

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC
964**

Première édition
First edition
1989-03

**Conception des salles de commande
des centrales nucléaires de puissance**

**Design for control rooms
of nuclear power plants**



Numéro de référence
Reference number
CEI/IEC 964: 1989

Validité de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique.

Des renseignements relatifs à la date de reconfirmation de la publication sont disponibles auprès du Bureau Central de la CEI.

Les renseignements relatifs à ces révisions, à l'établissement des éditions révisées et aux amendements peuvent être obtenus auprès des Comités nationaux de la CEI et dans les documents ci-dessous:

- **Bulletin de la CEI**
- **Annuaire de la CEI**
Publié annuellement
- **Catalogue des publications de la CEI**
Publié annuellement et mis à jour régulièrement

Terminologie

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 50: *Vocabulaire Electrotechnique International* (VEI), qui se présente sous forme de chapitres séparés traitant chacun d'un sujet défini. Des détails complets sur le VEI peuvent être obtenus sur demande. Voir également le dictionnaire multilingue de la CEI.

Les termes et définitions figurant dans la présente publication ont été soit tirés du VEI, soit spécifiquement approuvés aux fins de cette publication.

Symboles graphiques et littéraux

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera:

- la CEI 27: *Symboles littéraux à utiliser en électrotechnique*;
- la CEI 417: *Symboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles*;
- la CEI 617: *Symboles graphiques pour schémas*;

et pour les appareils électromédicaux,

- la CEI 878: *Symboles graphiques pour équipements électriques en pratique médicale*.

Les symboles et signes contenus dans la présente publication ont été soit tirés de la CEI 27, de la CEI 417, de la CEI 617 et/ou de la CEI 878, soit spécifiquement approuvés aux fins de cette publication.

Publications de la CEI établies par le même comité d'études

L'attention du lecteur est attirée sur les listes figurant à la fin de cette publication, qui énumèrent les publications de la CEI préparées par le comité d'études qui a établi la présente publication.

Validity of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information relating to the date of the reconfirmation of the publication is available from the IEC Central Office.

Information on the revision work, the issue of revised editions and amendments may be obtained from IEC National Committees and from the following IEC sources:

- **IEC Bulletin**
- **IEC Yearbook**
Published yearly
- **Catalogue of IEC publications**
Published yearly with regular updates

Terminology

For general terminology, readers are referred to IEC 50: *International Electrotechnical Vocabulary* (IEV), which is issued in the form of separate chapters each dealing with a specific field. Full details of the IEV will be supplied on request. See also the IEC Multilingual Dictionary.

The terms and definitions contained in the present publication have either been taken from the IEV or have been specifically approved for the purpose of this publication.

Graphical and letter symbols

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications:

- IEC 27: *Letter symbols to be used in electrical technology*;
- IEC 417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets*;
- IEC 617: *Graphical symbols for diagrams*;

and for medical electrical equipment,

- IEC 878: *Graphical symbols for electromedical equipment in medical practice*.

The symbols and signs contained in the present publication have either been taken from IEC 27, IEC 417, IEC 617 and/or IEC 878, or have been specifically approved for the purpose of this publication.

IEC publications prepared by the same technical committee

The attention of readers is drawn to the end pages of this publication which list the IEC publications issued by the technical committee which has prepared the present publication.

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC
964**

Première édition
First edition
1989-03

**Conception des salles de commande
des centrales nucléaires de puissance**

**Design for control rooms
of nuclear power plants**

© CEI 1989 Droits de reproduction réservés — Copyright - all rights reserved

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 l'éditeur.

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 the publisher

Bureau central de la Commission Electrotechnique Internationale 3, rue de Varembe Genève Suisse



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

XB

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

	Pages
AVANT-PROPOS	4
Articles	
1 Domaine d'application et but de la norme	6
1.1 Domaine d'application	6
1.2 But	6
1.3 Application de la présente norme	6
1.4 Définitions	6
1.5 Utilisation de la présente norme	14
2 Principes de conception pour la salle de commande principale	16
2.1 Objectifs principaux de la salle de commande principale	16
2.2 Objectifs de la conception fonctionnelle de la salle de commande principale	16
2.3 Principes de sûreté	16
2.4 Principes de disponibilité	16
2.5 Principes d'ingénierie des facteurs humains	18
2.6 Principes de conduite de l'exploitant	18
2.7 Relations avec les autres centres de contrôle et de gestion	18
3 Conception fonctionnelle de la salle de commande principale	20
3.1 Analyse fonctionnelle	20
3.2 Répartition des fonctions	22
3.3 Vérification de la répartition des fonctions	24
3.4 Validation de la répartition des fonctions	26
3.5 Analyse du travail	26
4 Spécifications fonctionnelles de conception	28
4.1 Nécessité d'une base de données sur les caractéristiques et capacités humaines	28
4.2 Localisation, environnement et protection	28
4.3 Dimensions et configuration	30
4.4 Agencement des panneaux	32
4.5 Aide à la localisation	32
4.6 Système d'information	34
4.7 Commandes	40
4.8 Intégration commandes-afficheurs	42
4.9 Systèmes de communication	42
4.10 Autres exigences	44
5 Vérification et validation du système intégré de salle de commande	48
5.1 Vérification du système de salle de commande	48
5.2 Validation du système de salle de commande	50
FIGURES	56
ANNEXE A - Guide de conception des salles de commande	60

CONTENTS

	Page
FOREWORD	5
Clause	
1 Scope and purpose of the standard	7
1.1 Scope	7
1.2 Purpose	7
1.3 Application of this standard	7
1.4 Definitions	7
1.5 Standard use	15
2 Design principles for the main control room	17
2.1 Main objectives of the main control room	17
2.2 Functional design objectives of the main control room	17
2.3 Safety principles	17
2.4 Availability principles	17
2.5 Human factors engineering principles	19
2.6 Utility operating principles	19
2.7 Relationship with other control and management centers	19
3 Functional design of the main control room	21
3.1 Function analysis	21
3.2 Assignment of functions	23
3.3 Verification of function assignment	25
3.4 Validation of functional assignment	27
3.5 Job analysis	27
4 Functional design specification	29
4.1 Provision of data base on human capabilities and characteristics	29
4.2 Location, environment and protection	29
4.3 Space and configuration	31
4.4 Panel layout	33
4.5 Location aids	33
4.6 Information system	35
4.7 Controls	41
4.8 Control-display integration	43
4.9 Communication system	43
4.10 Other requirements	45
5 Verification and validation of the integrated control room system	49
5.1 Control room system verification	49
5.2 Control room system validation	51
FIGURES	57
APPENDIX A - Design guide for control rooms	61

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CONCEPTION DES SALLES DE COMMANDE DES CENTRALES NUCLÉAIRES DE PUISSANCE

AVANT-PROPOS

- 1) Les décisions ou accords officiels de la CEI en ce qui concerne les questions techniques, préparés par des Comités d'Etudes où sont représentés tous les Comités nationaux s'intéressant à ces questions, expriment dans la plus grande mesure possible un accord international sur les sujets examinés.
- 2) Ces décisions constituent des recommandations internationales et sont agréées comme telles par les Comités nationaux.
- 3) Dans le but d'encourager l'unification internationale, la CEI exprime le vœu que tous les Comités nationaux adoptent dans leurs règles nationales le texte de la recommandation de la CEI, dans la mesure où les conditions nationales le permettent. Toute divergence entre la recommandation de la CEI et la règle nationale correspondante doit, dans la mesure du possible, être indiquée en termes clairs dans cette dernière.

