BS IEC 60964:2009

BSI British Standards

Nuclear Power Plants — Control rooms — Design

raising standards worldwide™

BSI
British Standards

National foreword

This British Standard is the UK implementation of IEC 60964:2009.

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

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

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

ISBN 978 0 580 55526 8

ICS 27.120.20

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2009

Amendments issued since publication

Amd. No.	Date	Text affected

BS IEC 60964:2009

IEC 60964

Edition 2.0 2009-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Control rooms – Design

Centrales nucléaires de puissance – Salles de commande – Conception

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

W

ICS 27.120.20

ISBN 2-8318-1031-4

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope and object 8
2 Normative references 8
3 Terms and definitions 9
4 Standard use 12
5 Design principles for the main control room 16
5.1 Main objectives of the main control room 16
5.2 Functional design objectives of the main control room 16
5.3 Safety principles 16
5.4 Availability principles 16
5.5 Human factors engineering principles 17
5.6 Utility operating principles 17
5.7 Relationship with other control and management centres 17
5.8 Operational experience 18
6 Functional design of the main control room 18
6.1 General 18
6.2 Functional analysis 18
6.2.1 General 18
6.2.2 Identification of functions 18
6.2.3 Information flow and processing requirements 18
6.3 Assignment of functions 19
6.3.1 General 19
6.3.2 Operator capabilities 19
6.3.3 I&C system processing capabilities 20
6.4 Verification of function assignment 20
6.4.1 General 20
6.4.2 Process 20
6.5 Validation of function assignment 21
6.5.1 General 21
6.5.2 Process 21
6.5.3 General evaluation criteria for validation 21
6.6 Job analysis 21
7 Functional design specification 22
7.1 General 22
7.2 Provision of data base on human capabilities and characteristics 22
7.3 Location, environment and protection 22
7.3.1 Location 22
7.3.2 Environment 22
7.3.3 Protection 23
7.4 Space and configuration 24
7.4.1 Space 24
7.4.2 Configuration 24
7.5 Panel layout 25
7.5.1 Priority 25
7.5.2 Positioning on control desks and panels 25

7.5.3 Mirror image layout 25
7.6 Location aids 25
7.6.1 Grouping of display information and controls 25
7.6.2 Nomenclature 26
7.6.3 Coding 26
7.6.4 Labelling 27
7.7 Information and control systems 27
7.7.1 General 27
7.7.2 Information functions 28
7.7.3 Control functions 31
7.8 Control-display integration 32
7.9 Communication systems 32
7.9.1 General 32
7.9.2 Verbal communication systems 33
7.9.3 Non-verbal communication systems 34
7.10 Other requirements 34
7.10.1 Power supplies 34
7.10.2 Qualification 34
7.10.3 Maintainability 34
7.10.4 Repairs 35
7.10.5 Testability 35
8 Verification and validation of the integrated control room system 35
8.1 General 35
8.2 Control room system verification 35
8.2.1 General 35
8.2.2 Process 35
8.2.3 General evaluation criteria for integrated system verification 35
8.3 Control room system validation 35
8.3.1 General 35
8.3.2 Process 35
8.3.3 General evaluation criteria for integrated system validation 36
Annex A (informative) Explanation of concepts 37

Figure 1 – Overview of control room system 14
Figure 2 – Overall design process and the relationship to clauses and subclauses of this standard 15

Table A.1 – Human and machine in functional domain and physical domain 38

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

This second edition cancels and replaces the first edition published in 1989.

The revision of the standard is intended to accomplish the following:

– to take into account the fact that software engineering techniques advanced significantly in the intervening years;
– to align the Standard with the new revisions of IAEA documents NS-R-1 and NS-G-1.3, which includes as far as possible adaptation of the definitions;
– to replace, where relevant, the previous requirements in the standard, where these are now given by references to Standards published since the first edition, especially IEC 60709, IEC 60780, IEC 60980, IEC 61225, IEC 61226, IEC 61227, IEC 61513, IEC 61771, IEC 61772, IEC 61839, IEC 62241 and ISO 11064;
– to review the existing requirements and to update the terminology and definitions.

