés sont un assemblage de composants et les composants eux-mêmes qui sont employés pour remplir la fonction.

La CEI 61226 fournit une méthode de catégorisation des FSE basée sur des critères qualitatifs associés au rôle. Un grand nombre de ces critères sont utilisés couramment dans l'industrie nucléaire dans la mesure où ils reconnaissent que la plus importante fonction de la sûreté nucléaire et la seule est de prévenir les accidents et d'en réduire les conséquences radiologiques. En conséquence, le classement des FSE, au sens de la CEI 61226 édition 3 est un processus déterministe qui prend peu en considération les techniques d'évaluation quantitative des risques.

Au cours des dix dernières années, les méthodes d'évaluation des risques, en particulier celles appliquées aux centrales nucléaires, se sont améliorées, bien que leur utilisation dans la conception des centrales nucléaires (ainsi qu'au niveau des demandes d'autorisation) soit très variable dans le monde. Dans certains pays, l'évaluation probabiliste des risques est considérée comme un élément essentiel du processus de conception et constitue l'acte final de sûreté; cela n'est pas le cas dans d'autres pays.

Les publications en 2000 du document AIEA NS-R-1 et en 2002 du document NS-G-1.3 ont mis l'accent sur la nécessité de prendre en compte au niveau du processus de catégorisation l'évaluation d'expert en matière de facteurs humains et les critères probabilistes. Pendant plusieurs années, il a été débattu de la manière dont une méthode de classement basée sur l'évaluation des risques pourrait être incorporée dans la CEI 61226 pour satisfaire à cette exigence. Comme indiqué précédemment, il existe des différences importantes dans l'utilisation des évaluations de risques dans le monde, ce qui soulève certaines questions pour le développement d'une Norme internationale, notamment:

1) Une méthode de classement basée sur l'évaluation des risques serait-elle acceptable en remplacement de l'approche déterministe? Si oui, quelles sont les exigences qu'il faut appliquer (en particulier concernant la norme relative à la modélisation et la validité des données)?

2) Si un classement basé sur l'évaluation des risques produit des classements de FSE différents de ceux obtenus par l'approche déterministe, laquelle des deux approches devrait être prépondérante?

3) Les deux approches doivent-elles être utilisées ensemble afin d'en retirer un bénéfice maximal? L'approche déterministe est basée sur des principes de sûreté nucléaire solides et parfaitement éprouvés, communs et admis par tous. Les résultats d'une méthode basée sur l'évaluation des risques pourraient engendrer le sur-classement ou le sous-classement de fonctions de I&C spécifiques (en raison des caractéristiques de conception spécifiques à l'installation). Comment limiter ce sur-classement ou ce sous-classement?

4) L'utilisation de l'évaluation des risques devrait-elle être rendue obligatoire en tenant compte de la robustesse de l'installation et des modifications de I&C pendant toute la durée de vie de l'installation ? D'une manière similaire, des exigences devraient-elles être incluses pour l'utilisation de l'évaluation des risques dans les prises de décisions concernant la maintenance préventive?

5) Comment doit on aborder le classement pour des installations dont la conception est novatrice et pour lesquelles le schéma de classement actuel de la CEI 61226 reposant sur les rôles n'est pas adapté, et comment le classement lié à des centrales nucléaires particulières peut être étendu à d'autres centrales nucléaires, telles que des réacteurs de faible puissance utilisés pour la recherche ou pour la production d'isotopes, des installations conçues pour manipuler des isotopes dont le niveau de radioactivité est élevé, des installations de fabrication de combustible nucléaire et de retraitement du combustible usagé ?

La révision de ce rapport technique a été faite en prenant en compte les publications de l'AIEA NS-R-1 et NS-G-1.3, qui exigent que le classement soit réalisé sur la base de méthodes déterministes qui sont complétées le cas échéant par le jugement de l'ingénieur et des considérations liées à l'évaluation des risques. La formulation précise du paragraphe 5.2 du document NS-R-1 ainsi que la liste des critères devant être pris en compte (développée dans le paragraphe 2.38 du document NS-G-1.3) mettent l'accent sur l'importance de ces derniers critères. Il est parfaitement clair que la prise en compte du jugement de l'ingénieur et des critères liés à l'évaluation des risques est une exigence, sauf si on peut montrer que cela n'est pas pertinent. Le paragraphe 3.4 appuie cette conclusion en exigeant que le responsable de la conception « *doit prendre en compte les résultats des analyses de sûreté déterministes et des analyses de sûreté probabilistes complémentaires* ». Le document de l'AIEA NS-G-1.14 met encore plus l'accent sur ce point en prônant l'adoption d'une approche équilibrée entre les méthodes déterministes et probabilistes.

Cette exigence, d'intégration des considérations liées à l'évaluation des risques dans le processus de classement (sauf si cela n'est pas pertinent), est d'une telle importance pour ce qui concerne le choix d'une méthode de classement que les paragraphes applicables du NS-G-1.3 sont reproduits ci-dessous (noter que le paragraphe 2.37 du document NS-G-1.3 est une citation fidèle du paragraphe 5.2 du document NS-R-1[1]):

> 2.37. En particulier, les exigences relatives à la conception exigent (Ref. [NS-R-1], para. 5.2) que la méthode de classement de l'importance pour la sûreté d'une structure, d'un système ou d'un composant soit principalement basée sur des méthodes déterministes, complétées le cas échéant par des méthodes probabilistes et un jugement technique et qu'il soit tenu compte de facteurs tels que:
>
> - La ou les fonctions de sûreté à remplir;
> - Les conséquences d'une défaillance du système d'I&C;
> - La probabilité pour le système d'I&C d'être sollicité pour accomplir une fonction de sûreté;
> - A la suite d'un EIP, le moment où le système d'I&C sera sollicité ou la

[1] Reproduit avec l'autorisation de l'AIEA.

période pendant laquelle il devra fonctionner.

2.38. Dans la méthode de classement, outre la prise en considération des facteurs susmentionnés, comme exigé dans le document NS-R-1, les facteurs suivants devraient également être pris en compte lors de la détermination de la classe du système d'I&C. Les critères, comme indiqué pour les facteurs suivants à titre d'exemple, devraient être choisis de manière à fournir une indication quantitative et/ou qualitative de l'importance relative pour la sûreté du système d'I&C en cours de classement:

- la probabilité des EIP et la gravité potentielle de leurs conséquences si le système d'I&C utilisé tombe en panne (par exemple, probabilité forte, moyenne ou faible avec des conséquences importantes, moyennes ou faibles (conséquences radiologiques par exemple));.
- le potentiel du système d'I&C à causer lui-même un EIP (c'est à dire les modes de défaillances du système d'I&C), les mesures prises pour les systèmes de sûreté ou pour d'autres systèmes d'I&C traités dans le présent guide de sûreté dans le cas d'un EIP de ce type (c'est à dire les mesures prises pour la détection d'une défaillance du système d'I&C) et la combinaison de la probabilité et des conséquences de cet EIP (c'est à dire la fréquence de défaillance et les conséquences radiologiques);
- la durée pendant laquelle le système est nécessaire après le déclenchement de la fonction de sûreté (par exemple, 12 heures maximum ou supérieure à 12 heures);
- la promptitude et la fiabilité avec lesquelles d'autres actions peuvent être mises en oeuvre (par exemple, immédiatement/fiabilité faible, au-delà de 30 minutes/fiabilité élevée);
- la promptitude (par exemple, 12 heures maximum, plus de 12 heures) et la fiabilité avec lesquelles une défaillance du système d'I&C peut être détectée et corrigée.

L'objectif de ce rapport est donc d'aider la communauté à atteindre un certain consensus au niveau d'une approche hybride de classement. Une telle approche pourrait éventuellement comporter un cadre de travail dans lequel les fonctions de sûreté fondamentales de dernier ressort pourraient être identifiées principalement sur des bases déterministes (et probablement être classées en catégorie A) alors que les fonctions primaires fonctionnant en continu qui maintiennent l'installation à pleine puissance nominale pourraient sûrement être classées en catégorie C. En conséquence, toutes les fonctions opérationnelles de l'installation, et en particulier celles qui devraient être classées en catégorie B, pourraient être classées en utilisant des méthodologies hybrides adaptées à la conception de l'installation et à l'approche d'autorisation nationale des états membre.

En 2001, la grande difficulté que représentait le développement d'un amendement à la CEI 61226 avait été identifiée. Pour faire progresser le débat, la première édition de ce rapport avait présenté un nombre d'approches différentes pour appliquer les critères associés au temps et à l'évaluation des risques pour le classement des FSE. Depuis lors, l'augmentation de l'utilisation des techniques d'EPS et en particulier la publication du document AIEA NS-R-1 et maintenant le développent du nouveau document AIEA NS-G-1.14 justifient la révision de ce rapport technique. Ainsi, ce rapport aborde le problème de l'équilibre des approches liées à l'évaluation des risques qualitative et quantitative, et il présente les détails des méthodologies quantitatives que l'on peut utiliser.

b) Position du présent rapport technique dans la collection de normes du SC 45A de la CEI

La CEI 61838, en tant que rapport technique, est un document du SC 45A de la CEI de quatrième niveau.

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

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

Il est important de noter qu'un rapport technique est par nature entièrement informatif. Il rassemble des données collectées à partir de différentes origines et il n'établit aucune exigence.

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

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

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

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

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

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

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

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

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – UTILISATION DES ÉVALUATIONS PROBABILISTES DE SÛRETÉ POUR LE CLASSEMENT DES FONCTIONS

1 Domaine d'application

Le présent rapport technique étudie différentes méthodes permettant d'utiliser les résultats des évaluations probabilistes des risques afin d'établir des critères de classement basés sur l'évaluation du risque, dans le but de pouvoir classer les FSE dans les quatre catégories établies par la CEI 61226.

L'utilisation des techniques de classement (catégorisation) à base d'évaluation des risques, conjointement avec l'approche de classement déterministe basée sur les rôles décrits dans la CEI 61226 édition 3, continuera à relever d'une décision des électriciens et/ou des organismes de réglementation au sein des Nations concernées. Néanmoins, il est attendu que ces approches prennent en compte les approches reconnues au niveau international telles que celles indiquées dans les normes et les guides de l'AIEA. Cependant, celles-ci sont essentiellement de haut niveau et pour les systèmes d'I&C l'AIEA laisse le soin au SC 45A de la CEI de déterminer les approches détaillées appropriées et de les identifier dans ses normes. Le niveau de consensus augmente pour ce qui est des sujets liés au classement, néanmoins du chemin reste encore à parcourir. La première édition de ce rapport technique publiée en 2001 a aidé à réviser la CEI 61226 publiée en 2005. L'objectif de la révision de la CEI 61838 était de stimuler le débat et d'encourager les convergences de vue pour que la révision suivante de la CEI 61226 puisse faire l'objet d'un accord et prendre en compte les dernières recommandations de l'AIEA, à savoir considérer explicitement les aspects liés à l'évaluation des risques et aux limites de temps de réponse.

Les principes de sûreté et l'utilité d'une approche d'évaluation des risques pour le classement sont discutés et la description de quatre approches différentes est présentée. Deux de ces approches sont utilisées sur des exemples pratiques et les résultats sont comparés pour évaluer la robustesse et le caractère généraliste des approches de l'évaluation des risques.

Il est par ailleurs fait référence dans ce rapport à des documents CEI et AIEA qui traitent du même sujet.

Ce rapport traite aussi des limites associées à l'utilisation exclusive des approches d'évaluation des risques ou bien à l'utilisation exclusive des approches basées sur les rôles, qui sont toutes deux incompatibles avec les recommandations qui vont être bientôt établies par le document AIEA NS-G-1.14.

2 Références normatives

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

CEI 60709:2004, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle importants pour la sûreté – Séparation*

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

CEI 61226:2009, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*

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

CEI 62138:2004, *Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

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

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

IAEA NS-G-1.14, *Safety Guide: Safety Classification of Structures, Systems and Components Important to Safety Important to Safety in Nuclear Power Plants (projet disponible en anglais seulement)*

INSAG-10: 1997, *La défense en profondeur en sûreté nucléaire*

INSAG-12: *Principes de sûreté des centrales nucléaires* 75-INSAG-3, Rev. 1

Glossaire de sûreté de l'AIEA, édition 2007

3 Termes et définitions

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

3.1
diversité
présence de plusieurs systèmes ou composants redondants pour l'accomplissement d'une fonction déterminée, lorsque ces différents systèmes ou composants possèdent des attributs différents afin de réduire le risque de défaillance de cause commune, y compris de défaillance de mode commun

[Glossaire de sûreté de l'AIEA, édition 2007]

3.2
matériel (équipement)
une ou plusieurs parties d'un système. Un matériel est un élément unique, identifiable (et généralement amovible) ou une partie d'un système

[CEI 61513]

3.3
fonction
but précis ou objectif devant être accompli, qui peut être spécifié ou décrit sans référence aux moyens physiques nécessaires pour son atteinte

[CEI 61226]

3.4
fonctionnalité
attribut d'une fonction définissant les opérations de transformation des informations d'entrée en information de sortie

[CEI 61513]

3.5
FSE d'I&C: fonctions, et systèmes et matériels associés
les fonctions sont réalisées dans le cadre d'une mission ou pour atteindre un objectif. Les systèmes et les matériels associés sont l'ensemble des composants et les composants eux-mêmes qui sont utilisés pour réaliser ces fonctions

[CEI 61513]

3.6
constituant important pour la sûreté
constituant faisant partie d'un groupe de sûreté et/ou dont le mauvais fonctionnement ou la défaillance pourrait entraîner une exposition à des rayonnements du personnel du site ou de personnes du public.