La présente norme a été établie par le Sous-Comité 45A: Instrumentation des réacteurs, du Comité d'Etudes n° 45 de la CEI: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

Règle des Six Mois	Rapport de vote
45A(BC)107	45A(BC)112

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

La publication suivante de la CEI est citée dans la présente norme:

Publication n° 231 (1967): Principes généraux de l'instrumentation des réacteurs nucléaires.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DESIGN FOR CONTROL ROOMS OF NUCLEAR POWER PLANTS

FOREWORD

- 1) The formal decisions or agreements of the IEC on technical matters, prepared by Technical Committees on which all the National Committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subjects dealt with.
- 2) They have the form of recommendations for international use and they are accepted by the National Committees in that sense.
- 3) In order to promote international unification, the IEC expresses the wish that all National Committees should adopt the text of the IEC recommendation for their national rules in so far as national conditions will permit. Any divergence between the IEC recommendation and the corresponding national rules should, as far as possible, be clearly indicated in the latter.

This standard has been prepared by Sub-Committee 45A: Reactor instrumentation, of IEC Technical Committee No. 45: Nuclear instrumentation.

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

Six Months' Rule	Report on Voting
45A(CO)107	45A(CO)112

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

The following IEC publication is quoted in this standard:

Publication No. 231 (1967): General principles of nuclear reactor instrumentation.

CONCEPTION DES SALLES DE COMMANDE DES CENTRALES NUCLÉAIRES DE PUISSANCE

1 Domaine d'application et but de la norme

1.1 *Domaine d'application*

La présente norme établit les exigences en matière d'interface homme/machine dans 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'ingénierie humaine tels qu'ils s'appliquent à une interface homme/machine pendant les situations normales et anormales de la centrale.

Un guide de conception est donné dans l'annexe A.

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 et pour les installations de traitement des effluents radioactifs. La conception détaillée des matériels ne fait pas partie du domaine d'application de cette norme.

1.2 *But*

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'interfaces 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.

1.3 *Application de la présente norme*

Cette norme s'applique aux salles de commande de conception nouvelle dont la conception débutera après sa publication. Si l'on désire l'appliquer aux salles de commande existantes ou en projet, une attention spéciale doit être portée au fait qu'elle prend en compte des facteurs tels que le niveau d'automatisation qui peuvent ne pas s'appliquer à des centrales plus anciennes.

1.4 *Définitions*

Les définitions suivantes sont applicables dans cette norme. Pour les autres termes, se reporter à la terminologie générale définie dans la CEI 231 (et ses compléments) et dans le programme NUSS de l'AIEA, tels les Guides de sûreté 50-SG-D3 et D8.

Alarmes

Signaux donnés par des verrines ou d'autres systèmes d'affichage pour alerter l'opérateur de défauts et d'évolutions hors tolérance des centrales et des matériels dans les conditions de fonctionnement de la centrale, et qui requièrent une action de sa part.

DESIGN FOR CONTROL ROOMS OF NUCLEAR POWER PLANTS

1 Scope and purpose of the standard

1.1 Scope

This standard establishes requirements for the man/machine interface in the main control rooms of nuclear power plants.

The standard also establishes requirements for selection of functions, design considerations and organization of the man/machine interface and procedures which shall be used systematically to verify and validate the functional design.

These requirements reflect the application of human engineering principles as they apply to the man/machine interface during normal and abnormal plant conditions.

Some design guidance is given in the Appendix A.

This standard does not cover special purpose or normally unattended control systems, 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.

1.2 Purpose

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 man-machine interface, constituents of the control room system.

1.3 Application of this standard

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 or design, special caution must be exercised as it assumes factors such as automation level that may not apply to older plants.

1.4 Definitions

The following definitions are intended for use in this standard. For other terms, refer to the general terminology defined in IEC 231 (and its supplements) and in IAEA NUSS programme, such as Safety guides 50-SG-D3 and D8.

Alarms

Signals given by annunciators or other display systems to alert the operator to plant and equipment faults and out-of tolerance changes in plant conditions requiring action by the operator.

Système d'alerte sonore

Système déclenchant une alerte sonore lors de situations anormales telles qu'un incendie, ou nécessitant l'évacuation de l'enceinte de confinement ou d'autres bâtiments.

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.

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 (voir A.1.4.1).

Equipe de salle de commande

Personnel stationnant en salle de commande, dont la responsabilité est d'atteindre les objectifs opérationnels de la centrale en la conduisant au travers d'interfaces "homme/machine". L'équipe de salle de commande comprend spécifiquement des opérateurs de supervision et des opérateurs qui manipulent effectivement les commandes; elle peut également inclure le personnel d'exploitation et les experts autorisés à être présents en salle de commande, par exemple pendant de longues séquences d'événements.

Commandes

Appareils utilisés par l'opérateur pour envoyer les signaux de commande aux systèmes de contrôle-commande et aux dispositifs de la centrale.

Système de communication

Installations, matériels, appareils, etc., qui permettent un échange d'informations entre l'équipe de conduite et l'équipe de direction, des opérateurs en local, et d'autres personnels de la centrale stationnant à l'extérieur des installations de la salle de commande.

Afficheurs

Appareils utilisés pour surveiller les conditions de fonctionnement et l'état de la centrale, par exemple l'état du processus, l'état des matériels, etc.

Ergonomie

Etude de la psychologie et des capacités humaines, dans l'environnement du travail et en fonction du matériel utilisé par le travailleur.

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.

Fonction

Activité ou rôle rempli par l'homme ou par des systèmes automatiques.

Audible warning systems

Systems giving audible warning of fault situations such as fire or the need for evacuation of containment or other buildings.

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.

Control room system

An integration of the man/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 (see A.1.4.1).

Control room staff

A group of plant personnel stationed in the control room, which is responsible for achieving the plant operational goals by controlling plant through man/machine interfaces. Typically, the control room staff consists of supervisory operators, and operators who actually manipulate controls but also may include those staff members and experts which are authorized to be present in the control room, e.g. during long lasting event sequences.

Controls

Devices which the operator uses to send demand signals to control systems and plant items.

Communication system

Facilities, equipment, devices, etc., which enable information exchange between the operating and managerial staff, local operators, and other plant personnel stationed outside the control room facilities.

Displays

Devices used for monitoring plant conditions and status, e.g. process status, equipment status, etc.

Ergonomics

The study of human capability and psychology in relation to the working environment and the equipment operated by the worker.

Format (Display format)

A pictorial display of information on visual display unit (VDU) such as message text, digital presentation, symbols, mimics, bar-chart, trend graphs, pointers, multi-angular presentation.

