IEC 60964

Edition 3.0 2018-11
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

Nuclear power plants – Control rooms – Design

IEC 60964:2018-11 RLV(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

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

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

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC 60964

Edition 3.0 2018-11
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

Nuclear power plants – Control rooms – Design

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.10; 27.120.20

ISBN 978-2-8322-6299-3

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – CONTROL ROOMS – DESIGN

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

International Standard IEC 60964 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This third edition cancels and replaces the second edition published in 2009. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) to review the usage of the term “task” ensuring consistency between IEC 60964 and IEC 61839;
b) to clarify the role, functional capability, robustness and integrity of supporting services for the MCR to promote its continued use at the time of a severe accident or extreme external hazard;
c) to review the relevance of the standard to the IAEA safety guides and IEC SC 45A standards that have been published since IEC 60964:2009 was developed;
d) to clarify the role and meaning of “task analysis”,
e) to further delineate the relationships with derivative standards (i.e. IEC 61227, IEC 61771, IEC 61772, IEC 61839, IEC 62241 and others of relevance to the control room design);
f) to consider its alignment with the Human Factors Engineering principles, specifically with the ones of IAEA safety guide on Human Factors (DS-492) to be issued.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
45A/1214/FDIS	45A/1224/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

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

IMPORTANT – The “colour inside” logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

INTRODUCTION

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

IEC 60964:1989 was developed to supply requirements relevant to the design of the main control room of NPPs and reviewed in 2009. The first two editions of IEC 60964 ~~has been~~ were used extensively within the nuclear industry. ~~It was however recognized that recent technical developments especially those which are based on software technology should be incorporated. It was also recognized that the relationships with derivative standards (i.e. IEC 61227, IEC 61771, IEC 61772, IEC 61839, and IEC 62241) should be clarified and conditioned.~~

It was however recognized that there was a need to develop an amendment for the 2009 edition to address:

- The usage of the term "task" needed to be examined.
- The role, functional capability, integrity of supporting services and robustness for the MCR should be clarified to promote its continued use at the time of a severe accident or extreme external hazard.
- The relevance of the standard to the IAEA safety guides and SC 45A standards published since 2009.

Given the size of the proposal amendment, it was decided that a new edition of IEC 60964 should be issued instead of an amendment. During the preparation of this third edition, it was agreed that the following points have to be covered:

- to clarify the role and meaning of “task analysis”;
- to further delineate the relationships with derivative standards (i.e. IEC 61227, IEC 61771, IEC 61772, IEC 61839, IEC 62241 and others of relevance to the control room design);
- to consider its alignment with the Human Factors Engineering principles, specifically with the ones of IAEA safety guide on Human Factors (DS-492) to be issued.

This IEC standard specifically focuses on the functional designing of the main control room of NPPs. It is intended that the Standard be used by NPP vendors, utilities, and by licensors.

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

IEC 60964 is the second level IEC SC 45A document tackling the generic issue of control room design.

IEC 60964 is to be read in association with the derivative standards mentioned above which are the appropriate IEC SC 45A documents which provide guidance on operator controls, verification and validations of design, application of visual display units, functional analysis and assignment, and alarm functions and presentation.

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

c) Recommendations and limitations regarding the application of the Standard

This standard is intended for application to new control rooms whose conceptual design is initiated after the publication of this standard. The recommendations of the standard may be used for refits, upgrades and modifications.

The primary purpose of this standard is to provide functional design requirements to be used in the design of the main control room of a nuclear power plant to meet operational and safety requirements.

This standard also provides functional interface requirements which relate to control room staffing, operating procedures and the training programme which are, together with the human-machine interface, constituents of the control room system.

To ensure that the Standard will continue to be relevant in future years, the emphasis has been placed on issues of principle, rather than specific technologies.

d) Description of the structure of the IEC SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top-level documents of the IEC SC 45A standard series ~~is~~ are IEC 61513 and IEC 63046. IEC 61513 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 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer~~s~~ 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, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 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 publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework and provides an interpretation of the general requirements of IEC 61508-1, 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 terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.~~

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear

power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC SC 45A to decide how and where general requirements for the design of electrical systems were to be considered. IEC SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 is published this NOTE 2 of the introduction of IEC SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – CONTROL ROOMS – DESIGN

1 Scope ~~and object~~

This document establishes requirements for the human-machine interface in the main control rooms of nuclear power plants. The document also establishes requirements for the selection of functions, design consideration and organization of the human-machine interface and procedures which ~~shall be~~ are used systematically to verify and validate the functional design. These requirements reflect the application of human factors engineering principles as they apply to the human-machine interface during ~~normal and abnormal~~ plant operational states and accident conditions (including design basis and design extension conditions) as defined in IAEA SSR-2/1 and IAEA NP-T-3.16. This document does not cover special purpose or normally unattended control points, such as those provided for shutdown operations from outside the main control room or for radioactive waste handling, or emergency response facilities. Detailed equipment design is outside the scope of this document.

The primary purpose of this document is to provide functional design requirements to be used in the design of the main control room of a nuclear power plant to meet operational and safety requirements. This document also provides functional interface requirements which relate to control room staffing, operating procedures, and the training programmes which, together with the human-machine interface, constitute the control room system.

This document is intended for application to new control rooms whose conceptual design is initiated after the publication of this document. If it is desired to apply it to an existing control room, special caution must be exercised so that the design basis is kept consistent.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *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/IEEE 60780-323, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

IEC 60960, *Functional design criteria for a safety parameter display system for nuclear power stations*

IEC 60965, *Nuclear power plants – Control rooms – Supplementary control ~~points~~ room 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 61225, *Nuclear power plants – Instrumentation and control systems important for safety – Requirements for electrical supplies*

IEC 61226, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

IEC 61227, *Nuclear power plants – Control rooms – Operator controls*

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

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

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

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

IEC 62003, *Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*

IEC 62241, *Nuclear power plants – Main control room – Alarm functions and presentation*

IEC 62645, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*

IEC 62646, *Nuclear power plants – Control rooms – Computer based procedures*

IEC 62859, *Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity*

ISO 11064 (all parts), *Ergonomic design of control centres*

~~IAEA NS-G-1.3, *Instrumentation and control systems important to safety in Nuclear Power Plants, 2002*~~

IAEA NS-G-1.9, *Design of the reactor coolant system and associated systems in nuclear power plants*

IAEA, NS-G-1.11, *Protection against internal hazards other than fires and explosions in the design of nuclear power plants*

IAEA NP-T-3.16, *Accident Monitoring Systems for Nuclear Power Plants*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply. For other terms, refer to the general terminology defined in IEC 61513 and in the IAEA ~~NUSS programme, such as Safety Guide NS-G-1.3~~ Safety Glossary.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
accident conditions
deviations from normal operation that are less frequent and more severe than anticipated operational occurrences

Note 1 to entry: Accident conditions comprise design basis accidents and design extension conditions.

[SOURCE: IAEA Safety Glossary, 2016]

3.2
alarm
item of diagnostic, prognostic, or guidance information, which is used to alert the operator and to draw his or her attention to a process or system deviation

Note 1 to entry: Specific information provided by alarms includes the existence of an anomaly for which corrective action might be needed, the cause and potential consequences of the anomaly, the overall plant status, corrective action to the anomaly, and feedback of corrective actions.

Two types of deviation may be recognised:

– Unplanned – Undesirable process deviations and equipment faults;

– Planned – Deviations in process conditions or equipment status that are the expected response to but could be indicative of undesirable plant conditions.

[SOURCE: IEC 62241:2004, 3.~~2~~21]

3.3
auxiliary control <operating> systems
operating systems that are installed outside the control room such as local-to-plant control points and local-to-plant shutdown systems

3.4
control room staff
group of plant personnel stationed in the control room, which is responsible for achieving the plant operational goals by controlling plant through human machine interfaces

Note 1 to entry: Typically, the control room staff consists of supervisory operators, and operators who actually monitor plant and plant conditions and manipulate controls but also may include those staff members and experts who are authorized to be present in the control room, e.g. during long lasting event sequences.

3.5
control room system
integration of the human-machine interface, the control room staff, operating procedures, training programme, and associated facilities or equipment which together sustain the proper functioning of the control room

3.6
controls
devices which the operator uses to send demand signals to control systems and plant items

Note 1 to entry: Controls as defined in this document (i.e. devices used for control actions) hold a different meaning from the one defined in the IAEA safety Glossary and are not replaceable.

3.7
design basis accident
postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits

[SOURCE: IAEA Safety Glossary, 2016]

3.8
design extension conditions
postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions include conditions in events without significant fuel degradation and conditions with core melting

[SOURCE: IAEA Safety Glossary, 2016]

3.9
displays
devices used for monitoring plant conditions and status, e.g. process status, equipment status

3.10
format
display format
pictorial display of information on a visual display unit (VDU) such as message text, digital presentation, symbols, mimics, bar-charts, trend graphs, pointers, multi-angular presentation

3.11
function
specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it

[SOURCE: IEC 61226:2009, 3.~~9~~7]

3.12
functional analysis
examination of the functional goals of a system with respect to available manpower, technology, and other resources, to provide the basis for determining how the function may be assigned and executed

3.13
functional goal
performance objectives that shall be satisfied to achieve the corresponding function

3.14
hierarchical goal structure
relationship between a functional goal and sub-functional goals structured in a hierarchical order

3.15
high-level mental processing
human act to process and/or interpret information to obtain reduced abstract information

3.16
human-machine interface
interface between operating staff and I&C system and computer systems linked with the plant. The interface includes displays, controls, and the Operator Support System interface

3.17
I&C system
system, based on ~~electrical and/or electronic and/or programmable electronic technology~~ E/E/PE items, performing plant I&C functions as well as service and monitoring functions related to the operation of the system itself

Note 1 to entry: The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices. The different functions within a system may use dedicated or shared resources.

Note 2 to entry: The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

Note 3 to entry: According to their typical functionality, IAEA distinguishes between automation and control systems, HMI systems, interlock systems and protection systems.

[SOURCE: ~~IEC 61513~~ IEC 62138:2018, 3.26]

3.18
job
set of tasks which are operationally related. The tasks within a job should be coherent with regard to required skill, knowledge and responsibility

3.19
job analysis
analysis identifying basic requirements which a job imposes on the control room staff structure, the operating procedures and training programme

3.20
local control points
local control facilities
points (or facilities) located outside the control room where local operators perform control activities

3.21
local operators
operating staff that perform tasks outside the control room

3.22
operating procedures
set of documents specifying operational tasks it is necessary to perform to achieve functional goals

3.23
operating staff
plant personnel working on shift to operate the plant

Note 1 to entry: The operating staff includes the control room staff, maintenance engineers, etc.

3.24
operator interaction
interrelation between operator and the I&C system. Specifically, display of plant status by the I&C system and corresponding operator action

3.25
Operator Support System
OSS
system or systems supporting the high-level mental information processing tasks assigned to the control room staff

3.26
performance requirements
quantitative requirements specifying performance ~~of tasks~~ which ensure the achievement of functional goals

3.27
plant operational goals
ultimate purposes of plant design, i.e. controlled generation of electricity and limitation of release of radioactivity to the environment

3.28
population stereotype
tendency for most persons in a group or population to give the same response to a particular stimulus, even when there are alternative responses. The population stereotype depends on the customs and habits of the population sampled

3.29
supplementary control room
location from which limited plant control and/or monitoring can be carried out to accomplish the safety functions identified by the safety analysis as required in the event of a loss of ability to perform those functions from the Main Control Room

Note 1 to entry: For existing plants, the Supplementary Control Room may be a special control room, but in many cases comprises sets of control panels and displays in switchgear rooms or similar areas. In the latter case, the term 'supplementary control point' is used in this document.

[SOURCE: IEC 60965:2016, 3.6]

3.30
severe accident
accident conditions more severe than a design basis accident and involving significant core degradation

[SOURCE: IAEA Safety Glossary, 2016]

3.31
task analysis
~~a detailed~~ identification and description of an operator's task, in terms of its components, to specify the detailed human activities involved, and their functional and temporal relationships

Note 1 to entry: Frequently, task analysis in understood to also include the evaluation of the operator's tasks. In the frame of IEC 60964, this evaluation is described in terms of V&V of function assignment and V&V of the integrated control room system (which also covers the operator tasks).

3.32
tasks
actions performed by ~~either human or machine~~ humans for the accomplishment of a functional goal

3.33
training programme
programme which is designed to train the control room staff so that they can acquire the skills and knowledge necessary for operational activities

3.34
validation
process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation is broader in scope, and may involve a greater element of judgement, than verification.

[SOURCE: IAEA Safety Glossary, ~~2007~~ 2016]

3.35
verification
~~the process of determining whether the quality or performance of a product or service is as stated, as intended or as required~~
confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity

[SOURCE: IAEA Safety Glossary, ~~2007~~ 2016]

3.36
Visual Display Unit
VDU
type of display incorporating a screen for presenting computer-driven images

4 Abbreviated terms

E/E/PE	Electrical/Electronic/Programmable Electronic
HMI	Human Machine Interface
I&C	Instrumentation and Control
MCR	Main Control Room
NPP	Nuclear Power Plant
OSS	Operator Support System
VDU	Visual Display Unit
V&V	Verification and Validation
SFP	Spent Fuel Pool

5 Standard use

This clause is provided to orient the user to the organization and focus of this document. Figure 1 shows an overview of a control room system. The goal of a control room design team is the successful completion of an integrated control room system. The control system is an integration of the human-machine interface, control room staff, operating procedures, training programme and the associated equipment and facilities. Annex A provides a supplemental explanation concerning the concept of the control room system.

The focus of this document is the establishment of the human-machine interface in the control room design. The document also establishes a means for developing staffing requirements, operating procedures and a training programme but does not provide detailed methodology for such development. ~~The various clauses and subclauses of this standard are developed.~~

After the scope, statements and specifications of design principles, the design process is shown in Figure 2 to include functional analysis, function assignment, function assignment verification, function assignment validation and job analysis. Then, the functional design specifications are developed as shown in Figure 2.

From these specifications, the detailed design, operating procedures and training programme are developed. Finally, the resultant system constituents are verified and the integrated control room system validated.

This document ~~is addressed to~~ focuses on the design process for the control room(s) ~~designer. This refers not necessarily to a single person~~, typically implemented by a design team which comprises a variety of competencies and disciplines. This includes at least the following areas:

- nuclear engineering;
- architectural design and civil engineering;

- systems engineering;
- I&C systems engineering;
- information and computer systems engineering;
- human factors engineering;
- plant operations and maintenance;
- training.

These competencies may be provided by permanent or temporary team members, or even by consultants.

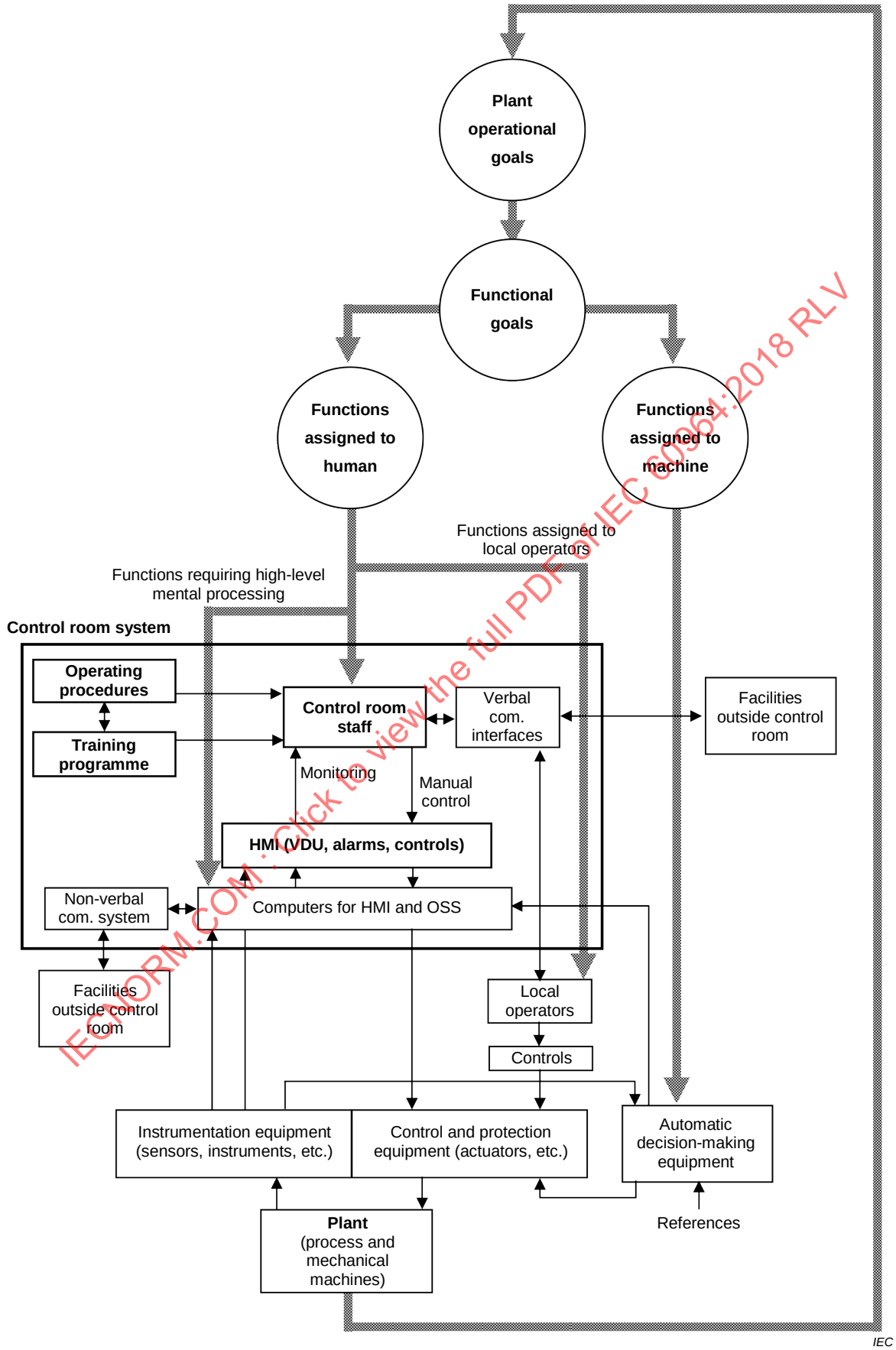


Figure 1 – Overview of control room system

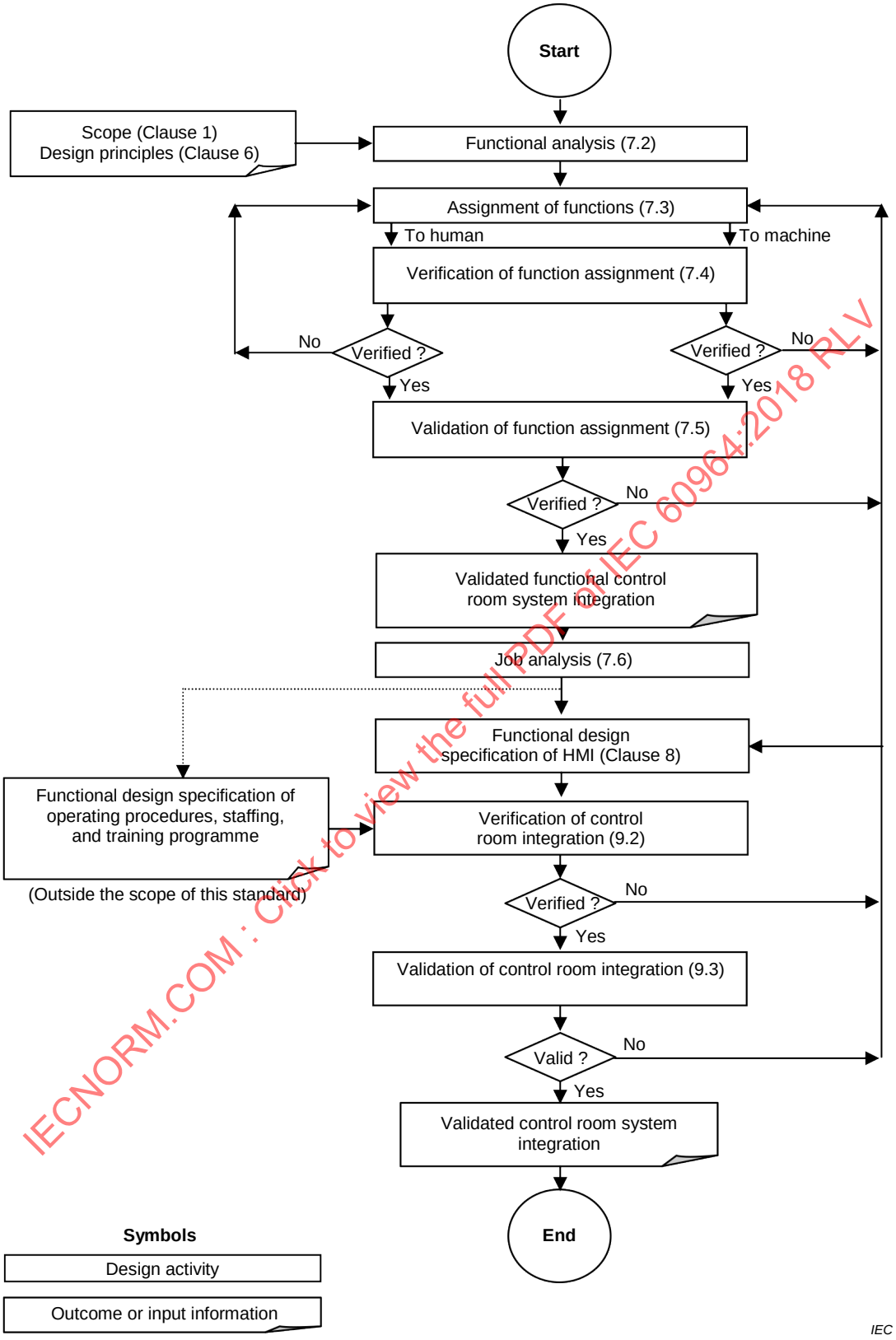


Figure 2 – Overall design process and the relationship to clauses and subclauses of this document

6 Design principles for the main control room

6.1 Main objectives ~~of the main control room~~

The nuclear power plant objective is that it can be operated safely and efficiently from the main control room in all plant operational states and accident conditions. The main control room provides the control room staff with the human-machine interface and related information and equipment, e.g. the communication interface, which are necessary for the achievement of the plant operational goals. In addition, it provides an environment under which the control room staff are able to perform their tasks without discomfort, excessive stress, or physical hazard.

