

Nuclear power plants — Use of probabilistic safety assessment for the classification of instrumentation and control functions

ICS 27.120.20

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI
Documents

AVA

Document Sharing Hub

National foreword

This British Standard reproduces verbatim IEC/TR 61838:2001 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Reactor instrumentation, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

From 1 January 1997, all IEC publications have the number 60000 added to the old number. For instance, IEC 27-1 has been renumbered as IEC 60027-1. For a period of time during the change over from one numbering system to the other, publications may contain identifiers from both systems.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the IEC/TR title page, pages 2 to 40, an inside back cover and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

This British Standard, having been prepared under the direction of the Engineering Sector Committee, was published under the authority of the Standards Committee and comes into effect on 15 May 2001

© BSI 05-2001

Amendments issued since publication

Amd. No.	Date	Comments

ISBN 0 580 36648 0

**RAPPORT
TECHNIQUE
TECHNICAL
REPORT**

**CEI
IEC**

TR 61838

Première édition
First edition
2001-02

**Centrales nucléaires –
Fonctions d'instrumentation et de contrôle-
commande importants pour la sûreté –
Utilisation des évaluations probabilistes
de sûreté pour le classement**

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



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CONTENTS

	Page
FOREWORD	4
INTRODUCTION	6
Clause	
1 Scope	8
2 Reference documents	8
3 Definitions and abbreviations.....	9
3.1 Definitions	9
4 Limitations regarding the use of PSA.....	12
5 The use of PSA: methods and results.....	12
5.1 Introduction.....	12
5.2 Use of PSA in the design of future NPPs	13
5.2.1 Overall scope	13
5.2.2 Methods.....	13
5.2.3 Plant analysis and modelling I&C in PSA	15
5.3 Benefits of the use of PSA for existing NPPs	15
6 The use of PSA for classification.....	16
6.1 General	16
6.2 Approach 1: time and reactor states based approach	17
6.2.1 Use of PSA in conjunction with a functional deterministic method	17
6.2.2 Classification of functions, systems and equipment	17
6.2.3 Associated technical requirements	20
6.2.4 Complementary use of PSA alongside the iterative design process	20
6.3 Approach 2: quantitative importance based approach	21
6.3.1 Quantitative assignment criteria	21
6.3.2 Quantitative criteria	21
6.3.3 Category assignment.....	24
6.3.4 Classification procedure	24
6.3.5 Determination of requirements	25
6.4 Approach 3: consequence – mitigation based approach.....	25
6.4.1 Historical probabilistic approach	25
6.4.2 Current probabilistic target	25
6.4.3 Safety related system classification	25
6.4.4 Application of design requirements	27
6.4.5 Conclusions from approach 3	27
6.5 Approach 4: defence-in-depth based approach	28
6.5.1 Introduction.....	28
6.5.2 The classification scheme	29
6.5.3 Combining the results.....	30

Annex A (informative) Proposal for modelling I&C in PSA.....	31
A.1 Scope	31
A.1.1 Background.....	31
A.1.2 I&C modelling in PSA	31
A.2 Modelling description	32
A.2.1 Global description	32
A.2.2 Sensor part	32
A.2.3 Logic part.....	33
A.2.4 Actuator part	33
A.3 Quantitative analysis: unavailability values.....	33
A.3.1 Use of less classified systems for safety functions and modelling in PSA	33
A.3.2 Sensor part	33
A.3.3 Specific logic part.....	34
A.3.4 Non-specific logic part.....	35
A.3.5 Actuator part	36
A.4 Use of modelling in the event trees of PSA	36
A.4.1 Taking account of different I&C configurations	36
A.4.2 Importance of the actuators.....	37
A.4.3 Integration in PSA event trees	38
Annex B (informative) Bibliography	40
Figure A.1 – Channel modelling	32
Figure A.2 – Voting distribution	37
Figure A.3 – Fault trees	38
Figure A.4 – Event trees	39
Table 1 – Classification of I&C FSE	19
Table 2 – Functional requirements	20
Table 3 – Equipment requirements	20
Table 4 – Prevention	29
Table 5 – Termination.....	30
Table 6 – Mitigation	30
Table A.1 – Unavailability of sensors	34
Table A.2 – Unavailability for specific logic part.....	34
Table A.3 – Unavailability for non-specific logic part.....	35

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports, or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this technical report may be the subject of patent rights. The 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: Reactor instrumentation, of IEC technical committee 45: Nuclear instrumentation.

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

Enquiry draft	Report on voting
45A/363/CDV	45A/388/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 3.

This document, which is purely informative, is not to be regarded as an International Standard.

Annexes A and B are given for information only.

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be:

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

INTRODUCTION

IEC 61226 "Nuclear power plants – Instrumentation and control systems important for safety – Classification" was published in 1993. The need to classify instrumentation and control functions on nuclear power plants originates from an International Atomic Energy Agency (IAEA) recommendation. 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 categories of safety significance, but it is the functions which determine the fundamental categorization.

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 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 is a deterministic process and takes no 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.

For several years, how a risk based classification scheme could be incorporated into IEC 61226 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 problems when drafting an International Standard, namely:

- a) 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?
- b) If a risk-based classification leads to different classifications of FSE compared to the deterministic approach, which should take precedence?
- c) 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. Risk assessment results could lead to the classification of specific I&C functions being downgraded (because of plant-specific design features). Should this downgrading be limited in some way?
- d) Should the use of risk assessments be mandated when considering the effectiveness of plant and I&C modifications throughout existence? Similarly, should requirements be included for the use of risk assessments in making decisions about preventive maintenance?