Function

An activity or role performed by man or automated systems.

Analyse fonctionnelle

Examen des objectifs fonctionnels d'un système compte tenu des capacités humaines, de la technologie et d'autres ressources, pour fournir la base de détermination pour l'affectation et l'exécution de la fonction.

Objectif fonctionnel

Objectif de performances qui doivent être satisfaites pour remplir la fonction correspondante.

Structure hiérarchisée d'objectifs

Relation entre un objectif fonctionnel et des sous-objectifs fonctionnels structurés dans un ordre hiérarchique.

Démarche intellectuelle

Démarche d'un homme pour traiter et/ou interpréter une information afin d'obtenir une information condensée et abstraite.

Ingénierie des facteurs humains

Domaine de connaissances relatif à l'étendue et aux limites des performances humaines en matière de conception des machines, de travail et d'autres modifications dans l'environnement physique de l'homme.

Erreur de conception

Constat, à partir de quelques tests, de l'inadaptation de la conception d'un système aux rôles et capacités d'un opérateur humain.

Système de contrôle-commande

Ensemble des matériels de commande automatique et manuelle, composé des systèmes d'instrumentation, de commande et d'information.

Travail

Ensemble de tâches liées opérationnellement. Les tâches à l'intérieur d'un travail doivent en principe être cohérentes en regard de la compétence, des connaissances et des responsabilités requises de l'opérateur.

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.

Points de commande locaux (ou installations)

Points (ou installations) situés à l'extérieur de la salle de commande d'où des opérateurs en local remplissent des activités de commande.

Opérateur local

Membre de l'équipe de conduite qui remplit des tâches à l'extérieur de la salle de commande.

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.

Functional goal

The performance objectives that shall be satisfied to achieve the corresponding function.

Hierarchical goal structure

Relationship between a functional goal and sub-functional goals structured in a hierarchical order.

High-level mental processing

An act of man to process and/or interpret information to obtain reduced, abstract information.

Human factors engineering

The area of knowledge dealing with the capabilities and limitations of human performance in relation to the design of machines, jobs, and other modifications of the human's physical environment.

Human engineering discrepancy

A departure, from some benchmark, of system design suitability for the roles and capabilities of the human operator.

I & C system

Instrumentation and control system. A hardware implementation of automatic and manual controls, which consists of instrumentation, control and information systems.

Job

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

Job analysis

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

Local control points (or facilities)

Points (or facilities) located outside the control room where local operators perform control activities.

Local operators

The operating staff who perform tasks outside the control room.

Machine

Matériel tel que appareil, équipement ou système de contrôle-commande (voir tableau A.1 et A.1.4.2).

Interface homme/machine

Interface entre l'équipe de conduite d'une part, les systèmes d'instrumentation et de contrôle-commande et les calculateurs reliés à la centrale d'autre part. Elle inclut les afficheurs, les commandes et l'interface "système support de l'opérateur".

Equipe de conduite

Personnel de la centrale en travail posté pour la conduite de la centrale. L'équipe de conduite comprend l'équipe de la salle de contrôle, les ingénieurs de la maintenance, etc.

Procédures de conduite

Ensemble de documents spécifiant les tâches de conduite qu'il est nécessaire de remplir pour atteindre les objectifs fonctionnels.

Interaction de l'opérateur

Relations entre l'opérateur et le système de contrôle-commande. De façon spécifique, affichage de l'état de la centrale par le système de contrôle-commande, et actions correspondantes de l'opérateur.

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.

Eléments de dimensionnement

Eléments caractéristiques quantitatifs des tâches qui garantissent le respect des objectifs fonctionnels.

Système de sonorisation

Système de haut-parleurs pour appeler des personnes sur le site.

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 de radioactivité dans l'environnement.

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.

Machine

Hardware such as devices, items of equipments and/or I & C systems (see table A.1 and A.1.4.2).

Man/machine interface

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

Operating staff

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

Operating procedures

A set of documents specifying operational tasks it is necessary to perform to achieve functional goals.

Operator interaction

Interrelation between operator and I & C system. Specifically, display of plant status by I & C system and corresponding operator action.

Operator Support System (OSS)

A system or systems supporting the high-level mental information processing tasks assigned to the control room staff.

Performance requirements

Quantitative requirements specifying performance of tasks which ensure the achievement of functional goals.

Public address-system

Loudspeaker system to call persons on locations in the plant.

Plant operational goals

Ultimate purposes of plant design, i.e. controlled generation of electricity and limitation of release of radioactivity to the environment.

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.

Analyse des tâches

Décomposition des tâches d'un opérateur, pour spécifier les activités humaines mises en jeu, et leurs relations fonctionnelles et temporelles.

Tâches

Actions remplies soit par un homme, soit par une machine pour atteindre un objectif fonctionnel.

Programme de formation

Programme conçu pour former l'équipe de salle de commande de telle sorte qu'elle puisse acquérir l'habileté et les connaissances nécessaires aux activités de conduite.

Validation

Tests et évaluation pour déterminer si la solution à un problème est en accord avec les exigences fonctionnelles, de performances et d'interfaces.

Vérification

Processus pour déterminer si les composants respectent les exigences spécifiées. Dans ce contexte, la vérification implique un pointage de chacun des composants individuels du système de salle de commande en regard des critères d'ingénierie humaine et de la centrale, et des exigences fonctionnelles et de conduite.

Unité de visualisation (VDU)

Type d'affichage incorporant un écran pour présenter des images pilotées par ordinateur, par exemple un tube à rayons cathodiques, un afficheur à plasma.

1.5 Utilisation de la présente norme

Ce paragraphe a pour but d'orienter l'utilisateur dans l'organisation et la focalisation de cette norme. La figure 1 montre une vue d'ensemble du système de 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. Les constituants de ce système sont l'équipe de salle de commande, l'interface homme/machine, les procédures de conduite et les programmes de formation.

L'objet premier de cette norme est la création 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, les procédures de conduite et le programme de formation, mais ne fournit pas de méthodologie détaillée pour ce développement. Les relations entre les différents articles et paragraphes de cette norme apparaissent à la figure 2.

Après le domaine d'application et les spécifications sur les principes de base de conception, la figure 2 fait apparaître que le processus de conception inclut l'analyse fonctionnelle, l'affectation et la vérification des fonctions et la validation du concept étudié. Les spécifications fonctionnelles détaillées sont établies comme le fait apparaître la partie droite de la figure 2.

A partir de ces spécifications, la conception détaillée, les procédures de conduite et le programme de formation sont établis. Finalement, les constituants du système résultant sont vérifiés et le système intégré de salle de commande validé.

L'annexe A est fournie comme guide au lecteur. Cette annexe inclut des paragraphes didactiques et des informations complémentaires avec quelques exemples.

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.

Tasks

Actions performed by either man or machine for the accomplishment of a functional goal.

Training programme

A programme which is designed to train the control room staff so that they can acquire skill and knowledge necessary for operational activities.

Validation

The test and evaluation to determine that a problem solution complies with functional, performance and interface requirements.

