IEC 61226

Edition 3.0 2009-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande

IEC 61226:2009

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

About the IEC

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

About IEC publications

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

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 It also gives information on projects, withdrawn and replaced publications.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

A propos de la CEI

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

A propos des publications CEI

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

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

IEC 61226

Edition 3.0 2009-07

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX V

ICS 27.120.20

ISBN 978-2-88910-448-2

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – CLASSIFICATION OF INSTRUMENTATION AND CONTROL 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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.

International Standard IEC 61226 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This third edition cancels and replaces the second edition published in 2005 and constitutes a technical revision. The main changes with respect to the previous edition are listed below:

- to introduce a definition for "non-hazardous stable state";
- to clarify limits of categories;
- to clarify requirements related to equipment used for beyond design events.

The text of this standard is based on the following documents:

FDIS	Report on voting
45A/745/FDIS	45A/767/RVD

Full information on the voting for the approval of this standard 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.

INTRODUCTION

a) Technical background, main issues and organisation of the standard

This International Standard responds to an International Atomic Energy Agency (IAEA) requirement[1] to classify nuclear power plants instrumentation and control systems according to their importance to safety. With distributed computer based I&C systems now being used for NPP instrumentation and control systems, the functions important to safety are distributed over several systems or subsystems. Therefore, it is the intent of this standard to

– classify the I&C functions important to safety into categories, depending on their contribution to the prevention and mitigation of postulated initiating events (PIE), and to develop requirements that are consistent with the importance to safety of each of the categories;
– assign specification and design requirements to I&C systems and equipment concerned which perform the classified functions.

According to IAEA recommendation,[2] the methods of classification are primarily based on the deterministic safety analysis, and should be complemented where appropriate by probabilistic methods. Several possible approaches for use of probabilistic safety assessment (PSA) for classification are described in IEC/TR 61838, “Nuclear power plants – Instrumentation and control important to safety – Use of probabilistic safety assessment for the classification of functions”.

This revision of the standard enables quantitative assessment to be partly taken into account.

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

IEC 61226 is directly referenced by IEC 61513 and is the second level SC 45A document tackling the issue of categorization of functions and classification of systems.

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

c) Recommendation and limitation regarding the application of this standard

Correct classification of functions directs the appropriate degree of attention by the plant's designers, operators and regulatory authorities to the specification, design, qualification, quality assurance (QA), manufacturing, installation, maintenance, and testing of the systems that ensure the safety functions.

---

1 IAEA NS-R-1 requirement 5.1.

2 The NS-R-1, section 5.2 requires that the method for classifying the safety significance of a structure, system or component shall be primarily based on deterministic methods complemented where appropriate by probabilistic methods and sound engineering judgment taking into account factors such as

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

b) the consequences of failure to perform the function;

c) the probability that it (the I&C system) will be required to perform a safety function;

d) the time following a PIE at which, or the period throughout which it (the I&C system) will be called upon to operate.

This standard establishes the criteria and methods to be used to assign the I&C functions of a NPP to three categories A, B and C, which depend on the importance of the function for safety, and an unclassified category for functions with no direct safety role. It outlines generic requirements for each category, and specifies basic technical requirements for matters such as QA, reliability, testing and maintenance.

The category to which a function is assigned determines generic and specific technical requirements. Generic requirements for each function are based on providing the appropriate level of assurance that it will be executed on demand with the required performance and reliability level. This applies to the aspects of functionality, reliability, performance, environmental durability and QA. The level of assurance to be shown for each of these aspects must be consistent with the importance of the function to safety.

i) Assurance of functionality is established by the creation of a complete and comprehensive requirements specification, and the application of appropriate standards and codes.

ii) Assurance of reliability is provided by the selection of appropriate components, structures and levels of redundancy and diversity in association with physical separation and/or barriers, electrical isolation and periodic testing during service.

iii) Assurance of performance is gained by the creation of specifications of the required performance, the application of QA procedures, verification and validation processes during design and manufacture, pre-service testing of the individual and integrated systems and equipment, and testing during service.

iv) Assurance of environmental durability is established by equipment qualification programmes to ensure that ageing effects and environmental conditions that exist when the equipment is required to operate do not degrade its performance below that required.

v) Assurance that the aspects of functionality, performance, environmental durability and reliability have been properly considered at each stage from conception, through design, manufacture, test, installation, commissioning and entry into service is provided by carrying out each stage of the work under the control of an appropriate QA program.

