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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.
If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.
Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

CONTENTS

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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*

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

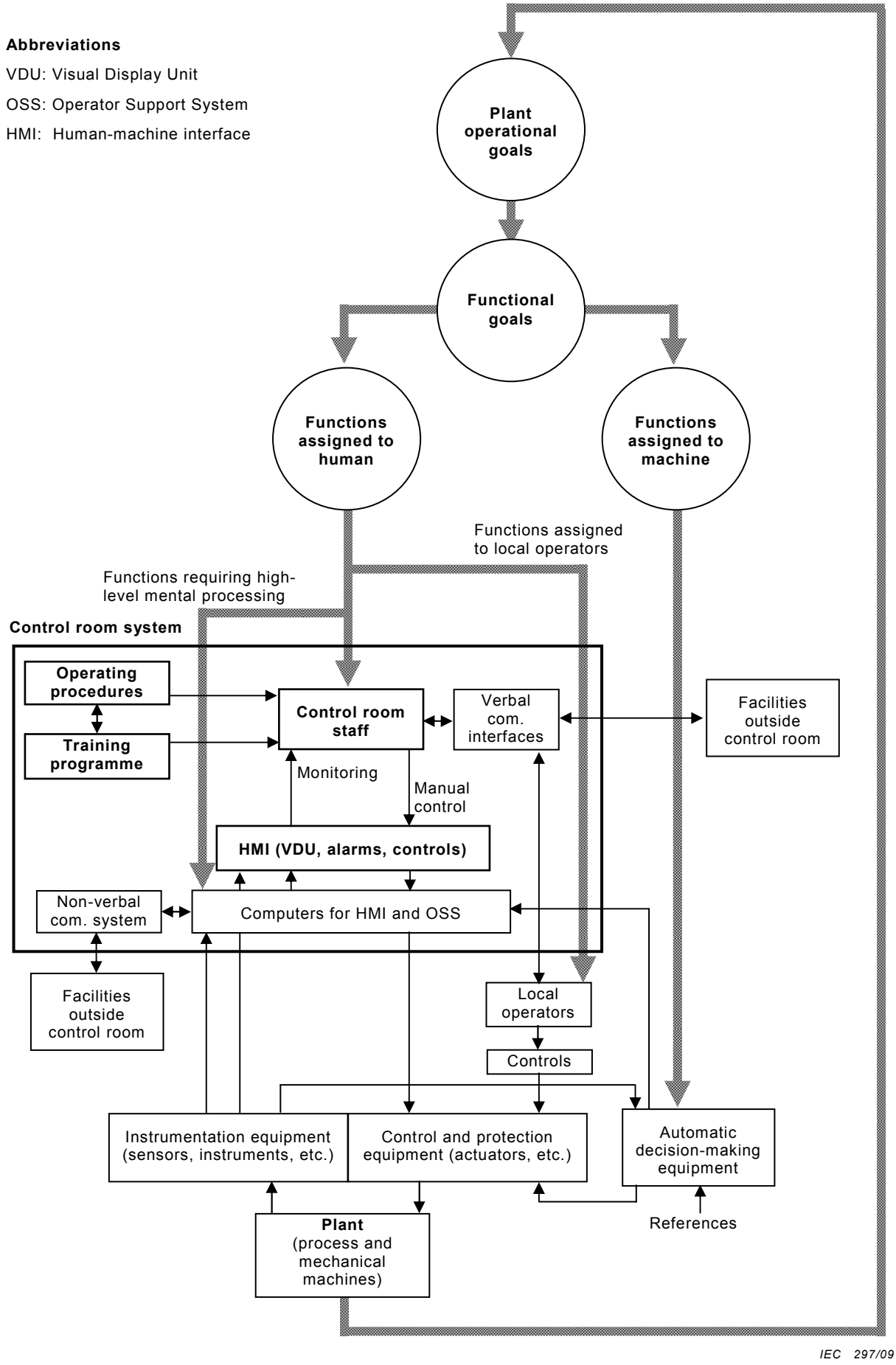

Figure 1 – Overview of control room system

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

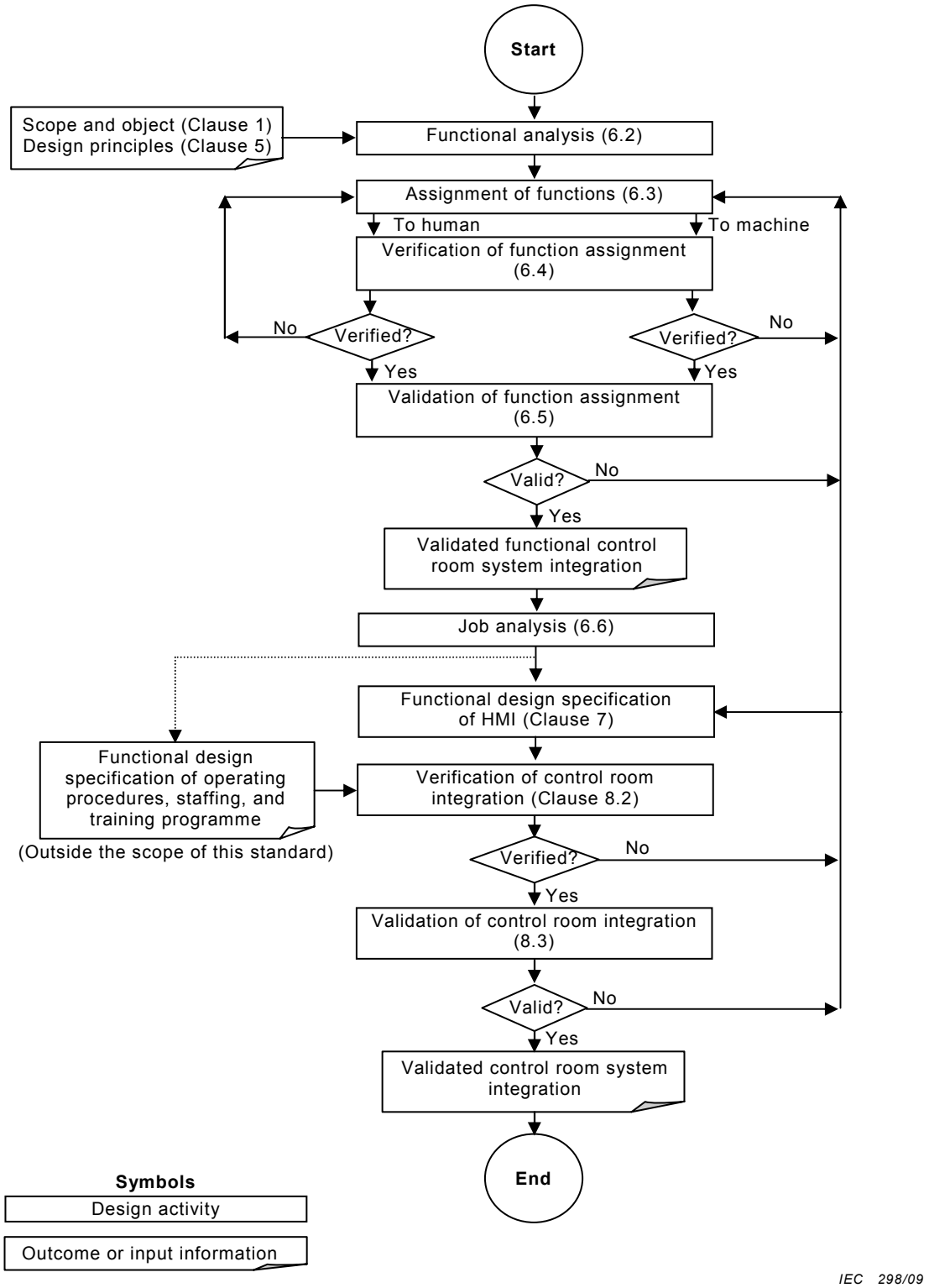

Figure 2 – Overall design process and the relationship to clauses and subclauses of this standard

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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:

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– 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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– 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:

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– 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:

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

- 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

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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).

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

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>

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

SOMMAIRE

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – CONCEPTION

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI 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, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 60964 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Cette deuxième édition annule et remplace la première édition publiée en 1989.

L'objectif de la révision de la norme est de:

– Prendre en compte le fait que les techniques de génie logiciel ont progressé de façon significative ces dernières années.
– Mettre en cohérence la norme avec les nouvelles révisions des documents de l'AIEA NS-R-1 et NS-G-1.3, ceci comprenant autant que possible une adaptation des définitions.
– Remplacer, lorsque nécessaire, les anciennes exigences de la norme, par les références aux normes publiées dans lesquelles elles apparaissent, plus particulièrement la CEI 60709, CEI 60780, CEI 60980, CEI 61225, CEI 61226, CEI 61227, CEI 61513, CEI 61771, CEI 61772, CEI 61839, CEI 62241 et l'ISO 11064.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– Faire la revue des exigences et mettre à jour la terminologie et les définitions.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/724/FDIS	45A/731/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.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

INTRODUCTION

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

La CEI 60964 publiée en 1989 avait été développée pour fournir des exigences applicables à la conception des salles de commande principales des centrales nucléaires. Cette première édition a été largement utilisée par l'industrie nucléaire. La nécessité de prendre en compte les récents développements techniques et en particulier ceux liés au génie logiciel a été reconnue, de la même façon que celle de clarifier et de définir les relations avec les normes dérivées (par exemple la CEI 61227, la CEI 61771, la CEI 61772, la CEI 61839, et la CEI 62241).

Cette norme CEI 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 la CEI

La CEI 60964 est le document du SC 45A de la CEI de deuxième niveau qui traite des questions générales liées à la conception des salles de commande.

La CEI 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 la CEI, 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 la CEI et relations avec d'autres documents de la CEI et d'autres organisations (AIEA,ISO)

Le document de niveau supérieur de la collection de normes produites par le SC 45A de la CEI est la CEI 61513. Cette norme traite des exigences 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, et structure la collection de normes du SC 45A de la CEI.

La CEI 61513 fait directement référence aux autres normes du SC 45A de la CEI traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

qualification, la séparation des systèmes, les défaillances de cause commune, les aspects logiciels et les aspects matériels relatifs aux systèmes programmés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la CEI 61513, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de la CEI, qui ne sont généralement pas référencées directement par la CEI 61513, 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 la CEI correspond aux rapports techniques qui ne sont pas des documents normatifs.

La CEI 61513 a adopté une présentation similaire à celle de la CEI 61508, avec un cycle de vie et de sûreté global, un cycle de vie et de sûreté des systèmes, et une interprétation des exigences générales des CEI 61508-1, CEI 61508-2 et CEI 61508-4 pour le secteur nucléaire. La conformité à la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire. Dans ce cadre, la CEI 60880 et la CEI 62138 correspondent à de la CEI 61508-3 pour le secteur nucléaire.