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

FDIS	Report on voting
45A/724/FDIS	45A/731/RVD

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

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

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

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

INTRODUCTION

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

IEC 60964:1989 was developed to supply requirements relevant to the design of the main control room of NPPs. The first edition of IEC 60964 has been 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.

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 document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

IEC 61513 refers directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC 45 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.

NUCLEAR POWER PLANTS – CONTROL ROOMS – DESIGN

1 Scope and object

This International Standard establishes requirements for the human-machine interface in the main control rooms of nuclear power plants. The standard also establishes requirements for the selection of functions, design consideration and organization of the human-machine interface and procedures which shall be 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 conditions. This standard 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 standard.

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 programmes which, together with the human-machine interface, constitute the control room system.

This standard is intended for application to new control rooms whose conceptual design is initiated after the publication of this standard. 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 referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

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

IEC 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)*

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

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

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*

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.

3.1
alarms
an 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 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.

[IEC 62241]

3.2
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

3.3
control room staff
a group of plant personnel stationed in the control room, who are responsible for achieving the plant operational goals by controlling the plant through the human-machine interface.

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

3.4
control room system
an 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

3.5
controls
devices which the operator uses to send demand signals to control systems and plant items

NOTE Controls as defined in this standard (i.e. devices used for control actions) hold a different meaning from the one defined in the IAEA safety Glossary and are not replaceable.

3.6
displays
devices used for monitoring plant conditions and status, e.g. process status, equipment status

3.7
format (display format)
a 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

3.8
function
specific purpose or objective to be accomplished, that can be specified or described without reference to the physical means of achieving it

[IEC 61226]

3.9
functional analysis
the 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

3.10
functional goal
the performance objectives that shall be satisfied to achieve the corresponding function

3.11
hierarchical goal structure
relationship between a functional goal and sub-functional goals structured in a hierarchical order

3.12
high-level mental processing
human act to process and/or interpret information to obtain reduced abstract information

3.13
human-machine interface
the 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

3.14
I&C system
system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself.

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 1 The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

NOTE 2 According to their typical functionality, IAEA distinguishes between automation and control systems, HMI systems, interlock systems and protection systems.

[IEC 61513]

3.15
job
a set of tasks which are operationally related. The tasks within a job should be coherent with regard to required skill, knowledge and responsibility

3.16
job analysis
an analysis identifying basic requirements which a job imposes on the control room staff structure, the operating procedures and training programme

3.17
local control points (or facilities)
points (or facilities) located outside the control room where local operators perform control activities

3.18
local operators
the operating staff that perform tasks outside the control room

3.19
operating procedures
a set of documents specifying operational tasks it is necessary to perform to achieve functional goals

3.20
operating staff
plant personnel working on shift to operate the plant. The operating staff includes the control room staff, maintenance engineers, etc.

3.21
operator interaction
interrelation between operator and the I&C system. Specifically, display of plant status by the I&C system and corresponding operator action

3.22
Operator Support System (OSS)
a system or systems supporting the high-level mental information processing tasks assigned to the control room staff

3.23
performance requirements
quantitative requirements specifying performance of tasks which ensure the achievement of functional goals

3.24
plant operational goals
ultimate purposes of plant design, i.e. controlled generation of electricity and limitation of release of radioactivity to the environment

3.25
population stereotype
the 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

3.26
task analysis
a detailed description of an operator's task, in terms of its components, to specify the detailed human activities involved, and their functional and temporal relationships

3.27
tasks
actions performed by either human or machine for the accomplishment of a functional goal

3.28
training programme
a programme which is designed to train the control room staff so that they can acquire the skills and knowledge necessary for operational activities

3.29
validation
the 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.

[IAEA Safety Glossary, 2007 edition]

3.30
verification
the process of determining whether the quality or performance of a product or service is as stated, as intended or as required

[IAEA Safety Glossary, 2007 edition]

3.31
Visual Display Unit (VDU)
a type of display incorporating a screen for presenting computer-driven images

4 Standard use

This clause is provided to orient the user to the organization and focus of this standard. 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 standard is the establishment of the human-machine interface in the control room design. The standard 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 standard is addressed to the control room designer. This refers not necessarily to a single person; typically it is 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;
- information and computer systems;
- human factors engineering;
- plant operations;
- training.

