BS EN 61226:2010

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

National foreword

This British Standard is the UK implementation of EN 61226:2010. It is identical to IEC 61226:2009. It supersedes BS IEC 61226:2009 which is withdrawn.

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.

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

ISBN 978 0 580 70133 7

ICS 27.120.20

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 30 September 2009

Amendments/corrigenda issued since publication

Date	Text affected
30 June 2010	This corrigendum renumbers BS IEC 61226:2009 as BS EN 61226:2010.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61226

March 2010

ICS 27.120.20

English version

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)

CENELEC

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

Central Secretariat: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 61226:2010 E

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.

———————

Endorsement notice

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

CONTENTS

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="3">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 rowspan="2">Anticipated operational occurrences</td><td rowspan="2">a)</td><td rowspan="2">Design basis accidents</td></tr>
<tr><td>b)</td><td>Severe accidents</td></tr>
<tr><td colspan="5"></td><td>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.

5.2 Background

The principle of defence in depth is firmly established in the safety design basis of nuclear power plants. The fundamental idea is that there should be several layers or echelons of defence in the prevention of unsafe conditions, and that the prevention of unsafe conditions, before mitigation is required, is always to be preferred. Because of the large number of functions that are required to operate and keep safe a NPP, a number that increases with the principle of defence in depth, it is important that the significance to safety of each function is known.

IAEA safety standard series NS-R-1 establishes the idea of classification of NPP systems according to their importance to safety, and gives examples of the classification of the major systems of several types of NPP. All structures, systems and components, including software for instrumentation and control (I&C), that are items important to safety, shall be first identified and then classified on the basis of their function and significance with regard to safety. They shall be designed, constructed and maintained such that their quality and reliability is commensurate with this classification.

The IAEA safety guide NS-G-1.3 gives guidance on the classification of systems according to the importance to safety of the functions they perform. It introduces time factors such as

– the duration that the I&C system is needed once it has been initiated;
– the time for which alternative actions can be taken;
– the timeliness by which hidden faults can be detected and remedied.

This standard extends the classification strategy presented in IAEA Safety Guide NS-G-1.3, and establishes the criteria and methods to be used to assign the I&C functions of a NPP to one of the three categories A, B and C, depending on their importance to safety, or to an unclassified category for functions with no direct safety role. I&C functions falling within the boundary of the safety systems will generally be assigned to category A or B. I&C functions defined as safety related will generally be assigned to categories B or C.

The safety importance of, and the corresponding requirements placed on, parts of the safety systems and safety related I&C systems will differ, so that it is appropriate to assign them to different safety classes. Some I&C systems can have a significant effect on safety and therefore require appropriate attention. Other I&C systems have intermediate, low, or no significance to safety. They have correspondingly less stringent requirements for ensuring system performance and safety justification, and therefore have different technical requirements.

National application of the principles and criteria of this standard may assign differing nomenclature to categories A, B and C. The national application shall be according to the principles, criteria and associated requirements given in this standard. This shall involve establishing and documenting an appropriate correspondence to the categories defined.

5.3 Description of categories

5.3.1 General

I&C systems in NPPs perform functions with different levels of importance to safety. The importance to safety of each I&C function depends upon its role in achieving and maintaining safety, the potential consequence of failure of the function to operate when required, and the probability of these consequences. Therefore, an initial safety analysis of the specific NPP design is required to be completed prior to the classification of the I&C functions. The severity of the potential consequences in the case of a postulated failure of an I&C function, defines the level of assurance that is required for the various attributes of the systems and equipment which deliver the function, most notably that of functionality, performance and reliability.

For the design, assessment and licensing procedures, safety categories A, B and C are defined, with associated sets of technical and quality requirements on the properties of the I&C systems to be applied for the design and implementation of I&C systems and equipment important to safety.

5.3.2 Category A

Category A denotes the functions that play a principal role in the achievement or maintenance of NPP safety to prevent DBE from leading to unacceptable consequences. This role is essential at the beginning of the transient when no alternative actions can be taken, even if hidden faults can be detected. These functions play a principal role in the achievement or maintenance of the non-hazardous stable state[3]. If specified manual actions are provided to reach the non-hazardous stable state, factors such as the availability of redundant, validated, information sources, sufficient duration of the grace time for operator evaluation of alternative sources of information, and whether the manual actions are the only possibility for mitigation of this sequence of events to preserve NPP safety, have to be considered.

Category A also denotes functions whose failure could directly lead to accident conditions which may cause unacceptable consequences if not mitigated by other category A functions. Category A functions have high reliability requirements. Consequently, it may be necessary to limit their functionality and complexity.