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA 50-C-QA (remplacé depuis par le document AIEA GS-R-3) pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de la CEI sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle-commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLES DE COMMANDE – CONCEPTION

1 Domaine d'application et objet

Cette Norme internationale établit des exigences en matière d'interface homme-machine pour la salle de commande principale des centrales nucléaires de puissance. Elle établit aussi les exigences en matière de choix fonctionnels, de conception et d'organisation de l'interface homme-machine, ainsi que les procédures qui doivent être 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 pendant les situations normales et anormales de la centrale. Cette norme 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 cette norme.

Le but premier de la présente norme 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. Cette norme 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.

Cette norme 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, il faut porter une attention spéciale pour maintenir la cohérence de la base de conception.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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).

CEI 60709, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Séparation*

CEI 60780, *Centrales nucléaires – Equipement électrique de sûreté – Qualification*

CEI 60960, *Critères fonctionnels de conception pour un système de visualisation des paramètres de sûreté pour les centrales nucléaires*

CEI 60965, *Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)*

CEI 60980, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

CEI 61225, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences pour les alimentations électriques*

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

CEI 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*

CEI 61227, *Centrales nucléaires de puissance – Salles de commande – Commandes opérateur*

CEI 61513, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*

CEI 61771, *Centrales nucléaires de puissance – Salle de commande principale – Vérification et validation de la conception*

CEI 61772, *Centrales nucléaires de puissance – Salle de commande principale – Utilisation des unités de visualisation*

CEI 61839, *Centrales nucléaires de puissance – Conception des salles de commande – Analyse fonctionnelle et affectation des fonctions*

CEI 62241, *Centrales nucléaires de puissance – Salle de commande principale – Fonctions et présentation des alarmes*

ISO 11064 (toutes les parties), *Conception ergonomique des centres de commande*

IAEA NS-G-1.3, *Instrumentation et contrôle commande importants pour la sûreté des centrales nucléaires, 2005*

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 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 la CEI 61513 et dans les documents du programme NUSS de l'AIEA, tels que le guide de sûreté NS-G-1.3.

3.1
alarmes
un élément informatif relatif au diagnostique, 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 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.

[CEI 62241]

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

3.2
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

3.3
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. L'équipe de salle de commande comprend en général des opérateurs supervisant et des opérateurs 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

3.4
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

3.5
commandes
appareils utilisés par l'opérateur pour envoyer les signaux de commande aux systèmes de contrôle-commande et aux dispositifs de la centrale

NOTE Les commandes telles que définies dans cette norme (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.

3.6
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

3.7
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

3.8
fonction
but précis ou objectif devant être accompli, qui peut être spécifié ou décrit sans référence aux moyens physiques nécessaires pour son atteinte

[CEI 61226]

3.9
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

3.10
objectif fonctionnel
objectif de performances qui doivent être satisfaites pour remplir la fonction correspondante

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

3.11
structure hiérarchisée d'objectifs
relation entre un objectif fonctionnel et ses sous-objectifs fonctionnels structurés dans un ordre hiérarchique

3.12
démarche intellectuelle
démarche humaine de traitement et/ou d'interprétation d'une information visant à obtenir une information condensée et abstraite

3.13
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 »

3.14
système d'I&C
système exécutant des fonctions d'I&C ainsi que des fonctions de service et d'affichage liées au fonctionnement du système lui-même. Sa technologie est électrique et/ou électronique et/ou électronique programmable

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 actionneurs et autres dispositifs de sortie. Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées

NOTE 1 Les éléments contenus dans un système d'I&C donné sont définis dans la spécification des limites de ce système.

NOTE 2 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.

[CEI 61513]

3.15
travail
ensemble de tâches liées opérationnellement. Il convient que les tâches à l'intérieur d'un travail soient en principe cohérentes en regard de la compétence, des connaissances et des responsabilités requises de la part de l'opérateur

3.16
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

3.17
points de commande locaux (ou installations)
points (ou installations) situés à l'extérieur de la salle de commande où des opérateurs locaux réalisent des activités de commande

3.18
opérateurs locaux
membres de l'équipe de conduite qui remplit des tâches à l'extérieur de la salle de commande

3.19
procédures de conduite
ensemble de documents spécifiant les tâches de conduite qu'il est nécessaire de remplir pour atteindre les objectifs fonctionnels

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

3.20
équipe de conduite
personnel de la centrale travaillant en poste pour conduire la centrale. L'équipe de conduite comprend l'équipe de la salle de commande, les techniciens de maintenance, etc.

3.21
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

3.22
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

3.23
exigences de performance
exigences quantitatives spécifiant les performances associées à une tâche qui assure l'accomplissement d'objectifs fonctionnels

3.24
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

3.25
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

3.26
analyse des tâches
description détaillée des tâches opérateur, au sens de ses composantes, pour spécifier les activités humaines mises en jeu et leurs relations fonctionnelles et temporelles

3.27
tâches
actions réalisées, soit par un homme, soit par une machine pour atteindre un objectif fonctionnel

3.28
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

3.29
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

[Glossaire de sûreté de l'AIEA, édition 2007]

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

3.30
vérification
processus permettant de déterminer si la qualité ou les performances d'un produit ou d'un service sont conformes à ce qui est déclaré ou prévu comme cela est requis

[Glossaire de sûreté de l'AIEA, édition 2007]

3.31
unité de visualisation (VDU – visual display unit en anglais**)**
type d'affichage incorporant un écran pour présenter des images pilotées par calculateur

4 Utilisation de la présente norme

Cet Article a pour but de présenter à l'utilisateur l'organisation et les points les plus importants de cette norme. 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 cette norme est la définition de l'interface homme-machine lors de la conception de la salle de commande; en outre, cette norme définit les moyens pour développer les spécifications concernant l'équipe de conduite, les procédures de conduite et le programme de formation, mais elle ne fournit pas de méthodologie détaillée pour ce développement. Les relations entre les différents articles et paragraphes de cette norme sont détaillées.

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.

Cette norme fait référence au concepteur de la salle de commande. Ce terme ne correspond pas nécessairement à une seule personne, mais en général, plutôt à 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;
– systèmes d'I&C;
– 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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