Les constituants importants pour la sûreté comprennent:

a) les structures, systèmes et composants dont le mauvais fonctionnement ou la défaillance pourraient entraîner une exposition indue à des rayonnements du personnel du site ou de personnes du public;

b) les structures, systèmes et composants qui empêchent les incidents de fonctionnement prévus d'aboutir à des conditions accidentelles;

c) les dispositifs prévus pour atténuer les conséquences d'un mauvais fonctionnement ou d'une défaillance de structures, systèmes ou composants.

[Glossaire de sûreté de l'AIEA, édition 2007]

NOTE 1 Dans ce rapport technique, les constituant considérés sont principalement des FSE d'I&C.

NOTE 2 La définition précédente "d'important pour la sûreté" fait référence en même temps aux systèmes et fonctions qui sont conçus explicitement pour assurer une fonction de sûreté (points b et c) et aux systèmes dont la défaillance pourrait entraîner la sollicitation d'une autre fonction (point a). Ce qui est différent de la définition du qualificatif « relatif à la sûreté » de la CEI 61508 qui est applicable seulement aux systèmes et fonctions conçus explicitement pour assurer une fonction de sûreté (points b et c).

3.7
sûreté nucléaire
obtention de conditions d'exploitation correctes, prévention des accidents ou atténuation de leurs conséquences, avec pour résultat la protection des travailleurs, du public et de l'environnement contre les risques radiologiques indus

[Glossaire de sûreté de l'AIEA, édition 2007]

3.8
performance
efficacité avec laquelle une fonction prévue est exécutée (par exemple temps de réponse, précision, sensibilité aux variations de paramètres)

[CEI 61226]

3.9
événement initiateur postulé, EIP
évènement dont on détermine au stade de la conception qu'il peut entraîner des incidents de fonctionnement prévus ou des conditions accidentelles

[Glossaire de sûreté de l'AIEA, édition 2007]

3.10
redondance
mise en place de structures, systèmes ou composants (identiques ou différents) supplémentaires, afin qu'un élément quelconque puisse remplir la fonction requise indépendamment de l'état de fonctionnement ou de défaillance d'un autre élément

[Glossaire de sûreté de l'AIEA, édition 2007]

3.11
catégorisation basée sur l'évaluation des risques
approche de catégorisation basée sur l'importance de la fonction objet de la catégorisation pour la sûreté (à savoir le niveau de risque éliminé par la fonction).

NOTE Cette approche oblige à réaliser en même temps l'analyse des conséquences éliminées ou réduites par la fonction et la fiabilité qui est demandée pour cette fonction au niveau de l'analyse de sûreté de l'installation. L'expression "catégorisation probabiliste" est souvent employée de façon abusive pour désigner cette approche. Une limitation de cette approche correspond au fait qu'elle oblige à réaliser une analyse lourde avant que l'on puisse mener à terme la catégorisation.

3.12
catégorisation basée sur le rôle fonctionnel
approche de catégorisation déterministe basée exclusivement sur le rôle de la fonction objet de la catégorisation. Celle-ci comprend habituellement la sélection du rôle prépondérant à partir d'une liste de rôles liée à chaque catégorie, telle qu'indiquée en 5.4 de la CEI 61226 édition 3. La liste des rôles associée à chaque catégorie est constituée de façon déterministe, en fonction de critères non-quantitatifs liés à l'importance des fonctions pour la sûreté.

NOTE Une limitation de cette approche correspond au fait qu'elle n'assure pas une approche systématique pour les fonctions qui ne correspondent pas exactement à celles de la liste fournie.

3.13
fonction de sûreté
but particulier à atteindre aux fins de la sûreté

[Glossaire de sûreté de l'AIEA, édition 2007]

3.14
système de sûreté
système important pour la sûreté destiné à garantir la mise à l'arrêt sûre du réacteur ou l'évacuation de la chaleur résiduelle du cœur, ou à limiter les conséquences des incidents de fonctionnement prévus et des accidents de dimensionnement

[Glossaire de sûreté de l'AIEA, édition 2007]

3.15
séquence significative
série ou ensemble d'évènements crédibles qui entraînerait des conséquences inacceptables telles que:

- rejet radioactif inacceptable sur le site ou au-delà dans l'environnement. Ceci peut être ou bien un rejet incontrôlé important à une fréquence située en dehors des limites de conception de l'installation, ou des rejets à une fréquence se situant dans les limites de conception de l'installation mais qui dépassent les limites d'amplitude et/ou de fréquence spécifiées;
- endommagement du combustible inacceptable. Ceci peut être un endommagement des gaines qui conduit à une augmentation inacceptable de l'activité du fluide primaire, ou un endommagement structurel du combustible qui limite les possibilités de le refroidir.

3.16
critère de défaillance unique
critère (ou contrainte) appliqué à un système, en vertu duquel ce dernier doit être capable de remplir sa (ses) fonctions en cas de défaillance unique

[Glossaire de sûreté de l'AIEA, édition 2007]

3.17
système
ensemble de composants interagissant suivant la conception, où un élément de ce système peut être considéré comme un autre système, appelé sous-système.

[CEI 61513]

3.18
indisponibilité
durée pendant laquelle un système ou un composant n'est pas capable d'assurer sa fonction

NOTE L'indisponibilité peut être la conséquence de la réparation d'un élément, de la détection d'un disfonctionnement, d'essai, ou bien elle peut être la conséquence d'un disfonctionnement non détecté.

4 Abréviations

ALARP	Aussi faible que pratiquement possible
DCC	Défaillance de Cause Commune
CDD	Conditions De Dimensionnement
ECD	Extension des Conditions de Dimensionnement
QE	Qualification aux conditions d'Environnement
FSE	Fonction(s) et systèmes et équipements associés qui la mettent en oeuvre
AMDE	Analyse des Modes de Défaillance et de leurs Effets
I&C	Instrumentation et contrôle commande
AIEA	Agence Internationale de l'Energie Atomique
CNPE	Centrale Nucléaire de Production d'Electricité
EIP	Evènement Initiateur Postulé
EPS	Etudes Probabilistes de Sûreté
AQ	Assurance Qualité
CDU	Critère de Défaillance Unique
QS	Qualification aux Séismes
V&V	Vérification et Validation
/ar	par année réacteur
/a	par an

5 Limitations correspondant à l'utilisation exclusive d'une des approches

5.1 Généralités

Les exigences du paragraphe 5.2 du document NS-R-1 de l'AIEA sont claires en ce qui concerne l'utilisation équilibrée à faire des méthodes déterministes et des méthodes basées sur l'évaluation des risques (ou méthodes probabilistes), de plus le projet de guide NS-G-1.14 met encore l'accent sur l'importance d'une méthodologie équilibrée. Pour développer cette idée, le présent article considère les limites associées aux tentatives d'approche de la question de la catégorisation sur la base exclusive d'une approche déterministe basée sur le rôle fonctionnel ou sur celle exclusive basée sur l'évaluation des risques.

5.2 Limitations correspondant à l'utilisation exclusive d'une approche liée aux EPS

L'utilisation des techniques d'évaluation probabiliste des risques permet d'obtenir des informations qui peuvent conduire à des décisions plus avisées ainsi qu'à un usage plus rentable et plus efficace des ressources afin d'améliorer la sûreté des centrales nucléaires. L'atteinte d'un consensus au niveau d'une norme internationale pour ce qui concerne l'utilisation des EPS dans la conception et comme support à l'exploitation des centrales nucléaires a cependant été limité en raison de plusieurs facteurs:

- le développement et l'utilisation des techniques d'évaluation probabiliste des risques continuent à évoluer au sein des états membres et leur niveau d'acceptation et leur niveau d'application dans le monde n'est pas cohérent;
- l'application des techniques d'évaluation probabiliste des risques en tant qu'outil de classement dans la conception d'une centrale nucléaire exige la réalisation d'EPS au stade précoce de la phase de conception. La réalisation d'une telle évaluation détaillée à ce stade n'est pas courante, d'une part en raison des modifications apportées à la conception et d'autre part en raison du manque de données quantitatives à ce premier stade.

Par ailleurs, même lorsque les EPS sont appliquées à une installation existante, l'analyse fait souvent l'objet de limites technologiques qui empêchent la réalisation de l'examen de cette installation en utilisant exclusivement les données probabilistes. Cela est dû au fait que les EPS peuvent ne pas être suffisamment précises et exhaustives. Ces limites résultent:

- des difficultés liées à la modélisation et à la quantification des défaillances de cause commune, des erreurs de logiciel et des erreurs humaines,
- du manque ou de l'indisponibilité d'informations spécifiques à l'installation,
- des limites dans la définition du niveau des EPS effectuées,
- de l'exclusion de certains événements initiateurs potentiels (par exemple incendies, inondations, séismes),
- d'une bonne connaissance des incertitudes.

A la lumière de ces éléments, on doit faire attention lors des prises de décision, comme par exemple pour ajouter une nouvelle fonction liée à la sûreté au niveau conception de l'installation et pour définir les exigences de fiabilité pour les fonctions de sûreté et celles liées à la sûreté. Ces éléments sont légèrement moins critiques pour ce qui est du processus de catégorisation car la catégorie ne devrait être sensible qu'à l'ordre de magnitude de la fiabilité demandée et non pas à sa valeur précise. Ceci est du au fait qu'une catégorie n'établit pas d'exigences fonctionnelles ou de qualification (sismique ou pour l'environnement) ou de fiabilité, elle détermine seulement le caractère rigoureux associé au processus de conception ou aux autres étapes du cycle de vie, ainsi l'objectif en est de garantir le niveau d'assurance approprié que devront satisfaire les exigences fonctionnelles et autres. Néanmoins un conservatisme approprié doit être de mise.

Pour toutes ces raisons (et naturellement du fait des exigences du document AIEA NS-R-1 imposant d'utiliser aussi des méthodes déterministes), l'utilisation des EPS, comme seule base pour la conception et le classement des fonctions de sûreté associées au I&C, n'est pas réaliste. Malgré ces limites, les EPS sont de toute évidence précieuses lorsqu'elles sont utilisées conjointement avec l'approche qualitative basée sur le principe de la défense en profondeur qui reste la base de conception de la sûreté des centrales nucléaires (voir les paragraphes 4.1 et 4.2 du document AIEA NS-R-1). Lorsque les EPS sont utilisées pendant la phase initiale de conception des futures centrales nucléaires ou pour le réexamen de sûreté des installations existantes, il convient de les utiliser en tant que complément de la méthode qualitative.

5.3 Limitations correspondant à l'utilisation exclusive d'une approche basée sur le rôle fonctionnel

L'utilisation d'un schéma de classement déterministe basé sur le rôle fonctionnel contient en lui-même la limitation de toute liste fixe: elle ne peut couvrir que les fonctions de sûreté liées aux conceptions faisant partie de la base de connaissance de ceux qui ont préparé la liste, et il est improbable que cette liste couvre toutes les caractéristiques des conceptions des installations novatrices et même d'installations existantes. Ceci est clairement mis en exergue par le paragraphe 2.4 du projet de document AIEA NS-G-1.14. Par exemple, considérons les facteurs de temps, les conséquences, et la réduction des risques:

- Une fonction de sûreté peut être classée en catégorie B suivant les critères fournis en 5.4.2 de la CEI 61226, par contre si dans certaines circonstances celle-ci doit intervenir ou être redondée manuellement en cas de défaillance dans un laps de temps très court, alors on ne peut prendre en compte l'action opérateur et il convient que la fonction soit être reclassée en catégorie A.
- Pour les réacteurs passifs, le système d'arrêt de sûreté, qui devrait être classé en catégorie A suivant 5.4.1 de la CEI 61226, dont les conséquence de la défaillance pourraient être négligeables, contredit certainement la définition actuelle de la catégorie A.
- Pour les conceptions d'installation pour lesquelles la fiabilité requise (pour satisfaire aux objectifs des EPS) joue sur la catégorie, certaines fonctions qui devraient être en catégorie C du fait des critères e) ou f) de 5.4.3 de la CEI 61226 édition 3, peuvent nécessiter une fiabilité supérieure à celle associée à la catégorie C. La fonction de repli (critère e) mise en œuvre dans de nombreuses conceptions en est un exemple (voir l'exemple de travail présenté en 9.1).
- Les rôles fonctionnels qui peuvent être (ou avoir été) affectés suivant un schéma basé sur les rôles fonctionnels et sur le retour d'expérience de conceptions existantes ne peuvent pas garantir qu'ils sont adaptés à la conception d'un nouveau réacteur. Ceci a été mis en évidence dans le projet du document AIEA NS-G-1.14 au paragraphe 2.4.

Ces points sont conformes à la liste fournie au paragraphe 5.2 du document AIEA NS-R-1 et doivent être pris en compte par les concepteurs. Cette liste, telle que celle en particulier développée dans le paragraphe 2.38 du document AIEA NS-G-1.3, est simplement trop longue et nécessite de considérer des détails propres à l'installation pour être prise en compte de façon pratique dans un schéma basé sur les rôles fonctionnels: le jugement de l'ingénieur et une approche telle que les arbres de défaillance sont nécessaires pour terminer le classement.

6 Questions ouvertes concernant la catégorisation

6.1 Généralités

Il n'est pas encore possible d'atteindre l'unanimité au niveau de la communauté internationale sur plusieurs sujets, bien que des progrès très importants aient été faits. Cet article a pour objectif de mettre en lumière ces sujets pour lesquels le débat est ouvert, et de rapprocher au final les points de vue. Celle-ci traite des points suivants:

a) La catégorisation détermine-t-elle les exigences ou les exigences sont-elles déterminées par la catégorisation?

b) Jusqu'à quel point les méthodes probabilistes ou basées sur l'évaluation des risques sont-elles déjà implicitement utilisées?

c) Quelle précision doivent avoir les EPS?

