

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

This document is a preview generated by EVS

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN 61226:2010 sisaldab Euroopa standardi EN 61226:2010 ingliskeelset teksti.

Standard on kinnitatud Eesti Standardikeskuse 30.04.2010 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.

Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 12.03.2010.

Standard on kättesaadav Eesti standardiorganisatsioonist.

This Estonian standard EVS-EN 61226:2010 consists of the English text of the European standard EN 61226:2010.

This standard is ratified with the order of Estonian Centre for Standardisation dated 30.04.2010 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.

Date of Availability of the European standard text 12.03.2010.

The standard is available from Estonian standardisation organisation.

ICS 27.120.20

Standardite reprodutseerimis- ja levitamiseõigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel on keelatud ilma Eesti Standardikeskuse poolt antud kirjaliku loata.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:
Aru 10 Tallinn 10317 Eesti; www.evs.ee; Telefon: 605 5050; E-post: info@evs.ee

Right to reproduce and distribute Estonian Standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without permission in writing from Estonian Centre for Standardisation.

If you have any questions about standards copyright, please contact Estonian Centre for Standardisation:
Aru str 10 Tallinn 10317 Estonia; www.evs.ee; Phone: +372 605 5050; E-mail: info@evs.ee

**Nuclear power plants -
Instrumentation and control important to safety -
Classification of instrumentation and control functions
(IEC 61226:2009)**

Centrales nucléaires de puissance -
Instrumentation et contrôle-commande
importants pour la sûreté -
Classification des fonctions
d'instrumentation
et de contrôle-commande
(CEI 61226:2009)

Kernkraftwerke -
Leittechnische Systeme
mit sicherheitstechnischer Bedeutung -
Kategorisierung leittechnischer
Funktionen
(IEC 61226:2009)

This European Standard was approved by CENELEC on 2010-03-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of the International Standard IEC 61226:2009, prepared by SC 45A, Instrumentation and control of nuclear facilities, of IEC TC 45, Nuclear instrumentation, was submitted to the CENELEC formal vote for acceptance as a European Standard and was approved by CENELEC as EN 61226 on 2010-03-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates are proposed:

- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2011-03-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2013-03-01

Annex ZA has been added by CENELEC.

As stated in the nuclear safety Directive 2009/71/EURATOM, Chapter 1, Article 2, item 2, Member States are not prevented from taking more stringent safety measures in the subject-matter covered by the Directive, in compliance with Community law. In a similar manner, this European Standard does not prevent Member States from taking more stringent nuclear safety measures in the subject-matter covered by this European Standard.

Review generated by EVS

Endorsement notice

The text of the International Standard IEC 61226:2009 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61508-1 NOTE Harmonized as EN 61508-1.

IEC 61508-2 NOTE Harmonized as EN 61508-2.

IEC 61508-3 NOTE Harmonized as EN 61508-3.

IEC 61508-4 NOTE Harmonized as EN 61508-4.

This document is a preview generated by EVS

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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)	EN 60812	-
IEC 60880	2006	Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions	EN 60880	2009
IEC 60964	-	Nuclear power plants - Control rooms - Design	EN 60964	-
IEC 60965	-	Nuclear power plants - Control rooms - 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	EN 60987	-
IEC 61000-4	Series	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques	EN 61000-4	Series
IEC 61000-6-2	-	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments	EN 61000-6-2	-
IEC 61513	2001	Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems	-	-

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61771	-	Nuclear power plants - Main control-room - Verification and validation of design	-	-
IEC 61772	-	Nuclear power plants - Control rooms - Application of visual display units (VDUs)	-	-
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	EN 62138	-
IAEA NS-R-1	2000	Safety of nuclear power plants: Design	-	-
IAEA GS-R-3	2006	The management system for facilities and activities : safety requirements	-	-
IAEA NS-G-1.3	2002	Instrumentation and control systems important to safety in nuclear power plants	-	-

This document is a preview generated by EVS

CONTENTS

FOREWORD.....	3
INTRODUCTION.....	5
1 Scope.....	8
2 Normative references	8
3 Terms and definitions	9
4 Abbreviations	13
5 Classification scheme.....	13
5.1 General.....	13
5.2 Background	14
5.3 Description of categories.....	14
5.3.1 General	14
5.3.2 Category A	15
5.3.3 Category B.....	15
5.3.4 Category C.....	15
5.4 Assignment criteria.....	16
5.4.1 General	16
5.4.2 Category A	16
5.4.3 Category B.....	16
5.4.4 Category C.....	17
6 Classification procedure	17
6.1 General.....	17
6.2 Identification of design basis	18
6.3 Identification and classification of functions.....	18
7 Assignment of technical requirements to categories	21
7.1 General requirements.....	21
7.2 Requirements related to functions	21
7.2.1 Basic requirements.....	21
7.2.2 Specific requirements.....	22
7.3 Requirements related to I&C systems.....	22
7.3.1 Basic requirements.....	22
7.3.2 Specific requirements.....	23
7.4 Requirements related to equipment.....	25
7.4.1 Basic requirements.....	25
7.4.2 Specific requirements.....	25
7.5 Requirements related to quality aspects	26
7.5.1 Basic requirements.....	26
7.5.2 Specific requirements.....	26
Annex A (informative) Examples of categories	30
Bibliography.....	32
Figure 1 – Method of classification.....	20
Table 1 – Tabular correlation between categories and other IEC standards	29

INTRODUCTION

a) 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/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]