Verification

The process of determining whether components meet the specified requirements. In this context, verification implies a check of individual components of the control room system against plant engineering criteria, human engineering criteria and operating and functional requirements.

Visual Display Unit (VDU)

A type of display incorporating a screen for presenting computer-driven images, e.g. cathode-ray tube, plasma display.

1.5 Standard use

This sub-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. Constituents of this system are the control room staff, the man/machine interface, the operating procedures, and the training programme.

The focus of this standard is the establishment of the man/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 relationships of various clauses and sub-clauses of this standard are shown in Figure 2.

After the scope, statements and specifications of design principles, the design process is shown in the figure to include function analysis, function assignment, function verification and design concept validation. Then, the detailed functional specifications are developed as shown on the right-hand side of 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.

Appendix A is provided as a readers guide. The appendix includes tutorial sub-clauses and supplementary information for the detailed procedures and specifications.

2 Principes de conception pour la salle de commande principale

2.1 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. La salle de commande fournit à l'équipe de salle de commande au travers d'une interface homme/machine et des matériels et informations associés, par exemple l'interface de communication, les éléments nécessaires pour atteindre les objectifs de conduite de la centrale. En outre, elle fournit un environnement dans lequel l'équipe de salle de commande est en mesure de remplir ses tâches sans risque physique, ni tension excessive, ni inconfort.

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

Les principaux objectifs de conception de la salle de commande sont de fournir aux opérateurs des informations précises, complètes et dans les délais, en regard du statut fonctionnel des systèmes et matériels de la centrale.

La conception doit permettre, pour tous les états opérationnels, y compris le rechargement du combustible, et les conditions accidentelles, d'optimiser les tâches, de minimiser la charge de travail requise pour surveiller et conduire la centrale et de fournir les informations nécessaires à d'autres installations extérieures à la salle de commande.

La conception de la salle de commande doit conduire à une répartition optimale des fonctions, en vue d'une utilisation maximale des capacités de l'opérateur et du système.

Un objectif supplémentaire dans la conception de la salle de commande est de réaliser efficacement la mise en service de l'installation et de permettre des modifications et la maintenance.

2.3 Principes de sûreté

La salle de commande doit être conçue de façon à permettre à la centrale nucléaire de puissance d'être conduite de façon sûre dans tous ses états opérationnels et de la ramener dans un état sûr après l'apparition de conditions accidentelles. Ainsi, les événements de dimensionnement sont à prendre en considération dans la conception de la salle de commande.

Les matériels dans la salle de commande doivent en principe être conçus, autant que possible, de telle sorte que des ordres de commande manuelle non sûrs ne puissent être émis, par exemple par l'utilisation d'un verrouillage logique dépendant de l'état de la centrale.

On doit également prendre en compte la nécessité d'une séparation fonctionnelle et physique, là où les systèmes de sûreté et les systèmes "de non-sûreté" sont disposés à proximité l'un de l'autre.

Des mesures appropriées doivent être prises pour la sauvegarde des occupants de la salle de commande contre des risques potentiels tels que des accès non autorisés, des rayonnements inattendus résultant de conditions accidentelles, des gaz toxiques ou toute conséquence d'incendie, qui pourraient nuire aux actions nécessaires des opérateurs.

Il doit y avoir suffisamment d'accès pour permettre à l'équipe de salle de commande de quitter ou atteindre la salle de commande, ou gagner d'autres points de commande lors de situations d'urgence.

2.4 Principes de disponibilité

Dans le souci de maximiser le facteur de puissance de la centrale afin d'assurer un retour satisfaisant des investissements financiers dans une centrale nucléaire de puissance, des dispositions doivent être prises lors de la conception de la salle de commande pour:

2 Design principles for the main control room

2.1 Main objectives of the main control room

A control room is provided from which the nuclear power plant can be operated safely and efficiently in all plant operational states and accident conditions. The control room provides the control room staff with the man/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 is able to perform their tasks without discomfort, excessive stress, or physical hazard.

2.2 Functional design objectives of the main control room

The principal objectives of the control room design are to provide the operator with accurate, complete, 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, optimize the tasks and minimize the workload required to monitor and control the plant, 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.

2.3 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 design basis events are to be considered in the design of the control room.

Equipment controlled from the control room should 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 safety and non-safety systems are brought into close proximity.

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.

2.4 Availability principles

With a view to maximizing the plant capacity factor to assure a satisfactory return on the financial investment in nuclear power plant, consideration shall be given in the control room design to:

- faciliter les conduites planifiées;
- minimiser l'occurrence de toute réduction de puissance non désirée ou d'arrêt d'urgence, causée par des prises de décisions ou des actions erronées des opérateurs ou par des défaillances locales associées à des mauvais fonctionnements ou à des défauts dans le système de contrôle-commande.

Les spécifications de conception en liaison avec la disponibilité ne doivent pas être en contradiction avec les principes de sûreté adoptés.

2.5 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 viser à obtenir pour la centrale, une sûreté et une disponibilité maximales, le concepteur doit porter une attention particulière aux facteurs humains, portant sur les caractéristiques humaines du personnel au regard de leurs capacités et limitations anthropométriques, physiologiques, de perception cognitive et de motricité.

2.6 Principes de conduite de l'exploitant

Comme partie intégrante de la salle de commande et de la philosophie de la conduite, on trouve l'encadrement et la formation des opérateurs. Pour maximiser la sûreté et l'efficacité de la conduite d'une centrale nucléaire de puissance, la salle de commande doit être pilotée avec un nombre suffisant de professionnels qualifiés.

Ils doivent être techniquement formés à la conduite en salle de commande et éduqués aux principes d'ingénierie relatifs à la conduite et à la sûreté des centrales nucléaires de puissance et avoir une connaissance approfondie de la localisation et des performances fonctionnelles des composants et sous-systèmes de la centrale.

Certaines tâches remplies par des opérateurs hors de la salle de commande, mettant en jeu le fonctionnement des matériels de la centrale, doivent être administrativement commandées et surveillées depuis la salle de commande.

Pour assurer la qualité de la conduite de la centrale nucléaire de puissance, l'exploitant doit en principe considérer les facteurs suivants dans la constitution de l'équipe de salle de commande:

- sélection du personnel et exigences de qualification;
- exigence d'une formation initiale et de recyclages pour les conditions normales, anormales et accidentelles;
- reformation périodique aux habitudes de conduite et opportunité d'accroître ses connaissances dans les principes d'ingénierie;
- motivation de l'équipe de salle de commande et de chaque individu durant la conduite normale et lors d'incidents.

2.7 Relations avec les autres centres de contrôle et de gestion

Pour aider le personnel en salle de commande à réagir à des conditions anormales de conduite, des centres de crises peuvent être disponibles pour être opérationnels durant des situations critiques.

Des points supplémentaires de conduite (panneau de repli) peuvent aussi être prévus.

Des matériels doivent être prévus pour des échanges d'informations avec ces installations. Ces matériels doivent effectuer ces fonctions indépendamment des autres moyens en salle de commande.

- facilitating planned operations;
- 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.

