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 It also gives information on projects, withdrawn and replaced publications.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

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.