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

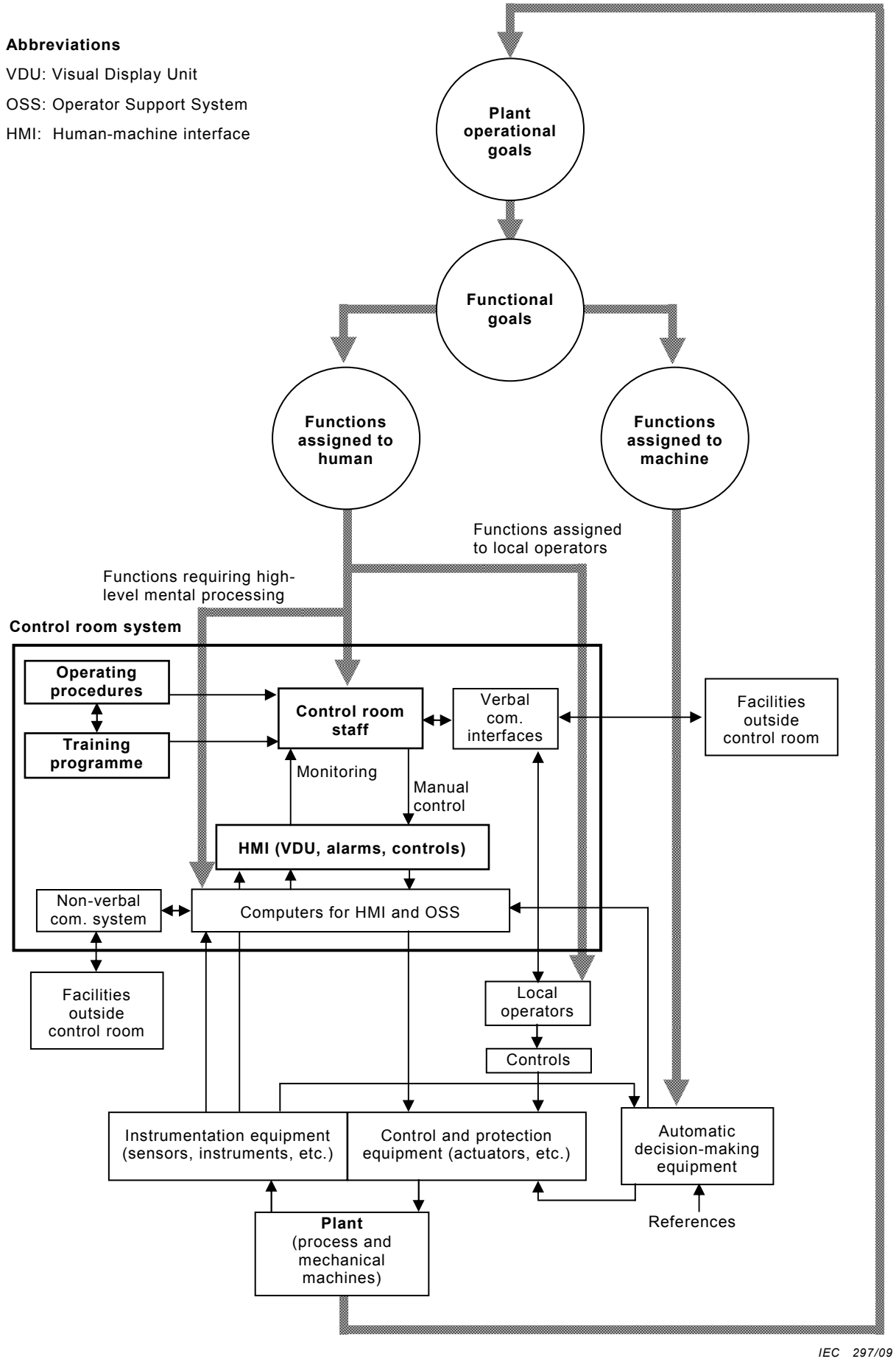

Figure 1 – Overview of control room system

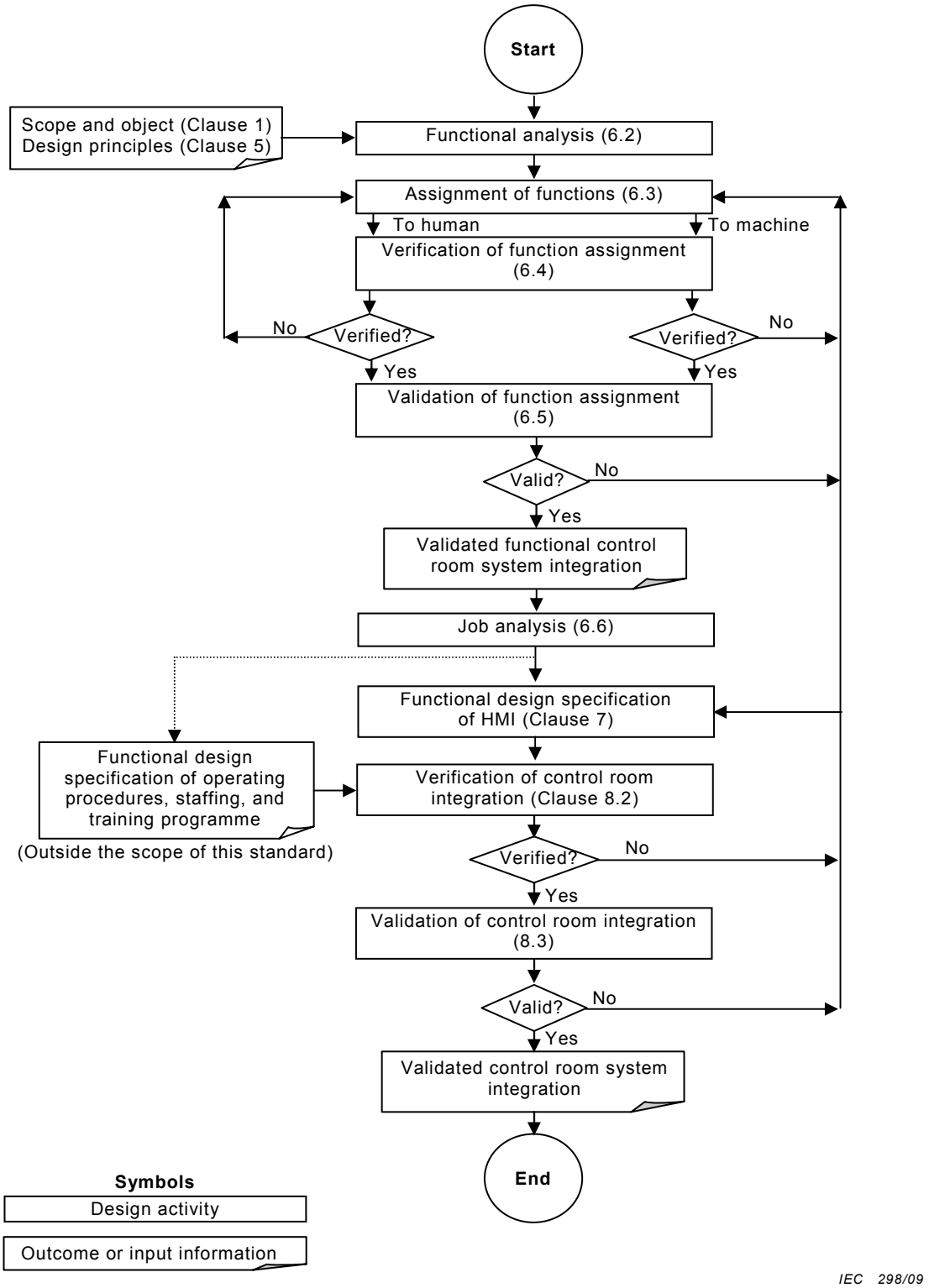

Figure 2 – Overall design process and the relationship to clauses and subclauses of this standard

5 Design principles for the main control room

5.1 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.

5.2 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 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.

5.3 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.

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.

5.4 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.

5.5 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.

5.6 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.