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

2.5 *Human factors engineering principles*

In order to provide an optimal assignment of functions which assures maximum utilization of the capabilities of man 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 anthropometric, perceptual, cognitive, physiological and motor response capabilities and limitations.

2.6 *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.

They 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 assure 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.

2.7 *Relationship with other control and management centers*

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

Supplementary control points may also be provided.

Equipment shall be provided for information exchange to these points and facilities. The equipment shall operate independently of the other equipment in the control room.

3 Conception fonctionnelle de la salle de commande principale

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

- analyse fonctionnelle;
- répartition des fonctions;
- vérification et validation des répartitions de fonctions;
- analyse du travail.

3.1 Analyse fonctionnelle

Afin d'atteindre les objectifs concrets de 2.1, en accord avec les principes de 2.2 à 2.7, on doit analyser les fonctions à remplir par une centrale nucléaire de puissance.

Cette analyse doit en principe identifier sous forme d'une structure hiérarchisée les objectifs à atteindre lors de la conception de la salle de commande pour tous les états de fonctionnement et les conditions accidentelles, les principaux objectifs étant la production d'électricité et la minimisation des rejets. Ces objectifs pourront être décomposés ultérieurement en sous-objectifs et utilisés dans le processus de décision du projet (voir A.3.1).

3.1.1 Identification des fonctions

En ce qui concerne les structures hiérarchisées d'objectifs, toutes les fonctions de la centrale associées à ces objectifs doivent en principe être identifiées et documentées. Une méthode pour identifier ces objectifs est donnée en A.3.1.1. Dans la définition des fonctions, l'analyse doit en principe être complète et prendre en compte les interactions entre la salle de commande et les installations et systèmes extérieurs à la salle de commande.

3.1.2 Flux d'informations et exigences de traitement

On doit mener une analyse pour déterminer le flux d'informations de base pour la conduite et les traitements requis pour accomplir les fonctions de conduite de la centrale, y compris les prises de décisions et les actions. Cette analyse est décrite en A.3.1.2.

Lors de l'identification des flux d'informations et des exigences de traitement, il est recommandé de prendre en compte plusieurs événements représentatifs de base de dimensionnement, de même que toutes les situations normales.

Les événements suivants doivent en principe être inclus:

- événement exigeant des actions jugées subjectivement être difficiles en termes de complexité de commande ou d'interprétation de l'information, de rapidité de commande, etc.;
- événement exigeant une grande garantie dans la réponse correcte de l'opérateur, par exemple certaines conditions accidentelles;
- événement important, en termes d'analyse probabiliste de risques;
- événement pour lequel le déclenchement de la centrale est hautement probable à moins qu'une action corrective soit effectuée à temps;
- événement dont le taux d'occurrence est élevé.

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

3 Functional design of the main control room

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 four steps as shown in Figure 2:

- functional analysis;
- functional assignment;
- verification and validation of function assignment;
- job analysis.

3.1 *Function analysis*

An analysis of the functions to be performed by nuclear power plant to achieve the actual objective of 2.1 consistent with principles of 2.2 to 2.7 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 (see Appendix A.3.1).

3.1.1 *Identification of functions*

With respect to hierarchical goal structures, all plant functions associated with these goals of the control room should be identified and documented. A means for identifying these goals is given in A.3.1.1. In defining functions the analysis should be comprehensive and take into account the interactions between the control room and facilities and systems outside the control room.

3.1.2 *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 A.3.1.2.

When identifying the information flow and processing requirements, the designer should use several representative design basis events as well as all normal operations.

The following events should be included:

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

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

3.2 Répartition des fonctions

Le concepteur doit conduire l'analyse des tâches pour déterminer quelles fonctions doivent en principe être confiées à l'homme et quelles fonctions doivent en principe être confiées à la machine. Un exemple de procédure est donné en A.3.2.1.

Les fonctions confiées à l'homme indiquées au tableau A.1 sont:

- la commande manuelle incluant les commandes en secours des commandes automatiques;
- la surveillance associée aux commandes manuelles et automatiques;
- les tâches avec démarche intellectuelle, telles que le diagnostic, pour déterminer les causes d'un fonctionnement et d'événements anormaux et imprévus et définir les actions correctrices.

Les fonctions assignées à la machine se réfèrent à celles qui sont remplies par des commandes automatiques, comme indiqué au tableau A.1.

Les principes et critères d'ingénierie des facteurs humains doivent être appliqués dans cette analyse.

Les principes et critères utilisés dans l'analyse doivent être documentés et inclure les facteurs concernant les capacités et les limites, à la fois de l'équipe de conduite et des systèmes de commandes automatiques.

Les critères de répartitions sont décrits en A.3.2.2 et la répartition est décrite en A.3.2.3.

3.2.1 Aptitude de l'opérateur

Dans les fonctions allouées à l'opérateur, il convient de distinguer celles pour lesquelles il effectue réellement une tâche de commande, celles où il supervise un système automatique en train de remplir des tâches de commande et celles où il est en train de réaliser des démarches intellectuelles telles que des diagnostics. De cette analyse doivent en principe résulter les informations nécessaires pour la conception de la structure du système d'informations et pour l'organisation fonctionnelle des ressources permettant d'atteindre chacune des prises de décision et des tâches de commande.

Pour les fonctions potentielles de l'opérateur, des estimations de sa capacité de travail en terme de charge, de précision, de vitesse et de durée doivent être préparées pour chaque aspect du traitement d'informations et chaque action de commande. Ces estimations doivent être utilisées pour la répartition initiale des fonctions. Elles doivent en principe être modifiées sur la base des résultats des vérifications et utilisées pour reconsidérer la répartition d'une fonction, aussi bien que pour fournir une définition plus détaillée des exigences vis-à-vis de l'opérateur.

Ces exigences, en liaison avec celles concernant les moyens de présentation, de commande et de communication, doivent être en rapport avec les tâches devant être remplies pour accomplir la fonction. Les tâches générales doivent en principe inclure les exigences concernant les moyens de présentation, de commande et de communication. Les critères sont discutés avec plus de détails en A.3.2.2.

Les types variés de données disponibles pour l'opérateur doivent en principe être groupés en se basant sur des tâches et non sur l'origine des données. Le but est d'organiser l'information provenant de sources variées en accord avec chacune des tâches de prise de décision, pour fournir à l'opérateur un système d'informations à la fois complet et compatible avec ses aptitudes.

3.2 *Assignment of functions*

The designer shall conduct task analysis to determine which functions should be assigned to the man and which functions should be assigned to the machine. An example of the procedure is given in A.3.2.1.

Functions assigned to man shown in table A.1 are:

- manual control including backup control to automatic control;
- 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 determine the 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.

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.

The assignment criteria are described in A.3.2.2 and the assignment is described in A.3.2.3.

3.2.1 *Operator capabilities*

The functions assigned to the operator should distinguish between those where he is actually performing a control task, where he is supervising an automatic system that is performing the control tasks and where he is performing high level mental processing tasks such as diagnosis. This analysis should result in the information needed for the conceptual information system structure and the functional organization of resources to perform each decision making and control task.