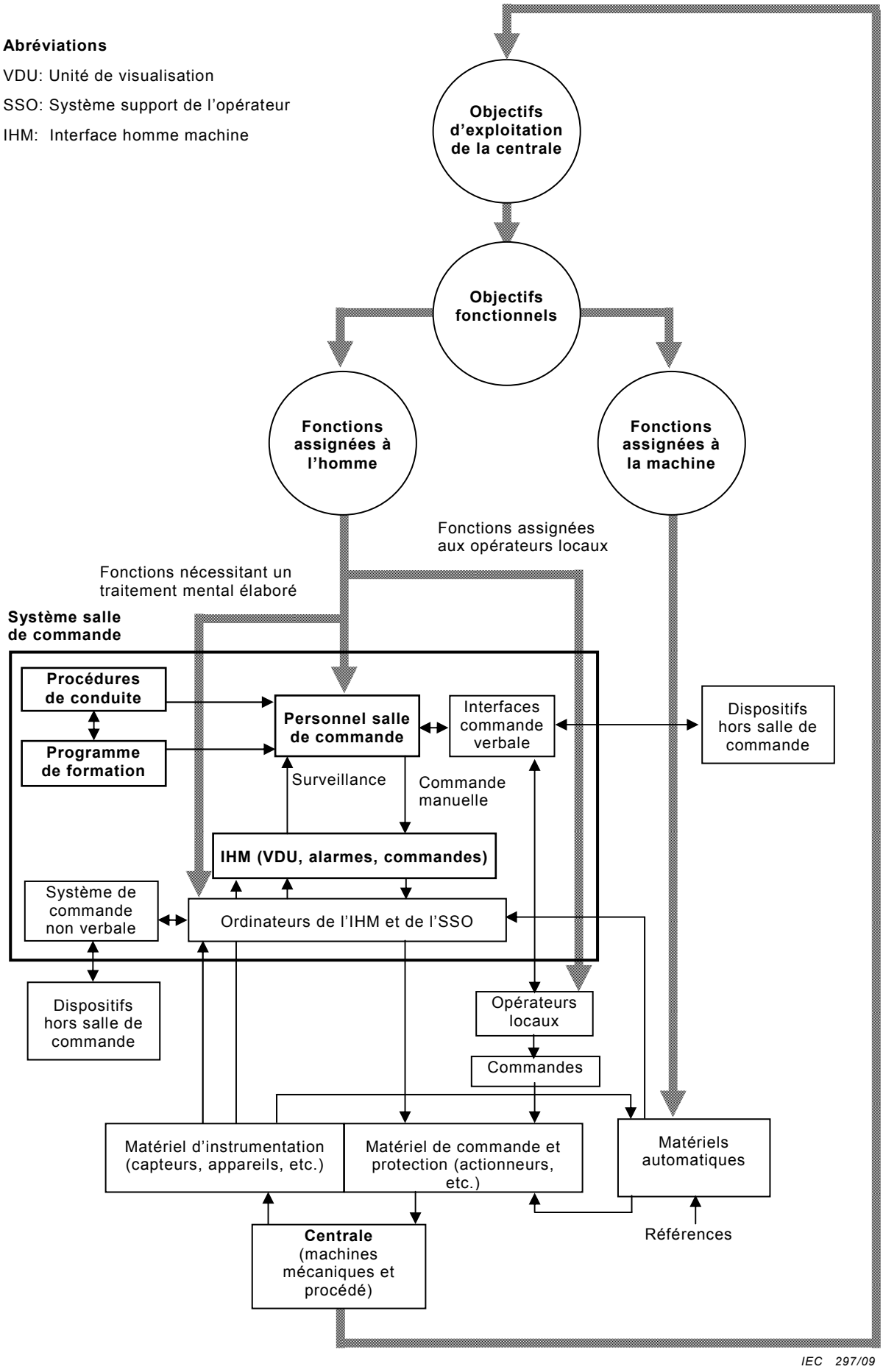

Figure 1 – Vue d'ensemble du système salle de commande

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

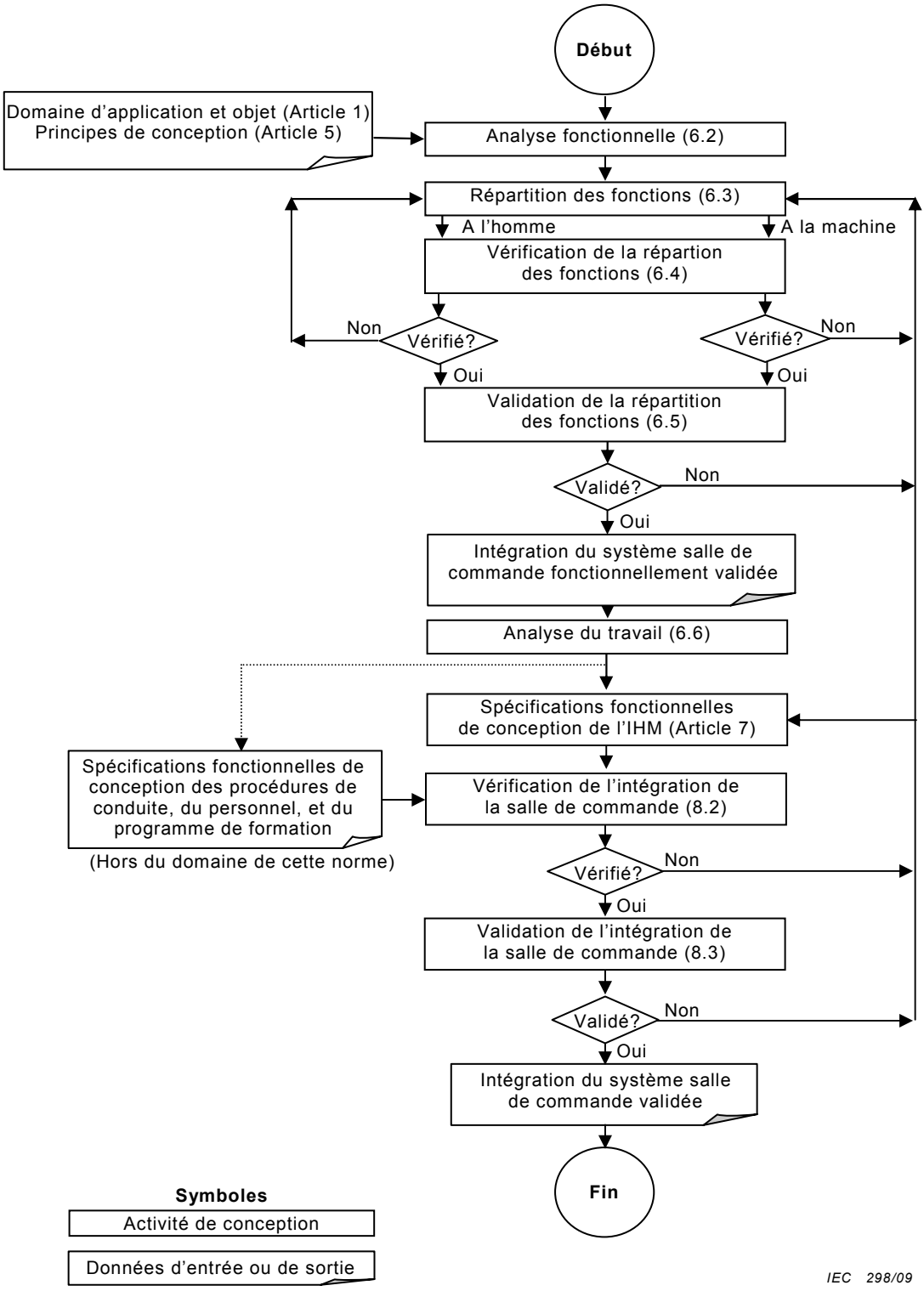

Figure 2 – Processus de conception d'ensemble et relations avec les articles et paragraphes de cette norme

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

5 Principes de conception de la salle de commande principale

5.1 Objectifs principaux de la salle de commande principale

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.

5.2 Objectifs de la conception fonctionnelle de la salle de commande principale

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 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 optimale des fonctions 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.

5.3 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.

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 pas 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. La CEI 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, comme le souligne la CEI 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.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

5.4 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.

5.5 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.

5.6 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 instruits 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, auditives et visuelles, toute altération physique et la taille;
– gestion et surveillance des structures et des responsabilités;
– profil des équipes et tension provoquée par le travail.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

5.7 Relations avec les autres centres de contrôle et de gestion

Pour aider le personnel en salle de commande à réagir à des conditions anormales d'exploitation, des centres de crise doivent être mis en place et être opérationnels durant ces situations critiques.

Un nombre suffisant de points supplémentaires de conduite doit être prévu pour assurer la sûreté si la salle de commande principale est endommagée ou devient non exploitable. La CEI 60965 établit les exigences relatives aux points de conduite supplémentaires.

Des matériels doivent être prévus pour le basculement du contrôle et de la surveillance de la salle de commande principale vers les points de conduite supplémentaires. Les matériels doivent fonctionner de façon indépendante par rapport aux autres matériels de la salle de commande.

5.8 Retour d'expérience en exploitation

Lorsqu'un retour d'expérience en exploitation est disponible sur des centrales existantes, il convient de le collecter, de l'analyser et d'en tirer de façon pertinente les leçons pour la conception des nouvelles centrales nucléaires. Un tel retour d'expérience peut pousser à l'utilisation ou à l'optimisation de solutions éprouvées ou même influencer la prise en compte de principes dans des domaines tels que les suivants:

– personnel;
– organisation de l'équipe de conduite et définition du travail;
– répartition des fonctions entre la salle de commande principale et les points de contrôle locaux;
– automatisation;
– conception du traitement, de la présentation et du contrôle de l'information.

6 Conception fonctionnelle de la salle de commande principale

6.1 Généralités

Une approche "système" de la conception fonctionnelle d'une salle de commande doit être utilisée et doit couvrir la salle de commande et les sujets indiqués à la Figure 1. Cette approche doit inclure les cinq étapes suivantes, comme indiqué à la Figure 2:

– analyse fonctionnelle;
– répartition des fonctions;
– vérification de la répartition fonctionnelle;
– validation de la répartition fonctionnelle;
– analyse du travail.

6.2 Analyse fonctionnelle

6.2.1 Généralités

Afin d'atteindre les objectifs concrets listés en 5.1 et 5.2, cohérents avec les principes établis de 5.3 à 5.8, une analyse des fonctions à remplir par la centrale doit être réalisée.

Il convient que cette analyse identifie la hiérarchie des objectifs de conception de la salle de commande pour tous les états de fonctionnement et les conditions accidentelles. Parmi ces objectifs, la production d'électricité et la minimisation des rejets radioactifs doivent être des objectifs principaux. Ces objectifs pourront être décomposés en sous-objectifs et utilisés dans le processus de décision associé à la conception.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Pour les descriptions et les exigences portant sur le processus d'analyse fonctionnelle, la CEI 61839 fait référence.

6.2.2 Identification des fonctions

Concernant la structure hiérarchisée des objectifs, il convient d'identifier et de documenter toutes les fonctions de la centrale associées aux objectifs. Un moyen d'identification de ces objectifs est fourni par la CEI 61839. Lors de la définition des fonctions, on doit prendre en compte les interactions entre la salle de commande et les installations et les systèmes à l'extérieur de la salle de commande.

6.2.3 Exigences portant sur le traitement et le flux d'information

On doit mener une analyse permettant de déterminer le flux d'information opérationnel de base et les traitements nécessaires pour assurer les fonctions de conduite de la centrale, y compris les prises de décisions et les actions. Cette analyse est décrite dans la CEI 61839.

Lors de l'identification des exigences portant sur le traitement et le flux d'information, il est recommandé de prendre en compte plusieurs évènements de dimensionnement représentatifs ainsi que toutes les situations normales d'exploitation.

Il convient de considérer les évènements suivants:

– évènements exigeant des actions jugées subjectivement difficiles en termes de complexité d'interprétations des données, de vitesse de commande, etc.;
– évènements nécessitant un niveau élevé de garantie pour l'exactitude des réponses de l'opérateur, par exemple pour certaines conditions accidentelles;
– évènements importants en termes d'évaluation probabiliste de risques;
– évènements pour lesquels l'arrêt d'urgence de la tranche est très probable si une action corrective n'est pas entreprise à temps;
– évènements pour lesquels les taux d'occurrence sont élevés.

Le nombre d'évènements considérés doit être suffisamment important pour couvrir correctement les fonctions associées à la structure hiérarchique des objectifs.

6.3 Répartition des fonctions

6.3.1 Généralités

L'analyse des tâches doit être menée pour déterminer quelles fonctions il convient de confier à l'homme et quelles fonctions il convient de confier aux machines.

Les fonctions affectées aux hommes présentées dans le Tableau A.1 de l'Annexe A sont:

– commandes manuelles (incluant les commandes en secours des automatismes);
– surveillance associée aux commandes manuelles et automatiques;
– tâches relevant d'une démarche intellectuelle, telles que les diagnostiques pour déterminer les causes de fonctionnements et d'évènements anormaux et imprévus et pour déterminer les actions correctives.

Les fonctions affectées aux machines sont celles assurées par les commandes automatiques fournies par le Tableau A.1.

Les critères de conception et les principes d'ingénierie des facteurs humains doivent être appliqués lors de cette analyse, voir ISO 11064.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Les principes et critères utilisés pour cette analyse doivent être documentés et doivent comprendre les facteurs traitant des capacités et des limites du personnel de la salle de commande et des systèmes de commandes automatiques.

Concernant les exigences détaillées portant sur le processus de répartition des fonctions, voir la CEI 61839.

6.3.2 Aptitude de l'opérateur

Pour les fonctions allouées à l'opérateur, il convient de distinguer les situations pour lesquelles il réalise en pratique une tâche de commande, les situations pour lesquelles il surveille un système automatique qui réalise les tâches de commande et les situations où pour réaliser sa tâche, il suit une approche intellectuelle, comme par exemple pour un diagnostique. Il convient que cette analyse produise les informations nécessaires à la structure du système d'information conceptuel et à l'organisation fonctionnelle des ressources pour prendre chaque décision et réaliser les tâches de commande.

Concernant les fonctions potentiellement confiées à l'opérateur, on doit pour chaque aspect relatif au traitement de l'information et aux actions de commande, estimer les capacités de traitement nécessaires en termes de charge de travail, de précision, de débit et de temps. Ces estimations doivent être utilisées pour la répartition initiale des fonctions. Il convient de modifier ces estimations sur la base des résultats de la vérification et de les utiliser pour reconsidérer la répartition des fonctions, ainsi que pour fournir une définition plus détaillée des capacités opérateur requises.

Ces exigences en liaison avec celles concernant les moyens de présentation, de commande et de communication, doivent être consistantes avec les tâches devant être réalisées pour assurer la fonction. Il est recommandé que les tâches générales comprennent les exigences d'affichage, de commande et de communication.