6.2 La catégorisation détermine-t-elle les exigences ou les exigences sont-elles déterminées par la catégorisation?

Une revue portant sur la façon de réaliser la catégorisation dans plusieurs états membre a mis à jour des philosophies de catégorisation divergentes, et a entraîné la formulation de la question suivante:

> La catégorisation détermine-t-elle les exigences ou les exigences sont elles déterminées par la catégorisation?

Le document de l'AIEA NS-R-1 exige le 'classement'[2] des structures, des systèmes[2] et des composants, par contre les recommandations portant sur le pourquoi donne lieu à interprétation. Le paragraphe 5.1 de cette norme indique:

> 5.1. Toutes les structures et tous les systèmes et composants, y compris les logiciels pour le contrôle commande, qui sont des constituants importants pour la sûreté, doivent d'abord être déterminés, puis classés selon leur fonction et leur importance pour la sûreté. Ils doivent être conçus, construits et entretenus de telle manière que leur qualité et leur fiabilité soient conformes à cette classification.

Cette formulation suggère que:

– Premièrement: les exigences fonctionnelles et le niveau d'élimination/réduction du risque (à savoir l'importance pour la sûreté) détermine la catégorie ou la classification, et que

– Deuxièmement: il convient que la catégorie détermine le niveau d'assurance qualité et l'assurance dans la conception qui devraient être demandées pour garantir que la structure, le système ou le composant soit conçu pour satisfaire à ses exigences fonctionnelles (y compris la robustesse en présence de conditions accidentelles). Plus la catégorie est élevée, plus l'assurance que les exigences fonctionnelles soient satisfaites doit être élevée.

Il serait entièrement cohérent d'interpréter, avec ce qui précède, la seconde phrase du document NS-R-1 dans le sens obligeant à appliquer des exigences d'assurance fonctionnelle supplémentaires adaptées à la catégorie. (Les exigences d'assurance fonctionnelle sont des exigences supplémentaires qui sont applicables à la mise en œuvre de la fonction et qui réduise la probabilité d'avoir des défaillances systématiques (conception) et/ou des défaillances aléatoires matériel. Des exemples en sont la redondance, les auto-tests logiciel et l'utilisation de chien de garde matériel dans les systèmes programmables.)

C'est à ce niveau que l'Article 7 de la CEI 61226 semble se positionner dans les étapes du processus de conception, bien qu'aucune distinction n'y soit faite entre les exigences fonctionnelles de base et les exigences d'assurance fonctionnelle. Dans ce paragraphe 7 de la CEI 61226, on suppose que la catégorie est déjà choisie, et qu'ainsi elle serve à définir des objectifs de fiabilité à satisfaire et dans certains cas particuliers des exigences d'assurance fonctionnelle telle que la redondance des alimentations électriques (la catégorie détermine les exigences). Ceci n'est pas important en pratique, étant donné que la catégorie a d'abord été déterminée sur la base des facteurs fondamentaux exigés par le document AIEA NS-R-1, voir le paragraphe 5.2:

a) la sûreté de la (des) fonction(s) devant être réalisée(s) par l'équipement;

b) les conséquences de la défaillance des équipements au niveau de la réalisation de sa fonction;

---

2 La CEI 61226 et la CEI 61513 clarifient l'emploi des termes "catégorie" et "classe" (et respectivement les verbes) ainsi que leurs utilisations respectives aux fonctions et aux systèmes. On catégorise les fonctions , qui sont alors mises en œuvre dans des systèmes qui doivent être suffisamment classés pour accueillir les fonctions. Voir en particulier 5.3.1.1. de la CEI 61513.

c) la probabilité que les équipements soient requis pour assurer une fonction de sûreté;

d) l'instant ou la période pour lequel les équipements seront requis pour fonctionner.

Ici par exemple, la fiabilité requise pour une fonction peut définir sa catégorie en A, et cette fiabilité requise imposera aussi les caractéristiques de redondance et d'indépendance pour ses alimentations électriques.

Sans aucun doute, l'assurance qualité a une influence sur la fiabilité, de la même façon que la fiabilité requise a une influence sur les procédures d'assurance qualité qui devront être appliquées lors de la conception, en exploitation et lors de la maintenance de la fonction. De plus, en pratique, il est impossible de concevoir un grand nombre de fonctions et de systèmes d'un bloc par rapport à un ensemble compact d'exigences fonctionnelles, d'assurance fonctionnelle et de qualité, c'est pourquoi ce bloc est scindé en 3 catégories. Ceci est en même temps pratique et favorable à la sûreté car cela normalise les exigences d'assurance fonctionnelle, telles que celles d'indépendance entre catégories ou entre voies, de redondance, de critère de défaillance unique ou d'autres attributs, par rapport aux catégories. En effet cette pratique communément répandue apparaît dans différentes normes.

En conséquence on a encore largement matière à débattre pour déterminer si les exigences déterminent la catégorie ou si la catégorie détermine les exigences. Une partie du débat tourne autour du manque de distinction claire entre les exigences fonctionnelles et celles d'assurance fonctionnelle.

Ceci amène à l'interprétation suivante:

a) les exigences fonctionnelles de base (à savoir celles s'appliquant dans le cadre de l'analyse de sûreté) déterminent la catégorie,

b) la catégorie détermine les exigences d'assurance fonctionnelle.

Alors que cette interprétation est communément répandue, il n'est pas certain qu'elle soit unanimement acceptée.

A la lumière des éléments ci-dessus, les participants à la préparation de la CEI 61838 ont discuté de cette interprétation, des raisons sous-jacentes amenant à la catégorisation, et ils ont ordonné ces raisons en fonction de leur importance (en ordre décroissant), tel qu'indiqué ci-dessous. Le premier élément de la liste a fait l'objet d'un accord unanime, pour le reste il y a eu un accord en général et il a eu peu de différends portant sur l'ordre de la liste.

- Fournir un niveau d'assurance approprié sur le fait que les exigences (fonctionnelle, fiabilité, qualification à l'environnement, qualification sismique) sont satisfaites, ceci sur la base de l'importance des fonctions pour la sûreté. Ce qui implique un niveau approprié d'AQ, d'indépendance de V&V, et d'exigences d'assurance fonctionnelle, etc.
- Préserver les propriétés de conception originales durant la durée de vie de l'installation, et ceci en prenant en compte les modifications et la maintenance, et d'éventuels remplacements de matériel par d'autres de capacité équivalente.
- Comprendre l'importance de la fonction pour la sûreté et le choix de matériel fait pour la réalisation de la fonction (l'inverse est aussi vrai).
- Identifier le matériel pour lequel les opérateurs doivent suivre des procédures appropriées qui sont plus détaillées que pour des systèmes de catégories inférieures.
- Assurer une planification long terme établissant des recommandations pour la maintenance afin de préserver les propriétés de conception originales.
- Optimiser en matière de coût et d'efficacité (pour que l'argent et les efforts soient dépensés sur les fonctions les plus importantes pour la sûreté).
- Etablir des exigences pour conserver de façon appropriée les enregistrements d'historiques.
- Faciliter la conception des barrière de défense.

- Satisfaire aux prescriptions légales dans le cas de l'approche ALARP (au R.U.)

6.3 Jusqu'à quel point les méthodes probabilistes ou basées sur l'évaluation des risques sont-elles déjà implicitement utilisées?

Alors que la catégorisation, réalisée par quelques états membres (en particulier le Canada et le Royaume-Uni) est basée sur l'évaluation des risques, la catégorisation est réalisée par la plupart des autres états membres principalement sur une base déterministe en suivant l'Article 5 de la CEI 61226.

Néanmoins, le paragraphe 5 de la CEI 61226 fait état explicitement de certaines considérations probabilistes, et même demande que les méthodes déterministes prennent en compte à un certain niveau des considérations probabilistes, comme cela est illustré par les 3 points suivants:

CEI 61226, 5.4.2 – Catégorie B

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

CEI 61226, 5.4.3 – Catégorie C

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

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

Considérations probabilistes apparaissant au niveau des méthodes déterministes

Même dans les états membre qui demandent l'application de méthodologies purement déterministe, certains éléments liés aux probabilités ou à l'évaluation des risques apparaissent pour confirmer la conception à certains niveaux. Par exemple, selon une de ces méthodologies si une EPS montre que certaines séquences d'évènements sont des contributeurs inacceptables au niveau du risque global d'endommagement du cœur, une nouvelle fonction peut être ajoutée à l'installation. Dans ces cas là, la nouvelle fonction peut être de catégorie C si la séquence d'événements comprend deux défaillances ou plus, mais elle sera probablement de catégorie A si seulement une défaillance est identifiée dans la séquence. Ceci est une reconnaissance implicite du fait que la fréquence de sollicitation de la nouvelle fonction a une influence sur sa catégorisation.

6.4 Quelle précision doivent avoir les EPS?

Une des interrogations formulées a propos de l'utilisation des approches basées sur l'évaluation des risques concerne la sensibilité des résultats des EPS aux erreurs et incertitudes portant sur les données relatives aux taux de défaillance. Ce paragraphe fournit quelques pistes proposées par les membres des états où les résultats d'EPS sont utilisés pour la catégorisation.

On note que lorsqu'on détermine la catégorie d'une nouvelle fonction de façon probabiliste, en utilisant les résultats des EPS, par définition la nouvelle fonction est exclue de la séquence d'évènements de façon à mettre en évidence la fiabilité qui sera requise.

- On considère premièrement que même dans le cas d'une méthodologie basée sur l'évaluation des risques, le spectre de fiabilité est dans les faits discrétisé d'une puissance de 10 d'une catégorie à la suivante. Ainsi des résultats précis d'EPS ne sont jamais nécessaires, ni ne font l'objet d'une confiance absolue.
- Deuxièmement, des études de sensibilité sont généralement réalisées lorsque les résultats sont proches des limites séparant les catégories. Si ces études indiquent que les résultats d'EPS présentent un degré de sensibilité élevé, alors la conception des

systèmes existants est réexaminée du fait qu'ils devraient être conçus de façon à être relativement insensibles aux taux de défaillance des composants.

- Troisièmement, on fait preuve de façon générale de conservatisme lorsque aucun des systèmes existants pris en compte dans les EPS ne peut faire état de valeur sans restriction. Par exemple, lorsque l'analyse de l'arbre de défaillance d'un système de protection réacteur montre que pour une séquence d'évènements étudiée, la P_{DD} du système de protection est ~10^{-4}, malgré ceci, la méthodologie de catégorisation limite habituellement la valeur revendiquée pour n'importe quel système ou fonction à 10^{-3} pour des fonctions de catégorie A (et plus bas pour les autres catégories). Ceci a deux effets au niveau conservatisme:
  - cela renforce généralement la défense en profondeur, et
  - cela augmente le niveau de catégorie requis pour la nouvelle fonction.

7 Pratiques courantes de certains états membres

7.1 Généralités

Cet article fournit un court résumé sur le degré actuel d'application des méthodes de catégorisation influencées par les techniques probabilistes ou d'évaluation des risques dans certains pays membres. Il présente les points considérés comme significatifs pris en compte lors de la discussion menée au niveau international, ainsi que les descriptions générales envoyées par plusieurs comités nationaux après les réunions.

7.2 Résumés courts

Ce paragraphe résume les principaux points formulés au cours de la discussion à propos du niveau courant de pratique de catégorisation à partir de l'évaluation des risques. Ces points offrent un panorama des pratiques courantes des états membre (certains comités nationaux, repérés par un astérisque, ont envoyé ultérieurement des résumés plus longs concernant leurs pratiques nationales et ceux-ci apparaissent en 7.3).

Canada * Des EPS sont menées pour un grand nombre d'évènements (~ 50), et celles-ci font partie intégrante du processus d'autorisation, car les régulateurs exigent en même temps des analyses déterministes comme probabilistes. La catégorisation est réalisée d'abord sur la base de la fiabilité requise pour une fonction (ou bien un λ_D pour un système procédé (fonctionnant de façon continue) ou bien une P_{DD} pour les systèmes de sûreté (fonctionnant à la demande). Dans certains cas, lorsque la fonction est aussi considérée dans l'analyse déterministe, la catégorie peut être déterminée en fonction de celle-ci (plus élevée que la catégorie déterminée sur l'analyse probabiliste).

France * Des EPS sont réalisées pour un grand nombre d'évènements possibles. Ceci pour prendre en compte les séquences amenant à un endommagement du cœur avec une fréquence associée dépassant le 10^{-7}/a, de nouvelles fonctions peuvent être ajoutées à l'installation ou un système existant peut être affecté à la réalisation d'une nouvelle fonction. Lorsque les cas comprennent deux défaillances indépendantes, la nouvelle fonction peut être de catégorie C. S'ils ne comprennent qu'une défaillance, la nouvelle fonction devra être de catégorie A.

Les EPS sont mises à jour tous les 10 ans.