6.2 Functional design objectives ~~of the main control room~~

The principal objectives of the control room design are to provide the operator with accurate, complete, operationally relevant and timely information regarding the functional status of plant equipment and systems.

The design shall allow for all operational states, including refuelling and accident conditions, optimise the operator tasks and reduce to an appropriate level the workload required to monitor and control the plant safely, and provide necessary information to other facilities outside the control room.

The control room design shall provide an optimal assignment of functions which achieves maximum utilization of operator and system capabilities.

An additional objective of the control room design is to permit station commissioning to take place effectively and to permit modifications and maintenance.

6.3 Safety principles

A control room shall be designed to enable the nuclear power plant to be operated safely in all operational states and to bring it back to a safe state after the onset of accident conditions. Such events shall be considered in the design of the control room.

Provisions for preventive and mitigative accident management shall be made both at monitoring and control level combining control room and manual actions, see IAEA NP-T-3.16.

Equipment controlled from the control room shall be designed, as far as practicable, so that an unsafe manual command cannot be carried out, e.g. by using a logical interlock depending on the plant status.

Account shall also be taken of the need for functional isolation and physical separation where redundant safety systems or safety and non-safety systems are brought into close proximity. IEC 60709 gives requirements for this. Account shall be taken of the need to ensure safety if the control room and its systems are affected by fire, and to reduce the possibility of fire to a practicable minimum, as outlined in IEC 60709.

Appropriate measures shall be taken to safeguard the occupants of the control room against potential hazards such as unauthorized access, undue radiation resulting from an accident condition, toxic gases, and all consequences of fire, which could jeopardize necessary operator actions.

There shall be adequate routes through which the control room staff can leave or reach the control room, or gain access to other control points, under emergency conditions.

6.4 Availability principles

With a view to maximizing the plant capacity factor, consideration shall be given in the control room design to:

– facilitating planned operations for load changing, start-up and shut-down;

– minimizing the occurrence of any undesired power reduction or plant trip caused by operators' erroneous decision-making and actions, or by local disturbances associated with malfunction or failure of I&C systems;

– achieving the design output and performance of the plant.

The availability-related design specifications shall not violate the adopted safety principles.

6.5 Human factors engineering principles

In order to provide an optimal assignment of functions which ensures maximum utilization of the capabilities of human and machine and aims to achieve the maximum plant safety and availability, the design shall pay particular attention to human factors principles and human characteristics of personnel with regard to their anthropometrics, perceptual, cognitive, physiological and motor response capabilities and limitations.

6.6 Utility operating principles

An integral part of the control room and operating philosophy is operator staffing and training. To maximize the safe and efficient operation of the nuclear power plant, the control room shall be manned with a sufficient number of skilled professional staff.

The control room staff shall be technically trained in control room operations and educated in those engineering principles related to nuclear power plant operations and safety, as well as having a thorough knowledge of the plant sub-systems and components, their function, performance and location.

Tasks performed by operators outside the control room that involve operation of plant equipment shall be administratively controlled and monitored from the control room.

To ensure the quality of operation of the nuclear power plant, the station operating authority should consider the following factors in control room staffing:

– personnel selection and qualification requirements;

– initial training and retraining requirements for normal, abnormal and accident conditions;

– periodic retraining of operating skills and opportunities to expand their knowledge in engineering principles;

– job responsibilities for control room staff and individuals during normal and emergency operations;

– personnel physical requirements concerning optical and auditory capacity, any physical impairment and height;

– management and supervision structures and responsibilities;

– shift patterns and job stress.

6.7 Relationship with other control and management centres

To assist the control room personnel in responding to abnormal operating conditions, emergency response facilities shall be available to function during emergency conditions.

Supplementary control rooms (or points) shall be provided, sufficient to ensure safety if the main control room is damaged or becomes inoperable. The requirements for supplementary control rooms (or points) are given in IEC 60965.

Equipment shall be provided for the change-over of the control and monitoring from the main control room to the supplementary control rooms (or points). The equipment shall operate independently of the other equipment in the control room.

6.8 Operational experience

When available, operational experience from existing nuclear power plants should be collected, analysed and fed back to the design of new power plants where applicable. Such experience may recommend use or optimisation of proven solutions or even influence the consideration of principles in domains such as follows:

- staffing;
- operating team organisation and job definition;
- function allocation between main control room and local control stations;
- automation;
- design of information processing, information presentation and controls.

7 Functional design of the main control room

7.1 General

A system based approach to the functional design of a control room shall be used covering the control room and the associated items in Figure 1. This approach shall include the following five steps as shows in Figure 2:

– functional analysis;
– function assignment;
– verification of function assignment;
– validation of function assignment;
– job analysis.

7.2 Functional analysis

7.2.1 General

An analysis of the functions to be performed by the nuclear power plant to achieve the objectives of 6.1 and 6.2 consistent with the principles of 6.3 to 6.8 shall be conducted.

This analysis should identify a hierarchy of goals for the control room design covering all operational states and accident conditions. These goals shall include the production of electricity and the minimization of activity release as principal goals. The goals may be developed further as sub-goals and used in the design decision process.

Refer to IEC 61839 for more detailed descriptions and requirements for the functional analysis process.

7.2.2 Identification of functions

With respect to hierarchical goal structures, all plant functions associated with the goals of the control room should be identified and documented. A means for identifying these goals is given in IEC 61839. In defining functions the analysis shall take into account the interactions between the control room and facilities and systems outside the control room.

7.2.3 Information flow and processing requirements

Analysis shall be performed to determine the basic operational information flow and processing required to accomplish the plant functions including decision making and operations. This analysis is described in IEC 61839.

When identifying the information flow and processing requirements, the designer should use several representative ~~design basis events as well as all normal operations~~ plant operational states (normal and anticipated operational occurrences) and accident conditions (design basis and design extension conditions).

The following events should be included;

– events requiring operations subjectively judged to be difficult in terms of complexity of data interpretation or control, control speed, etc.;
– events requiring the highest certainty of correct operator response, e.g. certain accident conditions;
– events important in terms of the probabilistic ~~risk~~ safety assessment;
– events in which plant trip is highly probable unless corrective action is taken in time;
– events whose occurrence rates are high;
– events which test out team-working.

The number of events to be included shall be large enough to cover adequately the functions associated with the hierarchical goal structure.

7.3 Assignment of functions

7.3.1 General

~~Task analysis~~ Functional analysis provides the required input to the assignment of functions process which shall be conducted to determine which functions should be assigned to the human and which functions should be assigned to the machine. Function analysis and assignment defines the operator tasks with their characteristics in a first level of detail and is the input to the task analysis.

Human factors engineering principles and design criteria shall be applied in this analysis (see ISO 11064).

Functions assigned to humans shown in Table A.1 in Annex A are:

– manual control (including backup control to automation);
– monitoring associated with both manual control and automatic control;
– high-level mental processing tasks such as diagnosis to determine the cause of abnormal and unforeseen operating conditions and events and to determine corrective actions.

Functions assigned to the machine refer to those which are achieved by automatic control as shown in Table A.1. In the case of assigning important safety functions to machine, consideration shall be given to also:

a) assign the monitoring of automatic systems to humans (to supervise correct operation and intervene in case of malfunctions);
b) provide feedback reflecting automatic actions;
c) enable human intervention in case of failures.

The principles and criteria used in the analysis shall be documented and shall include factors which deal with the capabilities and limitations of both the control room staff and the automatic control system.

Refer to IEC 61839 for more detailed requirements concerning the assignment of functions process.

7.3.2 Operator capabilities

The functions assigned to the operator should distinguish between those situations where he or she is ~~actually performing a control task, where the operator is supervising an automatic system that is performing the control tasks and where the operator is performing high level mental processing tasks such as diagnosis.~~:

– actually performing a control function,

– supervising an automatic system that is performing the control function, and

– performing high level mental processing tasks such as diagnosis.

This analysis should result in the information needed for the conceptual design of the information system ~~structure~~ and the functional organization of resources/means to perform each ~~decision making and control task~~ of the above functions.

For potential operator functions, estimates of processing capability required in terms of workload, accuracy, rate and time factors shall be prepared for each information processing aspect and control action. These estimates shall be used for the initial assignment of functions. The estimates should be modified based on verification results and used to reconsider the assignment of the function as well as to provide a more detailed definition of the required operator capabilities.

These requirements together with those for display, control and communication shall be consistent with the operator tasks which shall be performed to accomplish the function. The general operator tasks definitions should include ~~display~~ information, control and communication requirements .

The various types of data available to the operator should be grouped based upon the tasks and not on the sources of data. The purpose of grouping is to ~~organize~~ provide within the operator capabilities, a system using comprehensive information from various sources with respect to each ~~decision making~~ task ~~to provide a comprehensive information system for the operator within his capabilities~~ (see 7.6).

7.3.3 I&C system processing capabilities

Analysis of instrument and control system processing shall begin with a definition of system and equipment functional requirements and constraints, followed by a more detailed description of operational event sequences and human-machine interface requirements for each task. The purpose is to organize the machine information and capabilities with respect to the tasks defined for operator interaction. This organization will facilitate the assessment of the capabilities of both automatic controls and human control for each decision-making and control task.

Processing capabilities of the I&C system should ultimately include aspects such as quantity, response time, accuracy and human-machine interfaces requirements ~~that the system and equipment shall satisfy as well as human engineering requirements defining the human-machine interface for each component type~~ coherent with human factors engineering considerations.

To reduce the probability of operator error, the control systems should be designed to keep the plant within safe limits without any operator action during a specified period of time after initiation of certain abnormal conditions of the plant. This period of time shall be reflected in the functional requirements for the automatic control systems. The degree to which the operator needs to be informed about these automated actions should be considered to maintain situational awareness.

7.4 Verification of function assignment

7.4.1 General

An acceptable assignment of control room functions to human and machine shall be verified as shown in Figure 2. Evidence shall be presented that the proposed function assignment takes the maximum advantage of the capabilities of human and machine without imposing unfavourable requirements on either of them.

Refer to IEC 61771 for more detailed requirements for the verification of function assignment.

7.4.2 Process

The process developed for the verification shall include preparation, evaluation and resolution phases.

Before attempting to verify the proposed function assignment, the criteria used for the assignment shall be confirmed to be self-consistent.

The verifications shall subsequently confirm that:

– all the functions necessary for the achievement of the plant operational and safety goals are identified;

– the proposed function assignment is in accordance with criteria established for the assignment;

– sufficient requirements of each function are identified. These requirements include performance aspects (e.g. time constants, accuracy), those derived from safety principles, availability principles and station operating authority principles specified in this document, and those derived from other standards, regulations and guidelines;

– requirements from higher level functional goals merge at a lower functional level without conflict under all operational modes.

Modification (i.e. correction of mistakes or reassignment) and verification shall be made iteratively until all these criteria are satisfied.

7.5 Validation of function assignment

7.5.1 General

The proposed function assignment shall be validated to demonstrate that the system would achieve all the functional goals. In particular, the performance of the identified functions of 7.2 shall be evaluated under all the normal operations and several representative events including abnormal operation and accident conditions.

Refer to IEC 61771 for more detailed requirements for the validation of function assignment.

7.5.2 Process

The process developed for the validation shall include preparation, evaluation and resolution phases.

Selection criteria shall be developed to ensure that the events to be chosen for assessment are representative. In addition to all normal operations and events specified in 7.2.3, events caused by multiple failures should be considered for the assessment of functions assigned to humans.

After the completion of the selection of representative events, functions required in each event shall be identified and synthesized in time-sequential order.

7.5.3 General evaluation criteria for validation

The performance of functions shall be evaluated for all normal operations and the representative events. The general validation criteria shall be satisfied including the following:

– the number of functional goals and the work load rate required of the control room staff shall not exceed their capability;
– the assignment of functions to the control room staff and local operators is acceptable;
– the assignment of functions to automation is satisfactory and feasible.

7.6 Job analysis

In order to develop basic requirements for the control room staff structure, the operating procedures and the training programme, the designer should conduct a job analysis of the verified or validated function assignment and functional requirements.

The first step of the job analysis is to identify the characteristics and the number of tasks assigned to humans. Based on that, the designer can then define the organization and the number of operators, within the framework of the control room staff structure required by regulation and the utility normal practice.

Tasks assigned to an operator should not overload him or her and should be consistent with his or her responsibilities as defined by the control room staff structure. Furthermore, the designer should identify communications among operators and communications between control room operators that are necessary for the achievement of tasks.

The designer should also identify non-operational activities (e.g. reporting to authorities) inherent in some tasks by referring to appropriate documents.

When completed, the analysis should clarify:

– organisation and number of operators;
– operator competence required;
– operational responsibilities of operators;
– administrative duties of operators (e.g. reporting);
– operational interactions between operators;
– dialogues between operators and plant;
– communications between operators and plant personnel stationed outside the control room facilities;
– communication with management and supervisory staff.

Together with the results of the analysis for the function assignment (e.g. conceptual information structure), the items above should form the basis of the control room staff structure, the operating procedures and the training programme.

8 Functional design specification

8.1 General

This clause aims to specify the functional design requirements for the control room system and equipment that perform the assigned monitoring and control functions. It also specifies the interface between the human and the control room equipment.

The design shall be based on an integrated human-machine systems engineering approach.

8.2 Provision of data base on human capabilities and characteristics

When detailed design of a control room is carried out, a data base on human capabilities and characteristics shall be provided as fundamental human factors design data.

The data base shall include:

– anthropometric considerations;
– population stereotypes;
– auditory and visual capabilities and characteristics;
– human ability to process information;
– environmental factors.

As some of these data depend on the custom of the country, the data base may be specific to each country or each utility.

8.3 Location, environment and protection

8.3.1 Location

The control room shall be located for convenient plant operation and should meet the safety principles of 6.3.

8.3.2 Environment

Environmental conditions in the main control room shall be such that the operators can perform their tasks effectively and comfortably.

The environmental design of the control room shall include requirements for air conditioning, illumination and the auditory environment. The following requirements apply:

a) Air conditioning

The main control room shall be air conditioned. The air conditioning shall include measures to cope with accident conditions of the plant, e.g. by using filters or isolation capability.

b) Illumination

Design of the lighting system shall ensure ~~uniform~~ task-adequate lighting, avoidance of glare, reflections and shadows. The design shall address adequate emergency power supply of the lighting.

c) Auditory environment

Design of the auditory environment shall ensure easy communication within the operating team, minimal disturbance by ambient noise, and reliable perception of acoustic messages, alarms and emergency signals.

Guidance for environmental specifications under normal conditions is provided in ISO 11064.

It may be convenient to include within this specification the requirements for size and shape of the control room with provisional layouts, cable access arrangements, seismic requirements, room and panel colour and other finish details, for agreement with civil engineering interests and later confirmation in detail.

Appropriate measures shall be taken in the design to maintain control room operability and the monitoring and control of the plant even during ~~emergency~~ accident conditions. Requirements for the condition and duration for which the MCR environment has to be maintained under such conditions shall be defined. Procedures shall be established to operate features and systems installed to achieve the required duration.

8.3.3 Protection

The design of the control room shall provide, within the design basis, protection against fire, radiation, internal and external missiles, earthquake and hostile acts. The equipment shall be qualified in accordance with the design basis. For all items of equipment required to operate under design extension conditions, demonstrable evidence shall be provided that it is able to perform its function(s) under the applicable service conditions, see IEC/IEEE 60780-323.

The design shall ensure that such events cannot simultaneously jeopardize the main control room and the supplementary control points, mentioned in 6.7.

More specifically:

a) Fire protection

Attention should be given to using non-flammable materials only. The control room area shall be equipped with a fire detection and fire-fighting system.

Electrical equipment in the control room shall be designed to neither cause nor support a fire as far as this is reasonably achievable.

Cable circuits and switchgear associated with the control room shall be protected against the consequences of fire. Cable insulation and sheathing materials should be fire-retardant and meet national test criteria for flame propagation, release of combustion products and materials where applicable.

b) Radiation protection

The control room staff should be protected against direct radiation in any accident situation. The air intake ducts shall be equipped with a radioactivity monitoring system. If circumstances require, the control room ventilation system shall have the capability to isolate itself. Breathing apparatus shall be available to the staff.

c) Missile protection

The control room design shall include assessment and protection against missiles originating from inside and outside the control room. Guidance on the protection from missiles is given in the IAEA Safety Guide NS-G-1.11.

d) Earthquake protection

The control room equipment related to safety functions, the air-conditioning system and safety illumination system (i.e. the lighting designed to function post seismic event) shall be designed on the same seismic basis. Detailed requirement are provided in IEC 60980.

e) Hostile acts

Measures should be taken to restrict access to the control room and to protect it against hostile acts.

The security plan shall conform to the requirements of the regulations in each country. The security plan shall include the MCR assets subject to computer security protective measures including computer systems, computer system applications and network connections, see IEC 62645.

8.4 Space and configuration

8.4.1 Space

The control room shall have sufficient space to allow the control room staff to perform all necessary actions, while minimizing the need for operator movement in abnormal conditions.

Special attention should be paid to providing work areas, writing space and storage space for documents:

– Work areas which are manned on a continuous basis shall be designed for seated operation and adequate seating shall be provided, but should also permit operation whilst standing.

– Where writing and access to documentation form a normal part of the control room duties, adequate writing space shall be made available.
– Storage space for documents shall also be provided close to the operating position to avoid the documents being laid on consoles, desks, etc.
– Some space may be provided for extensions that might be required in the future (during design phases or during the main control room life time).

8.4.2 Configuration

The control room shall be designed giving due consideration to:

– station operating authority's operating principles;
– assignments of functions to the operators and I&C system;
– centralized or local control philosophy, which determines the extent of controls present in the control room;
– supervision criteria, which determine the use of overview displays, the number of VDUs, indicating instruments, recorders, alarms and indicating lights on the panels;
– technology choices (the degree of use of dedicated hard-wired controls and indications compared to the degree of soft control and VDUs including large screen displays, segregation between the different divisions, use of automatic control sequences, extent of automation and/or multiplexed controls);
– station operating authority and legal requirements, such as the number of operators in the control room required by operating policies or licensing authorities;
– installation of non-operational systems, such as fire alarm and fighting systems, and other site-related functions;
– space for administrative functions.

The control room shall have such operating areas as are necessary, where each operator can obtain access to all controls and information required to perform the tasks assigned to him in all operational and accident conditions.

The operating area and control room equipment such as control desks, boards and panels shall be arranged according to human factors engineering principles. The layout should be such that each operator is provided with easy access and good visibility of the control room equipment related to their responsibilities and such that each operator can see directly and speak with other operators normally present without undue interruption of the line of sight between them.

Refer to ISO 11064 for more detailed requirements.

Information displays and control elements shall be arranged according to consistent principles which should be well documented in the design process.

The arrangement shall be structured, especially in the case of control rooms based on the extensive use of dedicated controls and indicators, to simplify the system or component identification in normal operation, accident conditions and emergency situations, and minimize the probability of incorrect actuations arising from human error.

The above criteria may be used in combination with other design elements and the resulting rules shall be consistent for all operating areas.

8.5 Panel layout

8.5.1 Priority

Principles shall be established and applied for the layout and arrangement of alarms, displays and controls belonging to a function of a system as well as for priority rankings between

similar elements in the layout of the panels. The priority ranking rules derived from these principles shall be consistent for all panels in the plant.

8.5.2 Positioning on control desks and panels

The positioning of displays, indicators and controls on the panels and desks shall be based on the following criteria:

– alarm panels and fascias shall be visible from the operating area of the control room and shall be at a convenient height for operator visibility and legibility;

– frequently used controls shall be within convenient reach and the related indicators and displays shall be readable from the operating position.

Refer to ISO 11064 for more detailed requirements.

8.5.3 Mirror image layout

Mirror image layout of panels, controls and indicators shall be avoided in order to prevent left-right confusion.

8.6 Location aids

8.6.1 Grouping of display information and controls

It is essential that the displayed information and controls are logically grouped.

The following techniques may be used for grouping displayed information and controls :

a) Grouping by function

Information and controls should be grouped in relation to function or interrelationships within a system. Care shall be taken to identify the function in terms of the role that the information plays in achieving system objectives rather than of the source of information or method of measurement.

b) Grouping by sequence of use

Information and controls may be grouped on a sequential basis either by considering the display as a whole or by dividing the display into parts, each of which is organized on a sequential basis. Cause/ effect relationships should be reflected in the display.

Use should be made of natural groupings which conform to user population stereotype expectations (e.g. 1, 2, 3 – a, b, c, etc.). For the same reasons, the display should be organized in a corresponding manner, e.g. from left to right and from top to bottom.

c) Grouping by frequency of use

In this form of grouping, information which is most often used is collected together with the most used, say, at the top of the display and the least used at the bottom, and the controls most used nearest to the operator.

