

TECHNICAL REPORT

RAPPORT TECHNIQUE



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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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 It also gives information on projects, withdrawn and replaced publications.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

TECHNICAL REPORT

RAPPORT TECHNIQUE



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

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-1¹):

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, systems² 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, 5.3.4.1.

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 $\sim 10^{-4}$. 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 IV³ 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 consequences⁴. 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 frequency 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

State of reactor	I&C FSE to be used in the safety analysis			
	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 Authority⁵.

⁵ This document is available on the Autorité de sûreté 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 $10^{-7}/y$ 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 $10^{-5}/\text{ry}$.

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 damage⁶. 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.

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

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

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:

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

where

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

K_j is the j th 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:

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

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, lightning) 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 $< 3 \times 10^{-1}$ 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		$10^{-2} \dots 10^{-3}$	$10^{-2} \dots 10^{-3}$
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 $3 \times 10^{-1}/y$.			

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:

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