Allemagne *	Conformément à la réglementation allemande, le système de protection réacteur doit être conçu de façon à ne pas être un facteur déterminant au niveau indisponibilité du système de sûreté. L'interprétation habituelle de cette exigence est que la contribution de l'I&C au taux de défaillance d'ensemble d'un système lié à la sûreté est limitée à 10 % de celui dû aux composants mécaniques. Les EPS sont mises à jour tous les 10 ans.
Japon	Le classement de sûreté repose sur une approche déterministe. Néanmoins, des EPS sont réalisées pour un grand nombre d'évènements et l'utilisation de l'évaluation des risques complémentaire à l'approche déterministe classique est une tendance qui se développe. Considérant qu'il y a encore peu de retour d'expérience au Japon dans ce domaine, il est considéré que cela prendra encore quelques années pour modifier les guides de classement de sûreté pour concevoir sur la base de l'évaluation des risques. L'utilisation de l'évaluation des risques au Japon va débuter dans le domaine de l'exploitation, de l'inspection et des aspects sismiques. Des informations récentes et détaillées sur l'introduction d'une réglementation basée sur l'évaluation des risques au Japon peuvent être obtenues sur le site web de l'autorité de sûreté nucléaire du Japon (NSC). （http://www.nsc.go.jp）
Corée	Des EPS sont réalisées pour les centrales en exploitation comme pour celles en construction. Les EPS couvrent un grand nombre d'évènements possibles. On utilise un classement simple en 4 catégories. Jusqu'à présent les EPS non pas eu d'influence sur le classement, mais il y a plusieurs cas où les EPS ont été utilisées pour étendre la durée entre arrêts de tranche ainsi que les intervalles d'essai de surveillance des systèmes de sûreté.
Suède	Les EPS sont utilisées de façon extensive sur toutes les centrales. Elles ne sont pas utilisées directement pour le classement, mais pour identifier les systèmes demandant une attention particulière. C'est un outil utilisé quotidiennement sur le site de Ringals. Les autorités de sûreté demandent en même temps des rapports de type déterministe et de type probabiliste. La modélisation du logiciel pose problème dans les EPS.
Suisse	Avec l'entrée en vigueur en juin 2008 du nouveau guide réglementaire A06 (application des EPS), les EPS sont systématiquement utilisées pour la surveillance des réacteurs (pour ce qui concerne l'évaluation de la sûreté, des modifications de l'installation – et de l'analyse d'incident) comme un élément complémentaire pour la prise de décision. De plus le guide A06 décrit l'identification des composants, qui sont importants du point de vue des EPS. Une modification de ces composants nécessite l'accord de l'autorité de régulation.
Royaume-Uni *	Les EPS comprennent des modèles de taux de défaillances dangereuses (λ_D) pour les systèmes de régulation et P_{DD} pour les systèmes de sûreté. Les EPS de niveau 3 sont habituellement utilisées pour démontrer que les composants d'I&C ne sont pas des contributeurs majeurs.

7.3 Explications plus détaillées

Plusieurs comités nationaux ont envoyé des descriptions de leur pratique nationale courante pour ce qui concerne l'utilisation des outils reposant sur l'évaluation des risques chez eux. Celles-ci sont présentées ci-dessous par ordre alphabétique (en anglais):

- Canada
- France
- Allemagne
- Corée
- Royaume-Uni

Un résumé concis est fourni pour les longues descriptions.

Canada

Le processus d'autorisation au Canada repose sur la satisfaction d'exigences déterministes et probabilistes. La catégorisation est d'abord probabiliste, avec certains ajustements déterministes. Les centrales en cours d'exploitation utilisent la méthodologie de catégorisation expliquée en 8.4. Les futures centrales (aujourd'hui à l'étude) utiliseront une méthodologie, conforme au document AIEA NS-R-1, décrite en 8.5.

Les exigences d'autorisation déterministes sont de deux types: celles appelées cas d'accident simple (pour lesquelles tous les systèmes de sûreté sont censés fonctionner comme prévu à la conception) et celles appelées cas d'accident à caractère dual (pour lesquelles pour chaque EIP, chaque système de sûreté sollicité est censé tomber en panne). Il est reconnu que la probabilité d'un cas d'accident à caractère dual est considérablement moindre que celle d'un cas d'accident simple, et donc des niveaux de rejet bien plus élevés sont autorisés.

La satisfaction des objectifs probabilistes est démontrée par les EPS. Typiquement, une EPS comprend plus de 50 cas, tel que la perte des calculateurs de tranche, une perte d'alimentation de classe IV[3] , différentes brèches à différents endroits de différentes tailles, etc.

Au cours des revues de conception des installations les méthodes déterministes comme les méthodes reposant sur des EPS sont utilisées, et chacune d'elles peut être à l'origine de l'ajout de nouveaux systèmes d'atténuation des risques.

La catégorisation est réalisée en utilisant des méthodes basées sur l'évaluation des risques telles que décrites à l'Article 8. Dans certains cas, lorsqu'on doit ajouter de nouveaux systèmes d'atténuation des risques à la conception d'une installation, une nouvelle fonction liée à la sûreté peut être affectée à la catégorie B du fait de son rôle dans l'analyse déterministe même si sa catégorie telle que définie par la méthode basée sur l'évaluation des risques aurait pu être la catégorie C.

France

Résumé:

La sûreté des installations nucléaires françaises repose premièrement sur des concepts déterministes et sur la défense en profondeur, ainsi la catégorisation dans la conception de base est purement déterministe. La conception déterministe fait l'objet de revue en utilisant des EPS. Les EPS sont réalisées au cours de la conception originale de l'installation, et elles font l'objet de révision durant la durée de vie de l'installation. S'il apparaît qu'une séquence

3 Sur les centrales de type CANDU, les alimentations électriques de classe IV alimentent les pompes primaires de refroidissement.

d'accident contribue à la probabilité de la fusion du cœur au-delà de 10^{-7}/a, alors on augmente la catégorie d'une fonction existante, ou on ajoute une nouvelle fonction à l'installation. En certaines circonstances (décrites en 8.2.1.3) la catégorie de cette nouvelle fonction peut être déterminée sur la base de la fiabilité requise, mais sinon la catégorisation se fait sur une base déterministe.

Description complète:

La sûreté des installations nucléaires françaises (centrales nucléaires de puissance, réacteurs de recherche, installations d'enrichissement, etc.) repose principalement sur des concepts déterministes et la défense en profondeur (INSAG-10). La première étape de catégorisation est ainsi purement déterministe (8.2.1.1).

Au cours de la conception des nouvelles centrales nucléaires de puissance à fission, des méthodes probabilistes sont utilisées comme méthodes complémentaires pour identifier les séquences à contributeurs multiples menant aux accidents graves, dont la contribution ne peut être négligée au regard de la probabilité des accidents graves. L'objectif probabiliste d'ensemble lié au risque de fusion du cœur, prenant en compte les risques et les incertitudes et tous les états du réacteur, est de 10^{-5}/a, ainsi les séquences dont la probabilité est supérieure à 10^{-7}/a sont systématiquement prises en compte dans cette liste. La prise en compte de ces séquences peut se faire de deux façons: en augmentant la catégorie d'une fonction déjà existante ou en ajoutant une nouvelle fonction de sûreté. Dans ce dernier cas, la catégorie de la fonction doit être choisie pour faciliter la démonstration prouvant que la fiabilité requise est atteinte (paragraphe 8.2.1.3). L'allocation d'une fonction à un système dépend naturellement d'autres contraintes, telles que la classe du système (conformément à la CEI 61513), les exigences d'indépendance entre les systèmes et les fonctions, le maintien d'un niveau de complexité assez faible pour les systèmes classés de sûreté, etc.

Pour les installations existantes, une EPS est réalisée tous les dix ans pour confirmer que l'installation peut satisfaire dans de bonnes conditions aux exigences de sûreté applicables. Au cours de cette étape, les hypothèses faites pour les EPS précédentes sont vérifiées, par rapport au retour d'expérience collecté sur les installations du même type, et la validité de certaines peut être réévaluée. Si la probabilité des accidents graves, prenant en compte les risques et les incertitudes et tous les états du réacteur, est estimée être supérieure à 10^{-5}/a, on doit décider de modifications de conception pour satisfaire à cet objectif probabiliste.

En cas d'introduction d'un nouvel équipement d'I&C ou d'un groupe d'équipements, on réalise une analyse probabiliste qui complète la vérification de la satisfaction des exigences de conception applicables pour la nouvelle solution, ceci pour confirmer que les ensembles matériel rénovés présentent des propriétés équivalentes sinon meilleures que celles des ensembles remplacés. La fiabilité est vue comme une de ces propriétés. La validation du modèle et des hypothèses utilisés dans ce cas sont un point clef de la démonstration de cette propriété . Le choix du modèle doit être approprié à la complexité du comportement interne de l'équipement ou de l'ensemble d'équipements.

Les points clef suivant doivent être soulignés:

a) Les EPS ne peuvent pas être utilisées pour dégrader la catégorie d'une fonction existante. Elles sont utilisées pour identifier les points faibles et pour améliorer la conception (finalement en augmentant la catégorisation des fonctions ou en ajoutant des lignes de défense complémentaires).

b) Les EPS peuvent, dans certains cas, amener à réexaminer les périodes de maintenance mais elles ne peuvent pas être utilisées sans justification complémentaire pour réduire la fréquence de maintenance d'un matériel qualifié, qui doit résister à des conditions particulières (par exemple conditions d'accident grave d'APRP et post-APRP, etc.).

Cette méthode reste applicable pour toutes les installations nucléaires (réacteur de recherche, installations d'enrichissement, etc.). Néanmoins, elle doit être adaptée du fait de la définition des accidents graves et de la définition du niveau acceptable, en termes d'impact, qui varient suivant les installations. L'objectif de probabilité de 10^{-5}/a pour les accidents

graves peut varier suivant l'impact des accidents graves pour ces applications (qui peut être différent du scénario de fusion du cœur pris en compte pour les réacteurs à fission).

Allemagne

Conformément à la réglementation allemande, les procédures d'autorisation relatives aux décisions liées à la sûreté des centrales nucléaires de puissance en Allemagne, reposent sur des principes déterministes.

Les méthodes probabilistes sont employées comme méthodes complémentaires d'appui aux arguments comme par exemple:

- Une EPS est réalisée pour chaque centrale tous les dix ans, pour confirmer que l'installation remplit encore de façon satisfaisante les exigences de sûreté applicables.
- Lors de l'introduction de nouvelles technologies d'I&C, une analyse probabiliste est réalisée pour confirmer l'adéquation de la conception matériel par rapport à la technologie précédente qui était éprouvée et pour confirmer les intervalles de temps retenus pour les essais de surveillance.

Concernant la conception de sûreté d'ensemble, la méthodologie liée aux EPS est utilisée pour identifier les faiblesses et garantir l'équilibre des concepts de sûreté en supportant les décisions d'autorisation qui reposent sur la satisfaction d'exigences déterministes.

Corée

Les méthodes d'EPS ne sont pas utilisées pour le classement système ou pour la catégorisation fonctionnelle des systèmes d'I&C et/ou des fonctions des centrales nucléaires de puissance.

Les méthodes d'EPS ont été utilisées pour étendre les intervalles de test au niveau des essais de surveillance des systèmes de protection des réacteurs et des actionneurs des systèmes support de sauvegarde.

Les méthodes d'EPS sont employées pour augmenter le temps d'indisponibilité autorisé des matériels des systèmes liés à la sûreté.

Royaume-Uni

Résumé:

Les procédures d'autorisation concernant les décisions liées à la sûreté des centrales nucléaires de puissance au Royaume-Uni reposent sur des principes d'évaluation des risques. Les risques doivent être réduits autant que raisonnablement pratique, tel que cela est démontré par les EPS. La norme CEI 61508 est une norme importante utilisée comme guide.

Description complète:

Au Royaume-Uni les exploitants de centrales nucléaires (détenteurs d'autorisations) ont obligation de réduire les risques pour les travailleurs et le public autant qu'il est raisonnablement pratique. Un élément clef de la réponse des exploitants pour satisfaire à cette exigence est la démonstration que les risques associés à l'installation sont aussi faibles que raisonnablement pratique. Cette démonstration comprend une étude probabiliste de sûreté qui fournit les chiffres relatifs à la contribution des systèmes d'I&C aux objectifs globaux de l'installation concernant les risques. Habituellement les systèmes d'I&C contribuent à la fréquence d'initiation des évènements postulés (par exemple par la probabilité de défaillances dangereuse par an – PDDA) et/ou à la réduction des risques (par exemple la probabilité de défaillance à la demande – PDD). En conséquence, des objectifs probabilistes sont assignés aux différents systèmes d'I&C et une démonstration est exigée

pour prouver que les normes appropriées sont satisfaites. La CEI 61508 est un exemple de norme qui peut fournir des recommandations en ce qui concerne la gradation des objectifs de fiabilité/les niveaux d'intégrité de sûreté (les bandes PDD/PDDA) et qui est utilisée au Royaume-Uni.

Les fonctions sont catégorisées suivant leur importance pour la sûreté en utilisant des normes appropriées telles que la CEI 61226. Il faut noter que la CEI 61508 fournit de façon générique des recommandations pour les systèmes E/E/EPS (par exemple une fonction de catégorie A avec une PDD de 10^{-4} comme niveau d'intégrité devrait être réalisée en employant un équipement satisfaisant aux exigences SIL 4 de la CEI 61508 pour être cohérent avec la limite de PDD de 10^{-4} qui est imposée pour les applications nucléaires au Royaume-Uni), cependant, il devrait être préférable de se conformer aux normes du secteur nucléaire, comme par exemple la CEI 61513 pour ce qui concerne les limites imposées pour les niveaux de performance réputés atteints acceptables).

8 Etude des techniques de catégorisation basée sur l'évaluation des risques

8.1 Généralités

Comme présenté dans l'Article 5, les évaluations quantitatives du risque peuvent être utilisées pour compléter l'approche déterministe du classement des fonctions d'I&C. Il est bien connu que le développement et l'utilisation des techniques d'évaluation du risque (souvent appelées évaluations probabilistes du risque ou évaluations probabilistes de sûreté) sont bien avancés au sein de certains états membres mais qu'ils n'ont pas encore atteint un niveau d'acceptation cohérent au niveau de toutes les nations membres.