The most common method of establishing frequency of use is link-analysis in order to determine the connections between various items of information or controls and procedures.

This type of grouping is of limited application due to the risk of apparent illogicality in the display.

d) Grouping by priority

Here the information or controls are grouped by significance to the correct functioning of the system. Highest priority items should be placed in prime positions within a group.

e) Grouping by operating procedures

Information displays and controls should be grouped according to the operating procedures. The special equipment of displays and controls to be used in emergency conditions should be grouped separately from that used for normal operation.

f) Grouping by system with mimic arrangement

If mimics are used, care shall be taken to avoid conflicts with other criteria used, and to maintain the same mimic philosophy if alterations or additions to the process or to the instrumentation and controls will be required in the future.

Appropriate techniques should be selected and combined by balancing their respective properties. Each group shall be of a manageable size to allow rapid and accurate searching. Care should be taken to respect human performance constraints.

The grouping should be consistent with the assumption about the user's mental model of the plant.

Particular care shall be taken to avoid conflicts of grouping, especially when different grouping techniques are used simultaneously.

8.6.2 Nomenclature

The names and identities of each plant item, allowing for the many redundant items on a nuclear plant, shall be carefully considered and agreed on a project-wide basis for uniform use.

Specific abbreviations and acronyms (such as CVCS for chemical and volume control system) should be agreed and used consistently. A human factors review of these plant identifications may be advantageous.

8.6.3 Coding

Coding of controls and of information displayed can be used to distinguish between different types of control or classes of information, such as to distinguish between:

a) safety functions,

b) other functions important to safety, and

c) functions not important to safety.

Coding principles shall be established in an early stage of control room design and they should be consistent with national requirements and utility practices.

The coding system shall be consistent throughout the control room. Location, information, colour and illumination codes applied to displays and their associated controls shall be applied in a consistent way.

The coding method for an actual application shall be determined considering the relative advantages of the types of coding:

– physical coding (size coding, shape coding, colour coding, auditory coding, and intensity coding),

– information coding,

– location coding.

Refer to ISO 11064 for more detailed requirements.

Due to potential staff considerations (persons with colour deficient vision) and equipment considerations (fading-out of colours, partial failure of I&C equipment), colour shall not be the sole means of discrimination for information important to safety. The sole use of colour for coding should also be avoided in other areas.

8.6.4 Labelling

Adequate labelling shall be provided in the control room. The labelling shall be consistent with other labelling in the plant and in accordance with national requirements and utility practices. Refer to ISO 11064 for more detailed requirements.

The language and script used for all control room labels and identifiers, and for all displays, shall be uniform throughout the control room and should be that of the dominant language of the population in whose area the plant is located, except for technology reasons.

8.7 Information and control systems

8.7.1 General

Following the design process and requirements of IEC 61513 for the overall I&C architecture, there will be information and control systems implementing the human-machine interface in the main control room for plant monitoring and control.

The system architecture will depend on:

– safety classification;
– failure criteria;
– defence-in-depth strategy;
– qualification and reliability considerations;
– maintainability considerations;
– security considerations;
– choices imposed by the available technology.

The information and control systems will be implemented by one or several subsystems dealing with the various aspects of the human-machine interface and operator support functions. This typically includes computer-based systems with VDU-displays and soft-controls as well as dedicated indicators and controls. The requirements are summarized below.

8.7.2 Information functions

8.7.2.1 General

An information system shall be provided to inform operators of the plant status and variables important to safety and availability, which allows the control room operators to obtain a complete understanding of the plant state at all times. Particular consideration of the capability and reliability of their power supply and service systems shall be made for a subset of important plant parameters related to plant safety (see 8.10.1) and environment monitoring.

Sufficient information shall be available to allow the operating staff to achieve safe shut-down and hold-down for an indefinite period in accordance with regulatory requirements.

The system shall also provide information of the plant status to technical experts and to on-site and off-site safety experts during accident conditions.

The system shall have data acquisition, display and alarm functions. The system shall also have recording and memory functions for the plant process variables important to safety and availability, for analysis and for reporting within the operating organization and external authorities.

Information processing functions should also be provided to support high-level mental processing by the operators as a means of:

– aiding decision making;
– improving monitoring performance and capability.

This should be achieved by:

– ensuring high availability and reliability of information;
– providing information useful for formulating actions;
– facilitating good communication between control room staff;
– providing a record of transients and accidents for analysis purposes including access to recorded data;
– recording operator control actions where this is practicable;
– expanding available information to cover implicit data.

Categorisation of the information system functions shall be made in accordance with IEC 61226.

Specific requirements are as follows:

a) Information for operators

The operator shall be able to obtain at any time a complete understanding of the plant from the information systems. These shall enable the operators to:

– recognize any current or potential safety or availability hazards;
– know the actions being taken by automation systems;
– analyse the cause of any disturbance and follow its course;
– perform any necessary manual counteractions.

The design basis for information systems, including their measurement devices, shall take into account their importance to safety. The intended safety function of each system and its importance in enabling the operators to take proper pertinent actions in anticipated operational occurrences or accident conditions shall be identified in its design basis and shall be used as an input to any I&C categorization method selected.

Accident monitoring systems for Design Basis Accidents and Design Extension Conditions shall provide operators with the information that they need to develop an integrated understanding of the status of the reactor, containment and SFP in a manner that allows for the greatest understanding of the nature of the accident, the status of the integrity of the barriers to fission product release, and the potential magnitude and pathways for such a release.

b) Information function for non-shift experts

Although the control room is the information and control centre of the plant for the operators during both normal operation and accident conditions, it may also be used as the primary centre to direct the initial stages of off-site activities depending on national and utility principles for emergency operations support. See also IAEA Safety Guide NS-G-1.9.

It is preferable to accommodate visiting experts in a separate room and exclude them from the control room.

Information systems may be extended to supply information to separate outside support facilities.

c) Recording and printing

An adequate number of recorders or printers shall be provided in or adjacent to the main control room for analogue process variables and for binary signals in order to obtain chronological information about the performance and behaviour of the plant.

This is necessary for the following purposes:

– back-up information for shift operators giving short-term and long-term trends;

– general operational information for the plant management;

– short-term and long-term analyses of operation and accidents.

Consideration should be given to automatic recording of operation of the controls to allow analysis of operator actions.

8.7.2.2 Data acquisition and processing

The major functional requirements for data acquisition and processing are as follows:

– faults shall not cause any unsafe state or unacceptable economic losses in the plant operation;

– input data sampling, pre-processing and analysis rates shall be appropriate to satisfy operational requirements related to the parameter rates of change;

– data shall be updated at rates appropriate to operator tasks;

– there shall be no significant delays in processing plant data or operator requests even at times of peak loading;

– modification shall be possible throughout the operational life;

– a provision shall be made to allow the operators to easily identify invalid displayed information.

Further requirements are as follows:

The data acquisition and processing system should take into account all aspects of operability and reliability requirements, future plant modifications and maintainability.

This requires that an essential part of identifying and defining the data acquisition and processing system involves a comprehensive analysis (e.g., task analysis) which takes the performance of the control room staff into consideration. Such analysis will be able to identify data requirements including the necessary data availability and correctness.

The data acquisition and processing system shall be fully defined regarding:

– the frequency of data sampling and redundancy;

– pre-processing and consistency checking;

– the analysis required for off-normal conditions;

– the output required and the form of output, e.g., print or ~~VDU~~ electronic.

Raw data processing may consume a significant proportion of CPU time for a single computer based system. Similarly, ~~the tasks of analysis and data output or presentation~~ further data processing and display may consume computer time. An assessment should be done to determine the computer loading in normal and in peak loading conditions, before the system is put into service. This assessment should be confirmed by suitable tests on the fully installed system to demonstrate the viability of the system to the operating staff for the expected range of operating conditions. There shall be no significant delay in processing and presenting plant data or operator requests even at times of peak loading. Experience indicates that operators become impatient if there are delays to any function of a computer-based information system greater than about 1 s. ~~Longer response times are acceptable in some cases, e.g. accessing historical data or archive data, if a feedback cue is given to indicate that the processing is under way.~~ A feedback cue should be implemented if longer response times cannot be avoided, e.g. in case of accessing historical data or archive data.

Although some systems may use only a single computer to process the data and to provide information, redundancy of computers and of modules should be included to ensure service continues when any more frequent single fault occurs.

8.7.2.3 Display system

The display system shall be designed as a human-machine interface of the information system, considering human capabilities and characteristics.

The displays shall enable the operators to:

– know the actions being taken by the reactor protection system and other automatic systems, so as to be able to verify their state and perform necessary support actions;

– analyse the cause of disturbances and follow their course;

– perform any necessary manual counteractions.

The display shall enable the operators to recognize potential safety or availability hazards.

The major functional requirements of the display system are as follows:

– the display system in the control room shall cover appropriate variables, consistent with the assumptions of the safety analysis and with the information needs of the operator in normal operation and accident conditions;

– the accuracy, range, and scales of displays shall be consistent with the assumptions of the safety analysis and the supported operator tasks;

– displays shall be provided for indicating by-passed or deliberately inoperable conditions of the plant and auxiliaries;

– information displays important to safety shall be suitably located and specifically identified on control panels;

– the types of displays shall be selected in accordance with their purpose;

– the display system shall provide both information and alarm displays, which should provide an integrated approach to the display of plant conditions.

In general, VDU-based displays and information means will be used. Dedicated displays like analogue meters, digital indicators, lamps and trend recorders may be required e.g.

– for post-accident situations, due to qualification or diversity considerations, or

– if requirements for spatially dedicated display have to be fulfilled.

An adequate number of printers should be identified in order to provide hardcopies for the shift team, as material for team discussion and analysis and possibly legal documentation purposes.

Detailed guidance for VDU-displays is provided in IEC 61772; guidance for dedicated displays can be found in ISO 11064.

8.7.2.4 Alarms

Main control room alarms shall provide all information necessary for plant surveillance in abnormal plant conditions.

The alarm system should:

– display alarm information to enable the operator to understand the fault situation as it develops;

– enable the operator to remove irrelevant information but ensure that relevant and important information is presented in a manner matching the operator's capacity to understand;

– enable the operator to distinguish between alarms for which corrective actions are not complete and alarms which cannot be cancelled without the intervention of the maintenance service;

– avoid information overload.

The alarm system should have:

– processing functions, to give the operator the most representative information of abnormal conditions, and
– display functions, to permit the operator to easily identify an alarm and its seriousness.

Moreover, for each alarm, a procedure document, e.g. alarm sheet or plant item operating instruction, shall be provided to explain to the operator the likely reasons for the alarm and the corrective actions required.

Refer to IEC 62241 for more detailed requirements.

8.7.2.5 Operator support function

In order to enhance plant safety, availability and operability, operator support functions such as the following should be provided:

– safety parameter displays and surveillance functions (see IEC 60960);
– plant diagnosis functions;
– operator guide functions for normal operation and post-accident situations, e.g. symptom- and event based procedures. See also 62646 for computer based procedures requirements;
– functions for automatic on-power test.

So far as practicable such functions should be fully integrated into the overall design of the control room.

8.7.3 Control functions

This subclause deals with functional human factors specifications of controls used for manual control operations as well as for back-up to automatic control operations under both normal and abnormal operations. However, functional specifications of control functions as embodied by plant I&C systems, are outside the scope of this document.

a) General considerations

Controls shall be designed to ensure ease of operation and to minimize operator errors.

The controls selected shall be suitable for operator use in a control room environment and shall match the characteristics of the expected user population.

Controls shall meet the following requirements:

– to minimize operator error, control movements should conform to population stereotypes and should be compatible with the controlled variable;
– controls shall integrate feedback information for the selected function and integrate display of check-back information of the state of the controlled components;
– categorisation of control functions shall be commensurate with their importance to safety, in accordance with IEC 61226.

b) Prevention of erroneous actuation

To prevent human-induced events, erroneous activation of controls shall be minimized by means such as the following:

– locating controls at proper positions, thus avoiding accidental actuation in a control movement;
– use of protective structures, such as use of physical barriers, or recessed installation, movable covers or guards;

- provision of a second confirmatory action, e.g. with a release push button or with an additional soft control command;
- use of interlocks or permissive signals, with proper assignment of priorities;
- proper selection of physical characteristics, such as size, operating pressure or force, tactile, optical and/or acoustical feedback;
- any combination of the above.

c) Technology

Controls may be implemented as soft controls, multiplexed or dedicated controls and mixtures thereof.

The choice should be taken based on criteria such as follows:

- qualification and independence considerations;
- required speed of access and frequency of use;
- available technology.

IEC 61227 provides detailed guidance on this.

8.8 Control-display integration

Controls and their associated displays shall be correctly integrated to ensure effective operation of the plant by control room staff.

The control-display integration shall be in accordance with the proposed method of plant operation as shown in the analyses made according to 6.2 and 6.6.

The control-display integration shall meet the following principal requirements:

- controls should be located near the associated display. Operation of controls should produce a compatible change in the relevant display;
- the grouping of controls and their associated displays shall reflect the need to achieve system objectives and should be consistent with assumptions about the user's mental model of the plant;
- the organization of controls and displays shall reflect cause/effect relationships;
- the organization of controls shall embody user population stereotypes;
- the form of codes used for displays and their associated controls shall be entirely consistent.

8.9 Communication systems

8.9.1 General

Communication systems shall be provided in the control room to facilitate safe and efficient plant operation. Special consideration shall be given to the design of communication systems to be used to communicate with the emergency facilities in the abnormal or accident conditions.

Provision of non-verbal communication systems such as telefacsimile and data-links (between computers) are desirable, between the control room and other information centers in order to improve plant availability and safety. Considerations should be given to security when defining these communications systems, see IEC 62645 and IEC 62859 for requirements.

8.9.2 Verbal communication systems

8.9.2.1 On-site communications

For general communication under normal operational conditions a telephone system with an adequate number of extensions shall be installed. At least one of the extensions shall be located in the control room. Each extension may be connected to the public telephone system. An additional specific system shall be provided in the control room, which is not accessible from the public system and has a dedicated well known emergency call number which is labelled to all other extensions. This extension shall be used for transmitting only disturbance and accident reports to the control room personnel.

For communication in accident conditions to supplementary operating facilities and control points which are important to safety, a separate directly wired system shall be installed where appropriate. The system shall enable the control room personnel to communicate singly or in parallel with a selected number of extensions at the same time. The system shall also enable the control room personnel to communicate with the control room of any other unit with a separate control room at the same site. The system shall be supplied by a non-interruptible power supply system. Extension telephone jacks outside the control room shall be provided where necessary and be accessible also under accident conditions. The system may be extended also for operational use.

A public address system shall be provided to ~~address~~ broadcast messages to on-site personnel under any plant conditions.

For use during maintenance, testing or repair, communication by radio to the control room using mobile transmitters shall be provided, unless all relevant local points can be reached reliably enough by other systems. Radio frequency interference aspects (see IEC 62003) shall be considered in the design, cabling, location and testing of I&C systems. To minimize such interference, the frequency range and the maximum output power of these transmitters shall be limited and specified. Areas where transmitters may not be used, such as the control equipment room, shall be identified.

8.9.2.2 Off-site communications

For communication to the off-site station operating authority, emergency response facilities, governmental and public institutions, an exclusive communication system should be provided. Some of the extensions call numbers, especially one in the control room, shall not be known to the public.

The minimum connections to off-site shall be provided with necessary organizations and personnel. Important connections shall have redundant and diverse systems, e.g. one telephone and one radio system. The connections shall be defined in accordance with national requirements, with typical connections such as follows:

– to stand-by/ready-for-call personnel of the unit staff or other experts to help in emergency or accident conditions;
– to radiation measurement groups which perform tasks outside the site important to safety;
– to the relevant fire fighting station;
– to the local police station which is permanently manned;
– to the offices of the government and public agencies.

8.9.2.3 Arrangement

Communication equipment for operational communication duties and communication duties of the operators shall be installed in the operators' work stations.

The main control room shall also be designed as the communication centre of the plant for normal operation and during the early stages of an accident. Responsibilities and need for

communication in these phases shall be identified in a task analysis, and the communication equipment located accordingly. Preferably most of the equipment for communicating with off-site locations should be located on a special communication desk or panel with extensions on the main control desk and the control panels.

8.9.3 Non-verbal communication systems

Non-verbal communication systems may be provided in the main control room such as follows:

– a television system for monitoring the reactor operating floor and turbogenerator status which may also be used for accident situations;
– a telefacsimile system that should be connected to emergency response facilities in order to transfer plant status and operational suggestions if an emergency condition occurs.

8.10 Other requirements

8.10.1 Power supplies

The power supply arrangement for the control room shall have a reliability and availability consistent with those requirements of the I&C system, the safety system and the system important to safety. Systems important to safety in the control room, which are required to be available for use at all times during operation or accident conditions, shall be connected to non-interruptible power supplies.

Refer to IEC 61225 for more detailed requirements.

8.10.2 Qualification

A qualification programme consistent with that of overall plant equipment shall be provided to confirm that equipment important to safety and systems in the control room are capable of meeting, on a continuing basis, the design basis performance requirements (e.g. range, accuracy, response) needed for their functions under the environmental conditions likely to prevail at the time these will be needed. The programme shall include a plan to ensure that the equipment is qualified for the intended period of use, and provide for timely requalification or replacement, if necessary.

Refer to IEC/IEEE 60780-323 and IEC 60980 for more detailed requirements.

8.10.3 Maintainability

The equipment shall be designed to facilitate surveillance and maintenance and, in the case of failure, easy diagnosis and repair or replacement.

The contribution of repair time to equipment unavailability shall be evaluated at the design stage. The mean time to repair and the frequency of inspection shall be specified in the design base of each particular system. Knowledge of the means of detecting that a failure has occurred, e.g. a power supply system check (test), shall be a part of this evaluation.

Means provided for the maintenance of the systems shall be designed so that any effect on the safety of the plant is acceptable.

8.10.4 Repairs

The control room shall be designed, considering panel layout and equipment configuration, to ease repair of the equipment and systems in it. The design shall also include the consideration of repair facilities and spare parts.

8.10.5 Testability

The control room shall be designed to permit test and calibration, without difficulty, at necessary intervals for each of the necessary functions. See IEC 60671 for testability requirements.

9 Verification and validation of the integrated control room system

9.1 General

Upon completion of the initial conceptual design of an integrated control room system including the arrangements for control room staffing, the human-machine interface, the operating procedures and the training programme, its adequacy shall be verified and validated. In subsequent subclauses, the process and general evaluation criteria of verification and validation are specified for the human-machine interface. For other control room system constituents, i.e. the control room staff structure, the operating procedures and the training programme, the evaluation process and criteria should be developed separately using appropriate national standards, and internationally agreed guidelines available (see IAEA Safety Guides).

See IEC 61771 for more detailed requirements.

9.2 Control room system verification

9.2.1 General

Prior to and during detailed control room system integration, functional specifications of the control room system shall be verified to show that the specifications meet relevant criteria and functional requirements.

9.2.2 Process

The process developed for the verification shall include preparation, evaluation and resolution phases. Evaluation of the integrated control system shall be made at this stage including the operating procedures and the training programme which have been provided separately as shown in Figure 2.

9.2.3 General evaluation criteria for integrated system verification

The proposed control room system integration shall incorporate all the functional specifications and all other technical requirements correctly. See IEC 62646 for computer based procedures systems requirements, if applicable.

9.3 Control room system validation

9.3.1 General

Prior to and during detailed control room system design, the overall control room system integration shall be validated to show that it would achieve the performance intended. In particular, special attention shall be given to time dependent dynamic characteristics of the proposed integrated system.

9.3.2 Process

The process developed for the validation shall include preparation, evaluation and resolution phases.

Preparation for validation is made in a similar manner to the validation of function assignment (see 6.5), but operational expertise is particularly important at this stage.

An appropriate control room model which allows the evaluation of the time dependent dynamic characteristics of the proposed system should be developed. For a system whose concept is considerably different from conventional systems, a dynamic simulator is necessary for use for the validation. However, other choices such as a full scale mock-up may be adopted when either the difference is minor or a partial validation can be justified.

Multiple performance measures should be developed to allow redundant evaluation. Both qualitative and quantitative consistency of interrelated performance measures shall be examined to confirm the evaluation results.

Considerations should be given to creating a realistic test environment (e.g., physical arrangement, environmental conditions such as temperature, humidity, lighting, sound, etc.).

The validation programme should be organized in such a way that it makes use of commissioning tests. For example, commissioning tests should be used for aspects that could not be tested in the previous design phases such as evacuation of the main control room and for aspects that were identified as requiring further evaluation.

The evaluation criteria shall be consistent with all the relevant regulations, standards, guidelines, etc.

9.3.3 General evaluation criteria for integrated system validation

See IEC 61771 for requirements.

Annex A
(informative)

Explanation of concepts

A.1 Control room system

The control room system is an integration of the human-machine interface, control room staff, operating procedures, training programme, and associated equipment and facilities (see Figure 1).

There are two major plant operational goals (i.e. controlled generation of electricity and prevention of release of radioactivity to the environment). A number of functional goals have to be satisfied to achieve the plant operational goals. They are satisfied by controlling plant processes through controlled utilization of plant resources. There are essentially two ways of controlling the plant systems (i.e. automatic control and manual control including remote and local manual control).

Hardware systems implementing automatic control and remote manual control include control and safety systems, which are a part of the I&C system, and they include actuators, sensors, and other hardware devices.