Il est recommandé de grouper les différents types de données proposées à l'opérateur par rapport aux tâches et non par rapport à l'origine des données. Le but étant d'organiser l'information provenant de différentes sources par rapport aux tâches de prise de décision pour offrir à l'opérateur un système d'information à la fois complet et compatible avec ses aptitudes.

6.3.3 Capacités de traitement du système d'I&C

L'analyse des traitements du système d'I&C doit commencer par la définition des contraintes et des exigences fonctionnelles des systèmes et du matériel, suivie par une description plus détaillée des séquences évènementielles d'exploitation et des exigences portant sur l'interface homme-machine pour chaque tâche. Le but est d'organiser les informations et les capacités de la machine par rapport aux tâches définies pour interagir avec l'opérateur.

Cette organisation facilite l'évaluation des capacités à la fois de la machine et de l'homme pour accomplir chacune des tâches de prise de décision et de commande. Il est recommandé que les capacités de traitement du système d'I&C prennent en compte des exigences, en termes de quantité, de temps de réponse et de précision, que le système et le matériel doit satisfaire, tout comme des exigences d'ergonomie définissant l'interface homme-machine pour chaque type de composant.

Pour réduire la probabilité d'erreur opérateur, il est recommandé de concevoir les systèmes de contrôle-commande afin que ceux-ci maintiennent la centrale à l'intérieur de limites de sûreté, sans aucune action opérateur, pendant un laps de temps spécifié après l'apparition des conditions anormales de la centrale. La valeur de ce laps de temps doit être prise en compte au niveau des exigences fonctionnelles des systèmes de commande automatique.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

6.4 Vérification de la répartition des fonctions

6.4.1 Généralités

Une répartition satisfaisante des fonctions de la salle de commande entre l'homme et la machine doit être vérifiée comme l'indique la Figure 2. Il doit être prouvé que la répartition des fonctions proposée tire un avantage maximum des capacités de l'homme et de la machine, sans imposer d'exigences pénalisantes à aucun.

Pour ce qui est des exigences détaillées portant sur la vérification de la répartition des fonctions, voir la CEI 61771.

6.4.2 Processus

Le processus développé pour la vérification doit comprendre des phases de préparation, d'évaluation et de correction.

Avant de tenter de vérifier la répartition des fonctions proposée, on doit vérifier la cohérence d'ensemble des critères qui ont été utilisés pour la répartition.

Les vérifications doivent confirmer que:

– toutes les fonctions nécessaires pour atteindre les objectifs d'exploitation et de sûreté de la tranche sont identifiées;
– la répartition des fonctions proposée est en accord avec les critères établis pour celle-ci;
– un nombre suffisant d'exigences sont identifiées pour chaque fonction. Ces exigences comprennent des aspects de performance (par exemple, constantes de temps, précision), des aspects dérivés des principes de sûreté, de disponibilité et d'exploitation précisés dans cette norme, et des aspects dérivés d'autres normes, règles ou guides;
– les objectifs fonctionnels de haut niveau se déclinent aux niveaux fonctionnels inférieurs sans conflit dans tous les modes d'exploitation.

Les modifications (c'est-à-dire correction d'erreur ou réaffectation) et les vérifications doivent être faites de façon itérative jusqu'à ce que tous ces critères soient satisfaits.

6.5 Validation de la répartition des fonctions

6.5.1 Généralités

La répartition des fonctions proposée doit être validée pour montrer que le système atteindra ses objectifs fonctionnels. En particulier, les performances des fonctions identifiées en 6.2 doivent être évaluées pour toutes les conditions de fonctionnement normal et lors de l'apparition de plusieurs évènements représentatifs.

Pour ce qui est des exigences détaillées portant sur la vérification de la répartition des fonctions, voir la CEI 61771.

6.5.2 Processus

Le processus développé pour la validation doit comprendre des phases de préparation, d'évaluation et de correction.

Les critères de sélection doivent être élaborés pour garantir que les évènements qui seront choisis pour l'évaluation sont représentatifs. En plus des conditions de fonctionnement normal et des évènements indiqués en 6.2.3, il convient de considérer pour évaluer la répartition des fonctions confiées à l'homme, des évènements conséquences de défaillances multiples.

Après avoir terminé la sélection des évènements représentatifs, les fonctions nécessaires pour chaque événement doivent être identifiées et intégrées en une séquence temporelle.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

6.5.3 Critères d'évaluation générale pour la validation

Les performances des fonctions doivent être évaluées pour toutes les conditions de fonctionnement normal et les évènements représentatifs. Les critères de validation générale qui doivent être satisfaits comprennent les points suivants:

– le nombre d'objectifs fonctionnels à remplir et la charge de travail à assumer ne doivent pas dépasser la capacité du personnel de la salle de commande;
– la répartition des fonctions entre le personnel de la salle de commande et les opérateurs locaux est satisfaisante;
– la répartition des fonctions confiées aux automatismes est satisfaisante et les fonctions seront exécutées.

6.6 Analyse du travail

Afin d'établir les exigences de base pour la structure de l'équipe de salle de commande, les procédures de conduite et le programme de formation, il est recommandé que le concepteur réalise une analyse du travail à partir de la répartition des fonctions vérifiée et validée et des exigences fonctionnelles.

La première étape de l'analyse du travail consiste à identifier les caractéristiques et le nombre de tâches confiées à l'homme. Sur la base de ces éléments, le concepteur peut alors définir le nombre d'opérateurs et l'organisation qui seront nécessaires dans le cadre réglementaire et de pratique normale en exploitation relatifs à la structure du personnel de la salle de commande.

Il est recommandé que les tâches confiées à un opérateur n'entraînent pas de surcharge de celui-ci et que ces tâches soient cohérentes avec ses responsabilités telles que définies dans la structure du personnel de la salle de commande. De plus, il convient que le concepteur identifie les communications entre les opérateurs et les communications entre les opérateurs et la salle de commande qui sont nécessaires pour réaliser les tâches.

Il est recommandé que le concepteur identifie aussi les activités non opérationnelles (par exemple compte rendu aux autorités) inhérentes à certaines tâches en faisant référence aux documents appropriés.

Lorsque l'analyse est terminée, il convient que les points suivants soient clairs:

– organisation et nombre d'opérateurs;
– compétences opérateur exigées;
– responsabilité des opérateurs en exploitation;
– tâches administratives des opérateurs (par exemple compte rendu);
– interactions opérationnelles entre opérateurs;
– dialogues entre les opérateurs et la centrale;
– communications entre les opérateurs et le personnel de la centrale situé à l'extérieur de la salle de commande de l'installation;
– communication avec l'encadrement et le personnel de surveillance.

Il est recommandé que la structure du personnel de la salle de commande, les procédures de conduite et le programme de formation reposent sur les points cités ci-dessus, ainsi que sur les résultats de l'analyse de la répartition des fonctions (par exemple, la structure d'information conceptuelle).

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

7 Spécifications fonctionnelles de conception

7.1 Généralités

Cet article vise à spécifier les exigences fonctionnelles de conception pour le système de salle de commande et les matériels assurant les fonctions de contrôle et de surveillance assignées. Il spécifie aussi les interfaces entre l'homme et la salle de commande.

La conception doit être basée sur l'approche d'ingénierie des systèmes homme-machine intégrés.

7.2 Nécessité d'une base de données sur les caractéristiques et capacités humaines

On doit établir pour la conception détaillée de la salle de commande une base de données sur les caractéristiques et les capacités humaines, qui constitue une donnée fondamentale pour la prise en compte des facteurs humains.

La base de données doit comprendre:

– des considérations anthropométriques;
– les stéréotypes de population;
– les caractéristiques et capacités auditives et visuelles;
– les capacités humaines à traiter l'information;
– les facteurs d'environnement.

Comme ces données dépendent des habitudes du pays, la base de données peut être spécifique à chaque pays ou pour chaque exploitant.

7.3 Localisation, environnement et protection

7.3.1 Localisation

La salle de commande doit être située là où la conduite de la centrale est aisée et il convient qu'elle prenne en compte les principes de sûreté de 5.3.

7.3.2 Environnement

Les conditions d'ambiance de la salle de commande principale doivent être telles que les opérateurs puissent remplir leurs tâches de façon efficace et confortable.

La conception environnementale de la salle de commande doit comprendre des exigences pour le conditionnement de l'air, l'éclairage et l'environnement sonore. Les exigences suivantes sont applicables:

a) Conditionnement de l'air

   La salle de commande principale doit être climatisée. Le traitement de l'air doit mettre en oeuvre des moyens pour faire face aux conditions accidentelles de la centrale, par exemple en utilisant des filtres ou des moyens d'isolement.

b) Eclairage

   La conception du système d'éclairage doit assurer une lumière uniforme, en évitant les éclats, les reflets et les ombres.

c) Environnement sonore

   La conception de l'environnement sonore doit garantir une communication aisée au sein de l'équipe de conduite, un minimum de perturbations dues au bruit ambiant, et une perception fiable des messages sonores, des alarmes et de signaux d'urgence.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

L'ISO 11064 fournit des recommandations concernant les exigences portant sur l'environnement en conditions de fonctionnement normal.

Il peut être utile d'intégrer dans les spécifications des exigences portant sur la taille et la forme de la salle de commande à partir de plans provisoires, des exigences portant sur les chemins de câbles, des exigences relatives aux séismes, des exigences portant sur la couleur des pupitres ou des salles ou d'autres détails de finition, pour que celles-ci soient cohérentes avec le génie civil et soient confirmées ultérieurement.

Des mesures adaptées doivent être mises en place au niveau de la conception pour que l'opérabilité de la salle de commande et la possibilité de surveiller la tranche soient garanties même en conditions accidentelles.

7.3.3 Protection

La conception de la salle de commande doit prendre en compte dans son dimensionnement la protection contre l'incendie, contre les rayonnements, contre les missiles intérieurs et extérieurs, contre les tremblements de terre ou contre les actes hostiles. Les matériels doivent être qualifiés conformément au dimensionnement de base.

La conception doit garantir que de tels évènements ne peuvent pas simultanément mettre en péril la salle de commande principale et les points de commande supplémentaires mentionnés en 5.7.

Plus particulièrement:

a) Protection incendie

   Il convient de faire attention à n'utiliser que des matériaux non inflammables. La zone de la salle de commande doit être équipée de moyen de détection et de lutte incendie.

   Les matériels électriques de la salle de commande doivent être conçus autant que cela est possible pour ne provoquer, ni alimenter aucun incendie.