5.3.3 Category B

Category B denotes functions that play a complementary role to the category A functions in the achievement or maintenance of NPP safety, especially the functions required to operate after the non-hazardous stable state has been achieved, to prevent design basis events (DBE) from leading to unacceptable consequences, or mitigate the consequences of DBE. The operation of a category B function may avoid the need to initiate a category A function. Category B functions may improve or complement the execution of a category A function in mitigating the consequences of a DBE, so that plant or equipment damage or activity release may be avoided or minimised.

Category B also denotes functions whose failure could initiate a DBE or worsen the severity of a DBE. Because of the presence of a category A function to provide the ultimate prevention of or mitigation of the consequences of a DBE, the safety requirements for the category B function need not be as high as those for the category A function. This allows, if necessary, the category B functions to be of higher functionality than category A functions in their method of detecting a need to act or in their subsequent actions.

5.3.4 Category C

Category C denotes functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety. Category C includes functions that have some safety significance, but are not category A or B. They can be part of the total response to DBA but not be directly involved in mitigating the physical consequences of the accident, or be functions necessary for beyond design basis accidents.

---

[3] In order to cope with rapid transients, the plant is controlled during this phase by automatic actions. For slower transients, stable conditions can be obtained using manual actions, provided such actions are considered after a grace time. This type of grace time represents a design requirement of the plant corresponding to a delay of diagnosis and action, and based on human factors considerations. It does not mean that manual actions are not permitted during that time. In some countries, and for older plants, the limit of category A may be this grace time, in place of the non-hazardous stable state.

5.4 Assignment criteria

5.4.1 General

The criteria that shall be applied for assignment of functions to categories A, B and C are given below.

If a function does not meet any of the criteria given below, then it shall be "non-classified" (NC).

In the case of multiple assignment, the final assignment of a function to a category shall be the highest relevant category.

The final assignment of the function may be modified using probabilistic methods in consistency with the principles outlined in 6.3.

5.4.2 Category A

An I&C function shall be assigned to category A if it meets any of the following criteria:

a) functions required to reach the non-hazardous stable state, to prevent a DBE from leading to unacceptable consequences, or to mitigate its consequences;

b) functions, the failure or spurious actuation of which would lead to unacceptable consequences, and for which no other category A function exists that prevents the unacceptable consequences;

c) functions required to provide information and control capabilities that allow specified manual actions necessary to reach the non-hazardous stable state.

5.4.3 Category B

An I&C function shall be assigned to category B if it meets any of the following criteria and is not otherwise assigned to category A:

a) functions required after the non-hazardous stable state of a DBE has been reached, to prevent it from leading to unacceptable consequences, or to mitigate the consequences;

b) functions required to provide information or control capabilities that allow specified manual actions necessary after the non-hazardous stable state has been reached to prevent a DBE from leading to unacceptable consequences, or mitigate the consequences;

c) functions, the failure of which during normal operation, would require the operation of a category A function to prevent an accident whose study is required;

d) functions to reduce considerably the frequency of a DBE as claimed in the safety analysis;

e) plant process control functions operating so that the main process variables are maintained within the limits assumed in the safety analysis, if these control functions are the only means of control of these variables. If different means are provided, clause 5.4.4 a) may apply;

f) functions used to prevent or mitigate a radioactive release or fuel degradation outside of the limits and conditions of normal operation as defined in the safety analysis;

NOTE 1 This refers to functions that are not already covered by the analysis of DBE leading to category A classification.

g) functions that provide continuous or intermittent tests or monitoring of functions in category A to indicate their continued availability for operation and alert control room staff to their failures, if no alternative means (e.g. periodic tests) are provided to verify their availability[4].

NOTE 2 Where the monitoring function is the only means of detecting otherwise unrevealed failures, then assigning the function to category B ensures that the equipment providing the function is suitably qualified.

5.4.4 Category C

An I&C function shall be assigned to category C if it meets any of the following criteria and is not otherwise assigned to category A or category B:

a) plant process control functions operating so that the main process variables are maintained within the limits assumed in the safety analysis not covered by 5.4.3 e). In case a combination of category C functions is used, a justification of sufficiency shall be provided;

NOTE 1 According to national practices a possible acceptable application of clause 5.4.4 a) is the combination of a regulation function and suitable manual actuation based on independent alarms including a justification of the use of manual action.

b) functions used to prevent or mitigate a minor radioactive release, or minor degradation of fuel, within the NPP design basis;

NOTE 2 A minor release or minor fuel degradation is considered to be that which falls within the normal limits and conditions of operation (e.g. discharge limits).

c) functions that provide continuous or intermittent tests or monitoring of functions in category A and B to indicate their continued availability for operation and alert control room staff to their failures, and are not classified category B according to 5.4.3 g);

d) functions necessary to reach the safety probabilistic goals including those to reduce the expected frequency of a DBE;

e) functions to reduce the demands on a category A function, as claimed in the safety analysis;

f) functions to monitor and take mitigating action following internal hazards within the NPP design basis (e.g. fire, flood);

g) functions to warn personnel or to ensure personnel safety during or following events that involve or result in release of radioactivity in the NPP, or risk of radiation exposure;

h) functions to monitor and take mitigating action following natural events (e.g. seismic disturbance, extreme wind);

i) functions provided for the benefit of the accident management strategy to reach and maintain a safe state for beyond design accidents;

j) functions provided to minimise the consequences of severe accidents;

k) functions which provide access control for the NPP.