Operation of automatic control requires the control room staff to monitor its action through displays, and to take manual control, which includes back-up control, reset and others. Operation of remote manual control requires the intervention of the control room staff through controls and displays located in the main control room.

The controls and displays, which are also a part of the I&C system, have a physical interface with the control room staff, and therefore they are called the human-machine interface.

Local manual control is performed at any place outside the main control room by operators through local control facilities at the request of the control room staff. The instructions are given through the communication interface.

Besides automatic control, manual control and associated monitoring, the control room staff are required to perform high-level mental processing of information (e.g. interpretation of multiple readings, formulation of knowledge-based strategy).

There are various types of operator support systems (e.g. diagnostic systems, operation consulting systems, procedure synthesizers) which are intended to support the high-level mental processing. The control room staff may interface with them in a variety of ways – from simple unidirectional information retrieval through displays to high-level bidirectional communication through appropriate devices. The operator support system is a human-machine interface.

Communication with plant personnel and managerial staff stationed outside the main control room can be made through the communication interface.

A.2 “Human” and “machine”

Assigning functions to human means to achieve them by manual control, monitoring, high-level mental processing, or their combinations. Assigning functions to machine means to achieve them by automation. Therefore, human in the functional domain signifies the control room staff and machine in the functional domain signifies automation (Table A.1).

The term “machine” covers a number of hardware entities which include the I&C system and operator support system. It should be noted that the manual control system, controls, and displays which are parts of the I&C system are to enable the control room staff to achieve functions assigned to them.

Table A.1 – Human and machine in functional domain and physical domain

<table>
<tr><th colspan="2">Functional domain</th><th colspan="2">Physical domain</th></tr>
<tr><td>Functions are assigned to:</td><td>Functions are achieved by:</td><td>Machine (hardware)</td><td>Human</td></tr>
<tr><td>Human</td><td>High-level mental processing
Monitoring (associated with both manual control and automation)
Manual control (including back-up control to automation)</td><td>OSS
Displays
Controls
Manual control system
Human-machine interface
I&C system</td><td>Operating crew</td></tr>
<tr><td>Machine</td><td>Automation</td><td>Automatic control system</td><td></td></tr>
</table>

Bibliography

IEC 62954, *Nuclear power plants – Control rooms – Requirements for Emergency Response Facilities (ERC)*

IAEA Safety Standard Series No. SSR-2/1:2012, *Safety of Nuclear Power Plant: Design*

IAEA Safety Guide SSG-39, *Design of instrumentation and control systems in Nuclear Power Plants*

IAEA Safety Glossary:2016, *Terminology used in nuclear safety and radiation protection*

IEC 60964

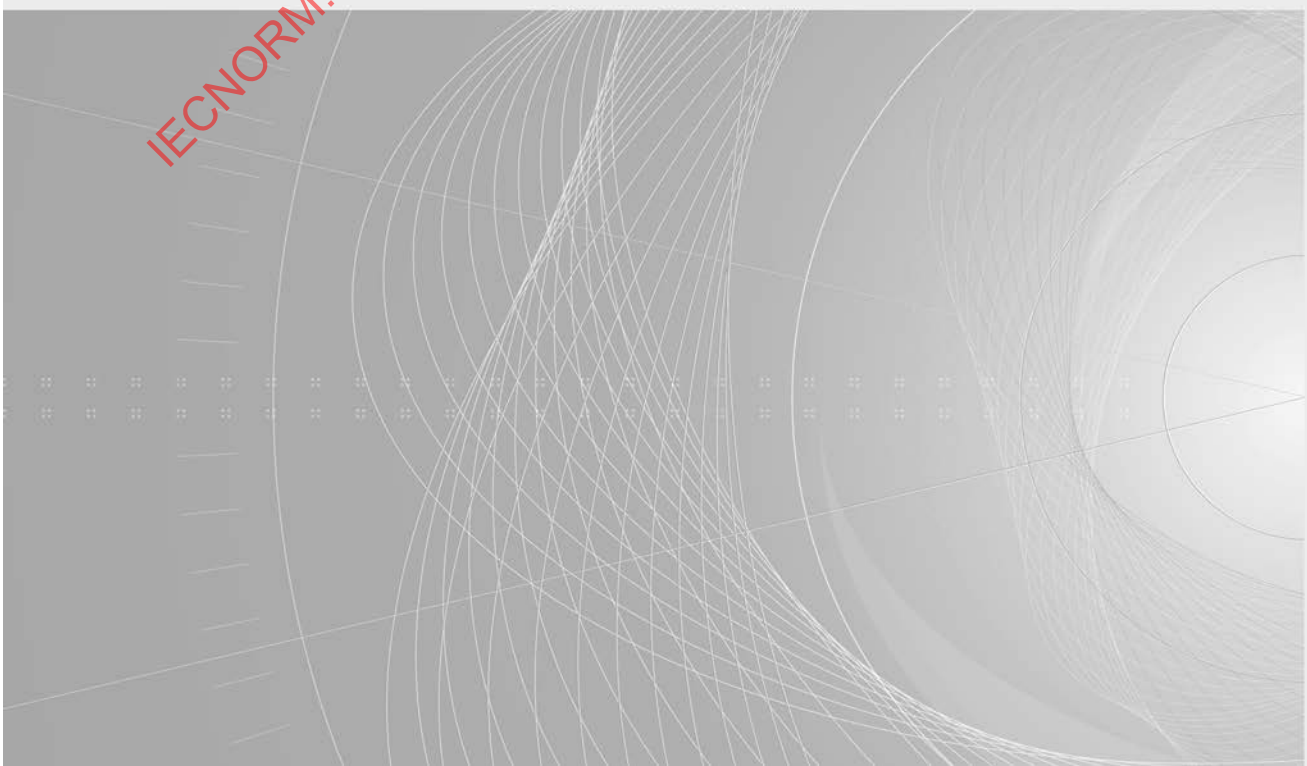
Edition 3.0 2018-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Control rooms – Design

Centrales nucléaires de puissance – Salles de commande – Conception



IEC 60964:2018-11(en-fr)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – CONTROL ROOMS – DESIGN

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60964 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This third edition cancels and replaces the second edition published in 2009. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) to review the usage of the term "task" ensuring consistency between IEC 60964 and IEC 61839;
b) to clarify the role, functional capability, robustness and integrity of supporting services for the MCR to promote its continued use at the time of a severe accident or extreme external hazard;
c) to review the relevance of the standard to the IAEA safety guides and IEC SC 45A standards that have been published since IEC 60964:2009 was developed;
d) to clarify the role and meaning of "task analysis",

e) to further delineate the relationships with derivative standards (i.e. IEC 61227, IEC 61771, IEC 61772, IEC 61839, IEC 62241 and others of relevance to the control room design);

f) to consider its alignment with the Human Factors Engineering principles, specifically with the ones of IAEA safety guide on Human Factors (DS-492) to be issued.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
45A/1214/FDIS	45A/1224/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

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

INTRODUCTION

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

IEC 60964:1989 was developed to supply requirements relevant to the design of the main control room of NPPs and reviewed in 2009. The first two editions of IEC 60964 were used extensively within the nuclear industry. It was however recognized that there was a need to develop an amendment for the 2009 edition to address:

- The usage of the term "task" needed to be examined.
- The role, functional capability, integrity of supporting services and robustness for the MCR should be clarified to promote its continued use at the time of a severe accident or extreme external hazard.
- The relevance of the standard to the IAEA safety guides and SC 45A standards published since 2009.

Given the size of the proposal amendment, it was decided that a new edition of IEC 60964 should be issued instead of an amendment. During the preparation of this third edition, it was agreed that the following points have to be covered:

- to clarify the role and meaning of “task analysis”,
- to further delineate the relationships with derivative standards (i.e. IEC 61227, IEC 61771, IEC 61772, IEC 61839, IEC 62241 and others of relevance to the control room design);
- to consider its alignment with the Human Factors Engineering principles, specifically with the ones of IAEA safety guide on Human Factors (DS-492) to be issued.

This IEC standard specifically focuses on the functional designing of the main control room of NPPs. It is intended that the Standard be used by NPP vendors, utilities, and by licensors.

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

IEC 60964 is the second level IEC SC 45A document tackling the generic issue of control room design.

IEC 60964 is to be read in association with the derivative standards mentioned above which are the appropriate IEC SC 45A documents which provide guidance on operator controls, verification and validations of design, application of visual display units, functional analysis and assignment, and alarm functions and presentation.

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

c) Recommendations and limitations regarding the application of the Standard

This standard is intended for application to new control rooms whose conceptual design is initiated after the publication of this standard. The recommendations of the standard may be used for refits, upgrades and modifications.

The primary purpose of this standard is to provide functional design requirements to be used in the design of the main control room of a nuclear power plant to meet operational and safety requirements.

This standard also provides functional interface requirements which relate to control room staffing, operating procedures and the training programme which are, together with the human-machine interface, constituents of the control room system.

To ensure that the Standard will continue to be relevant in future years, the emphasis has been placed on issues of principle, rather than specific technologies.

d) Description of the structure of the IEC SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 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.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC SC 45A to decide how and where general requirements for the design of electrical systems were to be considered. IEC SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 is published this NOTE 2 of the introduction of IEC SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – CONTROL ROOMS – DESIGN

1 Scope

This document establishes requirements for the human-machine interface in the main control rooms of nuclear power plants. The document also establishes requirements for the selection of functions, design consideration and organization of the human-machine interface and procedures which are used systematically to verify and validate the functional design. These requirements reflect the application of human factors engineering principles as they apply to the human-machine interface during plant operational states and accident conditions (including design basis and design extension conditions), as defined in IAEA SSR-2/1 and IAEA NP-T-3.16. This document does not cover special purpose or normally unattended control points, such as those provided for shutdown operations from outside the main control room or for radioactive waste handling, or emergency response facilities. Detailed equipment design is outside the scope of this document.

The primary purpose of this document is to provide functional design requirements to be used in the design of the main control room of a nuclear power plant to meet operational and safety requirements. This document also provides functional interface requirements which relate to control room staffing, operating procedures, and the training programmes which, together with the human-machine interface, constitute the control room system.

This document is intended for application to new control rooms whose conceptual design is initiated after the publication of this document. If it is desired to apply it to an existing control room, special caution must be exercised so that the design basis is kept consistent.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *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/IEEE 60780-323, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

IEC 60960, *Functional design criteria for a safety parameter display system for nuclear power stations*

IEC 60965, *Nuclear power plants – Control rooms – Supplementary control room 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 61225, *Nuclear power plants – Instrumentation and control systems important for safety – Requirements for electrical supplies*

IEC 61226, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

IEC 61227, *Nuclear power plants – Control rooms – Operator controls*

IEC 61513, *Nuclear power plants – Instrumentation and control 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 (VDUs)*

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

IEC 62003, *Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*

IEC 62241, *Nuclear power plants – Main control room – Alarm functions and presentation*

IEC 62645, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*

IEC 62646, *Nuclear power plants – Control rooms – Computer based procedures*

IEC 62859, *Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity*

ISO 11064 (all parts), *Ergonomic design of control centres*

IAEA NS-G-1.9, *Design of the reactor coolant system and associated systems in nuclear power plants*

IAEA, NS-G-1.11, *Protection against internal hazards other than fires and explosions in the design of nuclear power plants*

IAEA NP-T-3.16, *Accident Monitoring Systems for Nuclear Power Plants*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply. For other terms, refer to the general terminology defined in IEC 61513 and in the IAEA Safety Glossary.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
accident conditions
deviations from normal operation that are less frequent and more severe than anticipated operational occurrences

Note 1 to entry: Accident conditions comprise design basis accidents and design extension conditions.

[SOURCE: IAEA Safety Glossary, 2016]

3.2
alarm
item of diagnostic, prognostic, or guidance information, which is used to alert the operator and to draw his or her attention to a process or system deviation

Note 1 to entry: Specific information provided by alarms includes the existence of an anomaly for which corrective action might be needed, the cause and potential consequences of the anomaly, the overall plant status, corrective action to the anomaly, and feedback of corrective actions.

Two types of deviation may be recognised:

– Unplanned – Undesirable process deviations and equipment faults;

– Planned – Deviations in process conditions or equipment status that are the expected response to but could be indicative of undesirable plant conditions.

[SOURCE: IEC 62241:2004, 3.1]

3.3
auxiliary control <operating> systems
operating systems that are installed outside the control room such as local-to-plant control points and local-to-plant shutdown systems

3.4
control room staff
group of plant personnel stationed in the control room, which is responsible for achieving the plant operational goals by controlling plant through human machine interfaces

Note 1 to entry: Typically, the control room staff consists of supervisory operators, and operators who actually monitor plant and plant conditions and manipulate controls but also may include those staff members and experts who are authorized to be present in the control room, e.g. during long lasting event sequences.

3.5
control room system
integration of the human-machine interface, the control room staff, operating procedures, training programme, and associated facilities or equipment which together sustain the proper functioning of the control room

3.6
controls
devices which the operator uses to send demand signals to control systems and plant items

Note 1 to entry: Controls as defined in this document (i.e. devices used for control actions) hold a different meaning from the one defined in the IAEA safety Glossary and are not replaceable.

3.7
design basis accident
postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits

[SOURCE: IAEA Safety Glossary, 2016]

3.8
design extension conditions
postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions include conditions in events without significant fuel degradation and conditions with core melting

[SOURCE: IAEA Safety Glossary, 2016]

3.9
displays
devices used for monitoring plant conditions and status, e.g. process status, equipment status

3.10
format
display format
pictorial display of information on a visual display unit (VDU) such as message text, digital presentation, symbols, mimics, bar-charts, trend graphs, pointers, multi-angular presentation

3.11
function
specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it

[SOURCE: IEC 61226:2009, 3.7]

3.12
functional analysis
examination of the functional goals of a system with respect to available manpower, technology, and other resources, to provide the basis for determining how the function may be assigned and executed

3.13
functional goal
performance objectives that shall be satisfied to achieve the corresponding function

3.14
hierarchical goal structure
relationship between a functional goal and sub-functional goals structured in a hierarchical order

3.15
high-level mental processing
human act to process and/or interpret information to obtain reduced abstract information

3.16
human-machine interface
interface between operating staff and I&C system and computer systems linked with the plant. The interface includes displays, controls, and the Operator Support System interface

3.17
I&C system

system, based on E/E/PE items, performing plant I&C functions as well as service and monitoring functions related to the operation of the system itself

Note 1 to entry: The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices. The different functions within a system may use dedicated or shared resources.

Note 2 to entry: The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

Note 3 to entry: According to their typical functionality, IAEA distinguishes between automation and control systems, HMI systems, interlock systems and protection systems.

[SOURCE: IEC 62138:2018, 3.26]

3.18
job
set of tasks which are operationally related. The tasks within a job should be coherent with regard to required skill, knowledge and responsibility

3.19
job analysis
analysis identifying basic requirements which a job imposes on the control room staff structure, the operating procedures and training programme

3.20
local control points
local control facilities
points (or facilities) located outside the control room where local operators perform control activities

3.21
local operators
operating staff that perform tasks outside the control room

3.22
operating procedures
set of documents specifying operational tasks it is necessary to perform to achieve functional goals

3.23
operating staff
plant personnel working on shift to operate the plant

Note 1 to entry: The operating staff includes the control room staff, maintenance engineers, etc.

3.24
operator interaction
interrelation between operator and the I&C system. Specifically, display of plant status by the I&C system and corresponding operator action

3.25
Operator Support System
OSS
system or systems supporting the high-level mental information processing tasks assigned to the control room staff

3.26
performance requirements
quantitative requirements specifying performance which ensure the achievement of functional goals

3.27
plant operational goals
ultimate purposes of plant design, i.e. controlled generation of electricity and limitation of release of radioactivity to the environment

3.28
population stereotype
tendency for most persons in a group or population to give the same response to a particular stimulus, even when there are alternative responses. The population stereotype depends on the customs and habits of the population sampled

3.29
supplementary control room
location from which limited plant control and/or monitoring can be carried out to accomplish the safety functions identified by the safety analysis as required in the event of a loss of ability to perform those functions from the Main Control Room

Note 1 to entry: For existing plants, the Supplementary Control Room may be a special control room, but in many cases comprises sets of control panels and displays in switchgear rooms or similar areas. In the latter case, the term 'supplementary control point' is used in this document.

[SOURCE: IEC 60965:2016, 3.6]

3.30
severe accident
accident conditions more severe than a design basis accident and involving significant core degradation

[SOURCE: IAEA Safety Glossary, 2016]

3.31
task analysis
identification and description of an operator's task, in terms of its components, to specify the detailed human activities involved, and their functional and temporal relationships

Note 1 to entry: Frequently, task analysis in understood to also include the evaluation of the operator's tasks. In the frame of IEC 60964, this evaluation is described in terms of V&V of function assignment and V&V of the integrated control room system (which also covers the operator tasks).

3.32
tasks
actions performed by humans for the accomplishment of a functional goal

3.33
training programme
programme which is designed to train the control room staff so that they can acquire the skills and knowledge necessary for operational activities

3.34
validation
process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation is broader in scope, and may involve a greater element of judgement, than verification.

[SOURCE: IAEA Safety Glossary, 2016]

3.35
verification
confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity

[SOURCE: IAEA Safety Glossary, 2016]

3.36
Visual Display Unit
VDU
type of display incorporating a screen for presenting computer-driven images

4 Abbreviated terms

E/E/PE	Electrical/Electronic/Programmable Electronic
HMI	Human Machine Interface
I&C	Instrumentation and Control
MCR	Main Control Room
NPP	Nuclear Power Plant
OSS	Operator Support System
VDU	Visual Display Unit
V&V	Verification and Validation
SFP	Spent Fuel Pool

5 Standard use

This clause is provided to orient the user to the organization and focus of this document. Figure 1 shows an overview of a control room system. The goal of a control room design team is the successful completion of an integrated control room system. The control system is an integration of the human-machine interface, control room staff, operating procedures, training programme and the associated equipment and facilities. Annex A provides a supplemental explanation concerning the concept of the control room system.

The focus of this document is the establishment of the human-machine interface in the control room design. The document also establishes a means for developing staffing requirements, operating procedures and a training programme but does not provide detailed methodology for such development.

After the scope, statements and specifications of design principles, the design process is shown in Figure 2 to include functional analysis, function assignment, function assignment verification, function assignment validation and job analysis. Then, the functional design specifications are developed as shown in Figure 2.

From these specifications, the detailed design, operating procedures and training programme are developed. Finally, the resultant system constituents are verified and the integrated control room system validated.

This document focuses on the design process for the control room(s), typically implemented by a design team which comprises a variety of competencies and disciplines. This includes at least the following areas:

- nuclear engineering;
- architectural design and civil engineering;
- systems engineering;
- I&C systems engineering;
- information and computer systems engineering;
- human factors engineering;
- plant operations and maintenance;
- training.

These competencies may be provided by permanent or temporary team members, or even by consultants.