   Les circuits câblés et les appareils de protection et de coupure associés à la salle de commande doivent être protégés contre l'incendie. Il est recommandé que l'isolant des câbles et les matériaux de gainage soient ignifugés et satisfassent aux critères de tests nationaux en ce qui concerne la propagation du feu et le dégagement de produits de combustion, si nécessaire.

b) Protection contre les rayonnements

   Il est recommandé de protéger le personnel de la salle de commande contre les rayonnements directs en toutes situations accidentelles. Les prises d'air doivent être équipées de systèmes de surveillance des rayonnements. Lorsque les circonstances l'exigent, le système de ventilation de la salle de commande doit pouvoir s'isoler lui-même. Des appareils respiratoires doivent être disponibles pour le personnel.

c) Protection contre les missiles

   La conception de la salle de commande doit comprendre une évaluation et une protection contre les missiles d'origine interne comme externe à la salle de commande. Le guide de sûreté de l'AIEA, NS-G-1.11 fournit des recommandations au sujet de la protection contre les missiles.

d) Protection contre les tremblements de terre

   Les matériels de la salle de commande liés aux fonctions de sûreté, le système de conditionnement de l'air et le système d'éclairage de sûreté (par exemple l'éclairage conçu pour fonctionner suite à un séisme) doivent être conçus sur les même base de dimensionnement sismique. Des exigences détaillées sont fournies par la CEI 60980.

e) Protection contre les actes hostiles

   Il convient de prendre des mesures pour restreindre l'accès à la salle de commande et de la protéger contre les actes hostiles.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Le plan de sécurité doit être conforme aux exigences réglementaires applicables à chaque pays.

7.4 Dimensions et configuration

7.4.1 Dimensions

La salle de commande doit avoir des dimensions suffisantes pour permettre à l'équipe de salle de commande d'exécuter toutes les actions nécessaires, tout en réduisant au minimum les déplacements des opérateurs dans les situations anormales.

Il est particulièrement recommandé de veiller à prévoir des zones de travail, des zones pour écrire et de l'espace de rangement pour les documents:

– Les zones de travail qui sont occupées de façon continue par le personnel doivent être conçues pour travailler assis et des sièges appropriés doivent être fournis, cependant il est recommandé qu'elles permettent de travailler aussi debout.
– Quand une tâche oblige à écrire et à accéder régulièrement à la documentation en salle de commande on doit avoir à disposition un endroit pour écrire.
– L'espace de rangement pour la documentation doit être mis à disposition à proximité des zones de travail pour éviter que les documents ne traînent sur les consoles, les bureaux, etc.
– De l'espace libre doit être prévu pour de futures extensions (lors de la phase de conception ou lors de la durée de vie de la salle de commande principale).

7.4.2 Configuration

La configuration de la salle de commande doit être conçue en considérant:

– les principes de conduite de l'exploitant;
– la répartition des fonctions entre les opérateurs et les systèmes d'I&C;
– la philosophie de conduite centralisée ou locale qui détermine le nombre de commandes présentes en salle de commande;
– les critères de supervision qui déterminent l'utilisation de synoptique général, du nombre d'écrans de visualisation, d'enregistreurs, d'indicateurs d'alarme et de voyants sur les panneaux;
– les choix de technologie (degré d'utilisation d'afficheurs et de commandes dédiées (câblées) par rapport à une utilisation de commandes logicielles et d'écrans y compris de grands écrans synoptiques, séparation des différents trains, utilisation de séquences de commandes automatiques, degré d'utilisation des automatismes et/ou des commandes multiplexées);
– les exigences légales et celles de l'exploitant, telles que le nombre d'opérateurs présents en salle de commande exigé par la politique d'exploitation ou par les autorités;
– l'installation d'un système non opérationnel, tel que les systèmes de détection et de lutte incendie et d'autres systèmes liés aux fonctions de site;
– des zones pour les tâches administratives.

La salle de commande doit nécessairement comporter des zones de conduite d'où chaque opérateur peut accéder aux informations et aux commandes dont il a besoin pour effectuer les tâches qui lui sont assignées dans tous les modes d'exploitation et toutes les situations accidentelles.

La zone de conduite et les matériels de la salle de commande, tels les pupitres, les tableaux et les panneaux, doivent être disposés selon les principes d'ingénierie des facteurs humains. Il convient que la disposition soit prévue pour que chaque opérateur ait un accès facile et une bonne visibilité des matériels de la salle de commande, suivant ses responsabilités. Il convient que la disposition permette à chaque opérateur de voir directement et de parler avec

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

tous les autres opérateurs normalement présents, sans que leurs regards ne rencontrent d'obstacle entre eux.

Pour les exigences détaillées se reporter à l'ISO 11064.

Les moyens d'affichage des informations et les éléments de commande doivent être disposés selon des principes cohérents et bien documentés dans le processus de conception.

L'implantation doit être structurée, et ceci plus particulièrement dans le cas d'une utilisation importante d'enregistreurs et de commandes dédiées, de façon à simplifier l'identification des systèmes ou des composants, à la fois en fonctionnement normal, dans les conditions accidentelles de conduite et dans les situations d'urgence, de façon à minimiser la probabilité d'actions erronées dues à des erreurs humaines.

Les critères ci-dessus peuvent être utilisés en combinaison avec d'autres éléments de conception et les règles en résultant doivent être cohérentes pour toutes les zones de conduite.

7.5 Agencement des panneaux

7.5.1 Priorités

Des principes concernant la disposition et le rangement des alarmes, des afficheurs et des commandes appartenant à une fonction d'un système ainsi que les priorités entre les éléments semblables doivent être établis et appliqués lors de l'agencement des panneaux. Les règles qui en résultent doivent être cohérentes pour tous les panneaux de la centrale.

7.5.2 Position sur les panneaux et les tableaux de commande

La position des afficheurs, indicateurs et commandes sur les panneaux et pupitres doit être basée sur les critères suivants:

– les panneaux d'alarmes et les indicateurs doivent être visibles de l'ensemble de la zone de conduite de la salle de commande et doivent être à une hauteur convenable pour que les opérateurs puissent les voir et les lire;
– les commandes utilisées fréquemment doivent être atteintes facilement et les indicateurs et afficheurs qui s'y réfèrent doivent être lisibles depuis la position de conduite.

Pour les exigences détaillées se reporter à l'ISO 11064.

7.5.3 Symétrie

La disposition symétrique des panneaux, commandes et indicateurs doit être évitée afin de prévenir la confusion gauche-droite.

7.6 Aide à la localisation

7.6.1 Regroupement des moyens d'affichage des informations et des commandes

Il est essentiel que les informations affichées et les commandes soient regroupées de façon logique.

Les techniques suivantes peuvent être utilisées pour regrouper les informations affichées et les commandes:

a) Regroupement par fonction

Il convient de regrouper les informations et les commandes selon leurs fonctions ou leurs relations dans un système. On doit prendre soin d'identifier la fonction par le rôle que

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

l'information joue pour atteindre les objectifs du système plutôt que par la source d'information ou la méthode de mesure.

b) Regroupement selon les séquences d'utilisation

Les informations et commandes peuvent être regroupées sur une base séquentielle soit en considérant l'affichage comme un tout, soit en divisant l'affichage en différentes parties, chacune d'elles étant organisée sur une base séquentielle. Il convient de rendre apparentes les relations de cause à effet dans l'affichage.

Il est recommandé d'utiliser des regroupements naturels conformes aux attentes des stéréotypes de population (par exemple. 1, 2, 3 – a, b, c, etc.). Pour les mêmes raisons, il convient d'organiser l'affichage de la même façon, par exemple de gauche à droite et de bas en haut.

c) Regroupement selon la fréquence d'utilisation

Dans ce type de regroupement, les informations le plus souvent utilisées sont associées et présentées en partie haute de l'affichage; les informations les moins utilisées sont regroupées vers le bas. Les commandes les plus utilisées doivent être les plus proches de l'opérateur.

La méthode habituelle pour connaître les fréquences d'utilisation est l'analyse des liens qui permet de déterminer les relations entre les diverses informations ou commandes et les procédures.

Ce type de regroupement est d'application limitée, à cause du risque d'un manque de logique apparent lors de la présentation.

d) Regroupement par priorité

Les informations et commandes sont regroupées selon leur importance pour la réussite de la mission du système. Il convient de placer les éléments critiques en première position à l'intérieur d'un groupe.

e) Regroupement par procédures de conduite

Il convient de regrouper les moyens de présentation et de commandes en fonction des procédures de conduite. Il est recommandé de regrouper séparément les moyens de présentation et de commande spécifiques utilisés dans les situations d'urgence, de ceux utilisés en fonctionnement normal.

f) Regroupement par système sur synoptique

Si des synoptiques sont utilisés, on doit veiller à éviter des contradictions avec les autres critères utilisés, et à conserver la même doctrine pour le synoptique si des modifications ou adjonctions dans le processus étaient requises ultérieurement.

Il convient de choisir les techniques appropriées et de les combiner pour équilibrer leurs propriétés respectives. Chaque groupe doit être d'une dimension maîtrisable pour être appréhendé rapidement et avec précision. Il convient de prendre en compte les contraintes liées aux performances humaines.

Il convient que les regroupements soient cohérents avec les hypothèses faites à propos du modèle mental de l'utilisateur de la centrale.

Un soin particulier doit être pris pour éviter les conflits entre regroupements, particulièrement lorsque différentes techniques de regroupement sont utilisées en même temps.

7.6.2 Nomenclature

Les noms et les identifiants de chaque élément de la centrale, prenant en compte les nombreux éléments redondants d'une tranche nucléaire, doivent être soigneusement choisis et retenus pour être utilisés de façon uniforme sur l'ensemble du projet.

Il convient de se mettre d'accord et d'utiliser de façon cohérente les abréviations et les acronymes particuliers (tel que RCV pour le système de contrôle volumétrique et chimique). Une revue des facteurs humains de ces identifiants de tranche peut être intéressante.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

7.6.3 Codage

Le codage des commandes et des informations affichées peut être utilisé pour distinguer les différentes types de commandes et de classes d'information, comme par exemple pour distinguer (a) les fonctions de sûreté, (b) les autres fonctions importantes pour la sûreté, et (c) les fonctions qui ne sont pas importantes pour la sûreté.

Les principes de codage doivent être définis lors des premières étapes de conception de la salle de commande et il est recommandé qu'ils soient cohérents avec les exigences nationales et les pratiques de l'exploitant.

Le système de codage doit être cohérent pour toute la salle de commande. Il convient d'appliquer de façon cohérente les codes de localisation, d'information, de couleurs et d'éclairage utilisés au niveau de l'affichage et des commandes associées.

La méthode de codage d'une application réelle doit être déterminée en considérant les avantages relatifs des types de codages:

– Codage physique (par taille, par forme, par couleur, par signal sonore, par intensité).
– Codage de l'information.
– Codage de la localisation.