Les informations obtenues grâce à l'utilisation des EPS peuvent faciliter la prise efficace de décisions concernant les risques et permettre une utilisation plus efficace des ressources, en particulier pour les décisions pour lesquelles des ressources financières limitées doivent être investies au mieux pour garantir les meilleurs profits. Il est recommandé que les EPS soient utilisées dans les centrales nucléaires existantes pour déterminer les composants des systèmes d'I&C qui devraient être modifiés ou mis à niveau pour améliorer la sûreté, la conception et l'exploitation des installations et du système d'I&C. Ceci est particulièrement approprié lors des revues de sûreté des installations existantes.

Il convient que l'application de méthodes et de technologies liées aux EPS pour la catégorisation soit utilisée pour compléter l'approche déterministe basée sur le rôle fonctionnel qui affecte la catégorie des fonctions, en particulier pour les méthodes d'EPS, lorsque les données sont disponibles; ceci étant souvent vrai lorsqu'on décide de mise à niveau, ce qui n'est malheureusement pas le cas pour les nouvelles conceptions. Néanmoins, pour avoir les résultats les plus efficaces, il convient d'utiliser les EPS en regard de la conception de l'installation et de celle de son système d'I&C pour fournir de l'information pour le classement des fonctions d'I&C.

Une fois que le processus de conception itératif mixte (déterministe/EPS) de l'installation a convergé sur une conception techniquement réalisable (telle que décrite en 5.1.2.2 de la CEI 61513), les exigences de fiabilité et les exigences fonctionnelles portant sur les fonctions liées à la sûreté sont définies, la catégorisation peut alors être finalisée.

Ce rapport présente six différentes approches de l'utilisation des EPS. Cette liste de méthodes n'est pas exhaustive; en effet il existe de nombreux cas dans lesquels des techniques probabilistes peuvent faciliter les prises de décision pendant la conception d'une centrale nucléaire. Le présent rapport a pour objet de stimuler le débat sur l'utilisation optimale des techniques probabilistes pendant la phase de conception des systèmes d'instrumentation et de contrôle-commande d'une centrale nucléaire.

Les six approches sont les suivantes:

Approche 1, voir 8.2 – Approche basée sur le temps et l'état du réacteur

Cette approche a été introduite dans le document European Utility Requirements pour le classement des équipements, notamment de contrôle-commande.

Approche 2, voir 8.3 – Approche basée sur l'importance quantitative

Cette approche est basée entièrement sur une technique probabiliste pour déterminer la contribution de chaque fonction de I&C dans les séquences de défaillance de la centrale. De cette manière, l'importance de chaque fonction de I&C peut être quantitativement calculée. La technique a été utilisée dans une centrale aux Etats-Unis comme base de surveillance en service du risque.

Approche 3, voir 8.4 – Approche basée sur les conséquences et l'atténuation

Cette approche a été utilisée au Canada pour la conception des centrales nucléaires CANDU existantes. On note qu'une approche différente sera utilisée pour les projets de construction nouvelle au Canada.

Approche 4, voir 8.5 – Approche mixte déterministe-probabiliste basée sur le NS-R-1

Cette approche est maintenant utilisée au Canada pour la conception des nouvelles centrales nucléaires CANDU. Les états du réacteur sont définis conformément au document NS-R-1, en affectant à chaque état les fréquences et conséquences acceptables, puis en utilisant une approche très proche des méthodologies de la CEI 61226 actuelle.

Approche 5, voir 8.6 – Application des méthodologies basées sur l'évaluation des risques dans la réglementation américaine

Cette approche décrit les essais d'application du document Regulatory Guide 1.201 "Guidelines for Categorizing Structures, Systems, and Components (SSC) in Nuclear Power Plants According to Their Safety Significance" de la commission de régulation du nucléaire aux Etats-Unis. Dans la méthode de classement recommandée par ce Regulatory Guide, l'importance pour la sûreté des SSCs est déterminée en utilisant un processus de prise de décision intégré, qui prend en compte en même temps les risques et le traditionnel jugement de l'ingénieur.

Approche 6, voir Annexe B – Approche basée sur la défense en profondeur

Cette approche était décrite en 6.5 de la première édition, et a été conservée en Annexe B car elle est référencée au niveau des comparaisons.

Cette approche est axée sur l'utilisation des techniques probabilistes permettant de modifier le classement d'I&C déterminé au préalable par la méthode qualitative approuvée. Elle envisage la possibilité d'utiliser les techniques probabilistes dans le but de surclasser d'un niveau l'I&C afin de minimiser le risque de dépendance excessive des données probabilistes basées sur les fiabilités génériques des composants.

Cette approche n'a pas encore été appliquée à un classement des fonctions d'une centrale nucléaire.

8.2 Approche 1: Approche basée sur le temps et l'état du réacteur

8.2.1 Catégorisation des FSE au cours de la phase de conception

8.2.1.1 Etape 1 – Approche déterministe

La sûreté des installations nucléaires françaises (centrales nucléaires de puissance, réacteurs de recherché, installations d'enrichissement, etc.) repose principalement sur des concepts déterministes et sur la défense en profondeur (INSAG-10).

Les mesures prises en compte à la conception pour les centrales nucléaires françaises REP sont justifiées pour un nombre limité de conditions d'exploitation conventionnelle (les

évènements initiateurs et les séquences d'accident sont utilisés pour définir le dimensionnement des bâtiments, des systèmes et des matériels nécessaires au terme de la sûreté) conséquences d'initiateurs simples et par l'application de règles déterministes et de critères qui intègrent des marges et des éléments de conservatisme. Les résultats de ces études doivent respecter les critères dont l'objectif est de limiter les conséquences des évènements évalués.

Les situations d'exploitation sont classées en 4 catégories (catégories des états de tranche - PCC) basées sur leurs gammes de fréquence et leurs conséquences[4]. L'apparition d'un événement dans n'importe laquelle de ces catégories est liée au niveau des rejets ou d'exposition aux rayons maximum. Les conséquences du dépassement de ces niveaux sont jugées inacceptables, et des fonctions de prévention et/ou d'atténuation doivent être ajoutées. Ces fonctions sont catégorisées selon la CEI 61226.

Les conséquences de la défaillance d'un équipement d'I&C doivent être couvertes par ces cas. En effet, les défaillances des équipements d'I&C doivent être limitées à la conception pour que les défaillances consécutives n'entraînent pas de conséquences plus graves que celles permises pour la quatrième catégorie PCC-4 (qui est la plus grave). Les défaillances des équipements d'I&C non-classés ou appartenant à la classe 3 sont limitées par conception pour que les défaillances consécutives n'entraînent pas de conséquences plus graves que celles permise pour la deuxième catégorie (PCC-2).

Les conséquences des risques internes ou externes sont analysées sous l'hypothèse correspondant à la combinaison la plus pénalisante des défaillances de tous les équipements non conçus pour l'évènement initiateur et en démontrant que tous les équipements qualifiés pour l'évènement avec les équipements qui ne sont pas touchés par celui ci du fait des mesures de séparation prévues pour l'événement (incendie, inondation), sont suffisants pour empêcher l'apparition de conséquences inacceptables.

La première étape fournit les bases pour catégoriser les fonctions conformément à la CEI 61226 Ed. 3 comme suit:

– Catégorie A: 5.4.1
– Catégorie B: 5.4.2, points a), b), c), e)
– Catégorie C: 5.4.3, points b), c), f), j), k), l).

La catégorisation repose sur la distinction entre l'état contrôlé et l'état sûr final conformément à la CEI 61226.

La catégorie A correspond aux actions court-termes pour empêcher l'apparition de conséquences inacceptables et pour amener l'installation à l'état contrôlé. La catégorie B correspond aux fonctions permettant d'amener et d'atteindre l'état d'arrêt sûr pour lequel les durées de temps associées au processus sont plus longues et que toute défaillance peut être compensée par des mesures complémentaires pour que l'état contrôlé soit maintenu.

Du point de vue de la sûreté, l'état contrôlé doit être maintenu indéfiniment. Néanmoins, il est raisonnable d'accepter certaines relaxes des exigences pour le rejet à long terme de la chaleur de décroissance radioactive dans les REP. Ceci entraîne une relaxe des exigences concernant la garantie de maintien de l'arrêt après 24 h et l'acceptation des fonctions non classées après 72 h en faisant l'hypothèse qu'il existe des moyens complémentaires pour assurer ces fonctions dans des délais qui permettent d'éviter l'apparition de conséquences inacceptables.

Le Tableau 1 illustre ces relaxes:

4 Les PCC sont numérotés de PCC-1 à PCC-4, où PCC-4 a la fréquence la plus faible et les conséquences les plus graves.

Tableau 1 – Classement des FSE d'I&C

	FSE d'I&C à utiliser dans l'analyse de sûreté			
Etat du réacteur	**Evènement initiateur**	**Etat contrôlé**	**Etat d'arrêt sûr**	
Echelle de temps		24 h		72 h
Conditions de fonctionnement de dimensionnement	Catégorie A	Catégorie B	Catégorie C	Non classé
Extension des conditions de dimensionnement	Catégorie C			Non classé
Risques internes	Catégorie C			Non classé

L'indépendance qui est exigée (comme indiqué ci-dessus) entre les fonctions de catégorie C (telles que définies par la CEI 61226), participant aux niveaux successifs de défense en profondeur, est réalisée en les affectant à des systèmes indépendants (tels que définis par la CEI 61513). Les points suivants doivent être pris en compte avec soin au cours du processus de conception de l'architecture d'I&C:

- L'exigence d'indépendance entre les lignes successives de défense en profondeur pour n'importe quel scénario donné.
- L'exigence d'indépendance entre les niveaux de défense en profondeur. Le Tableau 2 relie les critères donnés en 5.4.3 de la CEI 61226 et les niveaux de défense en profondeur:

Tableau 2 – Correspondance entre la CEI 61226 et l'INSAG-10

Critère de catégorie C (CEI 61226 Ed. 3, 5.4.3)	**Niveau défense en profondeur correspondant (INSAG-10)**
Critère a/, c/, f/	Premier niveau défense en profondeur
Critère b/, g/, h/	Deuxième niveau défense en profondeur
Critère, d/ e/	Troisième niveau défense en profondeur
Critère i/, j/, g/	Quatrième niveau défense en profondeur

- La nécessité d'assurer l'alimentation électrique d'urgence et les exigences de séparation électrique entres les systèmes de sûreté, liés à la sûreté et non classés (voir la CEI 60709 pour les exigences sur le sujet).

8.2.1.2 Etape 2 – EPS de niveau 1 et identification des séquences individuelles ayant une contribution significative au niveau de la fréquence d'endommagement du cœur

Le processus de catégorisation est complété par les EPS. Dans ce cadre, le but des EPS est de montrer que l'objectif probabiliste visé pour les accidents graves, c'est-à-dire les accidents dont les conséquences peuvent dépasser les limites prévues par la conception de l'installation, est atteint.

L'objectif probabiliste est généralement fixé pour chaque type de réacteur suivant les conséquences accidentelles. Pour les nouveaux REP français, l'objectif probabiliste pour les séquences individuelles amenant à la dégradation du cœur est généralement fixé à une fréquence inférieure à 10^{-7}/a. L'objectif probabiliste d'ensemble concernant la dégradation du cœur, prenant en compte les risques et les incertitudes et tous les états du réacteur se situe en dessous de 10^{-5}/ra (INSAG-12). Les règles générales applicables pour les EPS françaises

sont données dans la Règle Fondamentale de Sûreté “Développement et utilisation des EPS” adoptée en 2002 par l’Autorité de Sûreté Nucléaire française[5].

Une EPS de niveau 1 a pour but de déterminer les scénarii à défaillances multiples représentant une contribution significative en ce qui concerne la fréquence d’endommagement du cœur. Les scénarii comprennent au moins deux causes événementielles indépendantes (initiateurs). D’autres parts, les conséquences produites par l’initiateur commun sont traitées de façon déterministe (en utilisant l’approche décrite ci-dessus à l’étape 1), sauf s’il est montré que la fréquence maximum de l’initiateur est négligeable au niveau de l’objectif de 10^{-7}/a, en dessous de quoi les évènements sont exclus. En pratique, chaque initiateur associé à un défaut de commande est traité de façon déterministe.

On peut citer les exemples de séquences complexes suivants qui font généralement partie des EPS de niveau 1 de référence:

- ATWS (“Anticipated Transient Without SCRAM”);
- perte totale de l’alimentation des générateurs de vapeur;
- petite brèche primaire et perte de l’injection de sûreté moyenne pression;
- petite brèche primaire et perte de l’injection de sûreté basse pression;
- perte totale d’alimentation électrique;
- perte totale de refroidissement.

8.2.1.3 Choix de la catégorie des fonctions tel que préconisé par les EPS

Dans certains cas, les EPS peuvent indiquer que les objectifs probabilistes ne sont pas atteints. Il existe deux possibilités pour couvrir chaque famille de scénarii à défaillances multiples, identifier et prendre en compte les contributeurs significatifs pour l’objectif de 10^{-7}/ra:

– bien une fonction non classée existe et celle-ci peut être utilisée pour le scénario et réduire à un niveau acceptable les conséquences de celui-ci (cas 1),

– ou il n’existe pas de telle fonction (cas 2).

Dans le premier cas, la fonction est affectée à une classe de sûreté et peut être prise en compte par l’EPS. Si cette fonction existante est de catégorie A ou B, ce classement est conservé.

Dans le deuxième cas, on ajoute une nouvelle fonction de catégorie A, B ou C. Cette fonction est classée en catégorie A si elle correspond aux fonctions décrites en 5.4.1 de la CEI 61226.

Dans les autres cas, la fiabilité de la fonction requise pour prendre en compte de façon appropriée les scénarii doit faire l’objet d’une déclaration. Il convient de démontrer que l’activation intempestive de la fonction n’entraîne pas de séquence de défaillances qui augmente le risque d’endommagement du cœur.