6 Classification procedure

6.1 General

An outline of the procedure is shown in Figure 1.

4 Subclause 4.2.6 of IEC 60671 provides further guidance on the class of equipment used to implement such functions and in particular notes that where: “test features could interfere in an inappropriate manner with the proper operation of the system or equipment performing the function important to safety, it shall be assigned to the same category”

6.2 Identification of design basis

A main input to the classification process of functions is the nature of the NPP and the reactor type (e.g. PWR (pressurized water reactor), BWR (boiling water reactor) or other reactor type), the associated PIEs, and the major design criteria on redundancy of mechanical and electrical systems and equipment. Another main input is the identification of the major mitigation functions, and their supporting functions, for each PIE.

The assessment of the frequency and consequences of PIEs leads to the identification of DBEs representing the design base of the plant. When considering the design features of the plant the specified ranges of operational states and accident conditions and the defined radiological limits have to be reflected. Individual safety principles that together make up an "integrated overall safety approach" ensure the safety of a NPP. These principles are used in the design by considering the identified DBEs and successive physical barriers to keep radioactive exposure within permitted limits. The DBEs and the major design criteria (redundancy, separation, etc) of the plant, as well as the identification of the prevention and mitigation functions, and their supporting functions are the main input to the classification process.

The importance to safety of each I&C function depends upon the role for achieving and maintaining the NPP safety and the potential consequence of failure of the function to operate when required. Therefore, an initial safety analysis of the specific NPP design is required to be completed prior to the classification of the I&C functions.

6.3 Identification and classification of functions

At an early stage in the design of the NPP, the safety relevant functions shall be identified. The process of identifying these functions and assigning them to the I&C function or to the human operators should be carried out according to IEC 60964. Following this initial identification of a function, a category for each function shall be assigned according to the criteria of Clause 5.

The method for classifying the safety significance of function shall primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment, with account taken of factors such as:

- the safety function(s) to be performed;
- the role of the function in preventing or mitigating postulated initiating events;
- the role of the function during all operating modes (e.g. start-up, normal operation, refuelling, etc);
- the role of the function following PIEs such as natural events (e.g. seismic disturbance, flood, extreme wind, lightning) and internal hazards (e.g. fire, internal flood, missiles, radioactive release from adjacent unit or chemical releases from other plants or industries);
- the consequences of failure of the I&C functions;
- the effects of spurious actuation of the I&C functions;
- the probability that it will be required to perform a function important to safety;
- the time following a DBE at which, or during which it will be required to operate;
- the maintenance, repair and testing strategy.

It will not be possible to identify in detail all the functions at an early stage in the design process, as the characteristics of the NPP will not then have been defined fully. The process of identification and classification of the functions must therefore continue iteratively throughout the design phase. Where an initial assignment of a function to a category is uncertain, then an explanatory note should be added to the categorisation.

Since individual functions may be involved in the implementation of several aspects of the requirements specification, such functions may be assigned to several categories. In that case, the highest category assigned shall be applied.

As the redundancy, diversity and other technical requirements of the functions are determined more exactly, for example after the safety analysis progresses and the operating procedures are developed, the classification list shall be refined and revised, to derive a final list. This list shall be documented and maintained under configuration control since it will be required by plant/I&C designers during the life of the NPP. Also, this list may be required by the regulatory authorities.