Throughout this standard, the auxiliary "shall" indicates requirements that are mandatory for compliance with the standard, the auxiliary "should" indicates requirements that are not mandatory for compliance with the standard but are strongly recommended and the auxiliary "may" indicates requirements that are optional.

d) Description of the structure of the 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 publications of IEC 61508 series 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 terms and definitions used by SC 45A standards are consistent with those used by the IAEA.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – CLASSIFICATION OF INSTRUMENTATION AND CONTROL FUNCTIONS

1 Scope

This International Standard establishes a method of classification of the information and command functions for nuclear power plants, and the I&C systems and equipment that provide those functions, into categories that designate the importance to safety of the function. The resulting classification then determines relevant design criteria.

The design criteria are the measures of quality by which the adequacy of each function in relation to its importance to plant safety is ensured. In this standard, the criteria are those of functionality, reliability, performance, environmental durability (including seismic) and quality assurance (QA).

This standard is applicable to all the information and command functions and the instrumentation and control (I&C) systems and equipment that provide those functions. The functions, systems and equipment under consideration provide automated protection, closed or open loop control and information to the operating staff. They keep the NPP conditions inside the safe operating envelope and provide automatic actions, or enable manual actions, that prevent or mitigate accidents, or that prevent or minimize radioactive releases to the site or wider environment. The I&C functions that fulfil these roles safeguard the health and safety of the NPP operators and the public.

This standard follows the general principles given in IAEA safety code NS-R-1 and safety guide NS-G-1.3, and it defines a structured method of applying the guidance contained in those codes and standards to the I&C systems that perform functions important to safety in a NPP. This standard should be read in association with the IAEA guides and IEC 61513 in implementing the requirements of IEC 61508 series.

2 Normative references

The following referenced documents are indispensable for the application of 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 60671:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 60709, *Nuclear power plants – Instrumentation and control systems important to safety – Separation*

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

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

IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

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

IEC 60965, *Supplementary control points for reactor shutdown without access to the main control room*

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

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

IEC 61000-4 (all parts), *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

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

IEC 61771, *Nuclear power plants – Main control room – Verification and validation of design*

IEC 61772, *Nuclear power plants – Main control room – Application of visual display units (VDU)*

IEC 61839, *Nuclear power plants – Design of control rooms – Functional analysis and assignment*

IEC 62138, *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, *Safety of nuclear power plants: Design*

IAEA GS-R-3:2006, *The management system for facilities and activities* (available in English only)

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

3 Terms and definitions

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

3.1
anticipated operational occurrence
operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety nor lead to accident conditions

[IAEA Safety Glossary:2007]

3.2
common cause failure
CCF
failure of two or more structures, systems or components due to a single specific event or cause

[IAEA Safety Glossary:2007]

3.3
design basis accident
DBA
accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits

[IAEA Safety Glossary:2007]

3.4
design basis event
DBE
group of design basis accidents and anticipated operational occurrences

NOTE See also 3.13.

3.5
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]

NOTE The following definition was given in 3.5 of IEC 60880 for the term "diversity": *Existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defence against common cause failure. It may be achieved by providing systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective in different ways*. It is totally consistent with the IAEA definition given here.

3.6
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, 3.17, modified]

3.7
function
specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it

3.8
functionality
attribute of a function which defines the operations which transform input information into output information

[IEC 61513, 3.25]

3.9
human factor engineering programme
programme that describes at least the human factors organisation, role and mission of human factors specialists and team, human factors activities and their integration in the design and validation process, list of deliverables to be provided at each step of the program

3.10
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]

NOTE Items important to safety considered in this standard are mainly I&C systems important to safety.