5.7 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 points shall be provided, sufficient to ensure safety if the main control room is damaged or becomes inoperable. The requirements for supplementary control 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 points. The equipment shall operate independently of the other equipment in the control room.

5.8 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.

6 Functional design of the main control room

6.1 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.

6.2 Functional analysis

6.2.1 General

An analysis of the functions to be performed by the nuclear power plant to achieve the objectives of 5.1 and 5.2 consistent with the principles of 5.3 to 5.8 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.

6.2.2 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.

6.2.3 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.

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 assessment;
– events in which plant trip is highly probable unless corrective action is taken in time;
– events whose occurrence rates are high.

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

6.3 Assignment of functions

6.3.1 General

Task analysis shall be conducted to determine which functions should be assigned to the human and which functions should be assigned to the machine.

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.

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

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.

6.3.2 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. This analysis should result in the information needed for the conceptual information system structure and the functional organization of resources to perform each decision making and control task.

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 tasks which shall be performed to accomplish the function. The general tasks should include display, 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 is to organize the information from various sources with respect to each decision making task to provide a comprehensive information system for the operator within his capabilities.

6.3.3 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 and accuracy requirements that the system and equipment shall satisfy as well as human engineering requirements defining the human-machine interface for each component type.

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.

6.4 Verification of function assignment

6.4.1 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.

6.4.2 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 standard, 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.

6.5 Validation of function assignment

6.5.1 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 6.2 shall be evaluated under all the normal operations and several representative events.

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

6.5.2 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 6.2.3, 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.

6.5.3 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.

6.6 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.

7 Functional design specification

7.1 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.

7.2 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.

7.3 Location, environment and protection

7.3.1 Location

The control room shall be located for convenient plant operation and should meet the safety principles of 5.3.

7.3.2 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 lighting, avoidance of glare, reflections and shadows.

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 of the plant even during emergency conditions of the plant.

7.3.3 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.

The design shall ensure that such events cannot simultaneously jeopardize the main control room and the supplementary control points, mentioned in 5.7.

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.

7.4 Space and configuration

7.4.1 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).

7.4.2 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.

7.5 Panel layout

7.5.1 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.

7.5.2 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.

7.5.3 Mirror image layout

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

7.6 Location aids

7.6.1 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.

7.6.2 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.

7.6.3 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.

7.6.4 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.

7.7 Information and control systems

7.7.1 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;
– 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.

7.7.2 Information functions

7.7.2.1 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.

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.

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.

7.7.2.2 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.

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 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.

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.

7.7.2.3 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.

7.7.2.4 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.

7.7.2.5 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;
– functions for automatic on-power test.

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

7.7.3 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 standard.

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.

7.8 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.

7.9 Communication systems

7.9.1 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.

7.9.2 Verbal communication systems

7.9.2.1 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 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 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.

7.9.2.2 Off-site communications

For communication to the off-site station operating authority, emergency 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.

7.9.2.3 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.

7.9.3 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.

7.10 Other requirements

7.10.1 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.

7.10.2 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 60780 and IEC 60980 for more detailed requirements.

7.10.3 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.

7.10.4 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.

7.10.5 Testability

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

8 Verification and validation of the integrated control room system

8.1 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.

8.2 Control room system verification

8.2.1 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.

8.2.2 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.

8.2.3 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.

8.3 Control room system validation

8.3.1 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.

8.3.2 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.

8.3.3 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 → OSS
Monitoring (associated with both manual control and automation) → Displays
Manual control (including back-up control to automation) → Controls
Manual control (including back-up control to automation) → Manual control system
Displays, Controls, Manual control system: Human-machine interface (I&C system)
Human-machine interface ↔ Operating crew</td><td></td><td></td></tr>
<tr><td>Machine</td><td>Automation</td><td>Automatic control system</td><td></td></tr>
</table>

_____

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9000 Fax: +44 (0)20 8996 7400

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

You may also buy directly using a debit/credit card from the BSI Shop on the website **www.bsigroup.com/shop**

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library.

Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre.

Tel: +44 (0)20 8996 7111
Fax: +44 (0)20 8996 7048 Email: info@bsigroup.com

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™

British Standards