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

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

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 10
2 Normative references 10
3 Terms and definitions 11
4 Abbreviations 14
5 Limitations regarding the use of individual approaches alone 14
5.1 General 14
5.2 Limitations regarding the use of a PSA-related approach alone 14
5.3 Limitations regarding the use of the deterministic role-based approach alone 15
6 Open issues regarding categorisation 16
6.1 General 16
6.2 Why categorize: To determine requirements, or do requirements determine the category? 16
6.3 To what degree are risk-based and probabilistic methods already used implicitly? 18
6.4 How precise do PSA results need to be? 18
7 Current practices in some member states 19
7.1 General 19
7.2 Brief summaries 19
7.3 More detailed explanations 20
8 A survey of risk-related techniques of categorisation 23
8.1 General 23
8.2 Approach 1: Time and reactor states based approach 25
8.2.1 Categorisation of FSE during the design phase 25
8.2.2 Impact of safety reviews on categorisation 29
8.3 Approach 2: Quantitative importance based approach 29
8.3.1 General 29
8.3.2 Quantitative assignment criteria 30
8.3.3 Quantitative criteria 30
8.3.4 Category assignment 32
8.3.5 Classification procedure 32
8.3.6 Determination of requirements 33
8.4 Approach 3: Consequence – mitigation based approach 33
8.4.1 History: A dual licensing requirement leading to the probabilistic approach 33
8.4.2 Current probabilistic targets 33
8.4.3 Classification of safety-related systems 34
8.4.4 Application of design requirements 34
8.4.5 Purpose of categorisation 35
8.4.6 Categorisation principles 35
8.4.7 Categorisation methodology 36
8.5 Approach 4: Combined deterministic-probabilistic approach Bbased on NS-R-1 37
8.5.1 General 37
8.5.2 Basis for the historical approach 38

8.5.3 Plant state basis 38
8.5.4 Defence in depth considerations 40
8.5.5 Basis for classification – Based on IEC 61226 40
8.5.6 Application of IEC 61226 41
8.5.7 Safety classification methodology 42
8.5.8 Deterministic criteria for safety function categories 43
8.5.9 Other classification considerations 44
8.5.10 Worked example 45
8.5.11 Conclusion 46
8.6 Approach 5: Application of risk methodologies in U.S.A. nuclear regulation 46
9 Comparison of risk-related categorisation results 48
9.1 CANDU plant stepback function 48
9.1.1 Problem statement 48
9.1.2 Solution using approach 3 49
9.1.3 Comparisons with other methods 50
9.2 Conclusions arising from the use of various approaches 50
Annex A (informative) The use of PSA: methods and results 52
Annex B (informative) Approach 6: Role-Reliability-Timeframe based approach 55
Bibliography 59

Figure 1 – Historical plant states and allowed releases 38
Figure 2 – Plant states and allowed releases 39
Figure 3 – Reliability requirements for state transition barriers 40
Figure 4 – Categories required to maintain plant states 41
Figure 5 – RISC Categories 47
Figure 6 – Event sequence and layer protection identification 49

Table 1 – Classification of I&C FSE 26
Table 2 – Correspondence between IEC 61226 and INSAG-10 26
Table 3 – Minimum Requirements by Level of Function 28
Table 4 – Equipment requirements 29
Table 5 – Safety significance 36
Table 6 – Failure impact type 36
Table 7 – Category determination 37
Table 8 – Application of the changes to the safety classification methodology 43
Table B.1 – Prevention 56
Table B.2 – Termination 57
Table B.3 – Mitigation 57