3.11
non-hazardous stable state
state of the plant, where stabilisation of any transient has been achieved, the reactor is subcritical, adequate heat removal is ensured and radioactive releases are limited

NOTE A transient is considered to be stabilised when, for all safety significant parameters, the margins (e.g. between the heat removal capacity and heat generation) are either stable or increasing, or sufficient margin remains to cover all expected physical processes.

3.12
performance
effectiveness with which an intended function is carried out (e.g. time response, accuracy, sensitivity to parameter changes)

3.13
plant states

<table>
<tr><td colspan="2">Operational states</td><td colspan="3">Accident conditions</td></tr>
<tr><td rowspan="3">Normal operation</td><td colspan="3">Design basis events</td><td colspan="2" rowspan="2">Beyond design basis accidents</td></tr>
<tr><td>Anticipated operational occurrences</td><td>a)</td><td>Design basis accidents</td></tr>
<tr><td colspan="3"></td><td>b)</td><td>Severe accidents</td></tr>
<tr><td colspan="3"></td><td colspan="2">Accident management</td></tr>
</table>

a) Accident conditions which are not explicitly considered design basis accidents but which are encompassed by them.

b) Beyond design basis accidents without significant core degradation.

NOTE This definition is consistent with the one of the IAEA safety glossary. It just indicates the position of the concept of “design basis event” compared to the other concepts.

3.14
postulated initiating event
PIE
event identified during design as capable of leading to anticipated operational occurrences or accident conditions

[IAEA Safety Glossary:2007]

3.15
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]

3.16
safety group
assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded

[IAEA Safety Glossary:2007]

3.17
safety related system
a system important to safety that is not part of a safety system

[IAEA Safety Glossary:2007]

3.18
safety system
a 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 accident

[IAEA Safety Glossary:2007]

3.19
single failure
a failure which results in the loss of capability of a system or component to perform its intended safety function(s), and any consequential failure(s) which result from it

[IAEA Safety Glossary:2007]

3.20
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, 3.61]

3.21
type test
conformity test made on one or more items representative of the production

[IEV 394-40-02]

3.22
unacceptable consequence
consequence of an operational state or of a PIE, that exceeds specified limits for the corresponding plant states, in terms of releases at the site or to the wider environment

NOTE Additional limits, such as unacceptable fuel damage, or damage to other main components may also be specified on a national basis. This might be either a massive, uncontrolled release caused by events with a frequency that is beyond the NPP's design basis, or events with a frequency that is in the design basis but leading to a magnitude exceeding specified limits. Additional limits, such as unacceptable fuel damage may also be specified. This might be damage to the fuel cladding 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. Damage to the other barriers may also be considered as unacceptable consequence.

4 Abbreviations

ALARA	As low as reasonably achievable
DBA	Design basis accident
DBE	Design basis event
FAT	Factory acceptance test
FMEA	Failure modes and effects analysis
HMI	Human machine interface
IAEA	International Atomic Energy Agency
I&C	Instrumentation and control
NPP	Nuclear power plant
PIE	Postulated initiating event
PRA	Probabilistic risk assessment
QA	Quality assurance
SAT	Site acceptance test

5 Classification scheme

5.1 General

Functions to be performed by I&C systems shall be assigned to categories according to their importance to safety. The importance to safety of a function shall be identified by means of the consequences in the event of its failure when it is required to be performed and the consequences in the event of a spurious actuation. The category determines the design and quality requirements for I&C systems and equipment. These requirements shall be defined independently from the technology of the equipment to be applied. Subclause 5.2 provides the background to the classification scheme.

Subclause 5.3 describes the three categories that are used to classify functions. The categories are based upon those defined originally in the first edition of IEC 61226 published in 1993.

Subclause 5.4 presents the assignment criteria for each category.

Clause 6 provides guidance on the classification process.

Clause 7 provides the technical requirements for each of the three categories. Most of the requirements apply to the systems and equipment that perform the functions, but some requirements apply only to the functions.

Annex A contains typical examples of the classification of NPP I&C functions. It is only for information because it may depend on the reactor type.