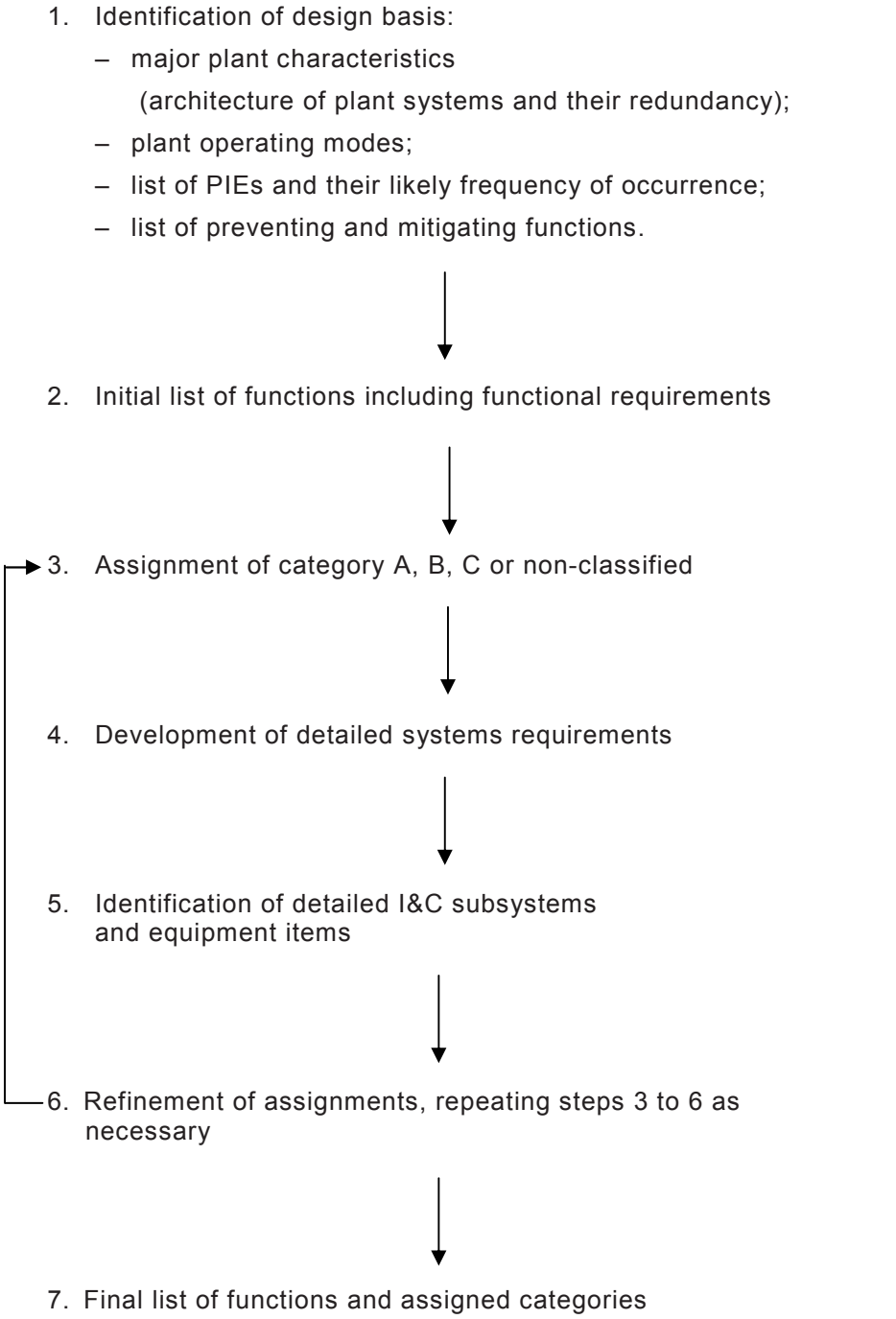

Figure 1 – Method of classification

7 Assignment of technical requirements to categories

7.1 General requirements

Technical requirements for each of the categories A, B and C are given in this clause. The requirements shall be applied to the specification, design, validation, qualification, manufacturing, installation, operation and maintenance phases of the I&C lifecycle as appropriate. The technical requirements constitute four groups:

– requirements that apply to the functions concerning the specification and validation of functionality, performance and reliability;

– requirements that apply to the design of I&C systems related to design characteristics such as redundancy, diversity, testability and separation. These characteristics determine primarily the reliability of the associated functions. The requirements also include HMI requirements;

– requirements concerning the equipment features for the assurance of seismic and environmental durability and electro-magnetic compatibility;

– requirements that are associated with the quality assurance, verification and maintenance which apply to functions, systems and equipment.

In most cases, these requirements are already detailed in appropriate codes and standards. The codes, guides and standards listed in Clause 2 of this standard are normative references and therefore provide the explicit requirements related to the I&C safety categories which are established by this standard. The correlation between the categories and the standards that shall be applied is summarised in Table 1. The detailed requirements from these standards are not repeated in this standard. The same table summarises the main types of requirements for each category. In the text below, some additional details are given.

Wherever possible, equipment with a documented, proven history of reliable operation in nuclear or other industrial applications should be used.

7.2 Requirements related to functions

7.2.1 Basic requirements

The basic requirement for assurance of functionality is the existence of a clear, comprehensive and unambiguous set of functional requirements and design specifications against which the functions shall be checked during design, manufacture, installation, and service, and shall be used as a reference for any in-service modifications.

The reliability required from any function in categories A, B or C should be determined by either a quantitative probabilistic assessment of the NPP, or by qualitative engineering judgement, and included in the specification. The performance required from any function in categories A, B or C shall be determined by appropriate analyses, and included in the specification. These analyses shall be carried out in a structured way following a set of approved procedures, and shall be documented.

Although the reliability requirements of functions in different categories may be the same, the level of assurance that the function will achieve the specified reliability will be different for the three categories, with category A requiring the highest assurance.

There shall be adequate separation between the functions of different categories.