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

SOMMAIRE

AVANT-PROPOS 62
INTRODUCTION 64
1 Domaine d'application 68
2 Références normatives 68
3 Termes et définitions 69
4 Abréviations 72
5 Limitations correspondant à l'utilisation exclusive d'une des approches 72
5.1 Généralités 72
5.2 Limitations correspondant à l'utilisation exclusive d'une approche liée aux EPS 73
5.3 Limitations correspondant à l'utilisation exclusive d'une approche basée sur le rôle fonctionnel 74
6 Questions ouvertes concernant la catégorisation 74
6.1 Généralités 74
6.2 La catégorisation détermine-t-elle les exigences ou les exigences sont-elles déterminées par la catégorisation? 75
6.3 Jusqu'à quel point les méthodes probabilistes ou basées sur l'évaluation des risques sont-elles déjà implicitement utilisées? 77
6.4 Quelle précision doivent avoir les EPS? 77
7 Pratiques courantes de certains états membres 78
7.1 Généralités 78
7.2 Résumés courts 78
7.3 Explications plus détaillées 80
8 Etude des techniques de catégorisation basée sur l'évaluation des risques 83
8.1 Généralités 83
8.2 Approche 1: Approche basée sur le temps et l'état du réacteur 84
8.2.1 Catégorisation des FSE au cours de la phase de conception 84
8.2.2 Impact des revues de sûreté sur la catégorisation 89
8.3 Approche 2: Approche basée sur l'importance quantitative 90
8.3.1 Généralités 90
8.3.2 Critères d'affectation quantitatifs 90
8.3.3 Critères quantitatifs 90
8.3.4 Affectation à une catégorie 92
8.3.5 Procédure de classement 93
8.3.6 Détermination des exigences 94
8.4 Approche 3: Approche basée sur les conséquences et l'atténuation 94
8.4.1 Historique: Une exigence réglementaire à caractère dual amenant à l'approche probabiliste 94
8.4.2 Objectifs probabilistes actuels 94
8.4.3 Classement des systèmes liés à la sûreté 95
8.4.4 Application des exigences de conception 95
8.4.5 Objectif de la catégorisation 95
8.4.6 Principes de catégorisation 96
8.4.7 Méthodologie de catégorisation 97
8.5 Approche 4: Une approche déterministe et probabiliste combinée basée sur le document NS-R-1 98
8.5.1 Généralités 98

8.5.2 Base de l'approche historique 99
8.5.3 Origine des états de la centrale 100
8.5.4 Considérations sur la défense en profondeur 101
8.5.5 Base du classement reposant sur la CEI 61226 102
8.5.6 Application de la CEI 61226 103
8.5.7 Méthodologie de classement de sûreté 104
8.5.8 Critère déterministe pour les catégories de fonction de sûreté 105
8.5.9 Autres considérations sur le classement 106
8.5.10 Exemple d'application 107
8.5.11 Conclusion 108
8.6 Approche 5: Application des méthodologies basées sur l'évaluation des risques dans la réglementation américaine 108
9 Comparaisons des résultats de catégorisation basée sur l'évaluation des risques 111
9.1 Fonction de repli sur une tranche CANDU plant 111
9.1.1 Enoncé du problème 111
9.1.2 Solution obtenue en utilisant l'approche 3 111
9.1.3 Comparaisons avec d'autres méthodes 112
9.2 Conclusions tirées de l'utilisation des différentes approches 113
Annexe A (informative) Utilisation des EPS: méthodes et résultats 115
Annexe B (informative) Approche 6: approche basée sur le rôle fonctionnel, la fiabilité et prise en compte du temps (qui était appelée "approche basée sur la défense en profondeur") 119
Bibliographie 123

Figure 1 – Historique des états de la centrale et des rejets autorisés 100
Figure 2 – Etats de la centrale et rejets autorisés 100
Figure 3 – Exigences de fiabilité relative aux barrières de changement d'état 101
Figure 4 – Catégories nécessaires au maintien des états de la centrale 103
Figure 5 – Catégories RISC 110
Figure 6 – Identification de la séquence d'évènements et des niveaux de protection 112

Tableau 1 – Classement des FSE d'I&C 86
Tableau 2 – Correspondance entre la CEI 61226 et l'INSAG-10 86
Tableau 3 – Exigences minimums par niveau de fonction 88
Tableau 4 – Exigences portant sur l'équipement 89
Tableau 5 – Importance de sûreté 97
Tableau 6 – Type de conséquences d'une défaillance 98
Tableau 7 – Détermination de la catégorie 98
Tableau 8 – Application des modifications à la méthodologie de classement de sûreté 105
Tableau B.1 – Prévention 120
Tableau B.2 – Achèvement 121
Tableau B.3 – Mitigation 121

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