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

These requirements together with those for display, control and communication shall be consistent with the tasks which shall be performed to accomplish the function. The general tasks should include display, control and communication requirements. These requirements are discussed in A.3.2.2.

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.

3.2.2 Capacité de traitement du système de contrôle-commande

L'analyse des traitements du système de contrôle-commande doit commencer par la définition des exigences et contraintes fonctionnelles du système et/ou des matériels, suivie par une description plus détaillée des séquences d'événements opérationnels et des exigences de l'interface homme/machine pour chaque tâche. Le but est d'organiser les informations et capacités de la machine en accord avec les tâches définies pour l'interaction de l'opérateur.

Cette organisation doit faciliter l'évaluation des capacités à la fois de la machine et de l'homme pour accomplir chacune des tâches de prises de décision et de commande. Les capacités de traitement du système de contrôle-commande doivent en principe inclure en fin de compte les spécifications, telles que des exigences en quantité, temps de réponse et précision auxquelles le système et/ou le matériel doivent satisfaire, aussi bien que les standards d'ingénierie humaine définissant l'interface homme/machine pour chaque type de composants.

Pour réduire la probabilité d'une erreur de l'opérateur, le système de contrôle-commande doit en principe être conçu pour maintenir la centrale et les matériels à l'intérieur de limites de sûreté sans aucune action de l'opérateur, un certain temps après l'initiation des conditions anormales de la centrale. Ce temps doit être reproduit dans les exigences fonctionnelles des systèmes de commande automatique.

3.3 Vérification de la répartition des fonctions

La répartition correcte des fonctions de la salle de commande entre l'homme et la machine doit être vérifiée comme indiqué à la figure 2. Il doit être prouvé que la répartition de fonctions proposée est la plus avantageuse pour l'homme et la machine sans imposer d'exigences défavorables à aucun d'entre eux.

3.3.1 Processus

Le processus développé pour la vérification doit inclure les phases de préparation, d'évaluation et de correction (voir A.3.3.1 et A.3.3.2 a) pour ces processus).

3.3.2 Critères généraux d'évaluation pour la vérification

Avant de tenter de vérifier la répartition des fonctions proposée, il doit être confirmé que les critères utilisés pour la répartition sont en accord avec eux-mêmes.

La vérification doit confirmer que:

- a) toutes les fonctions nécessaires pour atteindre les objectifs opérationnels et de sûreté de la centrale sont identifiées;
- b) les répartitions des fonctions proposées sont en accord avec les critères établis pour ces répartitions;
- c) toutes les exigences de chacune des fonctions sont identifiées et incluent les aspects de performance (par exemple, constantes de temps, précision), ceux dérivés des principes de sûreté, de disponibilité et d'exploitation spécifiés dans cette norme, ainsi que ceux dérivés d'autres normes, réglementations et guides;
- d) les exigences pour des objectifs fonctionnels de plus haut niveau sont confondues avec celles de niveau fonctionnel plus faible, sans conflit dans tous les modes opérationnels.

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

3.2.2 I & C system processing capabilities

Analysis of instrument and control system processing shall begin with a definition of system and/or equipment functional requirements and restraints, followed by a more detailed description of operational event sequences and man/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 specifications such as quantity, response time and accuracy requirements that the system and/or equipment shall satisfy as well as human engineering standards defining the man/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 condition of the plant. This period of time shall be reflected in the functional requirements for the automatic control systems.

3.3 Verification of function assignment

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

3.3.1 Process

The process developed for the verification shall include preparation, evaluation and resolution phases (see A.3.3.1 and A.3.3.2 a) for these processes).

3.3.2 General evaluation criteria for verification

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

The verification shall subsequently confirm that:

- a) all the functions necessary for the achievement of the plant operational and safety goals are identified;
- b) the proposed function assignment is in accordance with criteria established for the assignment;
- c) all 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;
- d) 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.

3.4 *Validation de la répartition des fonctions*

La répartition des fonctions proposée doit être validée pour démontrer qu'elle pourrait atteindre les objectifs fonctionnels. En particulier, les performances des séquences fonctionnelles, dans toutes les conditions de fonctionnement normal et lors de plusieurs événements représentatifs, doivent être prouvées.

3.4.1 *Processus*

Le processus développé pour la validation doit inclure les phases de préparation, d'évaluation et de correction (voir A.3.3.1 et A.3.3.2 b)).

Des critères de sélection doivent être développés pour assurer la représentativité des événements retenus pour l'évaluation. En plus de toutes les conditions de fonctionnement normal et des événements spécifiés en 3.1.2, les événements causés par de multiples défaillances doivent en principe être pris en considération pour l'évaluation des fonctions allouées à l'homme.

Après l'achèvement de la sélection des événements représentatifs, les fonctions requises pour chaque événement sont identifiées et synthétisées dans un ordre de déroulement séquentiel dans le temps.

3.4.2 *Critères généraux d'évaluation pour la validation*

Les performances des fonctions doivent être évaluées pour l'ensemble du fonctionnement normal et pour des événements représentatifs. Les critères généraux de validation doivent être satisfaits, y compris que:

- a) le nombre d'objectifs fonctionnels et le taux de charge de travail requis pour l'équipe de salle de commande n'excèdent pas leur capacité;
- b) la répartition de fonctions pour l'équipe de salle de commande et les opérateurs locaux est adéquate. En particulier, il ne doit pas en principe être exigé d'eux qu'ils coopèrent lorsqu'il s'agit de remplir une fonction qui est soit critique au point de vue temps, soit importante pour la sûreté ou la disponibilité de la centrale.

3.5 *Analyse du travail*

Afin d'établir simultanément les exigences de base pour la structure de l'équipe de salle de commande, les procédures de conduite et le programme de formation, le concepteur doit en principe conduire une analyse du travail pour la vérification et la validation de la répartition des fonctions et des exigences fonctionnelles.

L'analyse doit en principe clarifier:

- l'ensemble des compétences requises pour l'opérateur;
- les responsabilités de conduite des opérateurs;
- les tâches non opérationnelles des opérateurs (par exemple des rapports);
- les interactions opérationnelles entre opérateurs;
- les dialogues entre les opérateurs et la centrale;
- les dialogues entre les opérateurs et le personnel de centrale stationné à l'extérieur des installations de salle de commande.

En liaison avec les résultats de l'analyse pour la répartition des fonctions (par exemple la structure conceptuelle de l'information), la liste ci-dessus doit en principe former la base de la structure de l'équipe de salle de commande, des procédures de conduite et du programme de formation (voir A.3.5 pour une séquence de l'analyse).

3.4 *Validation of functional assignment*

The proposed function assignment shall be validated to demonstrate that the system would achieve all the functional goals. In particular, the performance of function sequences, under all the normal operations and several representative events, shall be assessed.

3.4.1 *Process*

The process developed for the validation shall include preparation, evaluation and resolution phases (see A.3.3.1 and A.3.3.2 b)).

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 3.1.2, events caused by multiple failures should be considered for the assessment of functions assigned to man.