Finalement, il convient de s’assurer que l’affectation de la fonction au système (conformément à la CEI 61513) confirme de façon sure que la défaillance de l’équipement d’I&C (classé ou non) ne peut déclencher un scénario de défaillances multiples, ni entraîner la défaillance de la fonction devant atténuer les conséquences de ce même scénario.

La catégorie de la fonction doit être choisie pour faciliter la démonstration prouvant que fiabilité déclarée est effectivement atteinte.

---

5 Ce document est disponible sur le site web de l’Autorité de sûreté nucléaire (ASN) (www.asn.fr).

La démonstration d'avoir une probabilité de défaillance à la demande inférieure à 10^{-3} pour un ensemble couvrant l'acquisition de données (y compris le capteur), le traitement logique et la logique de vote est extrêmement difficile avec du logiciel développé seulement en respectant les exigences associées à la catégorie C. Il est donc judicieux d'affecter de telles fonctions à la catégorie A. Pour les cas où cette fonction est requise pour atténuer une défaillance d'une autre fonction de catégorie A, il est essentiel de garantir l'indépendance de ces fonctions. Plusieurs approches sont possibles, la plus simple étant d'affecter les deux fonctions à deux systèmes de classe 1 indépendants.

La démonstration d'avoir une probabilité de défaillance à la demande inférieure à 10^{-2} pour un ensemble couvrant l'acquisition de données, le traitement logique et la logique de vote en suivant les processus associés à la Catégorie C, est a priori réalisable, mais cela demande de disposer de suffisamment de données de fiabilité.

8.2.1.4 Exigences minimums liées à chaque catégorie

Certaines exigences sont liées à la catégorie choisie, alors que d'autres sont liées à la classe du matériel ou du système, mais toutes dépendent des hypothèses faites sur l'indépendance et utilisées lors de l'analyse d'accident.

La liste des exigences est peut être à compléter mais elle comprend au minimum les suivantes, voir Tableau 3.

Tableau 3 – Exigences minimum par niveau de fonction

Catégorie		A	B	C
Critère de défaillance unique		OUI	OUI	NON, sauf si cette exigence aide à démontrer la fiabilité fonctionnelle ou l'aptitude à réaliser une fonction en cas de risque interne (incendie, inondation, etc.)
Alimentation électrique d'urgence		OUI	OUI	NON pas toujours, elle pourrait être exigée dans certains cas, par exemple si la fonction est prise en compte après un tremblement de terre, ou une perte totale d'alimentation électrique, etc.
Séparation physique	Entre voies redondantes	OUI (physique et électrique)		NON
	Entre systèmes de différentes classes	Entre systèmes classés et non classés de sûreté Entre systèmes de classe 1 et 2 et les autres systèmes qui pourraient interférer avec ceux-ci.		
Mise en marche automatique		Exigée si l'action doit être déclenchée dans les 30 min.	Exigée si l'action doit être déclenchée dans les 30 min.	Exigée si l'action doit être déclenchée dans les x min (x dépendant de l'analyse d'impact, est > 30 min pour les actions préventives et toujours > 20 min pour la mise en œuvre des moyens d'atténuation).

Des exigences d'indépendance supplémentaires sont imposées pour garantir:

- qu'aucune fonction de catégorie inférieure ne peut compromettre la réalisation d'une fonction de catégorie supérieure,
- qu'aucune défaillance d'équipement d'I&C ne peut mettre en péril des lignes de défense successives,
- qu'il n'y a pas de source de cause commune pouvant produire des défaillances multiples qui puissent compromettre la réalisation d'une fonction qui a été mise en place pour faire face à ces défaillances multiples.

Ces exigences d'indépendance sont soumises à la contrainte qui impose de ne pas introduire une complexité indue dans les systèmes de classe 1 ou 2.

La possibilité de tracer les exigences pour le logiciel est requise conformément à la CEI 60880 pour les systèmes de classe 1 et à la CEI 62138 pour les systèmes de classes 2 et 3.

Le Tableau 4 indique les autres exigences portant sur l'équipement:

Tableau 4 – Exigences portant sur l'équipement

Catégorie	A	B	C
Code de conception et de réalisation pour les systèmes électriques et les systèmes d'I&C (exemple le RCC-E)	OUI	OUI	OUI
Assurance qualité	OUI	OUI	OUI
Essais périodiques	OUI	OUI	OUI
Base de données de fiabilité des composants et modélisation de la fiabilité des composants	OUI	OUI	Conforme aux exigences issues des EPS
Qualification aux conditions de fonctionnement (voir la CEI 60780 pour les détails)	OUI	OUI	SI APPLICABLE (par exemple si utilisation déclarée pendant ou après une rupture de tuyauterie de terre, etc.)
Exigences de fiabilité minimale	OUI au niveau de l'acquisition et de la logique	OUI au niveau de l'acquisition et de la logique	OUI au niveau de l'acquisition et de la logique

8.2.2 Impact des revues de sûreté sur la catégorisation

Pendant la durée de vie de l'installation, une EPS de niveau 1 est réalisée comme partie intégrante des revues de sûreté périodiques. L'EPS utilise les données de retour d'expérience qui peuvent comprendre des données de fiabilité mises à jour, des hypothèses concernant les séquences et les mécanismes de défaillance, ainsi que les fréquences de certains EIP.

Le but d'une telle EPS est l'amélioration de la conception de l'installation durant sa durée de vie et l'aide à la prise de décision:

- en présentant les preuves relatives à la nécessité de mettre à niveau certains sous-systèmes,
- en identifiant les équipements qui nécessitent de meilleures procédures de maintenance,

- en mettant en évidence les possibilités de défaillances multiples qui sont significatives,
- en alimentant le retour d'expérience pour améliorer les données utilisées par des installations comparables.

L'EPS est nécessaire pour montrer que la fréquence globale d'endommagement du cœur reste bien en dessous de l'objectif initial de 10^{-5}/ra.

IMPORTANT: Les EPS ne peuvent pas être utilisées seules pour réduire la catégorie d'une fonction existante.

D'un autre coté, les EPS peuvent amener à réexaminer les intervalles de maintenance, la catégorie des fonctions existantes, ou l'ajout de nouvelles fonctions ou la rénovation de certaines parties de l'installation. Cependant, les résultats des EPS ne peuvent être utilisés sans justifications complémentaires pour augmenter les intervalles de maintenance des équipements qualifiés. L'âge des équipements doit être pris en compte dans la justification d'une telle évolution pour montrer qu'il n'y a pas de conséquences au niveau des possibilités déclarées de l'équipement en conditions normales comme accidentelles.

8.3 Approche 2: Approche basée sur l'importance quantitative

8.3.1 Généralités

L'importance pour la sûreté des fonctions d'instrumentation et de contrôle-commande peut être estimée en prenant en compte les conséquences de leurs défaillances, tel que le non-fonctionnement lorsqu'il est requis ou un fonctionnement intempestif. Les EIP servant de base à la conception de la centrale nucléaire peuvent être utilisés comme point de départ de l'évaluation. Il convient que cette évaluation inclue l'analyse de toutes les séquences prépondérantes d'événements, afin d'identifier les fonctions importantes à effectuer par l'I&C.

Cette prise en compte des fonctions effectuées par les FSE d'I&C peut être utilisée pour affecter chaque FSE à l'une des catégories définies dans la CEI 61226, à savoir la catégorie A, B, C ou le non-classement. Une affectation en «non classé» est faite si le FSE n'est pas important pour la sûreté.

Les FSE de I&C liés aux systèmes de sûreté, tels que définis dans le Guide de la sûreté 50-SG-D8 de l'AIEA (Notons que ce document est maintenant remplacé par le document NS-G-1.3), doivent en général être affectés à la catégorie A. Les FSE de I&C définis dans ce guide comme étant liés à la sûreté sont généralement affectés à la catégorie B ou C (et occasionnellement à la catégorie A).

8.3.2 Critères d'affectation quantitatifs

Afin de pouvoir établir l'importance de la sûreté de chaque fonction de I&C, on doit déterminer un ensemble de critères. Un exemple de ces critères est présenté ci-après, sur la base d'un travail qui a été effectué aux Etats-Unis. La technique est basée sur une analyse quantitative de la contribution au risque en utilisant la théorie de l'ensemble des coupes pour parvenir à une approche mathématique cohérente. Dans certains cas, une fonction peut être affectée à plusieurs catégories en raison de sa contribution à plusieurs séquences d'événements. Dans ce cas, il convient qu'au final la fonction soit affectée à la catégorie applicable la plus élevée.

8.3.3 Critères quantitatifs

8.3.3.1 Expressions quantitatives du risque pour les centrales nucléaires

Lorsqu'une évaluation quantitative du risque est effectuée sur une centrale nucléaire, une ou plusieurs des expressions suivantes du risque peuvent être développées en fonction du niveau de l'EPS réalisée:

- fréquence de la fusion du cœur (ou de l'endommagement du cœur) (EPS de niveau 1);

- fréquence des rejets radiologiques et termes sources associés (EPS de niveau 2);
- effets sur la santé, mesurés en terme de possibilités latentes et/ou aiguës (EPS de niveau 3).

En général, et comme minimum de base pour une EPS de niveau 1, une expression booléenne de l'endommagement du cœur est générée en termes d'union booléenne de toutes les séquences accidentelles des arbres d'événements menant à un endommagement du cœur[6]. Cette expression est généralement construite comme l'union booléenne de toutes les coupes minimales qui contribuent, au-delà d'un certain seuil minimal, à une ou plusieurs séquences accidentelles significatives. Autrement dit, l'endommagement du cœur peut être exprimé en termes de fréquences d'occurrence de tous les EIP. Les probabilités de chacune des séquences potentielles résultant d'un EIP individuel ou fréquence d'endommagement du cœur C(t*)* est la somme des fréquences pour lesquelles les événements initiateurs causent des dommages au cœur.

$$C(t) = \sum_{i=1}^{n_i} \Pr\left\{\begin{matrix}\text{Les FSE sont dans un état critique} \\ \text{lorsque l' événement se produit}\end{matrix}\right\} C_{f,i}(t)$$

$$C(t) = \sum_{i=1}^{n_i} \Pr\{U_i E_{i,k}\} C_{f,i}(t) \qquad (1)$$

où

Pr est la probabilité;

$E_{i,k}$ est l'événement de la coupe minimale «k» sachant que l'EIP «i» se produit;

U_i est l'union booléenne des coupes minimales contenant l'EIP «i»;

n_i est le nombre d'EIP;

$C_{f,i}(t)$ est la fréquence d'occurrence de l'EIP «i».

L'expression ci-dessus peut être évaluée, à condition que

- les FSE soient raisonnablement fiables (à savoir que la probabilité qu'au moins deux coupes minimales surviennent simultanément soit faible);
- les événements individuels composant les coupes minimales (à savoir les événements de base) puissent être considérés comme indépendants;
- la probabilité conditionnelle de défaillance par unité de temps «λ» soit une approximation suffisamment précise pour la fréquence de défaillance.

Dans ce cas, l'expression (1) devient:

$$C(t) = \sum_{i=1}^{n_i} \left\{ \sum_{\substack{j \\ i \in k_i}} \prod_{\substack{i \in K_j \\ i=1}} q_i \right\} \lambda_i \qquad (2)$$

où

j est le domaine d'indice pour les coupes minimales;

---

6 La fréquence d'endommagement du cœur est choisie comme un exemple de mesure du risque pour laquelle l'importance des contributions à la sûreté peut être déterminée pour les FSE. Cependant, l'approche utilisant l'importance pour l'évaluation de la sûreté est générale et peut être employée d'une manière similaire pour toute fréquence d'occurrence d'événement sommet (comme les fréquences de rejet et l'effet sur la santé qui peuvent être exprimées sous la forme d'une union booléenne de coupes minimales associées).

K_j est la j° coupe minimale;

$\in$ signifie «appartient à»;

q est la probabilité de l'événement;

I est le domaine d'indice des événements concernés;

$\lambda_i \cong C_{f,i}(t)$;

i est le domaine d'indice pour les EIP;

n_i est le nombre d'EIP dans toutes les coupes minimales.

NOTE Il convient de noter que le terme entre parenthèses dans l'expression (2) est une approximation de premier ordre pour l'indisponibilité due à l'état critique des FSE associés à l'EIP «i». Ce terme est la somme des probabilités des coupes minimales contenant l'EIP «i». L'expression (2) est généralement suffisamment exacte pour la plupart des calculs de risque et peut par conséquent être utilisée pour établir l'importance de la contribution des coupes minimales à la fréquence globale d'endommagement du cœur.

8.3.3.2 Importance pour l'évaluation de la sûreté

Si l'approche précédente est utilisée, l'importance pour la sûreté des FSE peut alors être déterminée en termes de fonctions de pondération qui évaluent la contribution de chacun des événements de base (et par conséquent les conditions de défaillances potentielles des FSE correspondants qui les composent) à la fréquence globale d'endommagement du cœur. Le développement d'une expression d'importance pour une fonction, et/ou les systèmes et équipements associés par lesquels elle est mise en œuvre, implique trois étapes:

a) l'établissement d'un nouvel événement sommet d'endommagement du cœur qui est l'union booléenne des coupes minimales contenant l'EIP ou l'événement concerné;

b) l'utilisation de l'expression (1) pour calculer la fréquence d'occurrence de ce nouvel événement sommet (pour les expressions de l'importance des EIP, un seul événement est utilisé comme événement initiateur pour le nouvel événement sommet);

c) diviser la fréquence d'occurrence résultante par la fréquence d'endommagement du cœur.