7.2.2 Specific requirements

7.2.2.1 Category A

The design shall be according to the requirements of recognized codes, guides and standards that are appropriate to the high level of assurance of functionality required for category A functions. The design shall aim to ease verification and validation of the final functionality by maintaining simplicity. This should result in the avoidance of unrelated lower category functions being implemented in category A systems (for example, special display calculations and translation of communication protocols should not be carried out by safety system software).

The reliability requirements for category A I&C functions shall be specified as indicated in 7.1. This shall be carried out by establishing the reliability requirements for the functions needed to achieve an acceptably low risk of unacceptable consequences, and then by determining from this the reliability requirements for the I&C functions.

7.2.2.2 Category B

The design process shall be carried out following appropriate recognized codes, guides and standards, or systems and equipment with a documented history of satisfactory operation in a similar application may be used.

7.2.2.3 Category C

The design should be examined to verify that the systems and equipment have been designed or tested to provide the specified functions under the full range of specified operating conditions, including the most adverse anticipated operational conditions or occurrences under which the function is required.

7.3 Requirements related to I&C systems

7.3.1 Basic requirements

Requirements for the system design shall ensure that the function will achieve the specified reliability. The basic requirements for assuring high reliability concern the provision of appropriate redundancy, diversity and spatial, physical and electrical separation, and effective HMI. For all systems, means of fault detection and repair shall be considered during design and subsequent modifications.

The assessments of reliability and availability shall take into account repair periods, testing and maintenance periods and the potential for both self-revealed and non-self-revealed failure. The assumptions made in the reliability analysis with respect to maintenance, testing, and repair periods shall be verified during operation and corrective action shall be taken if discrepancies are identified.

Specific requirements concerning human factor and HMI shall be included in the design process. These requirements should be the product of a human factor engineering program, implemented from the earliest stages of the design phase.

The design of the system shall allow on-line and/or periodic testing during operation to demonstrate that performance is maintained. Requirements on periodic tests and maintenance activities to ensure the long-term reliability of I&C systems important to safety are defined in 7.5.

Sufficient information and control equipment shall be located, preferably at a single location that is physically and electrically separated from the main control room so that the reactor can be placed and maintained in a safe shutdown state, with essential plant variables monitored when there would be a loss of ability to perform these functions in the main control room.

7.3.2 Specific requirements

7.3.2.1 Category A

An I&C system performing category A functions shall have redundancy. Appropriate separation shall be applied to ensure that any single internal hazard cannot disable redundant parts of the system. A single failure shall not lead to the failure of the intended safety function even during preventive maintenance, periodic testing, inspection or repair. The application of the single failure criterion shall be in accordance with the IAEA Code NS-R-1, 5.34-5.39.

NOTE 1 In consideration of inappropriate actuations of the I&C, only spurious actuations (single or multiple) which can be the result of one single failure in I&C subsystems or support systems are generally considered.

In the case that category A functions have to be performed by operators, purpose designed monitoring and control of systems shall be provided which are separated from other monitoring and control of systems and which are designed to be suitable and adequate for the required reaction time.

The reliability of the I&C systems that perform category A functions shall be assessed and compared to the specification. If discrepancies exist, these shall be resolved. The reliability assessment shall consider the effects of common cause failures, including hardware failures, software failures, and human errors during operation, maintenance, as well as modification and repair activities. The techniques used to assess these effects range from purely qualitative engineering judgement to detailed quantitative analyses, which may themselves depend on qualitative estimates. The type of analysis chosen shall be consistent with the reliability requirement, the higher the reliability requirement, the more rigorous the technique.

Where consideration of the effects of common cause failures shows the required reliability could not be achieved for redundant systems, diversity implemented in independent systems shall be applied (e.g. as determined by probabilistic criteria). The function concerned may then require two or more systems, independent from one another. When a category A function is performed by two or more independent systems, the systems should be class 1 systems. If it is desired to use systems of a lower class, at least one of the systems shall meet the requirements of class 1 systems and a safety justification shall be provided for systems not meeting class 1 system requirements to enable the acceptability of this to be assessed.

NOTE 2 For an individual system which is specified and designed in accordance with the highest quality criteria, a figure of the order of 10^{-4} failure/demand may be an appropriate overall limit to place on the reliability that may be claimed, when all of the potential sources of failure due to the specification, design, manufacture, installation, operating environment, and maintenance practices, are taken into account. This figure includes the risk of common mode failure in the redundant channels of the system, and applies to the whole of the system, from sensors through processing to the outputs to the actuated equipment. Claims for better reliabilities than this are not precluded, but will need special justification, taking into account all of the factors mentioned. Alternatively, the design of independent I&C systems important to safety with an acceptable level of diversity may be applied.