Pour les exigences détaillées se reporter à l'ISO 11064.

Pour des raisons liées au personnel (personne présentant une déficience au niveau de la vision des couleurs) et aux matériels (atténuation des couleurs, défaillance partielle des matériels d'I&C), la couleur ne doit pas être le seul moyen pour discriminer l'information importante pour la sûreté. Il est recommandé d'éviter d'utiliser seulement la couleur pour le codage dans d'autres zones.

7.6.4 Repérage

Il doit y avoir un repérage adéquat en salle de commande. Il doit être cohérent avec les autres repérages de la centrale et conforme aux exigences nationales et aux pratiques de l'exploitant. Pour les exigences détaillées se reporter à l'ISO 11064.

Le langage et l'écriture utilisés pour les repères, les identifiants, et pour tous les afficheurs doivent être les mêmes dans la salle de commande et il est recommandé que le langage soit le langage courant des personnes vivant dans la zone où est située la centrale, sauf raisons technologiques particulières.

7.7 Systèmes d'information et de commande

7.7.1 Généralités

Suivant le processus de conception et les exigences de la CEI 61513, l'interface homme-machine de la salle de commande principale permettant de surveiller et de commander l'installation se fait au travers de systèmes d'information et de commande.

L'architecture du système dépend:

– de la classe de sûreté;
– des critères de défaillance;
– de la stratégie de défense en profondeur;
– des considérations sur la qualification et la fiabilité;
– des considérations sur la maintenance;
– des choix imposés par la technologie disponible.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

La mise en œuvre des systèmes d'information et de commande sera faite par un ou plusieurs sous-systèmes traitant de différents aspects de l'interface homme-machine et des fonctions d'aide à l'opérateur. Généralement ceci comprend des systèmes numériques, des écrans, des commandes logicielles au même titre que des enregistreurs et des commandes dédiées. Les exigences portant sur le sujet sont fournies ci-dessous.

7.7.2 Fonctions d'information

7.7.2.1 Généralités

Un système d'information doit être à disposition pour informer les opérateurs sur l'état de la centrale et sur ses variables importantes pour la sûreté et la disponibilité, ce qui assure aux opérateurs de la salle de commande une compréhension globale de l'état de la tranche à chaque instant.

Un ensemble suffisant d'informations doit être disponible pour permettre au personnel d'exploitation d'atteindre un état d'arrêt sûr de tranche et de s'y maintenir indéfiniment conformément aux exigences réglementaires.

Le système doit aussi fournir les informations sur l'état de la tranche aux experts techniques ainsi qu'aux experts en sûreté sur-site ou hors-site, en conditions accidentelles.

Le système doit comprendre des fonctions d'acquisition et de présentation de données et d'alarmes. Le système doit aussi présenter des fonctions d'enregistrement et de mémorisation des variables du procédé importantes pour la sûreté et la disponibilité, pour analyse ou compte-rendu, pour l'organisation exploitante ou les autorités externes.

Il convient de prévoir des fonctions de traitement de l'information pour aider la démarche intellectuelle des opérateurs par:

– une aide à la décision,
– une amélioration des capacités et des performances de surveillance.

Pour cela il convient d':

– assurer une haute disponibilité et fiabilité de l'information;
– utiliser l'information utile pour définir des actions;
– faciliter une bonne communication entre les personnels de la salle de commande;
– assurer l'enregistrement des transitoires et des accidents pour les analyser ainsi que l'accès aux données enregistrées;
– enregistrer les commandes passées par les opérateurs lorsque cela est possible;
– augmenter la quantité d'informations disponibles pour couvrir les données implicites.

La catégorisation des fonctions du système d'information doit être faite conformément à la CEI 61226.

Des exigences particulières sont fournies ci-dessous:

a) Information des opérateurs

   L'opérateur doit pouvoir avoir à tout instant, à l'aide des systèmes d'information, une compréhension globale de l'état de la centrale. Ceux-ci doivent permettre aux opérateurs d':

   – identifier tout risque courant ou potentiel sur la sûreté ou la disponibilité;
   – identifier les actions déclenchées par les systèmes automatiques:
   – analyser les causes d'une défaillance et suivre son évolution;
   – effectuer toutes les actions correctrices manuelles nécessaires.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

La base de conception des systèmes d'information, y compris l'instrumentation de mesure, doit prendre en compte leur importance pour la sûreté. Les fonctions de sûreté se rapportant à chaque système, leur importance pour permettre à l'opérateur d'effectuer les opérations correctes lors des événements d'exploitation prévus ou en conditions accidentelles, doivent être identifiées dans la base de conception et doivent être utilisées comme entrées pour choisir les méthodes de classement des systèmes de contrôle-commande.

b) Fonction d'information pour les experts n'appartenant pas aux équipes de conduite

Bien que la salle de commande soit le centre d'information et de commande de la centrale pour les opérateurs en fonctionnement normal et en conditions accidentelles, elle peut également être utilisée comme centre primaire pour diriger les étapes initiales des activités hors-site, en fonction des principes en vigueur chez l'exploitant ou dans le pays, pour le support des opérations d'urgence. Voir également le guide de sûreté NS-G-1.9 de l'AIEA.

Il est préférable d'installer ces experts dans une salle séparée et de les exclure de la salle de commande.

Les systèmes d'information peuvent être étendus pour fournir des informations à des installations support séparées, extérieures au site.

c) Enregistrement et impression

Un nombre suffisant d'enregistreurs et d'imprimantes doit être maintenu en salle de commande ou à côté, pour les variables analogiques et pour les signaux binaires, afin d'obtenir une information chronologique sur les performances et le comportement de la centrale.

Ceci étant nécessaire pour:

– disposer d'un historique des informations pour les opérateurs des autres postes en leurs donnant les évolutions à court et long termes;

– disposer d'informations d'exploitation générale pour la gestion de la centrale;

– effectuer des analyses à court et long termes du fonctionnement et des accidents.

Il est recommandé de réaliser un enregistrement automatique des commandes opérateur pour analyser les actions de conduite.

7.7.2.2 Acquisition et traitement des données

Les exigences fonctionnelles principales du système d'acquisition et de traitement des données sont les suivantes:

– les défaillances ne doivent pas conduire à des états non sûrs ou avoir pour conséquences des pertes économiques inacceptables pour l'exploitation de la centrale;

– les vitesses d'échantillonnage des données d'entrée, de pré–traitement et d'analyse, doivent satisfaire aux exigences opérationnelles concernant les vitesses d'évolution des paramètres;

– la vitesse de mise à jour des données doit être cohérente par rapport aux tâches opérateur;

– il ne doit pas y avoir de retard significatif lors du traitement des données de tranche ou des demandes opérateur et ceci même en présence de pic de charge;

– les modifications doivent être possibles durant toute la vie opérationnelle du système;

– des dispositions doivent être prises pour permettre à l'opérateur d'identifier rapidement les données affichées invalides.

De plus on a les exigences complémentaires suivantes.

Il est recommandé que le système d'acquisition et de traitement prenne en compte tous les aspects concernant les exigences d'opérabilité et de fiabilité, de maintenabilité, ainsi que les futures modifications de la centrale.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Pour cela, une part essentielle de la définition et l'identification du système d'acquisition et de traitement correspond à une analyse complète (par exemple analyse des tâches) qui prend en compte les performances du personnel de salle de commande. Une telle analyse permettra d'identifier les exigences portant sur les données, y compris la disponibilité des données nécessaires et leur validité.

Les systèmes d'acquisition et de traitement des données doit être complètement spécifié en ce qui concerne:

– la fréquence d'échantillonnage des données et la redondance;
– les pré-traitements et la vérification de la consistance;
– les analyses nécessaires pour les conditions qui sortent de l'ordinaire;
– les sorties nécessaires ainsi que leur forme, par exemple impression ou affichage à l'écran.

Le traitement des données brutes peut consommer une part importante du temps d'exécution des processeurs d'un système numérique centralisé. De la même façon, les tâches d'analyse et de sortie ou de présentation des données peuvent consommer du temps d'exécution. Il convient de faire une évaluation de la charge du système numérique en fonctionnement normal et en pic de charge, avant que celui-ci ne soit mis en service. Il est recommandé de confirmer cette évaluation par des essais adaptés sur le système opérationnel installé, pour démontrer la viabilité du système, avec le personnel d'exploitation, dans la gamme complète des conditions de fonctionnement. Il ne doit pas y avoir de retard notable lors du traitement et de la présentation des données de tranche, même lors des pics de charge. L'expérience montre que l'opérateur est perturbé si la réponse d'une fonction d'un système numérique d'information est retardée de plus d'1 s. Des temps de réponse plus longs sont acceptables dans certains cas, par exemple accès aux historiques de données ou aux données archivées, si un signal de retour indique que le traitement est en cours.

Bien que certains systèmes n'utilisent qu'un seul ordinateur pour traiter les données et produire de l'information, il convient d'utiliser des ordinateurs et des modules redondants pour garantir un service continu lorsqu'une défaillance unique, des plus probables, se produit.

7.7.2.3 Système d'affichage

Le système d'affichage doit être conçu comme l'interface homme-machine du système d'information, prenant en compte les caractéristiques et les capacités humaines.

L'affichage doit permettre aux opérateurs de:

– connaître les actions déclenchées par le système de protection et les autres systèmes automatiques, pour être capable de vérifier leur état et de réaliser les actions support;
– analyser les causes de perturbations et suivre leur évolution;
– réaliser toutes contre-actions manuelles nécessaires.

L'affichage doit permettre aux opérateurs d'identifier tous risques liés à la sûreté ou à la disponibilité.

Les exigences fonctionnelles principales du système d'affichage sont les suivantes:

– le système d'affichage en salle de commande doit couvrir les variables appropriées, conformément aux hypothèses de l'analyse de sûreté et aux besoins d'information de l'opérateur en fonctionnement normal et dans les situations accidentelles;
– la précision, l'étendue et l'échelle des affichages doivent être conformes aux hypothèses de l'analyse de sûreté et aux tâches opérateurs supportées;
– des afficheurs doivent être prévus pour indiquer les conditions d'inhibition ou celles délibérément non opérationnelles de la centrale et des auxiliaires;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– des afficheurs d'information relatifs à la sûreté doivent être convenablement localisés et identifiés de façon spécifique sur les panneaux de commande;

– le type des afficheurs doit être choisit en fonction de leur rôle;

– le système d'affichage doit présenter l'information et les alarmes qu'il convient de fournir dans le cadre d'une approche intégrée de l'affichage des conditions de la centrale.