Exprimée mathématiquement, l'importance pour la sûreté des événements de base (ou des FSE dont ils sont constitués) pondérée par la fréquence d'endommagement du cœur est:

$$\text{IEC} = \frac{\text{Fréquence de l'union booléenne des coupes minimales contenant les événements intéressants}}{\text{Fréquence d'occurrence de l'événement sommet, C(t)}}$$

En conséquence, l'importance pour la sûreté est donnée simplement par la contribution relative des coupes minimales (contenant l'EIP ou l'événement concerné) à la fréquence totale d'endommagement du cœur. Dans de nombreux cas d'évaluation du risque, C(t) peut être représenté comme une constante selon le degré d'exactitude nécessaire pour établir un ordre raisonnable d'importance. Dans ce modèle de classement, il convient de noter que le numérateur est une fonction linéaire de la fréquence de défaillance des EIP. Pour les événements concernés, le numérateur est une fonction linéaire de l'indisponibilité de ces événements. Sur le plan conceptuel, l'importance des événements concernés (ou pivots) est une mesure constituante de l'importance dans la mesure où les événements ne provoquent pas l'occurrence de l'événement sommet (ici l'endommagement du cœur).

8.3.4 Affectation à une catégorie

Sur la base des importances dérivées de l'analyse précédente, les FSE d'instrumentation et de contrôle-commande peuvent être affectés aux catégories de classement conformément à une échelle d'importance. Il s'avère qu'une échelle logarithmique est la plus appropriée (bien que d'autres échelles puissent être utilisées). Par exemple, il convient qu':

- un FSE de I&C soit affecté à la catégorie A si son importance calculée est $1{,}0 > I \geq 0{,}01$;
- un FSE de I&C soit affecté à la catégorie B si son importance calculée est $0{,}01 > I \geq 0{,}001$;

- un FSE de I&C soit affecté à la catégorie C si son importance calculée est $0{,}001 > I \geq 0{,}0001$.

8.3.5 Procédure de classement

8.3.5.1 Généralités

En utilisant la méthode décrite dans les paragraphes précédents de 8.3, les fonctions de I&C peuvent être classées selon leur importance. La majorité des phases de conception d'une centrale nucléaire incluent des cycles itératifs pendant l'étude des options de conception. Pendant ces cycles, les exigences en matière de I&C sont progressivement affinées et les fonctions individuelles deviennent plus ou moins importantes pour la sûreté. Cette procédure est décrite ci-après.

8.3.5.2 Identification de la base de conception

L'une des entrées principales du processus de classement des FSE est la nature de la centrale nucléaire et le type de réacteur (par exemple PWR, BWR ou autre type de réacteur), les EIP associés et les principaux critères de conception sur la redondance des systèmes et équipements mécaniques et électriques. Une autre entrée principale est l'identification des principaux FSE de mitigation ainsi que leurs FSE supports, pour chaque EIP.

L'affectation des FSE aux catégories dépend de leurs rôles en matière de prévention ou de mitigation des EIP. Le processus de classement exige de tenir compte du rôle des FSE dans la prévention et la mitigation des EIP dans tous les modes de fonctionnement et états de la centrale (par exemple démarrage, fonctionnement normal, rechargement), dans la mesure où les FSE peuvent jouer un rôle important uniquement dans certains modes de fonctionnement et, également des EIP, tels que les catastrophes naturelles (par exemple perturbations sismiques, inondations, vents extrêmes, foudre) et les dangers (par exemple incendies, inondations internes, missiles, rejets radioactifs de la centrale nucléaire adjacente).

8.3.5.3 Identification et classement des FSE

A un stade précoce de la conception d'une centrale nucléaire, on doit identifier les fonctions ayant un rôle de sûreté. Il est recommandé que le processus d'identification de ces fonctions et d'affectation aux FSE de I&C ou aux opérateurs humains soit effectué conformément à la CEI 60964. Suite à cette identification initiale des FSE, il convient d'affecter une catégorie à chaque FSE.

Il ne sera pas possible d'identifier en détail tous les FSE à un stade précoce du processus de conception, dans la mesure où les caractéristiques de la centrale nucléaire n'auront pas encore été complètement définies. En conséquence, le processus d'identification et de classement des FSE doit continuer d'une manière itérative pendant toute la phase de conception. Lorsque l'affectation initiale des FSE à une catégorie est incertaine, il convient d'ajouter une note explicative au classement. Il convient que les fonctions effectuées par chaque système de I&C soient analysées afin d'identifier les sous-FSE au sein des FSE et d'affecter la catégorie appropriée à chaque sous FSE.

Dans la mesure où les FSE individuels peuvent être impliqués dans la mise en œuvre de plusieurs aspects des spécifications, le processus d'affectation peut engendrer l'affectation des FSE à plusieurs catégories. En cas d'affectations multiples, il convient que l'affectation finale de chaque FSE et de tous les sous-FSE soit la catégorie applicable la plus élevée.

Dans la mesure où les exigences en matière de redondance, diversité et autres aspects techniques des FSE sont déterminés d'une manière plus précise, par exemple au fur et à mesure que l'analyse de la sûreté progresse et que les procédures opérationnelles sont développées, la liste de classement est affinée et revue afin d'aboutir à une liste finale. Il convient que cette liste soit incluse dans la documentation requise pour obtenir et conserver la licence d'exploitation de la centrale nucléaire.

8.3.6 Détermination des exigences

Les exigences techniques et de qualité spécifiques aux FSE qui ont été affectés aux catégories A, B et C en utilisant l'approche probabiliste susmentionnée sont présentées dans la CEI 61226.

8.4 Approche 3: Approche basée sur les conséquences et l'atténuation

8.4.1 Historique: Une exigence réglementaire à caractère dual amenant à l'approche probabiliste

Le processus d'autorisation réglementaire au Canada repose aujourd'hui comme par le passé sur une base à caractère dual, déterministe et probabiliste, en vertu de laquelle les exigences d'un type comme de l'autre doivent être satisfaites.

Les exigences probabilistes découlent graduellement des exigences d'autorisation déterministes correspondant à deux scénarii déterministes nommés "les accidents simples" et « accidents à caractère dual ». Un « accident simple » correspond à la défaillance d'un système du procédé, alors qu'un « accident à caractère dual » est une défaillance d'un système du procédé combiné à une défaillance de n'importe lequel des systèmes de sûreté particuliers (ceux-ci correspondent aux fonctions de catégorie A). Les limites de rejet sont déterminées de façon séparée pour ces cas d'accident simples et à caractère dual. Du fait de l'indépendance complète des systèmes de sûreté particuliers, entre eux comme par rapport aux autres systèmes du procédé, la fréquence d'occurrence des accidents à caractère dual est bien plus faible que celle associée aux accidents simples et donc des limites de rejet plus élevées leurs sont accordées (à savoir, un risque similaire, où le risque est le produit d'une probabilité d'occurrence par la conséquence).

L'objectif associé au risque pour les premières tranches CANDU correspondait à une fréquence d'occurrence d'accident grave de moins de 10^{-5} par an. Cet objectif était satisfait en combinant les faibles fréquences d'occurrence de défaillance grave du procédé (évènements entraînant l'intervention des systèmes de sûreté particuliers) avec les taux faibles d'indisponibilité des systèmes de sûreté particuliers. Le taux global de défaillance pour les défaillances procédé graves, toutes causes confondues, devait être inférieur à un tous les trois ans, en prenant l'hypothèse d'avoir les défaillances des systèmes, conçus suivant les normes industrielles de l'époque, fonctionnant normalement. Les principaux systèmes d'atténuation qui prévenaient des rejets de combustible (arrêt, refroidissement d'urgence du cœur) et ceux destinés à contenir les produits de fission (enceinte), devaient tous présenter un taux d'indisponibilité de 3×10^{-3}.

8.4.2 Objectifs probabilistes actuels

Les considérations présentées ci-dessus ont été à l'origine des exigences de fiabilité actuelles de 1×10^{-3} pour l'indisponibilité de chacun des principaux systèmes d'atténuation (correspondant aux deux systèmes d'arrêt indépendants, au système de refroidissement d'urgence du cœur, et du système de confinement). Ceci veut dire que la fréquence de rejet majeur devrait se situer autour de 10^{-6} événement par an (à savoir une fréquence de défaillance procédé grave de (3×10^{-1}) avec deux systèmes d'atténuation ayant une indisponibilité de 10^{-3} chacun). Ceci est la base de l'objectif d'évaluation de sûreté probabiliste actuel, intégrant une marge d'analyse supplémentaire, de 10^{-7} évènement par an pour la perte des systèmes liés à la sûreté entraînant un rejet dépassant les doses réglementaires pour les événements individuels.

Pour la gamme de fréquences allant de 10^{-1} à 10^{-6} évènement par an, un certain nombre de limites de dose réglementaires s'appliquent pour en caractériser les conséquences, avec la limite qui augmente en fonction de la diminution de la fréquence de l'événement. Il convient de noter que les limites de dose réglementaires sont associées aux évènements initiateurs dans une gamme de fréquences estimée particulière, et non pas directement à la gamme de fréquences.

8.4.3 Classement des systèmes liés à la sûreté

Du fait de la nécessité de satisfaire aux critères déterministes, probabilistes et à ceux basés sur les risques, pour les rejets, des exigences de fiabilité sont imposées pour les systèmes qui jouent un rôle au niveau des séquences d'accident entraînant des rejets, que ce rôle soit lié à l'initiation, à l'arrêt ou à l'atténuation.

Habituellement, ce classement comprend les 3 catégories de systèmes suivantes, celles-ci ayant une importance décroissante pour la sûreté:

- Systèmes de sûreté particuliers, ayant un objectif d'indisponibilité de 1×10^{-3}:
  - Ensemble des systèmes d'arrêt d'urgence indépendants (arrêt réacteur)
  - Refroidissement d'urgence du cœur
  - Confinement
- Systèmes support de sûreté ayant un objectif d'indisponibilité dérivant du précédent, généralement 10^{-2},
  - Systèmes d'alimentation de secours d'urgence,
  - Pompes de refroidissement à long terme, etc.
- Systèmes de commande du procédé normaux dont la défaillance pourrait théoriquement débuter une séquence accidentelle ayant un objectif de probabilité de défaillance annuelle inférieur à 10^{-1}.
  - Systèmes de régulation du réacteur
  - Pompes de transport de la chaleur, etc.

L'utilisation croissante des EPS a par le passé mis en évidence le besoin d'ajouter de nouvelles fonctions d'atténuation qui ne relevaient pas clairement de ces trois cas, bien que la méthodologie générale utilisée pour le classement ait permis de trouver avec succès une affectation à une catégorie appropriée dans chaque cas. Un exemple de cela est présenté à l'Article 9 pour permettre de comparer les différentes méthodologies de catégorisation

8.4.4 Application des exigences de conception

Par le passé on pensait pouvoir développer des ensembles d'exigences à partir de l'importance pour la sûreté des systèmes liés à la sûreté, et que les objectifs de fiabilité visés par ces systèmes pourraient être utilisés pour choisir les ensembles de critères de conception appropriés. Cependant, ceci s'est révélé inutilisable pour les installations de type CANDU, si ce n'est pour quelques cas isolés. A la place, on a développé des exigences de conception pour chaque système lié à la sûreté sur la base de l'importance globale pour la sûreté des types de système (décrits ci-dessus), du jugement et de l'expérience des concepteurs et des analystes de sûreté, et enfin des résultats des analyses de sûreté et des EPS. Les objectifs de fiabilité des EPS (à savoir d'indisponibilité) sont utilisés pour développer des exigences particulières portant sur la redondance, la diversité et la protection contre les évènements de cause commune.

Depuis le milieu des années 90, néanmoins, des critères probabilistes ont été utilisés pour la sélection des exigences de conception lors de la conception des logiciels. Plus récemment, ceci a été étendu à l'ensemble des systèmes informatisés par l'industrie canadienne.

L'approche basée sur le risque s'applique sur la base des conséquences de la défaillance du système (fonction) à classer. Ceci est fait en associant la fonction de sûreté à sa fiabilité requise pour les séquences événementielles d'accidents.

8.4.5 Objectif de la catégorisation

La catégorisation est exigée par le document NS-R-1 (paragraphe 5.1) dans le but de garantir l'assurance qualité pour tous les aspects du système numérique lié à la sûreté qui sont

adaptés à l'importance pour la sûreté du système, et ceci de sa conception à son exploitation et pour sa maintenance.

Sans aucun doute les exigences d'assurance qualité ont une influence sur la fiabilité résultante ou atteinte par le système, mais c'est la fiabilité exigée qui détermine la catégorisation. On peut en général observer que plus la fiabilité exigée est importante, plus les autres exigences sont contraignantes, par exemple les dispositions applicables aux secours, aux défenses contre les défaillances de causes communes (au travers d'exigences telles que la séparation des voies, la qualification à l'environnement ou aux séismes, etc.), mais ces exigences proviennent des analyses d'accident ou des EPS, et non de la catégorie.