Having discussed these issues extensively, it has been recommended that an amendment to IEC 61226 is premature at this time. In order to advance the debate, however, this Technical Report presents a number of different approaches to the use of probabilistic risk assessment in the classification of FSE.

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

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 techniques, in conjunction with the consequence based classification approach given in IEC 61226, is currently decided by the utility and/or regulator within member Nations. In the absence of an internationally agreed approach, this should continue, but this Technical Report is intended to stimulate debate on this subject and encourage the convergence of views so that an IEC International Standard can be agreed.

The safety principles and the usefulness of a risk-based approach to classification are discussed and a description of four different approaches is presented.

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 probabilistic safety assessment (PSA) techniques.

Guidance is given in annex A on modelling instrumentation and control functions for probabilistic risk assessment.

2 Reference documents

IAEA publications

50-SG-D8:1984, *Safety-related instrumentation and control systems for nuclear power plants*

INSAG 3: *Basic safety principles for nuclear power plants*

IEC publications

IEC 60964:1989, *Design for control rooms of nuclear power plants*

IEC 61226:1993, *Nuclear power plants – Instrumentation and control systems important for safety – Classification*

3 Definitions and abbreviations

For the purposes of this technical report, the following definitions apply. The definitions are consistent with, or identical to (if marked with an asterisk) those used in other IEC or IAEA codes and standards.

3.1 Definitions

3.1.1

diversity

the existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defence against common mode failure. It may be achieved by providing systems that are different from each other, or by functional diversity, where similar systems achieve the specified objective by performing different functions, or by provision in the development process, for example by having separate design teams and verification and validation teams

NOTE This definition is wider than that used by the IAEA 50-C-D, which is as follows:

"The existence of redundant components or systems to perform an identified function, where such components or systems collectively incorporate one or more different attributes.

Examples of such attributes are: different operating conditions, different sizes of equipment, different manufacturers, different working principles and types of equipment that use different physical methods".

3.1.2

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 61226]

3.1.3

function*

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

[IEC 61226]

3.1.4

functionality

a qualitative indication of the range or scope of the functions that a system or item of equipment can carry out. A system that can carry out many complex functions has a "high functionality"; a system that can only carry out a few simple functions has a "low functionality"

[IEC 61226]

3.1.5

I&C FSE important for safety*

the I&C FSE that comprise:

- a) those I&C FSE whose malfunction or failure could lead to undue radiation exposure of the site personnel or members of the public;
- b) those I&C FSE that prevent anticipated operational occurrences from leading to a significant sequence;
- c) those I&C FSE that mitigate the consequences of malfunction or failure of structures, systems, or components

[IEC 61226]

3.1.6

NPP safety*

the prevention of an unplanned or uncontrolled release of radioactive material that might injure the health of the NPP operating staff or the public

[IEC 61226]

3.1.7

nuclear safety*

the ability of an NPP to avoid or prevent a nuclear accident, that is an unplanned or uncontrolled criticality of magnitude that causes damage

[IEC 61226]

3.1.8

on-line*

the state of a system that is carrying out its specified functions as required by the NPP design

[IEC 61226]

3.1.9

performance

the effectiveness with which an intended function is performed (e.g. time response, accuracy, sensitivity to parameter changes)

[IEC 61226]

3.1.10

postulated initiating event (PIE)*

events that lead to anticipated operational occurrences and accident conditions, their credible causal failure effects and their credible combinations

[IEC 61226]

3.1.11

redundancy*

provision of more than the minimum number of (identical or diverse) elements or systems, so that the loss of one does not result in the loss of the required function as a whole

[IEC 61226]

3.1.12

safety function*

a specific purpose that must be accomplished for safety

[IEC 61226]

3.1.13

safety system*

systems important for safety, provided to ensure, in any condition, the safe shutdown of the reactor and the heat removal from the core, and/or to limit the consequences of PIE and significant sequence

[IEC 61226]

3.1.14

safety related I&C FSE*

those I&C FSE important for safety that are not part of the safety systems

[IEC 61226]

3.1.15**significant sequence***

a 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

[IEC 61226]

3.1.16**single failure criterion***

an assembly of equipment satisfies the single failure criterion if it can meet its purpose despite a single random failure assumed to occur anywhere in the assembly. Consequential failures resulting from the assumed single failure are a part of the single failure

[IEC 61226]

3.1.17**sub-system***

a division of a system that in itself has the characteristics of a system

[IEC 61226]

3.1.18**system***

a set of interconnected elements constituted to achieve a given objective of carrying out a specified function

[IEC 61226]

Abbreviations

CCF	Common cause failure
DBC	Design basis conditions
DEC	Design extension conditions
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

4 Limitations regarding the use of PSA

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. The use of PSA techniques in the design and in-service support of NPPs has been limited, however, because of several factors:

- the development and use of probabilistic safety assessment techniques continues to evolve within member nations and its level of acceptance is 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.

Also, even when the PSA is applied to an existing design, there are often technical limitations in the analysis which 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 exclusion of operational states other than the full power state,
- 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 the case of a new design, the application of PSA results to I&C systems and equipment is further restricted by the inability of the designer to define in detail all the required I&C functions.

For these reasons, 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 which has been firmly established in the safety design basis of NPPs (see IEC 61226). 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, as described in the following clauses.

5 The use of PSA: methods and results

5.1 Introduction

The design of an NPP is principally based upon stringent deterministic requirements and on the well-understood and well-proven defence-in-depth principles. However, probabilistic studies can be carried out to determine, in a quantitative format, the relative importance of the instrumentation and control functions in the overall safety of the NPP.