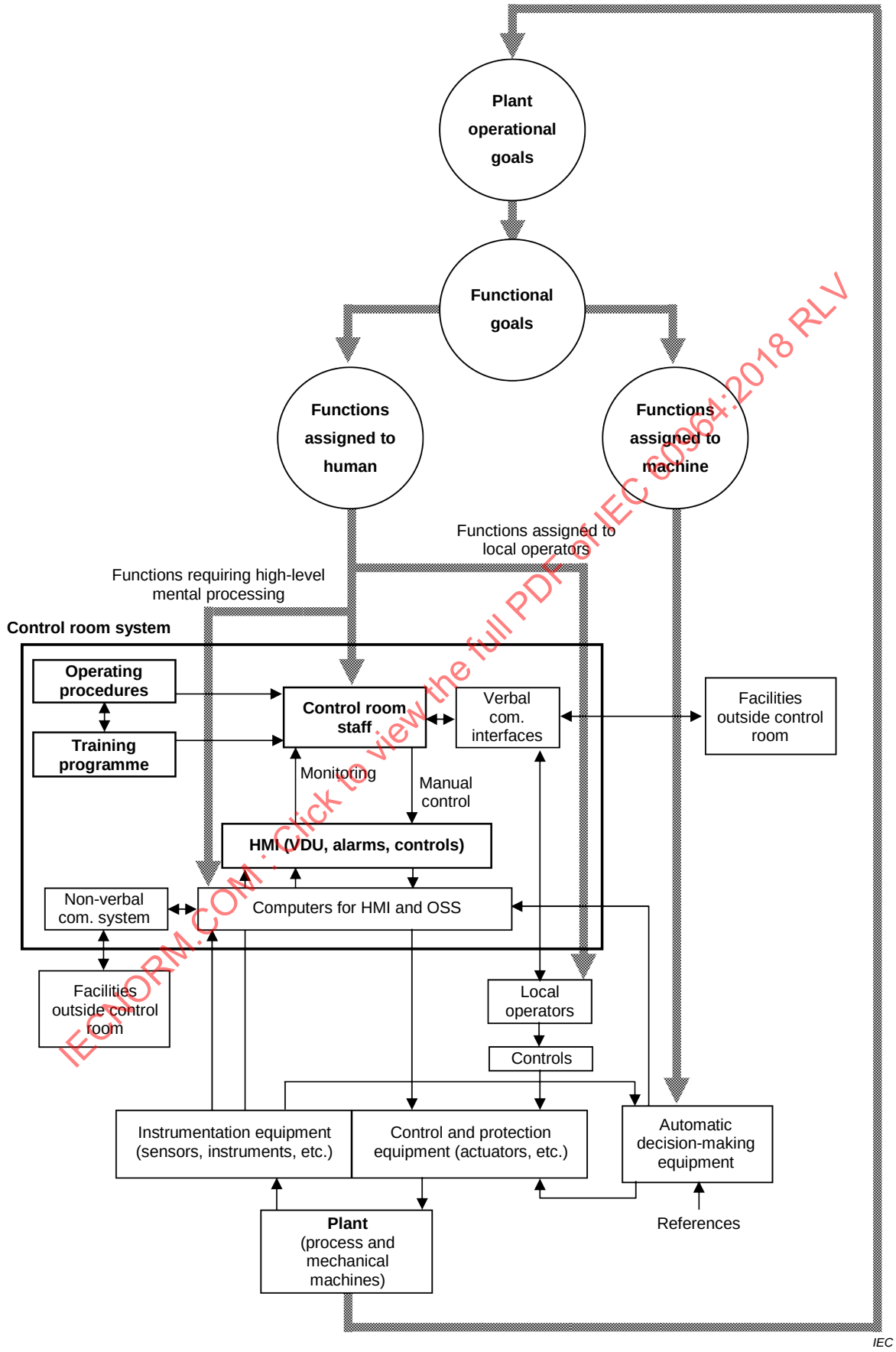


Figure 1 – Overview of control room system

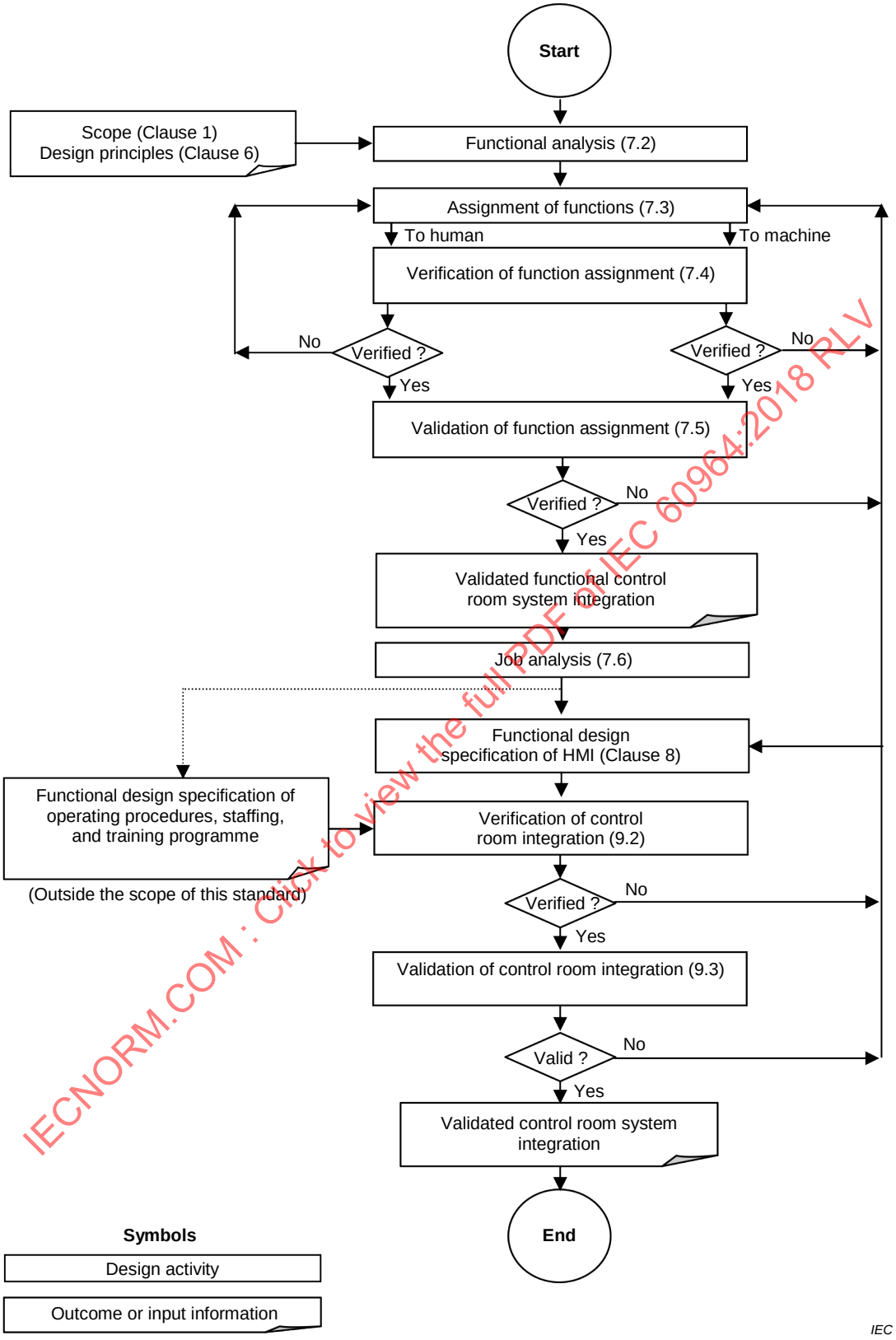


Figure 2 – Overall design process and the relationship to clauses and subclauses of this document

6 Design principles for the main control room

6.1 Main objectives

The nuclear power plant objective is that it can be operated safely and efficiently from the main control room in all plant operational states and accident conditions. The main control room provides the control room staff with the human-machine interface and related information and equipment, e.g. the communication interface, which are necessary for the achievement of the plant operational goals. In addition, it provides an environment under which the control room staff are able to perform their tasks without discomfort, excessive stress, or physical hazard.

6.2 Functional design objectives

The principal objectives of the control room design are to provide the operator with accurate, complete, operationally relevant and timely information regarding the functional status of plant equipment and systems.

The design shall allow for all operational states, including refuelling and accident conditions, optimise the operator tasks and reduce to an appropriate level the workload required to monitor and control the plant safely, and provide necessary information to other facilities outside the control room.

The control room design shall provide an optimal assignment of functions which achieves maximum utilization of operator and system capabilities.

An additional objective of the control room design is to permit station commissioning to take place effectively and to permit modifications and maintenance.

6.3 Safety principles

A control room shall be designed to enable the nuclear power plant to be operated safely in all operational states and to bring it back to a safe state after the onset of accident conditions. Such events shall be considered in the design of the control room.

Provisions for preventive and mitigative accident management shall be made both at monitoring and control level combining control room and manual actions, see IAEA NP-T-3.16.

Equipment controlled from the control room shall be designed, as far as practicable, so that an unsafe manual command cannot be carried out, e.g. by using a logical interlock depending on the plant status.

Account shall also be taken of the need for functional isolation and physical separation where redundant safety systems or safety and non-safety systems are brought into close proximity. IEC 60709 gives requirements for this. Account shall be taken of the need to ensure safety if the control room and its systems are affected by fire, and to reduce the possibility of fire to a practicable minimum, as outlined in IEC 60709.

Appropriate measures shall be taken to safeguard the occupants of the control room against potential hazards such as unauthorized access, undue radiation resulting from an accident condition, toxic gases, and all consequences of fire, which could jeopardize necessary operator actions.

There shall be adequate routes through which the control room staff can leave or reach the control room, or gain access to other control points, under emergency conditions.

6.4 Availability principles

With a view to maximizing the plant capacity factor, consideration shall be given in the control room design to:

– facilitating planned operations for load changing, start-up and shut-down;
– minimizing the occurrence of any undesired power reduction or plant trip caused by operators' erroneous decision-making and actions, or by local disturbances associated with malfunction or failure of I&C systems;
– achieving the design output and performance of the plant.

The availability-related design specifications shall not violate the adopted safety principles.

6.5 Human factors engineering principles

In order to provide an optimal assignment of functions which ensures maximum utilization of the capabilities of human and machine and aims to achieve the maximum plant safety and availability, the design shall pay particular attention to human factors principles and human characteristics of personnel with regard to their anthropometrics, perceptual, cognitive, physiological and motor response capabilities and limitations.

6.6 Utility operating principles

An integral part of the control room and operating philosophy is operator staffing and training. To maximize the safe and efficient operation of the nuclear power plant, the control room shall be manned with a sufficient number of skilled professional staff.

The control room staff shall be technically trained in control room operations and educated in those engineering principles related to nuclear power plant operations and safety, as well as having a thorough knowledge of the plant sub-systems and components, their function, performance and location.

Tasks performed by operators outside the control room that involve operation of plant equipment shall be administratively controlled and monitored from the control room.

To ensure the quality of operation of the nuclear power plant, the station operating authority should consider the following factors in control room staffing:

– personnel selection and qualification requirements;
– initial training and retraining requirements for normal, abnormal and accident conditions;
– periodic retraining of operating skills and opportunities to expand their knowledge in engineering principles;
– job responsibilities for control room staff and individuals during normal and emergency operations;
– personnel physical requirements concerning optical and auditory capacity, any physical impairment and height;
– management and supervision structures and responsibilities;
– shift patterns and job stress.

6.7 Relationship with other control and management centres

To assist the control room personnel in responding to abnormal operating conditions, emergency response facilities shall be available to function during emergency conditions.

Supplementary control rooms (or points) shall be provided, sufficient to ensure safety if the main control room is damaged or becomes inoperable. The requirements for supplementary control rooms (or points) are given in IEC 60965.

Equipment shall be provided for the change-over of the control and monitoring from the main control room to the supplementary control rooms (or points). The equipment shall operate independently of the other equipment in the control room.

6.8 Operational experience

When available, operational experience from existing nuclear power plants should be collected, analysed and fed back to the design of new power plants where applicable. Such experience may recommend use or optimisation of proven solutions or even influence the consideration of principles in domains such as follows:

- staffing;
- operating team organisation and job definition;
- function allocation between main control room and local control stations;
- automation;
- design of information processing, information presentation and controls.

7 Functional design of the main control room

7.1 General

A system based approach to the functional design of a control room shall be used covering the control room and the associated items in Figure 1. This approach shall include the following five steps as shows in Figure 2:

– functional analysis;
– function assignment;
– verification of function assignment;
– validation of function assignment;
– job analysis.

7.2 Functional analysis

7.2.1 General

An analysis of the functions to be performed by the nuclear power plant to achieve the objectives of 6.1 and 6.2 consistent with the principles of 6.3 to 6.8 shall be conducted.

This analysis should identify a hierarchy of goals for the control room design covering all operational states and accident conditions. These goals shall include the production of electricity and the minimization of activity release as principal goals. The goals may be developed further as sub-goals and used in the design decision process.

Refer to IEC 61839 for more detailed descriptions and requirements for the functional analysis process.

7.2.2 Identification of functions

With respect to hierarchical goal structures, all plant functions associated with the goals of the control room should be identified and documented. A means for identifying these goals is given in IEC 61839. In defining functions the analysis shall take into account the interactions between the control room and facilities and systems outside the control room.

7.2.3 Information flow and processing requirements

Analysis shall be performed to determine the basic operational information flow and processing required to accomplish the plant functions including decision making and operations. This analysis is described in IEC 61839.

When identifying the information flow and processing requirements, the designer should use several representative plant operational states (normal and anticipated operational occurrences) and accident conditions (design basis and design extension conditions).

The following events should be included;

– events requiring operations subjectively judged to be difficult in terms of complexity of data interpretation or control, control speed, etc.;
– events requiring the highest certainty of correct operator response, e.g. certain accident conditions;
– events important in terms of the probabilistic safety assessment;
– events in which plant trip is highly probable unless corrective action is taken in time;
– events whose occurrence rates are high;
– events which test out team-working.

The number of events to be included shall be large enough to cover adequately the functions associated with the hierarchical goal structure.

7.3 Assignment of functions

7.3.1 General

Functional analysis provides the required input to the assignment of functions process which shall be conducted to determine which functions should be assigned to the human and which functions should be assigned to the machine. Function analysis and assignment defines the operator tasks with their characteristics in a first level of detail and is the input to the task analysis.

Human factors engineering principles and design criteria shall be applied in this analysis (see ISO 11064).

Functions assigned to humans shown in Table A.1 in Annex A are:

– manual control (including backup control to automation);
– monitoring associated with both manual control and automatic control;
– high-level mental processing tasks such as diagnosis to determine the cause of abnormal and unforeseen operating conditions and events and to determine corrective actions.

Functions assigned to the machine refer to those which are achieved by automatic control as shown in Table A.1. In the case of assigning important safety functions to machine, consideration shall be given to also:

a) assign the monitoring of automatic systems to humans (to supervise correct operation and intervene in case of malfunctions);
b) provide feedback reflecting automatic actions;
c) enable human intervention in case of failures.

The principles and criteria used in the analysis shall be documented and shall include factors which deal with the capabilities and limitations of both the control room staff and the automatic control system.

Refer to IEC 61839 for more detailed requirements concerning the assignment of functions process.

7.3.2 Operator capabilities

The functions assigned to the operator should distinguish between those situations where he or she is:

– actually performing a control function,

– supervising an automatic system that is performing the control function, and

– performing high level mental processing tasks such as diagnosis.

This analysis should result in the information needed for the conceptual design of the information system and the functional organization of resources/means to perform each of the above functions.

For potential operator functions, estimates of processing capability required in terms of workload, accuracy, rate and time factors shall be prepared for each information processing aspect and control action. These estimates shall be used for the initial assignment of functions. The estimates should be modified based on verification results and used to reconsider the assignment of the function as well as to provide a more detailed definition of the required operator capabilities.

These requirements together with those for display, control and communication shall be consistent with the operator tasks which shall be performed to accomplish the function. The general operator tasks definitions should include information, control and communication requirements .

The various types of data available to the operator should be grouped based upon the tasks and not on the sources of data. The purpose of grouping is to provide within the operator capabilities, a system using comprehensive information from various sources with respect to each task (see 7.6).

7.3.3 I&C system processing capabilities

Analysis of instrument and control system processing shall begin with a definition of system and equipment functional requirements and constraints, followed by a more detailed description of operational event sequences and human-machine interface requirements for each task. The purpose is to organize the machine information and capabilities with respect to the tasks defined for operator interaction. This organization will facilitate the assessment of the capabilities of both automatic controls and human control for each decision-making and control task.

Processing capabilities of the I&C system should ultimately include aspects such as quantity, response time, accuracy and human-machine interfaces requirements coherent with human factors engineering considerations.

To reduce the probability of operator error, the control systems should be designed to keep the plant within safe limits without any operator action during a specified period of time after initiation of certain abnormal conditions of the plant. This period of time shall be reflected in the functional requirements for the automatic control systems. The degree to which the operator needs to be informed about these automated actions should be considered to maintain situational awareness.

7.4 Verification of function assignment

7.4.1 General

An acceptable assignment of control room functions to human and machine shall be verified as shown in Figure 2. Evidence shall be presented that the proposed function assignment takes the maximum advantage of the capabilities of human and machine without imposing unfavourable requirements on either of them.

Refer to IEC 61771 for more detailed requirements for the verification of function assignment.

7.4.2 Process

The process developed for the verification shall include preparation, evaluation and resolution phases.

Before attempting to verify the proposed function assignment, the criteria used for the assignment shall be confirmed to be self-consistent.

The verifications shall subsequently confirm that:

– all the functions necessary for the achievement of the plant operational and safety goals are identified;
– the proposed function assignment is in accordance with criteria established for the assignment;
– sufficient requirements of each function are identified. These requirements include performance aspects (e.g. time constants, accuracy), those derived from safety principles, availability principles and station operating authority principles specified in this document, and those derived from other standards, regulations and guidelines;
– requirements from higher level functional goals merge at a lower functional level without conflict under all operational modes.

Modification (i.e. correction of mistakes or reassignment) and verification shall be made iteratively until all these criteria are satisfied.

7.5 Validation of function assignment

7.5.1 General

The proposed function assignment shall be validated to demonstrate that the system would achieve all the functional goals. In particular, the performance of the identified functions of 7.2 shall be evaluated under all the normal operations and several representative events including abnormal operation and accident conditions.

Refer to IEC 61771 for more detailed requirements for the validation of function assignment.

7.5.2 Process

The process developed for the validation shall include preparation, evaluation and resolution phases.

Selection criteria shall be developed to ensure that the events to be chosen for assessment are representative. In addition to all normal operations and events specified in 7.2.3, events caused by multiple failures should be considered for the assessment of functions assigned to humans.

After the completion of the selection of representative events, functions required in each event shall be identified and synthesized in time-sequential order.

7.5.3 General evaluation criteria for validation

The performance of functions shall be evaluated for all normal operations and the representative events. The general validation criteria shall be satisfied including the following:

– the number of functional goals and the work load rate required of the control room staff shall not exceed their capability;
– the assignment of functions to the control room staff and local operators is acceptable;
– the assignment of functions to automation is satisfactory and feasible.

7.6 Job analysis

In order to develop basic requirements for the control room staff structure, the operating procedures and the training programme, the designer should conduct a job analysis of the verified or validated function assignment and functional requirements.

The first step of the job analysis is to identify the characteristics and the number of tasks assigned to humans. Based on that, the designer can then define the organization and the number of operators, within the framework of the control room staff structure required by regulation and the utility normal practice.

Tasks assigned to an operator should not overload him or her and should be consistent with his or her responsibilities as defined by the control room staff structure. Furthermore, the designer should identify communications among operators and communications between control room operators that are necessary for the achievement of tasks.

The designer should also identify non-operational activities (e.g. reporting to authorities) inherent in some tasks by referring to appropriate documents.

When completed, the analysis should clarify:

– organisation and number of operators;
– operator competence required;
– operational responsibilities of operators;
– administrative duties of operators (e.g. reporting);
– operational interactions between operators;
– dialogues between operators and plant;
– communications between operators and plant personnel stationed outside the control room facilities;
– communication with management and supervisory staff.

Together with the results of the analysis for the function assignment (e.g. conceptual information structure), the items above should form the basis of the control room staff structure, the operating procedures and the training programme.

8 Functional design specification

8.1 General

This clause aims to specify the functional design requirements for the control room system and equipment that perform the assigned monitoring and control functions. It also specifies the interface between the human and the control room equipment.

The design shall be based on an integrated human-machine systems engineering approach.

8.2 Provision of data base on human capabilities and characteristics

When detailed design of a control room is carried out, a data base on human capabilities and characteristics shall be provided as fundamental human factors design data.

The data base shall include:

– anthropometric considerations;
– population stereotypes;
– auditory and visual capabilities and characteristics;
– human ability to process information;
– environmental factors.

As some of these data depend on the custom of the country, the data base may be specific to each country or each utility.

8.3 Location, environment and protection

8.3.1 Location

The control room shall be located for convenient plant operation and should meet the safety principles of 6.3.

8.3.2 Environment

Environmental conditions in the main control room shall be such that the operators can perform their tasks effectively and comfortably.

The environmental design of the control room shall include requirements for air conditioning, illumination and the auditory environment. The following requirements apply:

a) Air conditioning

The main control room shall be air conditioned. The air conditioning shall include measures to cope with accident conditions of the plant, e.g. by using filters or isolation capability.

b) Illumination

Design of the lighting system shall ensure task-adequate lighting, avoidance of glare, reflections and shadows. The design shall address adequate emergency power supply of the lighting.

c) Auditory environment

Design of the auditory environment shall ensure easy communication within the operating team, minimal disturbance by ambient noise, and reliable perception of acoustic messages, alarms and emergency signals.

Guidance for environmental specifications under normal conditions is provided in ISO 11064.

It may be convenient to include within this specification the requirements for size and shape of the control room with provisional layouts, cable access arrangements, seismic requirements, room and panel colour and other finish details, for agreement with civil engineering interests and later confirmation in detail.

Appropriate measures shall be taken in the design to maintain control room operability and the monitoring and control of the plant even during accident conditions. Requirements for the condition and duration for which the MCR environment has to be maintained under such conditions shall be defined. Procedures shall be established to operate features and systems installed to achieve the required duration.

8.3.3 Protection

The design of the control room shall provide, within the design basis, protection against fire, radiation, internal and external missiles, earthquake and hostile acts. The equipment shall be qualified in accordance with the design basis. For all items of equipment required to operate under design extension conditions, demonstrable evidence shall be provided that it is able to perform its function(s) under the applicable service conditions, see IEC/IEEE 60780-323.

The design shall ensure that such events cannot simultaneously jeopardize the main control room and the supplementary control points, mentioned in 6.7.

More specifically:

a) Fire protection

Attention should be given to using non-flammable materials only. The control room area shall be equipped with a fire detection and fire-fighting system.

Electrical equipment in the control room shall be designed to neither cause nor support a fire as far as this is reasonably achievable.

Cable circuits and switchgear associated with the control room shall be protected against the consequences of fire. Cable insulation and sheathing materials should be fire-retardant and meet national test criteria for flame propagation, release of combustion products and materials where applicable.

b) Radiation protection

The control room staff should be protected against direct radiation in any accident situation. The air intake ducts shall be equipped with a radioactivity monitoring system. If circumstances require, the control room ventilation system shall have the capability to isolate itself. Breathing apparatus shall be available to the staff.

c) Missile protection

The control room design shall include assessment and protection against missiles originating from inside and outside the control room. Guidance on the protection from missiles is given in the IAEA Safety Guide NS-G-1.11.

d) Earthquake protection

The control room equipment related to safety functions, the air-conditioning system and safety illumination system (i.e. the lighting designed to function post seismic event) shall be designed on the same seismic basis. Detailed requirement are provided in IEC 60980.

e) Hostile acts

Measures should be taken to restrict access to the control room and to protect it against hostile acts.

The security plan shall conform to the requirements of the regulations in each country. The security plan shall include the MCR assets subject to computer security protective measures including computer systems, computer system applications and network connections, see IEC 62645.

8.4 Space and configuration

8.4.1 Space

The control room shall have sufficient space to allow the control room staff to perform all necessary actions, while minimizing the need for operator movement in abnormal conditions.