Testing may require suppression of output signals, or the provision of bypass facilities. If bypass facilities are incorporated, their integrity shall be justified to show that they cannot be applied in a way that would prevent the system from achieving its specified safety functions. For example, their use might be physically restricted to a single train of a redundant system at any one time.

For some implementations, additional redundancy may need to be provided to allow routine testing during plant operation. This is necessary, for example, when testing of an active channel cannot be performed at power and tests must be conducted during plant operations to ensure the necessary functional reliability. In such cases, it is not necessary to incorporate additional redundancy for the whole system.

The power supply shall be backed-up by auxiliary power sources.

For category A systems, a formal system failure analysis, for example a failure modes and effects analysis (FMEA), shall be carried out to identify system vulnerability to component

failures and to assess the adequacy of design strategies applied to detect such failures or to mitigate their consequences.

Where a system has built-in self-testing features, and these are claimed as part of the reliability analysis of the function, the failure analysis shall assess these features to find the coverage of the self-tests. Where the failure analysis shows that some failures may not be detected and revealed to the operators by the systems self-testing features, then proof tests shall be developed to reveal such failures. The intervals for the proof test shall be determined from the likely frequency of occurrence of the undetected failure and the reliability required of the function.

Where reliability data is not available, the test interval shall be chosen by comparison with other similar systems. As experience is accumulated, the test interval for the function shall be re-evaluated.

7.3.2.2 Category B

The reliability of systems that perform category B I&C functions shall be assessed and compared to the specification. A function in this category shall be accomplished by redundant and separated means, unless justification is provided. Such justification may be based upon, for example, the ability of the system to achieve its reliability targets without it, the acceptability of the consequences of the function's failure, or the time available to provide alternative responses if the function fails.

The power supply shall be backed-up by auxiliary power sources.

The components employed shall be shown to be of high quality and reliability, and means to ensure that faults can be quickly detected and repaired shall be incorporated.

The principal objectives for the functional design of systems required to provide information or control capabilities in the control room that allow specified manual actions necessary to mitigate the consequences of a DBE are to provide the operator with accurate, complete and timely information regarding the status of plant equipment and systems for all DBE, and to minimise movement required from the operator to monitor and control the plant.

On-line and/or periodic testing of performance shall include confirmation of the functional capacity of subsystems, especially individual testing of redundant trains.

7.3.2.3 Category C

A system in this category does not generally need redundancy or separation This may be provided if it is necessary to achieve the specified reliability of the function. Tolerance to internal and external hazards may be required.

The power supply may be backed-up by auxiliary power sources on a case by case basis.

For systems performing category C functions where redundancy is necessary to achieve the specified reliability, redundancy should be considered as for category B.

Where redundancy is provided, periodic individual testing of the functional capacity of all redundant systems or subsystems shall be included. On-line tests are a means of meeting this requirement.

7.4 Requirements related to equipment

7.4.1 Basic requirements

It is necessary to provide assurance that the equipment will not fail due to the environmental conditions that it may be subjected to during and following a PIE. This assurance may be provided by qualification of the equipment. When qualification is required, this may be achieved using one, or a combination of several different methods: for example, by tests, by analysis, a combination of these two, or possibly by using available data from operational experience. The worst anticipated environment, including earthquake, in which the equipment is required to operate shall be established and stated in the requirements specification.

When functions not originally intended for beyond design basis or severe accidents are expected to play a role in these accidents, the capabilities of their components should be evaluated in order to show that they are able to function in the environmental conditions to be expected.

7.4.2 Specific requirements

7.4.2.1 Category A

The measures taken to provide assurance that category A equipment will continue to operate under all anticipated operating conditions shall include equipment qualification. The results of the tests shall be recorded and retained in the lifetime records of the NPP. Any failures during the qualification tests shall be investigated, and the cause and rectification of the failure shall be documented.

7.4.2.2 Category B

Equipment in category B shall be subject to qualification, to be performed as for category A equipment.

7.4.2.3 Category C

Depending on its function, equipment in category C may require qualification. The design of the equipment should be systematically reviewed against the specification of the worst anticipated environment in which the equipment is required to operate.

Where the equipment is novel, or is required to operate in conditions for which commercial equipment is not normally designed (such as seismic events or extreme environmental conditions), a set of rules shall be established against which the equipment is designed, or an existing design evaluated. These rules shall be based on experience gained from the special design requirements of category A equipment. Equipment provided for the functions classified in application of criteria 5.4.4 i) and j) should be specifically designed for the extreme process and environmental conditions that could arise, as determined from analysis. The appropriateness of adopting equipment produced to commercial standards for the implementation of these functions shall be specifically reviewed.

For other cases, category C equipment may be accepted to normal commercial design standards unless the role of the equipment requires special qualification, for example seismic or fire prevention requirements, or to prevent overvoltages or electrical noise in category C equipment from affecting category A or B functions. Claims for operation in abnormal environmental conditions shall be supported by documentary evidence.