En général, les écrans et moyens d'information sont utilisés. Des afficheurs dédiés, tels que des enregistreurs analogiques, des indicateurs digitaux, des verrines, les enregistreurs de tendance peuvent être nécessaires par exemple:

– pour les situations post-accidentelles, pour des raisons de qualification ou de diversité ou

– si certaines exigences de séparation physique des afficheurs doivent être satisfaites.

Il convient de prévoir un nombre suffisant d'imprimantes de façon à fournir des copies d'écran aux équipes en poste, ou bien des supports d'analyse et de discussion pour l'équipe ou encore des documents qui peuvent s'inscrire dans un cadre légal.

La CEI 61772 fournit des recommandations détaillées portant sur l'utilisation des écrans, pour celles relatives aux afficheurs dédiés se reporter à l'ISO 11064.

7.7.2.4 Alarmes

Les informations nécessaires pour surveiller la centrale en conditions de fonctionnement anormales doivent être disponibles en salle de commande principale.

Il est recommandé que le système d'alarme:

– affiche les informations d'alarmes, pour aider l'opérateur à comprendre la situation de défaut qui se développe;

– permette à l'opérateur de supprimer les informations non pertinentes mais garantisse que les informations pertinentes et importantes sont présentées à celui-ci de façon adaptée par rapport à ses capacités de compréhension;

– permette à l'opérateur de distinguer entre les alarmes pour lesquelles les actions correctrices ne sont pas terminées et les alarmes qui ne peuvent être annulées sans une intervention du service de maintenance;

– évite la surcharge d'information.

Il convient que le système d'alarme possède:

– des fonctions de traitement pour donner à l'opérateur l'information la plus représentative en présence de conditions anormales, et

– des fonctions d'affichage pour permettre à l'opérateur d'identifier facilement une alarme et sa gravité.

En outre, pour chaque alarme, un document de procédure, par exemple une fiche d'alarme ou une procédure de conduite, doit être prévu pour expliquer à l'opérateur les raisons probables de l'alarme et les actions correctrices qu'il a à mener.

Pour les exigences détaillées se reporter à la CEI 62241.

7.7.2.5 Fonction support de l'opérateur

Afin d'améliorer la sûreté, la disponibilité et l'opérabilité de la centrale, il convient de prévoir des fonctions support de l'opérateur telles que:

– des fonctions de surveillance et d'affichage des paramètres de sûreté, voir la CEI 60960;

– des fonctions diagnostiques pour la centrale;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– des fonctions pour guider l'opérateur en fonctionnement normal comme en situation post-accidentelle, par exemple des procédures événementielles ou reposant sur les symptômes;
– des fonctions pour réaliser les essais en puissance.

Il convient, autant que possible, d'intégrer de telles fonctions dans la conception d'ensemble de la salle de commande.

7.7.3 Fonctions de commande

Ce paragraphe traite des spécifications fonctionnelles relatives aux facteurs humains pour les commandes utilisées pour la conduite manuelle et pour la conduite en secours des commandes automatiques dans les situations normales et anormales. Cependant, les spécifications fonctionnelles des fonctions de commande réalisées par les systèmes d'I&C de la centrale, se situent hors du domaine de cette norme.

a) Considérations générales

Les commandes doivent être conçues pour faciliter la conduite et pour minimiser les erreurs opérateur.

Les commandes doivent être adaptées à l'utilisation de l'opérateur dans un environnement de salle de commande et s'harmoniser avec les caractéristiques ergonomiques du groupe d'utilisateurs prévu.

Les commandes doivent respecter les exigences suivantes:

– pour réduire les erreurs opérateur, il convient que les mouvements des commandes soient conformes aux stéréotypes de population et qu'ils soient compatibles avec les variables commandées;
– les commandes doivent prendre en compte l'information renvoyée pour la fonction sélectionnée et comprendre un affichage pour contrôler l'information renvoyée relative à l'état du composant commandé;
– le classement des fonctions de commande doit être fait en fonction de leur importance pour la sûreté, conformément à la CEI 61226.

b) Prévention des activations intempestives

Pour éviter un évènement provoqué par l'homme, l'action intempestive des commandes doit être minimisée à l'aide des moyens suivants:

– localisation des commandes dans un endroit adapté, pour éviter les activations intempestives lors d'un mouvement de commande;
– utilisation de structures de protection, telles que des barrières physiques, ou encastrement ou couvercle ou protections amovibles;
– mise en place d'une deuxième action de confirmation, par exemple avec relâchement d'un bouton poussoir ou avec une commande logiciel complémentaire;
– utilisation de signaux de verrouillage ou respectivement permissifs, avec une affectation adaptée des priorités;
– sélection correcte des caractéristiques physiques, telles que la taille, la pression ou la force de fonctionnement, la perception tactile, optique et/ou acoustique;
– toutes combinaisons des moyens précédents.

c) Technologie

Les commandes peuvent être des commandes logiciel, ou des commandes dédiées ou multiplexées et des combinaisons de celles-ci.

Il convient que les choix reposent sur des critères tels que:

– considérations sur la qualification et l'indépendance;
– vitesse d'accès demandée et fréquence d'utilisation;
– technologie disponible.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

La CEI 61227 fournit des recommandations détaillées sur le sujet.

7.8 Intégration des commandes-afficheurs

Les commandes et leurs afficheurs doivent être correctement intégrés pour permettre au personnel de la salle de commande d'assurer une conduite efficace de la centrale.

L'intégration des commandes-afficheurs doit être conforme à la méthode proposée pour la conduite de la centrale, comme indiqué dans les analyses faites en 6.2 et 6.6.

L'intégration des commandes-afficheurs doit respecter les principales exigences suivantes:

– il convient que les moyens de commande soient situés près des afficheurs associés. Il convient qu'une action sur une commande produise un changement compatible sur l'afficheur associé;
– le regroupement des commandes et de leurs afficheurs associés doit refléter le besoin d'atteindre les objectifs du système et il est recommandé qu'il soit consistent avec les hypothèses concernant le modèle mental des utilisateurs;
– l'organisation des commandes et des afficheurs doit refléter les relations cause/effet;
– l'organisation des commandes doit prendre en compte les stéréotypes de la population des utilisateurs;
– la forme des codages utilisés pour les afficheurs et leurs commandes associées doit être entièrement cohérente.

7.9 Systèmes de communication

7.9.1 Généralités

Des systèmes de communication doivent être prévus en salle de commande pour faciliter une conduite sûre et efficace de la centrale. Un soin particulier doit être pris à la conception des systèmes de communication utilisés pour communiquer avec le centre de crise en conditions anormales ou accidentelles.

La mise en place de systèmes de communication non-orale tel qu'un système de fac-similé ou des liaisons informatiques sont souhaitables, entre la salle de commande et les autres centres d'information pour améliorer la disponibilité et la sûreté.

7.9.2 Systèmes de communication orale

7.9.2.1 Communications internes au site

Un système téléphonique avec un nombre suffisant de postes doit être installé pour les communications générales dans les conditions de fonctionnement normal. Un poste au moins doit être installé en salle de commande. Chaque poste peut être connecté au système de téléphone public. Un système supplémentaire particulier doit être accessible en salle de commande, celui-ci n'est pas accessible à partir du réseau public, il possède un numéro d'appel d'urgence bien connu, indiqué sur tous les autres postes. Ce poste doit être utilisé pour transmettre uniquement des messages concernant des perturbations ou des accidents au personnel de la salle de commande.

Un système séparé, en câblage direct doit être installé aux endroits appropriés pour communiquer en conditions accidentelles avec les installations de conduite et les points de commande supplémentaires importants pour la sûreté. Le système doit permettre au personnel de la salle de commande de communiquer simultanément avec un seul ou un nombre choisi de postes. Le système doit aussi permettre au personnel de la salle de commande de communiquer avec la salle de commande d'une autre unité ou avec une salle de commande séparée sur le même site. Le système doit être alimenté par un système d'alimentation non interruptible. Des prises de postes téléphoniques doivent être prévues à

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

l'extérieur de la salle de commande si nécessaire et elles doivent être accessibles en conditions accidentelles. Le système peut être aussi étendu à un usage opérationnel.

Un système d'adresse publique doit être mis en place pour le personnel sur site, quelles que soient les conditions de fonctionnement de la centrale.

Pour joindre la salle de commande durant la maintenance, essai ou réparation, un système de communication par radio utilisant des émetteurs portables doit être mis en place, à moins que tous les lieux considérés puissent être joints de façon fiable à l'aide d'autres systèmes. Les aspects relatifs aux interférences liées aux fréquences radio doivent être pris en compte à la conception, pour le câblage, pour la localisation et pour les essais des systèmes d'I&C. Pour réduire ces interférences, la gamme de fréquences et le niveau maximum de sortie de ces émetteurs doivent être limités et spécifiés. Les zones où ces émetteurs ne doivent pas être utilisés, tels que les locaux contenant les matériels de contrôle-commande, doivent être identifiés.

7.9.2.2 Communications à l'extérieur du site

Il convient de mettre en place un système de communication privé pour les communications avec les représentants de l'exploitant à l'extérieur du site, les équipes gouvernementales d'urgence ou avec les institutions publiques. Certains numéros de poste et en particulier un en salle de commande, ne doivent pas être connus du public.

Un nombre minimum de connexions nécessaires avec le personnel et les organisations à l'extérieur du site doit être prévu. Les connexions importantes doivent être supportées par des systèmes redondants et diversifiés, par exemple un téléphone et une radio. Les connexions doivent être définies conformément à des exigences nationales, dans les cas suivant:

– pour l'appel du personnel d'astreinte de l'unité ou d'autres experts en situations accidentelles;
– pour les équipes de mesure des rayonnements qui réalisent des tâches importantes pour la sûreté à l'extérieur du site;
– pour les installations de lutte et de protection incendie;
– pour la station de police locale ouverte en permanence;
– pour les bureaux des services publics et gouvernementaux.

7.9.2.3 Dispositions

Les matériels de communication utilisés pour les communications relatives à la conduite ou pour les communications des opérateurs doivent être installés sur le lieu de travail des opérateurs.

La salle de commande principale doit aussi être conçue comme un centre de communications de la centrale en fonctionnement normal et lors des premières phases d'un accident. Les responsabilités et les besoins en communications particuliers à ces phases doivent être identifiés lors de l'analyse de tâches, et les matériels de communication situés en conséquence. Il est préférable de mettre les matériels pour communiquer avec l'extérieur du site sur un pupitre de communication particulier ou sur un panneau avec des postes sur les principaux pupitres et panneaux de commande.

7.9.3 Systèmes de communication non-orale

Les systèmes de communication non-orale suivants peuvent être mis en place en salle de commande principale:

– un système de télévision pour surveiller l'intérieur du bâtiment réacteur et la turbine, ce système peut être aussi utilisé en situations accidentelles;

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

– un système fac-similé qu'il convient de connecter aux centres de crise pour y envoyer les documents reflétant l'état de la centrale et les suggestions de l'exploitant lorsque des conditions d'urgence surviennent.