Special attention should be paid to providing work areas, writing space and storage space for documents:

– Work areas which are manned on a continuous basis shall be designed for seated operation and adequate seating shall be provided, but should also permit operation whilst standing.

– Where writing and access to documentation form a normal part of the control room duties, adequate writing space shall be made available.
– Storage space for documents shall also be provided close to the operating position to avoid the documents being laid on consoles, desks, etc.
– Some space may be provided for extensions that might be required in the future (during design phases or during the main control room life time).

8.4.2 Configuration

The control room shall be designed giving due consideration to:

– station operating authority's operating principles;
– assignments of functions to the operators and I&C system;
– centralized or local control philosophy, which determines the extent of controls present in the control room;
– supervision criteria, which determine the use of overview displays, the number of VDUs, indicating instruments, recorders, alarms and indicating lights on the panels;
– technology choices (the degree of use of dedicated hard-wired controls and indications compared to the degree of soft control and VDUs including large screen displays, segregation between the different divisions, use of automatic control sequences, extent of automation and/or multiplexed controls);
– station operating authority and legal requirements, such as the number of operators in the control room required by operating policies or licensing authorities;
– installation of non-operational systems, such as fire alarm and fighting systems, and other site-related functions;
– space for administrative functions.

The control room shall have such operating areas as are necessary, where each operator can obtain access to all controls and information required to perform the tasks assigned to him in all operational and accident conditions.

The operating area and control room equipment such as control desks, boards and panels shall be arranged according to human factors engineering principles. The layout should be such that each operator is provided with easy access and good visibility of the control room equipment related to their responsibilities and such that each operator can see directly and speak with other operators normally present without undue interruption of the line of sight between them.

Refer to ISO 11064 for more detailed requirements.

Information displays and control elements shall be arranged according to consistent principles which should be well documented in the design process.

The arrangement shall be structured, especially in the case of control rooms based on the extensive use of dedicated controls and indicators, to simplify the system or component identification in normal operation, accident conditions and emergency situations, and minimize the probability of incorrect actuations arising from human error.

The above criteria may be used in combination with other design elements and the resulting rules shall be consistent for all operating areas.

8.5 Panel layout

8.5.1 Priority

Principles shall be established and applied for the layout and arrangement of alarms, displays and controls belonging to a function of a system as well as for priority rankings between

similar elements in the layout of the panels. The priority ranking rules derived from these principles shall be consistent for all panels in the plant.

8.5.2 Positioning on control desks and panels

The positioning of displays, indicators and controls on the panels and desks shall be based on the following criteria:

– alarm panels and fascias shall be visible from the operating area of the control room and shall be at a convenient height for operator visibility and legibility;

– frequently used controls shall be within convenient reach and the related indicators and displays shall be readable from the operating position.

Refer to ISO 11064 for more detailed requirements.

8.5.3 Mirror image layout

Mirror image layout of panels, controls and indicators shall be avoided in order to prevent left-right confusion.

8.6 Location aids

8.6.1 Grouping of display information and controls

It is essential that the displayed information and controls are logically grouped.

The following techniques may be used for grouping displayed information and controls :

a) Grouping by function

Information and controls should be grouped in relation to function or interrelationships within a system. Care shall be taken to identify the function in terms of the role that the information plays in achieving system objectives rather than of the source of information or method of measurement.

b) Grouping by sequence of use

Information and controls may be grouped on a sequential basis either by considering the display as a whole or by dividing the display into parts, each of which is organized on a sequential basis. Cause/ effect relationships should be reflected in the display.

Use should be made of natural groupings which conform to user population stereotype expectations (e.g. 1, 2, 3 – a, b, c, etc.). For the same reasons, the display should be organized in a corresponding manner, e.g. from left to right and from top to bottom.

c) Grouping by frequency of use

In this form of grouping, information which is most often used is collected together with the most used, say, at the top of the display and the least used at the bottom, and the controls most used nearest to the operator.

The most common method of establishing frequency of use is link-analysis in order to determine the connections between various items of information or controls and procedures.

This type of grouping is of limited application due to the risk of apparent illogicality in the display.

d) Grouping by priority

Here the information or controls are grouped by significance to the correct functioning of the system. Highest priority items should be placed in prime positions within a group.

e) Grouping by operating procedures

Information displays and controls should be grouped according to the operating procedures. The special equipment of displays and controls to be used in emergency conditions should be grouped separately from that used for normal operation.

f) Grouping by system with mimic arrangement

If mimics are used, care shall be taken to avoid conflicts with other criteria used, and to maintain the same mimic philosophy if alterations or additions to the process or to the instrumentation and controls will be required in the future.

Appropriate techniques should be selected and combined by balancing their respective properties. Each group shall be of a manageable size to allow rapid and accurate searching. Care should be taken to respect human performance constraints.

The grouping should be consistent with the assumption about the user's mental model of the plant.

Particular care shall be taken to avoid conflicts of grouping, especially when different grouping techniques are used simultaneously.

8.6.2 Nomenclature

The names and identities of each plant item, allowing for the many redundant items on a nuclear plant, shall be carefully considered and agreed on a project-wide basis for uniform use.

Specific abbreviations and acronyms (such as CVCS for chemical and volume control system) should be agreed and used consistently. A human factors review of these plant identifications may be advantageous.

8.6.3 Coding

Coding of controls and of information displayed can be used to distinguish between different types of control or classes of information, such as to distinguish between:

a) safety functions,

b) other functions important to safety, and

c) functions not important to safety.

Coding principles shall be established in an early stage of control room design and they should be consistent with national requirements and utility practices.

The coding system shall be consistent throughout the control room. Location, information, colour and illumination codes applied to displays and their associated controls shall be applied in a consistent way.

The coding method for an actual application shall be determined considering the relative advantages of the types of coding:

– physical coding (size coding, shape coding, colour coding, auditory coding, and intensity coding),

– information coding,

– location coding.

Refer to ISO 11064 for more detailed requirements.

Due to potential staff considerations (persons with colour deficient vision) and equipment considerations (fading-out of colours, partial failure of I&C equipment), colour shall not be the sole means of discrimination for information important to safety. The sole use of colour for coding should also be avoided in other areas.

8.6.4 Labelling

Adequate labelling shall be provided in the control room. The labelling shall be consistent with other labelling in the plant and in accordance with national requirements and utility practices. Refer to ISO 11064 for more detailed requirements.

The language and script used for all control room labels and identifiers, and for all displays, shall be uniform throughout the control room and should be that of the dominant language of the population in whose area the plant is located, except for technology reasons.

8.7 Information and control systems

8.7.1 General

Following the design process and requirements of IEC 61513 for the overall I&C architecture, there will be information and control systems implementing the human-machine interface in the main control room for plant monitoring and control.

The system architecture will depend on:

– safety classification;
– failure criteria;
– defence-in-depth strategy;
– qualification and reliability considerations;
– maintainability considerations;
– security considerations;
– choices imposed by the available technology.

The information and control systems will be implemented by one or several subsystems dealing with the various aspects of the human-machine interface and operator support functions. This typically includes computer-based systems with VDU-displays and soft-controls as well as dedicated indicators and controls. The requirements are summarized below.

8.7.2 Information functions

8.7.2.1 General

An information system shall be provided to inform operators of the plant status and variables important to safety and availability, which allows the control room operators to obtain a complete understanding of the plant state at all times. Particular consideration of the capability and reliability of their power supply and service systems shall be made for a subset of important plant parameters related to plant safety (see 8.10.1) and environment monitoring.

Sufficient information shall be available to allow the operating staff to achieve safe shut-down and hold-down for an indefinite period in accordance with regulatory requirements.

The system shall also provide information of the plant status to technical experts and to on-site and off-site safety experts during accident conditions.

The system shall have data acquisition, display and alarm functions. The system shall also have recording and memory functions for the plant process variables important to safety and availability, for analysis and for reporting within the operating organization and external authorities.

Information processing functions should also be provided to support high-level mental processing by the operators as a means of:

– aiding decision making;
– improving monitoring performance and capability.

This should be achieved by:

– ensuring high availability and reliability of information;
– providing information useful for formulating actions;
– facilitating good communication between control room staff;
– providing a record of transients and accidents for analysis purposes including access to recorded data;
– recording operator control actions where this is practicable;
– expanding available information to cover implicit data.

Categorisation of the information system functions shall be made in accordance with IEC 61226.

Specific requirements are as follows:

a) Information for operators

The operator shall be able to obtain at any time a complete understanding of the plant from the information systems. These shall enable the operators to:

– recognize any current or potential safety or availability hazards;
– know the actions being taken by automation systems;
– analyse the cause of any disturbance and follow its course;
– perform any necessary manual counteractions.

The design basis for information systems, including their measurement devices, shall take into account their importance to safety. The intended safety function of each system and its importance in enabling the operators to take proper pertinent actions in anticipated operational occurrences or accident conditions shall be identified in its design basis and shall be used as an input to any I&C categorization method selected.

Accident monitoring systems for Design Basis Accidents and Design Extension Conditions shall provide operators with the information that they need to develop an integrated understanding of the status of the reactor, containment and SFP in a manner that allows for the greatest understanding of the nature of the accident, the status of the integrity of the barriers to fission product release, and the potential magnitude and pathways for such a release.

b) Information function for non-shift experts

Although the control room is the information and control centre of the plant for the operators during both normal operation and accident conditions, it may also be used as the primary centre to direct the initial stages of off-site activities depending on national and utility principles for emergency operations support. See also IAEA Safety Guide NS-G-1.9.

It is preferable to accommodate visiting experts in a separate room and exclude them from the control room.

Information systems may be extended to supply information to separate outside support facilities.

c) Recording and printing

An adequate number of recorders or printers shall be provided in or adjacent to the main control room for analogue process variables and for binary signals in order to obtain chronological information about the performance and behaviour of the plant.

This is necessary for the following purposes:

– back-up information for shift operators giving short-term and long-term trends;

– general operational information for the plant management;

– short-term and long-term analyses of operation and accidents.

Consideration should be given to automatic recording of operation of the controls to allow analysis of operator actions.

8.7.2.2 Data acquisition and processing

The major functional requirements for data acquisition and processing are as follows:

– faults shall not cause any unsafe state or unacceptable economic losses in the plant operation;

– input data sampling, pre-processing and analysis rates shall be appropriate to satisfy operational requirements related to the parameter rates of change;

– data shall be updated at rates appropriate to operator tasks;

– there shall be no significant delays in processing plant data or operator requests even at times of peak loading;

– modification shall be possible throughout the operational life;

– a provision shall be made to allow the operators to easily identify invalid displayed information.

Further requirements are as follows:

The data acquisition and processing system should take into account all aspects of operability and reliability requirements, future plant modifications and maintainability.

This requires that an essential part of identifying and defining the data acquisition and processing system involves a comprehensive analysis (e.g., task analysis) which takes the performance of the control room staff into consideration. Such analysis will be able to identify data requirements including the necessary data availability and correctness.

The data acquisition and processing system shall be fully defined regarding:

– the frequency of data sampling and redundancy;

– pre-processing and consistency checking;

– the analysis required for off-normal conditions;

– the output required and the form of output, e.g., print or electronic.

Raw data processing may consume a significant proportion of CPU time for a single computer based system. Similarly, further data processing and display may consume computer time. An assessment should be done to determine the computer loading in normal and in peak loading conditions, before the system is put into service. This assessment should be confirmed by suitable tests on the fully installed system to demonstrate the viability of the system to the operating staff for the expected range of operating conditions. There shall be no significant delay in processing and presenting plant data or operator requests even at times of peak loading. Experience indicates that operators become impatient if there are delays to any function of a computer-based information system greater than about 1 s. A feedback cue should be implemented if longer response times cannot be avoided, e.g. in case of accessing historical data or archive data.

Although some systems may use only a single computer to process the data and to provide information, redundancy of computers and of modules should be included to ensure service continues when any more frequent single fault occurs.

8.7.2.3 Display system

The display system shall be designed as a human-machine interface of the information system, considering human capabilities and characteristics.

The displays shall enable the operators to:

– know the actions being taken by the reactor protection system and other automatic systems, so as to be able to verify their state and perform necessary support actions;
– analyse the cause of disturbances and follow their course;
– perform any necessary manual counteractions.

The display shall enable the operators to recognize potential safety or availability hazards.

The major functional requirements of the display system are as follows:

– the display system in the control room shall cover appropriate variables, consistent with the assumptions of the safety analysis and with the information needs of the operator in normal operation and accident conditions;
– the accuracy, range, and scales of displays shall be consistent with the assumptions of the safety analysis and the supported operator tasks;
– displays shall be provided for indicating by-passed or deliberately inoperable conditions of the plant and auxiliaries;
– information displays important to safety shall be suitably located and specifically identified on control panels;
– the types of displays shall be selected in accordance with their purpose;
– the display system shall provide both information and alarm displays, which should provide an integrated approach to the display of plant conditions.

In general, VDU-based displays and information means will be used. Dedicated displays like analogue meters, digital indicators, lamps and trend recorders may be required e.g.

– for post-accident situations, due to qualification or diversity considerations, or
– if requirements for spatially dedicated display have to be fulfilled.

An adequate number of printers should be identified in order to provide hardcopies for the shift team, as material for team discussion and analysis and possibly legal documentation purposes.

Detailed guidance for VDU-displays is provided in IEC 61772; guidance for dedicated displays can be found in ISO 11064.

8.7.2.4 Alarms

Main control room alarms shall provide all information necessary for plant surveillance in abnormal plant conditions.

The alarm system should:

– display alarm information to enable the operator to understand the fault situation as it develops;
– enable the operator to remove irrelevant information but ensure that relevant and important information is presented in a manner matching the operator's capacity to understand;
– enable the operator to distinguish between alarms for which corrective actions are not complete and alarms which cannot be cancelled without the intervention of the maintenance service;
– avoid information overload.

The alarm system should have:

– processing functions, to give the operator the most representative information of abnormal conditions, and

– display functions, to permit the operator to easily identify an alarm and its seriousness.

Moreover, for each alarm, a procedure document, e.g. alarm sheet or plant item operating instruction, shall be provided to explain to the operator the likely reasons for the alarm and the corrective actions required.

Refer to IEC 62241 for more detailed requirements.

8.7.2.5 Operator support function

In order to enhance plant safety, availability and operability, operator support functions such as the following should be provided:

– safety parameter displays and surveillance functions (see IEC 60960);

– plant diagnosis functions;

– operator guide functions for normal operation and post-accident situations, e.g. symptom- and event based procedures. See also 62646 for computer based procedures requirements;

– functions for automatic on-power test.

So far as practicable such functions should be fully integrated into the overall design of the control room.

8.7.3 Control functions

This subclause deals with functional human factors specifications of controls used for manual control operations as well as for back-up to automatic control operations under both normal and abnormal operations. However, functional specifications of control functions as embodied by plant I&C systems, are outside the scope of this document.

a) General considerations

Controls shall be designed to ensure ease of operation and to minimize operator errors.

The controls selected shall be suitable for operator use in a control room environment and shall match the characteristics of the expected user population.

Controls shall meet the following requirements:

– to minimize operator error, control movements should conform to population stereotypes and should be compatible with the controlled variable;

– controls shall integrate feedback information for the selected function and integrate display of check-back information of the state of the controlled components;

– categorisation of control functions shall be commensurate with their importance to safety, in accordance with IEC 61226.

b) Prevention of erroneous actuation

To prevent human-induced events, erroneous activation of controls shall be minimized by means such as the following:

– locating controls at proper positions, thus avoiding accidental actuation in a control movement;

– use of protective structures, such as use of physical barriers, or recessed installation, movable covers or guards;

– provision of a second confirmatory action, e.g. with a release push button or with an additional soft control command;

– use of interlocks or permissive signals, with proper assignment of priorities;

- proper selection of physical characteristics, such as size, operating pressure or force, tactile, optical and/or acoustical feedback;
- any combination of the above.

c) Technology

Controls may be implemented as soft controls, multiplexed or dedicated controls and mixtures thereof.

The choice should be taken based on criteria such as follows:

- qualification and independence considerations;
- required speed of access and frequency of use;
- available technology.

IEC 61227 provides detailed guidance on this.

8.8 Control-display integration

Controls and their associated displays shall be correctly integrated to ensure effective operation of the plant by control room staff.

The control-display integration shall be in accordance with the proposed method of plant operation as shown in the analyses made according to 6.2 and 6.6.

The control-display integration shall meet the following principal requirements:

- controls should be located near the associated display. Operation of controls should produce a compatible change in the relevant display;
- the grouping of controls and their associated displays shall reflect the need to achieve system objectives and should be consistent with assumptions about the user's mental model of the plant;
- the organization of controls and displays shall reflect cause/effect relationships;
- the organization of controls shall embody user population stereotypes;
- the form of codes used for displays and their associated controls shall be entirely consistent.

8.9 Communication systems

8.9.1 General

Communication systems shall be provided in the control room to facilitate safe and efficient plant operation. Special consideration shall be given to the design of communication systems to be used to communicate with the emergency facilities in the abnormal or accident conditions.

Provision of non-verbal communication systems such as telefacsimile and data-links (between computers) are desirable, between the control room and other information centers in order to improve plant availability and safety. Considerations should be given to security when defining these communications systems, see IEC 62645 and IEC 62859 for requirements.

8.9.2 Verbal communication systems

8.9.2.1 On-site communications

For general communication under normal operational conditions a telephone system with an adequate number of extensions shall be installed. At least one of the extensions shall be located in the control room. Each extension may be connected to the public telephone system. An additional specific system shall be provided in the control room, which is not accessible from the public system and has a dedicated well known emergency call number

which is labelled to all other extensions. This extension shall be used for transmitting only disturbance and accident reports to the control room personnel.

For communication in accident conditions to supplementary operating facilities and control points which are important to safety, a separate directly wired system shall be installed where appropriate. The system shall enable the control room personnel to communicate singly or in parallel with a selected number of extensions at the same time. The system shall also enable the control room personnel to communicate with the control room of any other unit with a separate control room at the same site. The system shall be supplied by a non-interruptible power supply system. Extension telephone jacks outside the control room shall be provided where necessary and be accessible also under accident conditions. The system may be extended also for operational use.

A public address system shall be provided to broadcast messages to on-site personnel under any plant conditions.

For use during maintenance, testing or repair, communication by radio to the control room using mobile transmitters shall be provided, unless all relevant local points can be reached reliably enough by other systems. Radio frequency interference aspects (see IEC 62003) shall be considered in the design, cabling, location and testing of I&C systems. To minimize such interference, the frequency range and the maximum output power of these transmitters shall be limited and specified. Areas where transmitters may not be used, such as the control equipment room, shall be identified.

8.9.2.2 Off-site communications

For communication to the off-site station operating authority, emergency response facilities, governmental and public institutions, an exclusive communication system should be provided. Some of the extensions call numbers, especially one in the control room, shall not be known to the public.

The minimum connections to off-site shall be provided with necessary organizations and personnel. Important connections shall have redundant and diverse systems, e.g. one telephone and one radio system. The connections shall be defined in accordance with national requirements, with typical connections such as follows:

– to stand-by/ready-for-call personnel of the unit staff or other experts to help in emergency or accident conditions;
– to radiation measurement groups which perform tasks outside the site important to safety;
– to the relevant fire fighting station;
– to the local police station which is permanently manned;
– to the offices of the government and public agencies.

8.9.2.3 Arrangement

Communication equipment for operational communication duties and communication duties of the operators shall be installed in the operators' work stations.

The main control room shall also be designed as the communication centre of the plant for normal operation and during the early stages of an accident. Responsibilities and need for communication in these phases shall be identified in a task analysis, and the communication equipment located accordingly. Preferably most of the equipment for communicating with off-site locations should be located on a special communication desk or panel with extensions on the main control desk and the control panels.

8.9.3 Non-verbal communication systems

Non-verbal communication systems may be provided in the main control room such as follows:

– a television system for monitoring the reactor operating floor and turbogenerator status which may also be used for accident situations;

– a telefacsimile system that should be connected to emergency response facilities in order to transfer plant status and operational suggestions if an emergency condition occurs.

8.10 Other requirements

8.10.1 Power supplies

The power supply arrangement for the control room shall have a reliability and availability consistent with those requirements of the I&C system, the safety system and the system important to safety. Systems important to safety in the control room, which are required to be available for use at all times during operation or accident conditions, shall be connected to non-interruptible power supplies.

Refer to IEC 61225 for more detailed requirements.

8.10.2 Qualification

A qualification programme consistent with that of overall plant equipment shall be provided to confirm that equipment important to safety and systems in the control room are capable of meeting, on a continuing basis, the design basis performance requirements (e.g. range, accuracy, response) needed for their functions under the environmental conditions likely to prevail at the time these will be needed. The programme shall include a plan to ensure that the equipment is qualified for the intended period of use, and provide for timely requalification or replacement, if necessary.

Refer to IEC/IEEE 60780-323 and IEC 60980 for more detailed requirements.

8.10.3 Maintainability

The equipment shall be designed to facilitate surveillance and maintenance and, in the case of failure, easy diagnosis and repair or replacement.

The contribution of repair time to equipment unavailability shall be evaluated at the design stage. The mean time to repair and the frequency of inspection shall be specified in the design base of each particular system. Knowledge of the means of detecting that a failure has occurred, e.g. a power supply system check (test), shall be a part of this evaluation.

Means provided for the maintenance of the systems shall be designed so that any effect on the safety of the plant is acceptable.

8.10.4 Repairs

The control room shall be designed, considering panel layout and equipment configuration, to ease repair of the equipment and systems in it. The design shall also include the consideration of repair facilities and spare parts.