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

3.4.2 *General evaluation criteria for validation*

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

- a) the number of functional goals and the work load rate required of the control room staff shall not exceed their capability;
- b) the assignment of functions to the control room staff and local operators is acceptable. In particular, it should not require them to perform cooperative, mutually dependent tasks for the achievement of a function which is either time critical or important to the plant safety or the plant availability.

3.5 *Job analysis*

In order to develop basic requirements further 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 analysis should clarify:

- operator competence required;
- operational responsibilities of operators;
- non operational 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.

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 (see A.3.5 for a sequence of the analysis).

4 Spécifications fonctionnelles de conception

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 également les interfaces entre l'homme et la salle de commande.

La conception doit être basée sur l'approche d'ingénierie de systèmes "homme/machine" intégrés.

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

Pour la conception détaillée de la salle de commande, une base de données sur les caractéristiques et capacités humaines doit être établie comme donnée fondamentale pour la prise en compte des facteurs humains.

La base de données doit inclure:

- des considérations anthropométriques;
- les stéréotypes de population;
- les aspects physiologiques;
- l'aptitude humaine à traiter l'information;
- les facteurs d'environnement.

Comme ces données dépendent des habitudes du pays, la base de données est spécifique pour chaque pays. Il est montré en A.4.1 comment constituer cette base de données et quelques exemples y sont indiqués.

4.2 Localisation, environnement et protection

4.2.1 Localisation

La salle de commande doit être située là où la conduite de la centrale est aisée et doit en principe respecter les exigences de sûreté de 2.3.

4.2.2 Environnement

Les conditions d'environnement de la salle de commande principale doivent être telles que les opérateurs puissent remplir leur tâche de façon efficace et confortable.

Les spécifications d'environnement doivent inclure des exigences sur:

- la climatisation;
- l'environnement sonore;
- l'éclairage.

Ces spécifications d'environnement sont développées en A.4.2.2.

Des mesures appropriées doivent être prises lors de la conception pour maintenir l'opérabilité de la salle de commande et la surveillance de la centrale, même durant les conditions accidentelles de la centrale.

4.2.3 Protection

La conception de la salle de commande doit prendre en compte la protection contre le feu, les rayonnements, les missiles internes et externes, les tremblements de terre et les actes hostiles. Ces protections sont décrites en A.4.2.3.

4 Functional design specification

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 man and the control room equipment.

The design shall be based on an integrated man/machine systems engineering approach.

4.1 *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 will be specific to each country. In A.4.1 it is shown how to provide such a data base and some examples of these data.

4.2 *Location, environment and protection*

4.2.1 *Location*

The control room shall be located for convenient plant operation and should meet the safety principles of 2.3.

4.2.2 *Environment*

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

The environmental specification shall include requirements for:

- air conditioning;
- auditory environment;
- illumination.

These environmental specifications are discussed in A.4.2.2 .

Appropriate measures shall be taken in the design to maintain control room operability and monitoring of the plant even during emergency conditions of the plant.

4.2.3 *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 protection is described in A.4.2.3.

4.3 Dimensions et configuration

4.3.1 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 de l'opérateur dans les situations anormales.

On doit en principe particulièrement veiller à y prévoir des zones de travail, des endroits pour écrire et des meubles de rangement pour stocker les documents comme indiqué en A.4.3.1.

4.3.2 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 de contrôle-commande;
- la philosophie de la conduite centralisée ou locale, qui détermine le nombre de commandes présentes en salle de commande;
- les critères de supervision, qui déterminent le nombre d'écrans de visualisation, d'enregistreurs, d'indicateurs d'alarmes et de voyants sur les panneaux;
- le type de centrale et les choix technologiques (séparation entre voies, utilisation de séquences automatiques, dimensions des instruments et des commandes, extension de l'automatisation et/ou des commandes multiplexées);
- les exigences légales et celles des exploitants, tel le nombre d'opérateurs dans la salle de commande, exigé par la politique d'exploitation ou par les autorités.

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 les situations accidentelles.

La zone de conduite et les matériels de la salle de commande, tels les pupitres, tableaux et panneaux, doivent être disposés selon les principes d'ingénierie des facteurs humains.

Les prescriptions concernant le regroupement des zones de conduites, les matériels en salle de commande et leur disposition sont exposées en A.4.3.2 a) et b); celles relatives à la dimension et la forme des matériels sont exposées en A.4.3.2 c).

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 conçue de façon à simplifier l'identification des systèmes ou des composants, à la fois en fonctionnement normal, dans les conditions accidentelles de conduite, dans les situations d'urgence et 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 résultantes doivent être cohérentes pour toutes les zones de conduite.

4.3 *Space and configuration*

4.3.1 *Space*

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

Special attention should be paid to providing work areas, writing space and storage space for documents, as described in A.4.3.1.

4.3.2 *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 number of VDUs, indicating instruments, recorders, alarms and indicating lights on the panels;
- plant and technological choices (segregation between different divisions, use of automatic control sequences, dimensions of instruments and controls, 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.

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.

Refer to A.4.3.2 a) and b) on requirements for grouping of operating areas and the control room equipment and their arrangement, and A.4.3.2 c) for requirements on size and shape of equipment.

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 to simplify the system or component identification in both normal operation, accident conditions and emergency situations, and minimize the probability of incorrect actuations arising from human error.

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

4.4 Agencement des panneaux

4.4.1 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 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.

4.4.2 Position sur les panneaux et 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;
- 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.

Un exemple est donné en A.4.4.2.

4.4.3 Symétrie

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

4.5 Aide à la localisation

4.5.1 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. Six techniques principales sont données en A.4.5.1. Le regroupement doit en principe être en accord avec le modèle mental de l'utilisateur du système.

Un soin particulier doit être apporté pour éviter des conflits de regroupement, en particulier lorsque différentes techniques sont utilisées simultanément.

4.5.2 Codages

Les principes de codage doivent être établis dans une étape précoce de la conception de la salle de commande et il convient qu'ils soient cohérents avec ceux des autres centrales et des simulateurs de formation, pour chaque pays.

Le système de codage doit être identique pour toute la salle de commande. La forme des codes utilisés pour les afficheurs et les commandes associées doit être totalement cohérente. Cela s'applique aux codes de localisation, d'information, de couleurs et d'éclairement.

La méthode de codage d'une application réelle doit être déterminée en considérant les avantages relatifs des types de codages. Les types de codages et leurs directives sont indiqués en A.4.5.2.

Lorsque des personnes présentant des déficiences de vision des couleurs sont employées comme opérateurs, la couleur ne doit pas en principe être le seul moyen de discrimination.

4.5.3 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 stéréotypes nationaux et aux normes. Se référer à A.4.5.3 pour des exigences types.

4.4 *Panel layout*

4.4.1 *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 rankings rules derived from these principles shall be consistent for all panels in the plant.

4.4.2 *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.
- frequently used controls shall be within convenient reach and the related indicators and displays shall be readable from the operating position.

See A.4.4.2 for examples.

4.4.3 *Mirror image layout*

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

4.5 *Location aids*

4.5.1 *Grouping of display information and controls*

It is essential that the displayed information and controls are logically grouped. Six fundamental grouping techniques are given in A.4.5.1. The grouping should be consistent with the user's mental model of the system.