7.5 Requirements related to quality aspects

7.5.1 Basic requirements

The general requirements are related to quality assurance performed during the design, the manufacture, the installation, the commissioning and the operation phases, in order to ensure the correct performance of the relevant systems and equipment.

The objectives of QA are configuration management, change control and traceability. The design shall be documented in sufficient detail to support the manufacture, installation, commissioning and operational phases of the NPP, and the verifications performed at each step. Adequate attention shall be paid to the provision of documentation to permit future modification of the design.

In addition, special QA and testing should be undertaken for developments in proportion to the relative novelty or complexity of the new design or modification. These development activities should be documented as appropriate to the importance to safety of the functions.

A QA plan shall be established according to an appropriate adequate code or standard. This shall require specifications of performance and testing to be defined and verified.

Testing of components, modules, subsystems, and systems shall be carried out according to the QA plan to show satisfactory performance during manufacturing, assembly, and site installation periods, as appropriate to the category of the function.

Tests shall be carried out on components, modules and subsystems to ensure that, with the manufacturing QA, the functions are fulfilled according to the requirements specification. Combined tests of the installed I&C system with the mechanical and fluid systems shall take place at the NPP before operation of the NPP in a mode requiring the availability of the safety functions provided by the system.

The intention of the site tests is the same, regardless of category, but the quality control and documentation requirements vary according to category, as stated hereinafter.

Testing during operation shall be executed to demonstrate that the status of the hardware components of the I&C important to safety is not degraded by faults. I&C systems shall be designed to permit adequate testing and to detect failures within the equipment. Deficiencies identified shall be corrected following a modification control procedure. Suitable records of those corrections shall be kept. Where redundancy is provided, individual checks of the functionality of the redundant channels shall be included. The test interval shall be chosen so that the assessed failure rate or probability of failure to operate on demand meets the requirements of the reliability analysis.

Where computer equipment is used, a software life cycle quality programme appropriate to the category of the function shall be implemented.

7.5.2 Specific requirements

7.5.2.1 Category A

The QA requirements shall be according to IAEA safety standard GS-R-3. The documentation shall enable the history of the items of equipment to be established, including design, manufacturing, and operating aspects. This shall include all equipment down to the module level within the design. The configuration shall be controlled down to the lowest traceable element. Traceability of lot numbers, materials, etc. shall extend throughout the system down to the level of individual modules.

The QA documentation shall allow an investigator to trace backward from a piece of hardware or software to the specification that defines the requirements for it, and to work forwards from any requirement in the specification to the components that implement it.

Type testing shall have been carried out to show that equipment of identical construction to that to be installed at the NPP will function as required by the design when subjected to the anticipated operating environment.

Functional testing of components, modules, subsystems and, whenever practicable, complete systems, shall be carried out. These tests shall be witnessed by the licensee, or his representative.

Functional testing may be performed at the factory or at the site. Tests performed at the factory and at the site shall be co-ordinated to ensure that a full coverage by all tests together is achieved. Where it is not possible to prove that full coverage of all of the specified functions can be achieved, special justification shall be provided.

Site testing shall test, as far as practicable, that all specified safety functions of the installed systems and equipment can be achieved with the required performance. This testing shall take into account variations in operating parameters. This is the site acceptance test (SAT), and shall be witnessed by the licensee, or his representative.

On-line or periodic tests shall demonstrate that the ability to perform all required safety functions including all subsystems necessary to perform these functions is not degraded. Test intervals shall be chosen taking due account of the level of self-monitoring so that the reliability targets for the I&C important to safety are fulfilled taking into account the expected or monitored failure rate of the I&C components.

7.5.2.2 Category B

The QA requirements shall be according to IAEA safety standard GS-R-3. The documentation shall enable the history of the items of equipment to be established, including design, manufacturing, and operating aspects The level of detail to which QA applies to category B functions, systems, or equipment may be lower than that applied to category A functions, systems, or equipment, although the QA programme should be consistent with that for category A.

Type testing shall have been carried out with equipment of similar construction to that to be installed at the NPP provided that analysis has been performed to show that differences in the equipment do not invalidate the test results.

Functional testing shall have been carried out prior to operation to show that each specified function can be achieved by the system using equipment of similar construction to that to be installed at the NPP. Some or all of this testing may be done on site.

SAT testing shall show, as far as is practicable, that all specified safety functions of the installed equipment can be achieved. Tests of control equipment shall show the ability to respond correctly to transients and changes in demand. Testing of display and alarm equipment shall include injection tests of relevant input signals to show satisfactory performance.

7.5.2.3 Category C

Systems and equipment performing category C functions may be accepted at a commercial QA level.

The licensee may accept that the manufacturer's tests are adequate to demonstrate that the specified performance will be achieved. These tests shall be performed on similar equipment.

Specific type and functional testing should be performed when necessary, but is not generally required.