8.4.6 Principes de catégorisation

Les principes fondamentaux qui sont appliqués pour l'approche basée sur le risque dans la catégorisation sont:

a) Les concepts ayant des racines déterministes comparables dans le principe à l'application du critère de défaillance unique, du fait duquel les accidents simples comme ceux à caractère dual doivent être analysés (et qui sont en fait alignés sur cette base).

b) Des lignes de protection multiples sont nécessaires (défense en profondeur):

   (Par exemple, aucun système informatisé ou câblé ne peut prétendre avoir une indisponibilité meilleure que 10^{-3}: ceci force à utiliser des fonctions ou systèmes défensifs indépendants multiples).

c) A chaque ligne de protection est assignée une fiabilité requise, ou bien sa fiabilité requise est déterminée par la fréquence de l'évènement initiateur et la fiabilité des autres fonctions participant à la séquence évènementielle (ceci détermine l'indisponibilité permise pour les fonctions sollicitées à la demande ou la fréquence de défaillance permise pour les fonctions fonctionnant en continu). Les EPS fournissent souvent les données pour cela.

d) En général, les exigences de fiabilité les plus contraignantes sont associées aux fonctions de sûreté les plus significatives (par exemple celles dont la défaillance entraînerait les conséquences les plus graves).

e) Des exigences de fiabilité garantissant que certaines séquences évènementielles satisfont à des objectifs particuliers ont été associées à certains rôles et fonctions de sûreté:

   - Fréquence de la perte du contrôle de réactivité du réacteur < 10^{-1} par an (ce critère sera durci pour les futurs réacteurs),
   - Fréquence de demande, au global, portant sur les fonctions de catégorie A, qui requièrent une réponse dans un laps de temps très court, toutes causes confondues < 3×10^{-1} par an,
   - L'indisponibilité pour une fonction de catégorie A doit être < 10^{-3}, mais celle-ci n'est généralement pas prise en compte comme étant meilleure que 10^{-3} dans le cadre de la catégorisation des autres fonctions ou systèmes.

f) Les logiciels communs sont considérés comme des causes communes de défaillance dans les systèmes multivoies, ainsi alors que la séparation en différentes voies peut être prise en compte pour les défaillances aléatoires du matériel On ne peut pas prendre en compte la redondance, si on a du logiciel commun entre les voies redondantes.

g) La défaillance d'une fonction liée à la conception quel que soit le rôle de la fonction liée à la sûreté est considérée (prévention/atténuation, régulation du procédé, surveillance, et essais) et elle est affectée à la catégorie la plus contraignante.

h) On considère aussi la défaillance d'un système d'atténuation, telle que celui-ci démarre intempestivement et inopportunément, initiant ainsi une séquence évènementielle d'accidents ou interférant avec une autre fonction de l'installation (On note que cette prise en compte a été ajoutée pour être conforme aux éditions 2 et 3 de la CEI 61226 et le paragraphe 2.38 du document AIEA NS-G-1.3.)

i) Les défaillances partielles sont aussi prises en compte car elles peuvent jouer dans certains cas le rôle de facteur limitant.

j) Lorsque la fonction à catégoriser nécessite la réalisation d'actions de sûreté par l'opérateur, l'ensemble de la fonction (y compris les capteurs, les alarmes et les affichages, ainsi que les éléments terminaux) est catégorisée comme si elle était automatique.

k) La catégorie détermine seulement les aspects liés à l'assurance qualité du développement et de la maintenance des systèmes informatisés, elle ne définit ni la fiabilité, ni la qualification requise, ni même quelques exigences fonctionnelles ou de performances. En d'autres termes, la catégorie reflète les exigences de sûreté, elle ne les définit pas elle-même.

NOTE On suppose que la rigueur observée au niveau de l'assurance qualité pour le processus de conception a une influence sur la fiabilité obtenue: C'est pourquoi la catégorisation est réalisée pour assurer qu'un niveau de rigueur correct est défini est observé.

8.4.7 Méthodologie de catégorisation

Pour catégoriser toutes fonctions liées à la sûreté, le spectre de la fiabilité requise est découpé et le terme "importance de sûreté" décrit le segment du spectre ainsi découpé que la fonction ou le système peuvent être amenés à satisfaire. Le Tableau 5 suivant illustre l'importance de sûreté en termes de métrique de fiabilité applicable:

Tableau 5 – Importance de sûreté

Importance de sûreté	Exemples	Systèmes sollicités à la demande	Systèmes fonctionnant en continu
		Exigence liée à l'indisponibilité	Exigence liée au taux de défaillance (d/a)
Haute	Arrêt d'urgence réacteur Refroidissement d'urgence du coeur	$\leq 10^{-3}$	$\leq 10^{-3}$
Moyenne		10^{-2} ....10^{-3}	10^{-2} ....10^{-3}
Basse	Système de commande normal du procédé	$> 10^{-2}$	$> 10^{-2}$ a)

a) On note que la somme de taux de défaillance des systèmes qui entraînent la mise en oeuvre d'un système de catégorie A est limitée à moins de 3×10^{-1}/a.

Il est important de noter que "l'importance de sûreté" traduit les conséquences de la défaillance de la fonction de sûreté, telle qu'exposée ci-dessus en 8.4.3.

Du fait de la complexité des systèmes informatisés, la nature des défaillances doit être prise en compte. Certaines défaillances partielles de systèmes liés à la sûreté peuvent être plus préjudiciables que des défaillances totales et franches car elles peuvent masquer un problème et retarder les actions de systèmes alternatifs, ou bien ces défaillances peuvent avoir un impact sur un autre système. Pour ces raisons et d'autres, la catégorisation prend en compte ces défaillances partielles en les classant en trois types de défaillance, tels que présentés au Tableau 6. Dans tous les cas, l'impact de la défaillance le plus contraignant détermine la catégorie.

Tableau 6 – Type de conséquences d'une défaillance

Type de conséquences la défaillance	Description des conséquences de la défaillance
Type I	Défaillance complète de la fonction de sûreté ou toute défaillance qui empêche une fonction de sûreté de remplir ses critères de performances prévus dans l'analyse de sûreté
Type II	Défaillance partielle de la fonction de sûreté qui peut en limiter sa vitesse d'exécution, son étendue ou sa redondance interne, mais qui ne l'empêche pas de satisfaire aux performances minimales requises par l'analyse de sûreté (par exemple un des composants redondants multiples peut être l'objet d'une défaillance, mais les effets de cette défaillance se situent à l'intérieur des tolérances prévues par l'analyse)
Type III	Défaillance partielle qui n'a pas de conséquences sur les performances prévues de la fonction de sûreté dans l'analyse de sûreté (par exemple un indicateur d'état peut être l'objet d'une défaillance, alors que la fonction de sûreté est pleinement opérationnelle)

Le Tableau 7 illustre l'étape finale du processus de catégorisation, au niveau duquel on combine l'importance de sûreté au type de conséquences de la défaillance pour déterminer la catégorie.

Tableau 7 – Détermination de la catégorie

Catégorie		Type de conséquences de la défaillance		
		Type I	Type II[a)]	Type III
Importance pour la sûreté	Haute	A	B	Non classé
	Moyenne	B	C	Non classé
	Basse	C	Non classée	Non classé

[a)] En supposant que la défaillance partielle n'ait pas d'impact sur aucune autre fonction de l'installation.

Le processus de catégorisation se déroule habituellement comme suit:

a) La ou les fonctions de sûreté du système pour lesquelles du logiciel est nécessaire sont définies à partir de l'analyse de sûreté déterministe ou probabiliste.

b) L'analyse de sûreté et les EPS font l'objet de revue pour déterminer les exigences liées à l'indisponibilité ou à la fiabilité du système informatisé, et cela est alors utilisé pour affecter une mesure de fiabilité appelée « l'importance pour la sûreté » du système telle que présentée par le Tableau 5.

c) Différentes sortes de modes de défaillance sont considérés, tels que décrits ci-dessus, et le type de conséquences de la défaillance est choisi dans le Tableau 6. Ceci est une extension de l'approche classique qui ne considère que les défaillances complètes et dans certains cas écarte des séquences évènementielles plus contraignantes.

d) Le Tableau 7 est utilisé pour choisir un des quatre niveaux de catégorie de logiciel.

Si le logiciel réalise plus d'une fonction, alors le processus est répété pour chaque rôle fonctionnel, est la catégorie la plus contraignante est retenue.

8.5 Approche 4: Une approche déterministe et probabiliste combinée basée sur le document NS-R-1

8.5.1 Généralités

Le développement d'une méthodologie de classement de sûreté probabiliste qui a été utilisée pour les installations modernes est décrite ci-dessous. Ceci comprend les critères utilisés pour déterminer l'importance de sûreté de la fonction, des structures, des systèmes et des composants qui réalisent cette fonction. Une caractéristique majeure de cette approche repose sur le fait que l'approche couvre les structures et les systèmes et pas seulement les fonctions d'I&C.

Pour les réacteurs CANDU avancés, il a été décidé de développer une méthode de classement de sûreté, basée en même temps sur des principes déterministes et probabilistes, qui serait applicable à tous les composants qui sont importants pour la sûreté, et qui satisfasse pleinement aux exigences du document NS-R-1 de l'AIEA dont le paragraphe 5.2 indique que:

"La méthode suivie pour le classement d'une structure, d'un système ou d'un composant selon son importance pour la sûreté doit se fonder principalement sur des méthodes déterministes, complétées s'il y a lieu, par des méthodes probabilistes et un jugement technique, compte de facteurs tels que:

la (les) fonctions de sûreté à remplir par le constituant;

les conséquences qu'auraient le non-accomplissement de cette (ces) fonction(s);

la probabilité que le constituant soit appelé à remplir une fonction de sûreté;

le moment où il sera appelé à fonctionner à la suite d'un EIP ou la période pendant laquelle il devra fonctionner.".

Un des points clef du paragraphe du document AIEA NS-R-1 cité ci-dessus est l'exigence relative au « complément apporté par des méthodes probabilistes aux exigences déterministes ». Sur la base de cette exigence, il a été alors décidé de développer une méthode de classement de sûreté qui serait totalement compatible avec les méthodes probabilistes – à savoir, qui prendrait en compte la plupart des systèmes et composants dans les EPS – tout en conservant les critères de classement déterministes. Ceci comprend la prise en compte des probabilités et conséquences des rejets de matières radioactives, ainsi que ceux d'autres matières qui seraient dangereuses pour l'environnement. Elle serait aussi applicable à toutes les structures, systèmes et composants qui réalisent une fonction de sûreté .

8.5.2 Base de l'approche historique

On note que depuis les années 60 on a appliqué pour les tranches CANDU des critères probabilistes ou reposant sur les risques aux systèmes et composants qui réalisent des fonctions de sûreté de prévention ou d'atténuation importantes. Les critères ont été initialement définis comme une approche basée sur les défaillances simples mais aussi à caractère dual, où une « défaillance procédé grave » était supposée survenir avec une certaine fréquence d'occurrence et le critère de dose était défini avec tous les « systèmes de sûreté particuliers » opérationnels (défaillance simple), et un second critère de dose était défini avec un des « systèmes de sûreté particuliers » défaillant (défaillance à caractère dual). Une exigence relative à l'indisponibilité était définie pour chacun des « systèmes de sûreté particuliers » qui établissait l'exigence relative à la fréquence pour les rejets afin de satisfaire au critère de dose. Ceci établissait en fait trois états de la centrale distincts (fonctionnement normal, défaillance simple et défaillance à caractère dual) une fois définis les critères de fréquence et de dose de rayonnements (voir Figure 1).

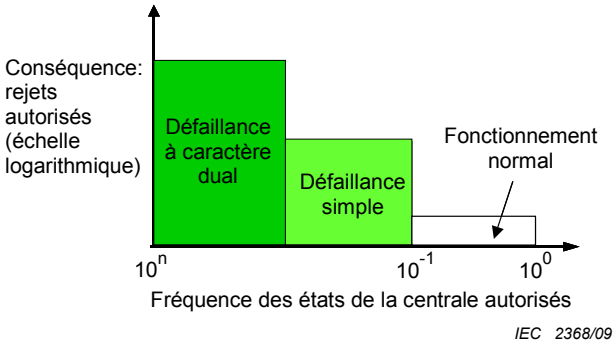


Figure 1 – Historique des états de la centrale et des rejets autorisés

Les objectifs de fiabilité système et les autres exigences de sûreté furent établis sur la base de leurs fonctions correspondant à chacun de ces états de la centrale, en termes de types de systèmes définis (systèmes de sûreté particuliers, systèmes support de sûreté, et autres systèmes liés à la sûreté). Ces exigences reposaient principalement sur les fonctions d'atténuation pour conditions accidentelles, avec aussi certaines exigences visant à prévenir les accidents. Comme indiqué en 5.4 de ce rapport, ceci représente une base pour une méthodologie cohérente de catégorisation pour les systèmes d'I&C liés à la sûreté. L'objectif était d'étendre ce concept de façon cohérente par rapport au document NS-R-1, à toutes les structures, composants et systèmes.

8.5.3 Origine des états de la centrale

Il a été décidé d'adopter les états de la centrales décrits dans le document de l'AIEA NS-R-1 (paragraphe 3.4: '…identifier les états de la centrale et les regrouper en un nombre limité de catégories suivant leur probabilité d'occurrence … ') pour définir les critères probabilistes (à savoir la fréquence et les conséquences des rejets). Les états de la centrale identifiés en conformité avec le document NS-R-1sont:

- Fonctionnement Normal (FN),
- Incident de Fonctionnement Prévu (IFP),
- Accidents de Dimensionnement (AD), et
- Accidents Hors Dimensionnement (AHD).

Pour chacun de ces états, les fréquences autorisées de fonctionnement et les autorisations de rejets sont définis (voir Figure 2).

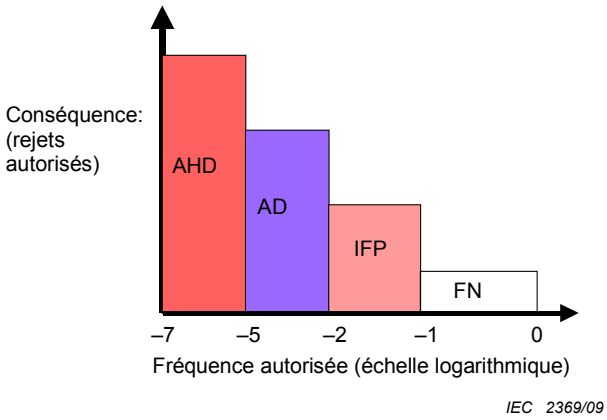


Figure 2 – Etats de la centrale et rejets autorisés