

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

ICS 27.120.20

National foreword

This British Standard is the UK implementation of IEC 61226:2005.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Reactor instrumentation.

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

In the opinion of the UK committee, specific clauses of IEC 61226 Edition 2.0 imply requirements that are contrary to the custom, practice, and regulatory expectations as set down by the United Kingdom Health and Safety Executive's Nuclear Installations Inspectorate and the understanding in the United Kingdom of the IAEA safety guides. Users of this standard are therefore advised that, in the United Kingdom, this standard should be read in conjunction with the attached National annex NA (informative) that explains how the requirements of this standard could be used for plant that is subject to regulatory licensing.

The specific parts of this standard that are the subject of the National annex NA are:

- clause 5.3 (description of categories) and clause 5.4 (assignment criteria);
- clause 7.4.1 (basic equipment requirements), and
- Annex A (examples of categories).

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2007

© BSI 2007

ISBN 978 0 580 60524 6

Amendments issued since publication

Amd. No.	Date	Comments
17452 Corrigendum No. 1	30 November 2007	Correction to national foreword

INTERNATIONAL STANDARD

IEC
61226

Second edition
2005-02

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



Reference number
CEI/IEC 61226:2005

CONTENTS

INTRODUCTION.....	3
1 Scope	6
2 Normative references	6
3 Terms and definitions	8
4 Abbreviations	10
5 Classification scheme	11
5.1 Introduction	11
5.2 Background	11
5.3 Description of categories	12
5.3.1 General	12
5.3.2 Category A	12
5.3.3 Category B	13
5.3.4 Category C	13
5.4 Assignment criteria	13
5.4.1 Category A	13
5.4.2 Category B	14
5.4.3 Category C	14
6 Classification procedure	15
6.1 Identification of design basis	15
6.2 Identification and classification of functions	15
7 Assignment of technical requirements to categories	18
7.1 General requirements	18
7.2 Requirements related to functions	18
7.2.1 Basic requirements	18
7.2.2 Specific requirements	19
7.3 Requirements related to I&C systems	19
7.3.1 Basic requirements	19
7.3.2 Specific requirements	20
7.4 Requirements related to equipment	22
7.4.1 Basic requirements	22
7.4.2 Specific requirements	22
7.5 Requirements related to quality aspects	23
7.5.1 Basic requirements	23
7.5.2 Specific requirements	24
Annex A (informative) Examples of categories	27
National annex (informative) Commentary on categories and assignment criteria	29
Figure 1 – Method of classification	17
Table 1 – Tabular correlation between categories and other IEC standards	26

INTRODUCTION

Technical background, main issues and organisation of the standard

This International Standard responds to an International Atomic Energy Agency (IAEA) requirement¹ 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 61838:2001: “Nuclear power plants – Instrumentation and control functions important for safety – Use of probabilistic safety assessment for the classification”.

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

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 the fourth paragraph of this introduction.

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 an 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.

- a) Assurance of functionality is established by the creation of a complete and comprehensive requirements specification, and the application of appropriate standards and codes.
- b) 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.
- c) 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.
- d) 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.
- e) 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 term "shall" indicates requirements that are mandatory for compliance with the standard, the term "should" indicates requirements that are not mandatory for compliance with the standard but are strongly recommended and the term "may" indicates requirements that are optional.

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 SC 45A standard series is IEC 61513. It provides general requirements for instrumentation and control systems and equipment (I&C systems) that are used to perform functions important to safety in nuclear power plants (NPPs). IEC 61513 structures the SC 45A standard series.

IEC 61513 refers directly to other 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, SC 45A standards generally 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 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, parts 1, 2 and 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, Part 3 for the nuclear application sector.

IEC 61513 refers to ISO as well as to IAEA 50-C-QA for topics related to quality assurance.

The SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of nuclear power plants and in the IAEA safety series, in particular the requirements NS-R-1, "Safety of Nuclear Power Plants: Design" and the safety guide NS-G-1.3, "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 SYSTEMS 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 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 an NPP. This standard should be read in association with the IAEA guides and IEC 61513 in implementing the requirements of IEC 61508.

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 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, *Nuclear power plants – I&C systems important to safety – Software aspects for computer-based systems performing category A functions*³

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

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, *Programmed digital computers important to safety for nuclear power stations*

IEC 61000-4 (all parts), *Electromagnetic Compatibility – Testing and measurement techniques*

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

IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61513, *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 Safety Standard Series Requirements NS-R-1:2000, *Safety of Nuclear Power Plants: Design*

IAEA Code 50-C/SG-Q:2001, *Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations*

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

³ To be published.

3 Terms and definitions

For the purposes of this document, the following definitions – given in alphabetical order – apply. They are consistent, or where it was possible, identical with those used in other current IEC or IAEA codes, guides and standards.

3.1

anticipated operational occurrences

all operational processes deviating from normal operation which are expected to occur once or several times during the operating life of the plant and which, in view of appropriate design provisions, do not cause any significant damage to items important to safety or lead to accident conditions

3.2

common cause failure

CCF

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

3.3

design basis accident

DBA

accident conditions against which the nuclear power plant 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

3.4

design basis event

DBE

term used to address the group of design basis accidents and anticipated operational occurrences

3.5

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.

NOTE This definition (source: IEC 60880) is wider than that used by the IAEA NS-G-1.3 which is as follows:

"The presence of two or more systems or components to carry out an identified function, where the different systems or components have different attributes so as to reduce the possibility of common mode failure."

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.

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

3.9

human factor engineering programme

programme that describes at least 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

I&C systems important for safety

I&C systems whose malfunction or failure could lead to undue radiation exposure of the site personnel or members of the public, and those I&C systems that prevent anticipated operational occurrences from leading to unacceptable consequences

3.11

plant states

Operational states		Accident conditions			
	Design basis events			Beyond design basis accidents	
Normal operation	Anticipated operational occurrences	a)	Design basis accidents		
				b)	Severe accidents
				Accident management	
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.					

3.12

performance

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

3.13

postulated initiating events

PIE

events identified during design as capable of leading to anticipated operational occurrences or accident conditions

3.14

redundancy

provision of alternative (identical or diverse) structures, systems or components, so that the loss of one does not result in the loss of the required function as a whole

3.15

safety group

assembly of equipment designated to perform all actions required for a particular PIE to ensure that the limits specified in the design basis for DBE are not exceeded