SATs should be carried to show that the system achieves the specified safety related functionality and performance.

Periodic testing of performance may be limited to checks at refuelling outages, or at similar shutdown periods, for functions which are not continuously operating.

Table 1 – Tabular correlation between categories and other IEC standards

Category	Applicable IEC standards		Main requirements for			
	Systems	Equipment	Functions	Design of systems	Equipment features	General
General	IEC 61513 IEC 60964, IEC 60965 IEC 61771, IEC 61772 IEC 61839 IEC 60709	IEC 61000-4 IEC 61000-6-2	Functional specification	Testability HMI specification	Electromagnetic compatibility	QA program Quality control FAT, SAT Periodic testing
A	 IEC 60812[5] IEC 60880 IEC 60987	IEC 60780, IEC 60980	Appropriate codes, standards, guides Separation from lower categories High assurance of reliability	Single failure criterion Independence, separation Design to cope with internal common cause failure Diversification case by case FMEA Back-up power supply	Qualification to postulated environment and to seismic conditions	IAEA GS-R-3 Verification on identical equipment Full FAT/SAT Frequent periodic testing
B	 IEC 60987 IEC 62138	IEC 60780, IEC 60980	Appropriate codes, standards, guides Separation from lower categories	Single failure criterion, separation both possibly at functional level Back-up power supply	Qualification to environment and seismic conditions that the equipment must withstand	IAEA GS-R-3 Verification on similar equipment Limited SAT and periodic testing
C	IEC 62138			Redundancy and separation case by case	Qualification case by case	Normal industrial practice Periodic test if not used continuously

5 When failure analysis is FMEA.

Annex A
(informative)

Examples of categories

A.1 General

This annex provides examples of assignment of typical functions and typical I&C systems to categories A, B and C. It should be noted, however, that these examples may not necessarily all apply to all reactor types.

A.2 Category A

A.2.1 Typical functions

The I&C functions assigned to category A are necessary for

a) reactor shutdown and maintenance of sub-criticality;
b) isolation of containment;
c) provision of information for essential operator action;
d) decay heat transport to the ultimate heat sink.

A.2.2 Typical I&C systems

Typical I&C systems are as follows:

a) reactor protection system;
b) safety actuation system and safety system support features;
c) key instrumentation and displays to permit pre-planned operator actions that are defined in the NPP operating instructions, and that are required to ensure NPP safety in the short term.

A.3 Category B

A.3.1 Typical functions

The I&C functions assigned to category B are necessary for

a) used fuel pool cooling system;
b) main cooling system isolation;
c) post accident monitoring system;
d) automatic control of the NPP primary and secondary circuit conditions, keeping variables in the limits assumed in the safety analysis, and prevention of events from escalating to accidents;
e) monitoring/controlling the handling of fuel where failure could cause radiation release or fuel degradation outside the limits and conditions of normal operation.

A.3.2 Typical I&C systems

Typical I&C systems are as follows:

a) NPP automatic control system or preventative protection system;

b) part of the decay heat transport to ultimate heat sink not necessary in the short term;

c) instrumentation needed to apply operating procedures for DBE;

d) safety circuits and interlocks of fuel handling systems used when the reactor is shut down.

A.4 Category C

A.4.1 Typical functions

The I&C functions assigned to category C may include

a) monitoring and controlling performance of individual systems and items of equipment during the post-accident phase to gain early warning of the onset of problems, and to keep radioactive releases ALARA;

b) limiting the consequences of internal hazards;

c) those for which operating mistakes could cause minor radioactive releases, or lead to radioactive hazard to the NPP operating staff;

d) those necessary to warn of internal or external hazard (fire, flood, explosions, seismic events, etc.);

e) access control;

f) communication to warn of significant on- or off-site releases for the purposes of implementing the NPP's emergency plan.

A.4.2 Typical I&C systems

Typical I&C systems are as follows:

a) alarm system;

b) radwaste stream monitoring and interlocks, area radiation monitoring;

c) access control system;

d) emergency communication systems;

e) control room data processing system;

f) fire suppression system;

g) seismic monitoring system;

h) NPP site meteorological station.

Bibliography

IEC 60050-394, *International Electrotechnical Vocabulary – Part 394: Nuclear instrumentation – Instruments, systems, equipment and detectors*

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

NOTE Harmonized as EN 61508-1.

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

NOTE Harmonized as EN 61508-2.

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

NOTE Harmonized as EN 61508-3.

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

NOTE Harmonized as EN 61508-4.

IEC/TR 61838, *Nuclear power plants – Instrumentation and control important to safety – Use of probabilistic safety assessment for the classification of functions*

IAEA Safety Glossary:2007, *Terminology used in nuclear safety and radiation protection*

———————

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.

Publication	Year	Title	EN/HD	Year
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	-	-

Publication	Year	Title	EN/HD	Year
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	-	-