8.10.5 Testability

The control room shall be designed to permit test and calibration, without difficulty, at necessary intervals for each of the necessary functions. See IEC 60671 for testability requirements

9 Verification and validation of the integrated control room system

9.1 General

Upon completion of the initial conceptual design of an integrated control room system including the arrangements for control room staffing, the human-machine interface, the operating procedures and the training programme, its adequacy shall be verified and validated. In subsequent subclauses, the process and general evaluation criteria of verification and validation are specified for the human-machine interface. For other control room system constituents, i.e. the control room staff structure, the operating procedures and the training programme, the evaluation process and criteria should be developed separately using appropriate national standards, and internationally agreed guidelines available (see IAEA Safety Guides).

See IEC 61771 for more detailed requirements.

9.2 Control room system verification

9.2.1 General

Prior to and during detailed control room system integration, functional specifications of the control room system shall be verified to show that the specifications meet relevant criteria and functional requirements.

9.2.2 Process

The process developed for the verification shall include preparation, evaluation and resolution phases. Evaluation of the integrated control system shall be made at this stage including the operating procedures and the training programme which have been provided separately as shown in Figure 2.

9.2.3 General evaluation criteria for integrated system verification

The proposed control room system integration shall incorporate all the functional specifications and all other technical requirements correctly. See IEC 62646 for computer based procedures systems requirements, if applicable.

9.3 Control room system validation

9.3.1 General

Prior to and during detailed control room system design, the overall control room system integration shall be validated to show that it would achieve the performance intended. In particular, special attention shall be given to time dependent dynamic characteristics of the proposed integrated system.

9.3.2 Process

The process developed for the validation shall include preparation, evaluation and resolution phases.

Preparation for validation is made in a similar manner to the validation of function assignment (see 6.5), but operational expertise is particularly important at this stage.

An appropriate control room model which allows the evaluation of the time dependent dynamic characteristics of the proposed system should be developed. For a system whose concept is considerably different from conventional systems, a dynamic simulator is necessary for use for the validation. However, other choices such as a full scale mock-up may be adopted when either the difference is minor or a partial validation can be justified.

Multiple performance measures should be developed to allow redundant evaluation. Both qualitative and quantitative consistency of interrelated performance measures shall be examined to confirm the evaluation results.

Considerations should be given to creating a realistic test environment (e.g., physical arrangement, environmental conditions such as temperature, humidity, lighting, sound, etc.).

The validation programme should be organized in such a way that it makes use of commissioning tests. For example, commissioning tests should be used for aspects that could not be tested in the previous design phases such as evacuation of the main control room and for aspects that were identified as requiring further evaluation.

The evaluation criteria shall be consistent with all the relevant regulations, standards, guidelines, etc.

9.3.3 General evaluation criteria for integrated system validation

See IEC 61771 for requirements.

Annex A
(informative)

Explanation of concepts

A.1 Control room system

The control room system is an integration of the human-machine interface, control room staff, operating procedures, training programme, and associated equipment and facilities (see Figure 1).

There are two major plant operational goals (i.e. controlled generation of electricity and prevention of release of radioactivity to the environment). A number of functional goals have to be satisfied to achieve the plant operational goals. They are satisfied by controlling plant processes through controlled utilization of plant resources. There are essentially two ways of controlling the plant systems (i.e. automatic control and manual control including remote and local manual control).

Hardware systems implementing automatic control and remote manual control include control and safety systems, which are a part of the I&C system, and they include actuators, sensors, and other hardware devices.

Operation of automatic control requires the control room staff to monitor its action through displays, and to take manual control, which includes back-up control, reset and others. Operation of remote manual control requires the intervention of the control room staff through controls and displays located in the main control room.

The controls and displays, which are also a part of the I&C system, have a physical interface with the control room staff, and therefore they are called the human-machine interface.

Local manual control is performed at any place outside the main control room by operators through local control facilities at the request of the control room staff. The instructions are given through the communication interface.

Besides automatic control, manual control and associated monitoring, the control room staff are required to perform high-level mental processing of information (e.g. interpretation of multiple readings, formulation of knowledge-based strategy).

There are various types of operator support systems (e.g. diagnostic systems, operation consulting systems, procedure synthesizers) which are intended to support the high-level mental processing. The control room staff may interface with them in a variety of ways – from simple unidirectional information retrieval through displays to high-level bidirectional communication through appropriate devices. The operator support system is a human-machine interface.

Communication with plant personnel and managerial staff stationed outside the main control room can be made through the communication interface.

A.2 “Human” and “machine”

Assigning functions to human means to achieve them by manual control, monitoring, high-level mental processing, or their combinations. Assigning functions to machine means to achieve them by automation. Therefore, human in the functional domain signifies the control room staff and machine in the functional domain signifies automation (Table A.1).

The term “machine” covers a number of hardware entities which include the I&C system and operator support system. It should be noted that the manual control system, controls, and displays which are parts of the I&C system are to enable the control room staff to achieve functions assigned to them.

Table A.1 – Human and machine in functional domain and physical domain

<table>
<tr><th colspan="2">Functional domain</th><th colspan="2">Physical domain</th></tr>
<tr><td>Functions are assigned to:</td><td>Functions are achieved by:</td><td>Machine (hardware)</td><td>Human</td></tr>
<tr><td>Human</td><td>High-level mental processing
Monitoring (associated with both manual control and automation)
Manual control (including back-up control to automation)</td><td>OSS
Displays
Controls
Manual control system
Human-machine interface
I&C system</td><td>Operating crew</td></tr>
<tr><td>Machine</td><td>Automation</td><td>Automatic control system</td><td></td></tr>
</table>

Bibliography

IEC 62954, *Nuclear power plants – Control rooms – Requirements for Emergency Response Facilities (ERC)*

IAEA Safety Standard Series No. SSR-2/1:2012, *Safety of Nuclear Power Plant: Design*

IAEA Safety Guide SSG-39, *Design of instrumentation and control systems in Nuclear Power Plants*

IAEA Safety Glossary:2016, *Terminology used in nuclear safety and radiation protection*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – CONCEPTION

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 60964 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Cette troisième édition annule et remplace la deuxième édition publiée en 2009. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) l'utilisation du terme «tâche» en garantissant la cohérence entre l'IEC 60964 et l'IEC 61839;
b) la clarification du rôle, des capacités fonctionnelles, de robustesse et d'intégrité des services support pour la salle de commande principale pour garantir sa continuité d'utilisation au moment de la survenance d'accident grave ou de risques externes extrêmes;

c) la revue de la pertinence de cette norme par rapport aux guides de sûreté de l'AIEA et aux normes de l'IEC SC 45A qui ont été publiés depuis le développement de l'IEC 60964:2009;

d) la clarification du sens et du rôle de «l'analyse des tâches»;

e) la définition des relations avec les normes dérivées (par exemple l'IEC 61227, l'IEC 61771, l'IEC 61772, l'IEC 61839, l'IEC 62241 et les autres normes pertinentes pour la conception des salles de commande);

f) l'alignement par rapport aux principes d'ergonomie, en particulier ceux du Guide de Sûreté de l'AIEA sur les facteurs humains qui doit être publié prochainement.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
45A/1214/FDIS	45A/1224/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

INTRODUCTION

a) Contexte technique, questions importantes et structure de cette norme

L'IEC 60964 publiée en 1989 avait été développée pour fournir des exigences applicables à la conception des salles de commande principales des centrales nucléaire et elle a été révisée en 2009. Les deux premières éditions ont été largement utilisées par l'industrie nucléaire. Il a été reconnu qu'il était nécessaire de développer un amendement pour l'édition de 2009 pour couvrir les points suivants:

- utilisation du terme «tâche» en garantissant la cohérence entre l'IEC 60964 et l'IEC 61839;
- clarification du rôle, des capacités fonctionnelles, de robustesse et d'intégrité des services support pour la salle de commande principale pour garantir sa continuité d'utilisation au moment de la survenance d'accident grave ou de risques externes extrêmes;
- revue de la pertinence de cette norme par rapport aux guides de sûreté de l'AIEA et des normes de l'IEC SC 45A qui ont été publiés depuis le développement de l'IEC 60964:2009.

Considérant la taille de la proposition d'amendement, il a été décidé de publier une nouvelle édition de l'IEC 60964 à la place de l'amendement. Durant la préparation de cette troisième édition il a été décidé de couvrir les points suivants:

- clarifier le sens et le rôle de «l'analyse des tâches»;
- clarifier et définir les relations avec les normes dérivées (par exemple l'IEC 61227, l'IEC 61771, l'IEC 61772, l'IEC 61839, l'IEC 62241 et les autres normes pertinentes pour la conception des salles de commande);
- considérer son alignement par rapport aux principes d'ergonomie, en particulier ceux du Guide de Sûreté de l'AIEA sur les facteurs humains qui doit être publié prochainement.

Cette norme IEC s'intéresse plus particulièrement à la conception fonctionnelle des salles de commande principales des centrales nucléaires. Cette norme a été développée pour être utilisée par les vendeurs de centrales nucléaires, les exploitants et par les régulateurs.

b) Position de la présente norme dans la collection de normes du SC 45A de l'IEC

L'IEC 60964 est le document du SC 45A de l'IEC de deuxième niveau qui traite des questions générales liées à la conception des salles de commande.

L'IEC 60964 doit être lue avec les normes dérivées citées ci-dessus qui sont les documents pertinents fournissant les recommandations relatives aux commandes opérateurs, à la vérification et à la validation de la conception, à l'utilisation des unités d'affichage, à l'analyse fonctionnelle et l'affectation des fonctions et aux fonctions et présentation des alarmes.

Pour plus de détails sur la collection de normes du SC 45A de l'IEC, voir le point d) de cette introduction.

c) Recommandations et limites relatives à l'application de cette norme

Cette norme a été développée pour être appliquée aux nouvelles salles de commande dont la conception débute après la publication de celle-ci. Les recommandations fournies par la norme peuvent être utilisées pour les rénovations, les mises à niveau et les modifications.

L'objectif principal de la norme est de fournir des exigences de conception fonctionnelles qui puissent être utilisées pour la conception des salles de commande principales des centrales nucléaires pour satisfaire aux exigences de sûreté et d'exploitation.

Cette norme fournit aussi des exigences d'interface fonctionnelle liées au personnel de la salle de commande, aux procédures d'exploitation et au programme de formation qui sont avec l'interface homme-machine des composants du système de la salle de commande.

Afin de garantir la pertinence de cette norme pour les prochaines années, l'accent a été mis sur les questions de principes plutôt que sur les questions particulières liées à la technologie.

d) Description de la structure de la collection des normes du SC 45A de l'IEC et relations avec d'autres documents de l'IEC, et d'autres organisations (AIEA, ISO)

Les documents de niveau supérieur de la collection de normes produites par le SC 45A de l'IEC sont les normes IEC 61513 et IEC 63046. La norme IEC 61513 traite des exigences générales relatives aux systèmes et équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires. La norme 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique; elle couvre les systèmes d'alimentation électrique jusqu'à et y compris les alimentations des systèmes d'I&C. Les normes IEC 61513 et IEC 63046 doivent être considérées ensemble et au même niveau. Les normes IEC 61513 et IEC 63046 structurent la collection de normes du SC 45A de l'IEC et forment un cadre complet, cohérent et consistant établissant les exigences générales relatives aux systèmes d'I&C et électriques des centrales nucléaires de puissance.

Les normes IEC 61513 et IEC 63046 font directement référence aux autres normes du SC 45A de l'IEC traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, la défense contre les défaillances de cause commune, la conception des salles de commande, compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes numériques programmables, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes, de second niveau, forment, avec les normes IEC 61513 et IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont généralement pas référencées directement par les normes IEC 61513 ou IEC 63046, sont relatives à des matériels particuliers, à des méthodes ou à des activités spécifiques. Généralement ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

Un quatrième niveau qui est une extension de la collection de normes du SC 45A de l'IEC correspond aux rapports techniques qui ne sont pas des documents normatifs.

Les normes de la collection produite par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté et de sécurité de haut niveau établis par les normes de sûreté de l'AIEA pertinentes pour les centrales nucléaires, ainsi qu'avec les documents pertinents de la collection de l'AIEA pour la sécurité nucléaire (NSS), en particulier avec le document d'exigences SSR-2/1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires , avec le guide de sûreté SSG-39 qui traite de la conception de l'instrumentation et du contrôle commande des centrales nucléaires, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires, et avec le guide de mise en œuvre NSS17 traitant de la sécurité informatique pour les installations nucléaires. La terminologie et les définitions utilisées pour la sûreté et la sécurité dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

Les normes IEC 61513 et IEC 63046 ont adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau sûreté nucléaire, les normes IEC 61513 et IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, de l'IEC 61508-2 et de l'IEC 61508-4 pour le secteur nucléaire. Dans ce domaine, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à l'IEC 61508-3

pour le secteur nucléaire. Les normes IEC 61513 et IEC 63046 font référence aux normes ISO ainsi qu'aux documents AIEA GS-R partie 2 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au second niveau, la norme IEC 62645 est le document chapeau du SC 45A de l'IEC portant sur la sécurité nucléaire. Elle est élaborée à partir des principes pertinents de haut niveau des normes ISO/IEC 27001 et ISO/IEC 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le secteur nucléaire; elle est coordonnée étroitement avec la norme IEC 62443. Au second niveau, la norme IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et la norme IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

NOTE 1 Il est fait l'hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales.

NOTE 2 Le domaine du SC 45A de l'IEC a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015 des discussions ont eu lieu au sein du SC 45A de l'IEC pour décider de la façon et de l'endroit pour établir les exigences générales portant sur la conception des systèmes électriques. Les experts du SC 45A de l'IEC ont recommandé que pour établir des exigences générales pour les systèmes électriques une norme indépendante soit développée au même niveau que l'IEC 61513. Le projet IEC 63046 est lancé pour atteindre cet objectif. Lorsque la norme IEC 63046 sera publiée la présente NOTE 2 de l'introduction sera supprimée.

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – CONCEPTION

1 Domaine d'application

Le présent document établit des exigences en matière d'interface homme-machine pour la salle de commande principale des centrales nucléaires de puissance. Il établit aussi les exigences en matière de choix fonctionnels, de conception et d'organisation de l'interface homme-machine, ainsi que les procédures utilisées pour vérifier et valider systématiquement la conception fonctionnelle. Ces exigences reflètent les principes d'ergonomie tels qu'ils s'appliquent à une interface homme-machine pour les états opérationnels de la tranche et les conditions accidentelles (y compris les conditions de dimensionnement et les conditions hors dimensionnement), tels que définis par l'AIEA SSR-2/1 et l'AIEA NP-T-3.16. Ce document ne couvre pas les systèmes de commande spécifiques ou isolés tels que ceux prévus pour les opérations d'arrêt de l'extérieur de la salle de commande, pour les installations de situations de crise, pour les installations de traitement des effluents radioactifs. La conception détaillée des matériels ne fait pas partie du domaine d'application de ce document.

Le but premier du présent document est d'établir des exigences fonctionnelles pour la conception des salles de commande des centrales nucléaires de puissance afin de respecter les exigences de conduite et de sûreté. Ce document présente aussi les exigences d'interface fonctionnelles en rapport avec la structure de l'équipe de salle de commande, les procédures de conduite et le programme de formation qui sont en association avec l'interface homme-machine, les constituants du système de salle de commande.

Ce document s'applique aux salles de commande de conception nouvelle dont la conception débute après sa publication. Si on désire l'appliquer à des salles de commande existantes, une attention spéciale est à porter pour maintenir la cohérence de la base de conception.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60671, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

IEC 60709, *Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-commande et électriques importants pour la sûreté – Séparation*

IEC/IEEE 60780-323, *Installations nucléaires– Equipements électriques importants pour la sûreté – Qualification*

IEC 60960, *Critères fonctionnels de conception pour un système de visualisation des paramètres de sûreté pour les centrales nucléaires*

IEC 60965, *Centrales nucléaires de puissance – Salles de commande – Salle de commande supplémentaire pour l'arrêt des réacteurs sans accès à la salle de commande principale*

IEC 60980, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

IEC 61225, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences pour les alimentations électriques*

IEC 61226, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*

IEC 61227, *Centrales nucléaires de puissance – Salles de commande – Commandes opérateurs*

IEC 61513, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

IEC 61771, *Centrales nucléaires de puissance – Salle de commande principale – Vérification et validation de la conception*

IEC 61772, *Centrales nucléaires de puissance – Salles de commande – Utilisation des unités de visualisation*

IEC 61839, *Centrales nucléaires de puissance – Conception des salles de commande – Analyse fonctionnelle et affectation des fonctions*

IEC 62003, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences relatives aux essais de compatibilité électromagnétique*

IEC 62241, *Centrales nucléaires de puissance – Salle de commande principale – Fonctions et présentation des alarmes*

IEC 62645, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences relatives aux programmes de sécurité applicable aux systèmes programmés*

IEC 62646, *Centrales nucléaires de puissance – Salles de commande – Procédures informatisées*

IEC 62859, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences pour coordonner sûreté et cybersécurité*

ISO 11064 (toutes les parties), *Conception ergonomique des centres de commande*

IAEA NS-G-1.9, *Design of the reactor coolant system and associated systems in nuclear power plants*

IAEA, NS-G-1.11, *Protection against internal hazards other than fires and explosions in the design of nuclear power plants*

IAEA NP-T-3.16, *Accident Monitoring Systems for Nuclear Power Plants*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent. Pour les autres termes se référer à la terminologie générale définie dans l'IEC 61513 et dans le Glossaire de sûreté de l'AIEA.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
conditions accidentelles
écarts par rapport au fonctionnement normal plus graves que les incidents de fonctionnement prévus, et comprenant les accidents de dimensionnement et les accidents graves

[SOURCE: AIEA, Glossaire de sûreté, 2016]

3.2
alarme
élément informatif relatif au diagnostic, au pronostique ou à une recommandation, qui est utilisé pour alerter l'opérateur et pour attirer son attention sur une déviation du procédé ou d'un système

Note 1 à l'article: L'information particulière fournie par les alarmes couvre l'existence d'anomalies pour lesquelles une action corrective pourrait être nécessaire, la cause et les conséquences potentielles de l'anomalie, l'état général de la centrale, l'action corrective correspondant à l'anomalie et le retour de l'action corrective.

Deux types de déviation peuvent être distingués:

– Non prévue – Déviation du procédé indésirable et défaillance de matériels;

– Prévue – Déviation du procédé dans des conditions ou états des matériels qui sont les réponses prévues, mais qui peuvent être indicatives de conditions indésirables pour la centrale.

[SOURCE: IEC 62241:2004, 3.1]

3.3
systèmes auxiliaires de commande <de conduite>
systèmes de conduite installés hors de la salle de commande, tels les panneaux de repli et les systèmes d'arrêt décentralisés

3.4
équipe de salle de commande
personnel présent en salle de commande, responsable de l'atteinte des objectifs opérationnels de la centrale, en conduisant celle-ci au moyen des interfaces homme machine

Note 1 à l'article: L'équipe de salle de commande comprend, en général, des opérateurs surveillant l'état de l'installation et manipulant effectivement les commandes; elle peut inclure le personnel d'exploitation et les experts autorisés à être présents en salle de commande, par exemple durant de longues séquences d'évènements.

3.5
système de salle de commande
ensemble constitué de l'interface homme-machine, de l'équipe de salle de commande, des procédures de conduite, du programme de formation et des installations ou matériels associés qui contribuent conjointement à une utilisation correcte de la salle de commande

3.6
commandes
appareils utilisés par l'opérateur pour envoyer les signaux de commande aux systèmes de contrôle-commande et aux dispositifs de la centrale

Note 1 à l'article: Les commandes telles que définies dans le présent document (à savoir des appareils utilisés pour commander des actions) véhiculent un sens différent de celui défini dans le glossaire de sûreté de l'AIEA et ne sont pas remplaçables.

3.7
accident de dimensionnement
accident hypothétique conduisant à l'apparition de conditions accidentelles par rapport auxquelles une installation nucléaire est conçue pour résister conformément à des critères de conception établis spécifiés et dans lesquelles l'endommagement du combustible et les rejets de matières radioactives restent en dessous des limites autorisées

[SOURCE: AIEA, Glossaire de sûreté, 2016]

3.8
conditions hors dimensionnement
conditions accidentelles hypothétiques qui ne sont pas prises en compte dans les accidents de dimensionnement mais qui le sont dans le processus de conception de l'installation conformément aux méthodes de type «meilleure estimation», et dans lesquelles les rejets de matières radioactives sont maintenus dans des limites acceptables. Les conditions hors dimensionnement comprennent les conditions correspondant aux évènements sans dégradation significative du combustible et les conditions avec fusion du cœur.