7.10 Autres exigences

7.10.1 Alimentations électriques

L'ensemble des sources de puissance alimentant la salle de commande doit avoir une fiabilité et une disponibilité satisfaisantes par rapport aux exigences portant sur les systèmes d'I&C, les systèmes de sûreté et les systèmes importants pour la sûreté. Les systèmes importants pour la sûreté dont la disponibilité permanente est requise en fonctionnement normal et en situations accidentelles, doivent être connectés à des alimentations électriques non interruptibles.

Pour plus d'exigences détaillées, voir la CEI 61225.

7.10.2 Qualification

Un programme de qualification cohérent avec l'ensemble des matériels de la centrale doit être mis en place pour confirmer l'aptitude des matériels importants pour la sûreté et des systèmes présents en salle de commande, à remplir de façon continue les exigences de performance de la conception de base (par exemple gamme, précision, réponse) requises par leurs fonctions, dans les conditions d'environnement susceptibles d'exister aux moments où on en a besoin. Le programme doit inclure un plan pour s'assurer que le matériel est qualifié pour la période considérée d'utilisation et effectuer des requalifications ou des remplacements en temps utile, si nécessaires.

Pour plus d'exigences détaillées, voir la CEI 60780 et la CEI 60980.

7.10.3 Maintenabilité

Les matériels doivent être conçus pour faciliter la surveillance et la maintenance, et en cas de défaillance, le diagnostique et la réparation ou le remplacement.

La contribution du temps de réparation à l'indisponibilité doit être évaluée à cette étape de la conception. Le temps moyen de réparation et la fréquence d'inspection doivent être spécifiés dans la base de conception de chaque système particulier. La connaissance des moyens de détection des défaillances survenues, par exemple test de l'alimentation électrique, doit faire partie de cette évaluation.

Les moyens prévus pour la maintenance du système doivent être conçus de telle sorte qu'ils n'entraînent aucun effet inacceptable sur la sûreté de la centrale.

7.10.4 Réparations

En ce qui concerne l'agencement des panneaux et la configuration des matériels, la salle de commande doit être conçue de telle sorte qu'il soit aisé de réparer les matériels et les systèmes dans cette salle de commande. La conception doit aussi couvrir les moyens de réparation et les pièces de rechange.

7.10.5 Testabilité

La salle de commande doit être conçue pour permettre de réaliser facilement des essais et des étalonnages, aux intervalles de temps requis pour chacune des fonctions nécessaires.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

8 Vérification et validation du système intégré de salle de commande

8.1 Généralités

La conception initiale d'un système intégré de salle de commande qui comprend l'équipe de salle de commande, l'interface homme-machine, les procédures de conduite, le programme de formation, doit se terminer par sa vérification et sa validation. Dans les paragraphes suivants, le processus et les critères généraux d'évaluation, de vérification et de validation sont spécifiés pour l'interface homme-machine. Pour les autres composants du système de salle de commande, c'est-à-dire la structure de l'équipe, les procédures de conduite et les programmes de formation, il convient de développer séparément les procédures d'évaluation et les critères ou bien de se référer aux normes nationales et aux guides internationaux approuvés disponibles (voir les guides de sûreté AIEA).

Pour plus d'exigences détaillées, voir la CEI 61771.

8.2 Vérification du système de salle de commande

8.2.1 Généralités

Les spécifications fonctionnelles du système de salle de commande doivent être vérifiées avant et pendant l'intégration du système de salle de commande détaillée pour montrer que ces spécifications satisfont aux critères et aux exigences fonctionnelles pertinentes.

8.2.2 Processus

Le processus développé pour la vérification doit inclure les phases de préparation, d'évaluation et de correction. A cette étape, l'évaluation du système de commande intégré doit inclure les procédures de conduite et le programme de formation qui ont été prévus séparément comme indiqué à la Figure 2.

8.2.3 Critères d'évaluation générale pour la vérification du système intégré

L'intégration du système de salle de commande proposé doit inclure de façon correcte toutes les spécifications fonctionnelles et toutes les autres exigences techniques.

8.3 Validation du système de salle de commande

8.3.1 Généralités

Avant et pendant la conception détaillée du système de salle de commande, on doit valider l'intégration de l'ensemble du système pour montrer qu'il peut atteindre les performances visées. En particulier, une attention spéciale doit être portée aux caractéristiques dynamiques du système proposé une fois intégré.

8.3.2 Processus

Le processus développé pour la validation doit comprendre les phases de préparation, d'évaluation et de correction.

La préparation est menée de façon semblable à celle concernant la répartition des fonctions (voir 6.5), mais l'expertise de conduite est particulièrement importante à cette étape.

Il convient de développer un modèle de salle de commande approprié permettant l'évaluation des caractéristiques dynamiques du système proposé. Pour un système dont la conception est notablement différente des systèmes classiques, l'utilisation d'un simulateur dynamique est nécessaire. Cependant d'autres choix, tels qu'une maquette à l'échelle 1 peuvent être adoptés lorsque la différence est mineure ou qu'une validation partielle peut être justifiée.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Il convient de réaliser plusieurs mesures de performance pour permettre une évaluation redondante. La cohérence qualitative et quantitative des mesures de performance interdépendantes doit être examinée pour confirmer les résultats d'évaluation.

Il convient d'essayer de concevoir des essais d'ambiance réalistes (par exemple, dispositions physiques, conditions d'ambiance telles que la température, l'humidité, l'éclairage, les bruits, etc.).

Il convient d'organiser le programme de validation pour qu'il utilise les essais de mise en service. Par exemple il convient d'utiliser les essais de mise en service pour les aspects qui ne peuvent être testés dans les phases précédentes, tels que l'évacuation de la salle de commande principale, ainsi que les aspects qui ont été identifiés comme nécessitant une évaluation ultérieure.

Les critères d'évaluation doivent être cohérents avec les règlements, normes, directives, recommandations applicables, etc.

8.3.3 Critères d'évaluation générale pour la validation du système intégré

Pour les exigences voir la CEI 61771.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

Annexe A
(informative)

Explication des concepts

A.1 Système salle de commande

Le système salle de commande est un système intégré constitué de l'interface homme-machine, du personnel de salle de commande, des procédures de conduite, du programme de formation, et des matériels associés et des installations (voir la Figure 1).

La centrales a deux objectifs opérationnels principaux (à savoir, maîtriser sa production d'électricité et prévenir les rejets radioactifs dans l'environnement). Un certain nombre d'objectifs fonctionnels doivent être satisfaits pour que les objectifs opérationnels soient atteints. La satisfaction de ces objectifs fonctionnels correspond au contrôle du procédé de la centrale en gérant l'utilisation des ressources de celle-ci. Il y a principalement deux façons de commander les systèmes de la centrale (à savoir les commandes automatiques et les commandes manuelles qui comprennent les commandes déportées et les commandes manuelles locales).

Les systèmes matériels support des commandes automatiques et des commandes manuelles déportées comprennent les systèmes de sûreté et de commande, qui font partie des systèmes d'I&C et ils comprennent les actionneurs, les capteurs et autres dispositifs matériels.

Lors du fonctionnement des commandes automatiques, la surveillance du déroulement de celui-ci, sur les affichages, la mise en œuvre de commandes manuelles ou de secours, de réinitialisation par le personnel de salle de commande sont nécessaires. La mise en œuvre de commandes manuelles déportées demande l'intervention du personnel de salle de commande sur des commandes et des affichages situés en salle de commande principale.

Les commandes et afficheurs, qui font aussi partie des systèmes d'I&C, sont en interface physique avec le personnel de la salle de commande, pour cela ils sont appelés interface homme-machine.

Les commandes locales manuelles sont lancées d'un endroit situé hors de la salle de commande principale par l'opérateur utilisant les installations de commande locales à la demande du personnel de salle de commande. Les instructions sont transmises au moyen de l'interface de communication.

En plus des commandes automatiques, des commandes manuelles et de la surveillance associée, le personnel de salle de commande doit traiter l'information par une démarche intellectuelle (par exemple en interprétant différentes valeurs lues, en élaborant des stratégies à base cognitive).

Il y a différents types de systèmes support de l'opérateur (par exemple: systèmes de diagnostique, systèmes d'aide à l'exploitation, synthétiseur de procédures) qui sont destinés à accompagner la démarche intellectuelle. Le personnel de salle de commande peut s'interfacer avec ceux-ci de différentes façons – simple recherche unidirectionnelle d'information jusqu'aux affichages interactifs liés aux démarches intellectuelles au moyen d'appareils appropriés. Le système support de l'opérateur est une interface homme-machine.

La communication entre le personnel de la centrale et l'équipe de direction située à l'extérieur de la centrale peut s'établir au travers de l'interface de communication.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

A.2 Des hommes et des machines

Assigner des fonctions à l'homme signifie que celles-ci seront réalisées au travers de commandes manuelles, de surveillance, de démarches intellectuelles ou de combinaisons de ces moyens. Assigner des fonctions à la machine signifie que celles-ci seront réalisées par des automatismes. Ainsi, homme en termes fonctionnels signifie personnel de salle de commande et machine signifie automatismes (Tableau A.1).

Le terme machine couvre un certain nombre d'entités matériel qui inclut les systèmes d'I&C et les systèmes support de l'opérateur. Il convient de noter que le système de commande manuel, les commandes et les afficheurs qui font partie du système de contrôle commande permettent au personnel de salle de commande de réaliser les fonctions qui lui sont assignées.

Tableau A.1 – Hommes et machines dans le domaine fonctionnel et le domaine physique

<table>
<tr><th colspan="2">Domaine fonctionnel</th><th colspan="2">Domaine physique</th></tr>
<tr><td>Fonctions affectées à:</td><td>Fonctions réalisées par:</td><td>Machine (matériel)</td><td>Homme</td></tr>
<tr><td>L'homme</td><td>Démarche intellectuelle
Surveillance (associé avec les commandes manuelles et auto.)
Commandes manuelles (y compris secours et commandes des automatismes)</td><td>SSO
Afficheurs
Commandes
Système de commandes manuelles
Interface homme machine
Systèmes d'I&C</td><td>Equipe de conduite</td></tr>
<tr><td>La machine</td><td>Automatismes</td><td>Système de commande automatique</td><td></td></tr>
</table>

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch

LICENSED TO MECON Limited. - RANCHI/BANGALORE
FOR INTERNAL USE AT THIS LOCATION ONLY, SUPPLIED BY BOOK SUPPLY BUREAU.