[SOURCE: AIEA, Glossaire de sûreté, 2016]

3.9
afficheurs
appareils utilisés pour surveiller les conditions de fonctionnement et l'état de la centrale, par exemple l'état du procédé, l'état des matériels

3.10
image
affichage d'image
représentation graphique d'informations affichées sur écran de visualisation telle qu'un texte de message, une représentation numérique, des symboles, des synoptiques, des bargraphes, des courbes, des curseurs, une présentation multi-angulaire

3.11
fonction
but précis ou objectif devant être accompli, qui peut être spécifié ou décrit sans référence aux moyens physiques nécessaires pour son atteinte

[SOURCE: IEC 61226:2009, 3.7]

3.12
analyse fonctionnelle
examen des objectifs fonctionnels d'un système compte tenu des capacités humaines, de la technologie et des autres ressources, pour fournir la base de détermination pour l'affectation et l'exécution de la fonction

3.13
objectif fonctionnel
objectif de performances qui doivent être satisfaites pour remplir la fonction correspondante

3.14
structure hiérarchisée d'objectifs
relation entre un objectif fonctionnel et ses sous objectifs fonctionnels structurés dans un ordre hiérarchique

3.15
démarche intellectuelle
démarche humaine de traitement et/ou d'interprétation d'une information visant à obtenir une information condensée et abstraite

3.16
Interface Homme Machine
IHM
interface entre l'équipe de conduite d'une part, les systèmes d'I&C et les calculateurs reliés à la centrale d'autre part. Elle inclut les afficheurs, les commandes et l'interface «système support de l'opérateur»

3.17
système d'I&C
système réalisé sur la base d'éléments E/E/PE, exécutant des fonctions d'I&C de la centrale ainsi que des fonctions de service et de surveillance liées au fonctionnement du système lui-même

Note 1 à l'article: Le terme est utilisé comme terme général comprenant tous les éléments du système, tels que les alimentations électriques, les capteurs et autres dispositifs d'entrée, les bus de données et autres chemins de communication, les interfaces vers les actionneurs et autres dispositifs de sortie. Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées.

Note 2 à l'article: Les éléments contenus dans un système d'I&C donné sont définis dans la spécification des limites de ce système.

Note 3 à l'article: Selon leurs fonctionnalités propres, l'AIEA fait la distinction entre les systèmes de contrôle et de commande, les systèmes d'IHM, les systèmes de verrouillage et les systèmes de protection.

[SOURCE: IEC 62138:2018, 3.26]

3.18
travail
ensemble de tâches liées opérationnellement. Il convient que les tâches à l'intérieur d'un travail soient cohérentes en regard de la compétence, des connaissances et des responsabilités requises de la part de l'opérateur.

3.19
analyse du travail
analyse identifiant les exigences de base qu'un travail impose à l'équipe de salle de commande, compte tenu des procédures de conduite et des programmes de formation

3.20
points de commande locaux
installations de commande locales
points (ou installations) situés à l'extérieur de la salle de commande où des opérateurs locaux réalisent des activités de commande

3.21
opérateurs locaux
membres de l'équipe de conduite qui remplit des tâches à l'extérieur de la salle de commande

3.22
procédures de conduite
ensemble de documents spécifiant les tâches de conduite qu'il est nécessaire de remplir pour atteindre les objectifs fonctionnels

3.23
équipe de conduite
personnel de la centrale travaillant en poste pour conduire la centrale

Note 1 à l'article: L'équipe de conduite comprend l'équipe de la salle de commande, les techniciens de maintenance, etc.

3.24
interaction de l'opérateur
relation entre l'opérateur et le système d'I&C, plus particulièrement, affichage de l'état de la centrale par le système d'I&C, et actions correspondantes de l'opérateur

3.25
système support de l'opérateur
SSO
un ou des systèmes visant à aider l'équipe de salle de commande dans les tâches exigeant une démarche intellectuelle

3.26
éléments de dimensionnement
éléments quantitatifs caractérisant les tâches qui garantissent le respect des objectifs fonctionnels

3.27
objectifs opérationnels de la centrale
finalité de la conception de la centrale, c'est-à-dire une production maîtrisée d'électricité et la limitation de rejets radioactifs dans l'environnement

3.28
stéréotype de population
tendance pour la plupart des personnes d'un groupe à donner la même réponse à une stimulation particulière, même lorsqu'il y a d'autres réponses possibles. Le stéréotype de population dépend des traditions et des habitudes de la population

3.29
salle de commande supplémentaire
emplacement à partir duquel la commande limitée de la centrale et/ou sa surveillance peuvent être assurées pour réaliser les fonctions de sûreté identifiées dans l'analyse de sûreté, comme prescrit en cas de perte de la possibilité de réaliser ces fonctions à partir de la salle de commande principale

Note 1 à l'article: Pour les installations existantes, la salle de commande supplémentaire peut être une salle de commande particulière, mais dans la plus part des cas celle-ci correspond à un ensemble de panneaux de commande et d'affichage dans des locaux électriques ou dans des zones similaires. Dans ce dernier cas, le terme «point de commande supplémentaire» est utilisé.

[SOURCE: IEC 60965:2016, 3.6]

3.30
accident grave
conditions accidentelles plus graves qu'un accident de dimensionnement qui donnent lieu à une dégradation importante du cœur

[SOURCE: AIEA, Glossaire de sûreté, 2016]

3.31
analyse des tâches
description détaillée des tâches opérateur, pour spécifier les activités humaines mises en jeu et leurs relations fonctionnelles et temporelles

Note 1 à l'article: Souvent on entend que l'analyse de tâches comprend aussi l'évaluation des tâches opérateur. Dans le cadre de l'IEC 60964, cette évaluation est décrite en termes de V&V de la fonction de répartition et de V&V du système intégré de conduite (qui couvre aussi les tâches opérateur).

3.32
tâches
actions réalisées par un homme pour atteindre un objectif fonctionnel

3.33
programme de formation
programme conçu pour former l'équipe de salle de commande de telle sorte qu'elle puisse acquérir les compétences et les connaissances nécessaires aux activités de conduite

3.34
validation
processus permettant de déterminer si un produit ou un service est adapté pour réaliser de façon satisfaisante sa mission prévue. La validation recouvre un domaine plus large que la vérification et fait appel plus largement au jugement.

[SOURCE: AIEA, Glossaire de sûreté, 2016]

3.35
vérification
confirmation par examen et apport d'éléments objectifs que les résultats d'une activité sont conformes aux objectifs et exigences établis pour cette activité

[SOURCE: AIEA, Glossaire de sûreté, 2016]

3.36
unité de visualisation
VDU
type d'affichage incorporant un écran pour présenter des images pilotées par calculateur

Note 1 à l'article: L'abréviation «VDU» est dérivée du terme anglais développé correspondant «Visual Display Unit».

4 Termes abrégés

E/E/PE	Electrique, électronique et électronique programmable
IHM	Interface Homme Machine
I&C	Instrumentation et Contrôle-commande
SCP	Salle de commande principale
NPP	Centrale nucléaire de puissance
SSO	Système support de l'opérateur
VDU	Unité de visualisation
V&V	Vérification et validation
SFP	installation de refroidissement du combustible

5 Utilisation du présent document

Cet article a pour but de présenter à l'utilisateur l'organisation et les points les plus importants de ce document. La Figure 1 montre une vue d'ensemble du système de la salle de commande. Le but d'une équipe de conception de salle de commande est de réussir la réalisation d'un système intégré de salle de commande. Le système de commande est un ensemble qui intègre l'interface homme-machine, l'équipe de salle de commande, les procédures de conduite, le programme de formation et les matériels et dispositifs associés. L'annexe A fournit des explications supplémentaires sur le concept de système de salle de commande.

L'objet premier de ce document est la définition de l'interface homme-machine lors de la conception de la salle de commande; en outre, le présent document définit les moyens pour développer les spécifications concernant l'équipe de conduite, les procédures de conduite et

le programme de formation, mais il ne fournit pas de méthodologie détaillée pour ce développement.

Après le domaine d'application et les spécifications des principes de base de conception, la Figure 2 présente le processus de conception comprenant l'analyse fonctionnelle, l'affectation des fonctions, la vérification et la validation de l'affectation des fonctions et l'analyse du travail. Puis les spécifications de conception fonctionnelle sont établies comme le fait apparaître la Figure 2.

La conception détaillée, les procédures de conduite et le programme de formation sont développés à partir de ces spécifications. Enfin, les composantes du système résultant sont vérifiées et le système de salle de commande intégré est validé.

Ce document traite principalement du processus de conception de la ou des salles de commande, généralement mis en œuvre par une équipe de conception qui comprend différentes compétences, et différentes disciplines. Ceci couvre en particulier les domaines suivants:

- ingénierie nucléaire;
- architecture et génie civil;
- ingénierie des systèmes;
- ingénierie des systèmes d'I&C;
- ingénierie des systèmes d'information et calculateurs;
- ingénierie des facteurs humains;
- exploitation de la centrale;
- formation.

Ces compétences peuvent être celles de membres permanents ou intérimaires de l'équipe ou même de consultants.

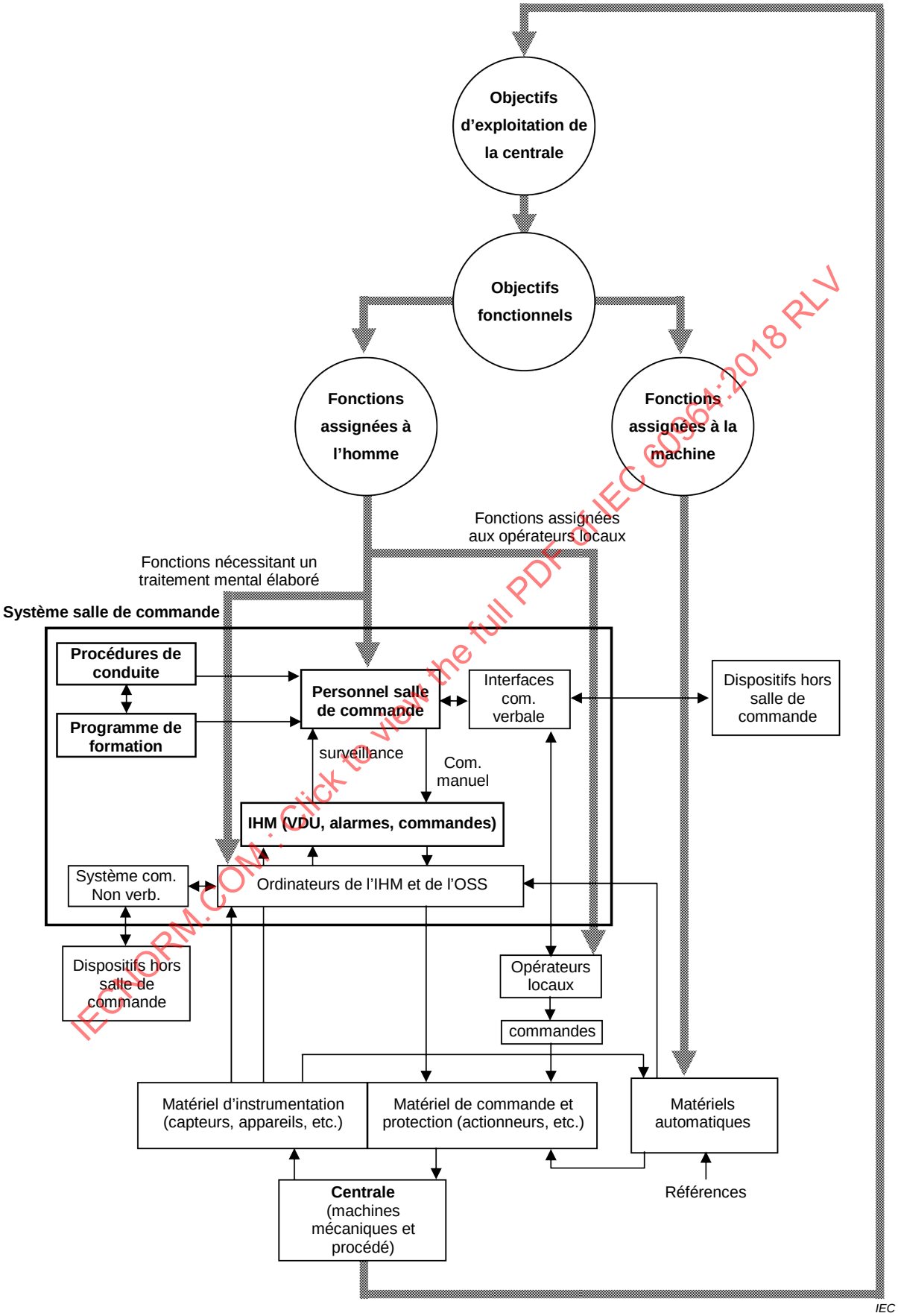


Figure 1 – Vue d'ensemble du système salle de commande

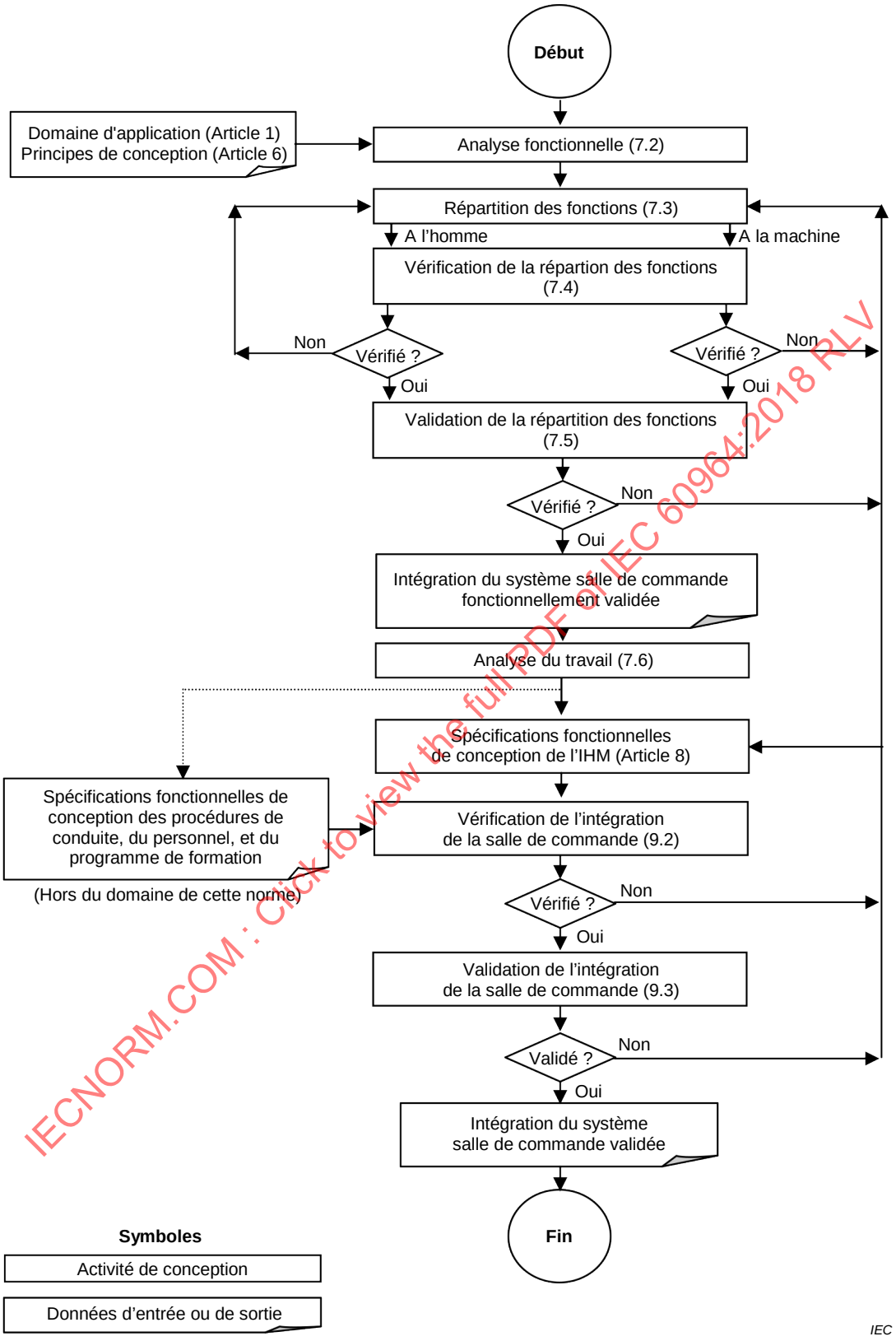


Figure 2 – Processus de conception d'ensemble et relations avec les articles et paragraphes du présent document

6 Principes de conception de la salle de commande principale

6.1 Objectifs principaux

Une centrale nucléaire de puissance doit pouvoir être conduite sûrement et efficacement dans tous ses états de fonctionnement et dans les conditions accidentelles depuis une salle de commande principale. L'équipe de salle de commande a accès en salle de commande principale à une interface homme-machine et à de l'information et des matériels associés, par exemple, l'interface de communication nécessaire pour atteindre les objectifs d'exploitation de la centrale. De plus elle fournit un environnement dans lequel l'équipe de salle de commande est en mesure de remplir ses tâches confortablement, sans tension excessive, ni risque physique.

6.2 Objectifs de la conception fonctionnelle

Les objectifs principaux de la conception de la salle de commande consistent à fournir aux opérateurs des informations précises, complètes, opérationnellement pertinentes et dans les délais, en ce qui concerne l'état fonctionnel des matériels et des systèmes de la centrale.

Pour tous les états opérationnels, y compris le rechargement du combustible et les conditions accidentelles, la conception doit permettre d'optimiser les tâches opérateur et de réduire à un niveau adapté la charge de travail requise pour surveiller et conduire la centrale de façon sûre, et de fournir les informations nécessaires à d'autres installations extérieures à la salle de commande.

La conception de la salle de commande doit garantir une affectation des fonctions optimale qui permet une utilisation maximale des capacités du système et de l'opérateur.

Un objectif supplémentaire de la conception de la salle de commande est de réaliser une mise en service efficace de la centrale et de permettre les modifications et la maintenance.

6.3 Principes de sûreté

La salle de commande doit être conçue de façon à conduire la centrale nucléaire de puissance de façon sûre dans tous ses états opérationnels et de la ramener en état sûr après l'apparition de conditions accidentelles. De tels événements doivent être pris en compte lors de la conception de la salle de commande.

Des mesures de prévention et de compensation pour la gestion des accidents doivent être mises en place, y compris des fonctions de commande et de surveillance et des actions combinées réalisées à partir de la salle de commande principale et localement, voir le document AIEA NP-T-3.16.

Les matériels de la salle de commande doivent être conçus, autant que possible, de telle sorte que des ordres de commande manuels non sûrs ne puissent être émis, par exemple par l'utilisation de verrouillages logiques dépendant de l'état de la centrale.

On doit aussi prendre en compte les besoins d'isolement fonctionnel et de séparation physique pour les systèmes de sûreté redondants ou lorsque des systèmes de sûreté et non-classés de sûreté viennent à être proches. L'IEC 60709 fournit des exigences pour cela. On doit prendre en compte le besoin d'assurer la sûreté si la salle de commande et ses systèmes sont atteints par le feu et de réduire autant que pratiquement possible les possibilités d'incendie, tel que le souligne l'IEC 60709.

Des mesures appropriées doivent être prises pour la sauvegarde des occupants de la salle de commande contre les risques potentiels tels que les accès non autorisés, un niveau de rayonnement élevé conséquence de conditions accidentelles, des gaz toxiques, et toutes les conséquences d'incendie qui pourraient compromettre la réalisation des actions opérateur nécessaires.

Il doit y avoir des accès adaptés pour permettre à l'équipe de la salle de commande de rejoindre ou de quitter la salle de commande ou de gagner d'autres points de commande, en conditions accidentelles.

6.4 Principes de disponibilité

Dans le souci de maximiser le facteur de puissance de la centrale, des dispositions doivent être prises en compte lors de la conception de la salle de commande pour:

– faciliter les opérations d'exploitation prévues pour changer le combustible, démarrer, s'arrêter;

– minimiser l'occurrence de toute réduction de puissance non désirée ou d'arrêt d'urgence conséquences de prises de décision ou d'actions erronées d'opérateur ou de perturbations locales dues au mauvais fonctionnement ou à des défaillances de systèmes d'I&C;

– atteindre la production et les performances de la centrale prévues à la conception.

Les spécifications de conception liées à la disponibilité ne doivent pas être en contradiction avec les principes de sûreté retenus.

6.5 Principes d'ingénierie des facteurs humains

Afin de réaliser une répartition optimale des fonctions assurant une utilisation maximale des capacités de l'homme et de la machine et de viser à obtenir pour la centrale, une sûreté et une disponibilité maximales, le concepteur doit porter une attention particulière aux facteurs humains ayant trait aux caractéristiques humaines du personnel en ce qui concerne leurs capacités et limitations anthropométriques, physiologiques, de perception cognitive et de motricité.

6.6 Principes de conduite de l'exploitant

L'encadrement et la formation font partie intégrante de la salle de commande et de la philosophie de conduite. Pour maximiser la sûreté et l'efficacité de la conduite de la centrale, la salle de commande doit être pilotée avec un nombre suffisant de professionnels compétents.

Ils doivent être techniquement formés à la conduite en salle de commande et éduqués pour ce qui est des principes d'ingénierie relatifs à la conduite et à la sûreté des centrales nucléaires. Ils doivent par ailleurs avoir une connaissance approfondie de la localisation, de la fonction et des performances des composants et des sous-systèmes de la centrale.

Les tâches réalisées par les opérateurs hors de la salle de commande qui impliquent la mise en oeuvre de matériels de la centrale doivent être administrativement contrôlées et surveillées de la salle de commande.

Pour assurer la qualité de la conduite de la centrale, il convient que le responsable d'exploitation prenne en compte les facteurs suivants dans la constitution de l'équipe de salle de commande:

– exigences de sélection et de qualification du personnel;

– exigences de formation initiale et de recyclage pour les conditions de fonctionnement normal, incidentel et accidentel;

– rappel de formation périodique aux règles d'exploitation et possibilité de développer des connaissances dans les principes d'ingénierie;

– responsabilisation de l'équipe de salle de commande et de chaque individu pour l'exploitation normale et en cas d'urgence;

– exigences physiques pour le personnel portant sur les capacités physiques, optiques, auditives, toute altération physique et la taille;