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

4.5.2 *Coding*

Coding principles shall be established in an early stage of control room design and they should be consistent with those of other plants and training simulators in each country.

The coding system shall be consistent throughout the control room. The form of codes used for displays and their associated controls shall be entirely consistent. This applies to location, information, colour and illumination codes.

The coding method for an actual application shall be determined considering the relative advantages of the types of coding. The types of coding and their guidelines are shown in A.4.5.2.

Where colour deficient persons may be employed as operators, colour should not be the sole means of discrimination.

4.5.3 *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 stereotypes and standards. Refer to A.4.5.3 for typical requirements.

4.6 Système d'information

4.6.1 Fonctions d'information

Les systèmes d'information doivent être conçus pour informer les opérateurs de l'état de la centrale et des variables importantes pour la sûreté et la disponibilité.

Ces systèmes doivent fournir aux experts de sûreté sur le site et hors du site des informations sur l'état de la centrale pendant les conditions accidentelles.

Le système doit aussi avoir des fonctions d'acquisition de données, d'affichage et d'alarme. Il doit aussi avoir des fonctions d'enregistrement et de mémorisation pour les variables du processus importantes pour la sûreté et la disponibilité, pour l'analyse et pour envoyer ces informations aux services de conduite et aux autorités extérieures.

Un système d'information doit en principe être prévu pour aider la démarche intellectuelle des opérateurs par :

- une aide à la prise de décision;
- une amélioration des performances et des capacités de surveillance;
- une amélioration de la disponibilité et de la fiabilité de l'information;
- un retour d'expérience dans l'organisation des actions;
- une amélioration de la communication entre les équipes de salles de commande;
- une amélioration de l'enregistrement des transitoires et des accidents à des fins d'analyse;
- un accroissement de l'information disponible pour recouvrir des données implicites.

Se référer à A.4.6.1 où les fonctions d'information sont prescrites.

Les fonctions d'information peuvent être constituées de systèmes individuels ou de sous-fonctions faisant partie d'un ensemble contrôle-commande informatisé.

4.6.2 Système d'acquisition et de traitement des données

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

- le système doit en principe être conçu de telle sorte que ses défaillances ne conduisent pas à un état non sûr ou à des pertes économiques inacceptables dans l'exploitation de la centrale;
- les vitesses d'échantillonnage des données d'entrées, de prétraitement et d'analyse, doivent satisfaire aux exigences opérationnelles concernant les vitesses d'évolution des paramètres;
- les données doivent être mises à jour à des vitesses appropriées aux tâches des opérateurs;
- le système doit être conçu en considérant le système de présentation et les équipements d'affichage d'alarme, et une information suffisante doit être disponible pour atteindre, en accord avec les exigences de la réglementation, un état d'arrêt sûr et y rester durant une durée illimitée;
- le système doit être apte à être modifié pendant toute sa vie opérationnelle.

4.6 *Information system*

4.6.1 *Information functions*

Information systems shall be provided to inform operators of the plant status and variables important to safety and availability.

The system shall provide information of the plant status 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;
- improving availability and reliability of information;
- providing feedback for organization of actions;
- improving communication between control room staff;
- improving a record of transients and accidents for analysis purposes;
- expanding available information to cover implicit data.

Refer to A.4.6.1 for requirements for the information functions.

Information functions may be provided either within individual systems, or as sub-functions of a computerised plant instrumentation, information and control system.

4.6.2 *Data acquisition and processing system*

The major functional requirements of the data acquisition and processing system are as follows:

- the system should be designed such that the system faults do 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;
- the system shall be designed considering the display system and annunciation equipment, and 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 be capable of modification throughout its operational life.

4.6.3 Système d'affichage

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

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 et l'étendue de mesure des afficheurs doivent être conformes aux hypothèses de l'analyse de sûreté;
- un afficheur doit être prévu pour l'indication des conditions de bipasse ou de celles délibérément non opérationnelles de la centrale et des auxiliaires;
- les afficheurs d'informations relatives à la sûreté doivent être convenablement localisés et identifiés, de façon spécifique, sur les panneaux de commande;
- des afficheurs appropriés doivent être choisis selon le rôle de chacun.

Les types d'afficheurs sont décrits en A.4.6.3.

a) Afficheurs comportant des indicateurs et des lampes

Voir A.4.6.3 (1) pour les exigences.

b) Afficheurs constitués par des écrans de visualisation

Les exigences fonctionnelles principales des moyens de présentation constitués par des écrans de visualisation sont les suivants:

- l'information nécessaire doit être disponible pour l'opérateur chaque fois que c'est nécessaire;
- l'information présentée sur les écrans de visualisation doit être compréhensible par l'opérateur;
- l'image doit fournir les informations attendues par les opérateurs sans ambiguïté ni perte de signification;
- les symboles doivent en principe être normalisés et la gamme de tailles de symboles doit en principe être limitée;
- le sens des flux et la chronologie des événements dans les représentations des schémas doivent en principe être en accord avec les stéréotypes de population et les synoptiques des tableaux de la salle de commande.

Les présentations sur écran de visualisation doivent être conçues en considérant les facteurs humains et les critères de conception de 4.4 et 4.5 et en se référant à A.4.1, A.4.4, A.4.5 et A.4.6, et doivent être compatibles avec, d'une part, les commandes et l'instrumentation associée, et, d'autre part, avec les besoins perceptifs et cognitifs de l'opérateur. Voir A.4.6.3 (2).

4.6.4 Système d'alarmes

a) Spécifications du système d'alarmes

Les alarmes en salle de commande principale doivent fournir toutes les informations nécessaires pour la surveillance de la centrale dans les conditions anormales.

4.6.3 Display system

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

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 and range of displays shall be consistent with the assumptions of the safety analysis.
- a display shall be provided for indicating by-passed or deliberately inoperable conditions of plant and auxiliaries.
- safety-related information displays shall be suitably located and specifically identified on control panels.
- appropriate types of display shall be selected depending on the purpose of an individual display.

The types of displays are described in A.4.6.3.

a) Display using indicators and lamps

See A.4.6.3 (1) for requirements.

b) Displays using VDU

The major functional requirements for VDU displays are as follows:

- necessary information shall be available to the operators whenever it is required;
- information shown on VDU shall be clearly understood by the operators;
- the display shall communicate the intended information to the operators without ambiguity or loss of meaning;
- symbols should be standardized and the range of symbol sizes should be limited;
- direction of process flow paths and sequence events in schematic displays should be in accordance with population stereotypes and any mimics on control room panels.

VDU displays shall be designed considering human factors and design criteria shown in 4.4, 4.5 and referring to appropriate requirements in A.4.1, A.4.4, A.4.5 and A.4.6, and should be compatible with both the associated controls and instrumentation and the perceptual and cognitive needs of an operator. Refer to A.4.6.3 (2).

4.6.4 Alarm system

a) Alarm system specifications

Main control room alarms shall provide all information necessary for surveillance of plant in off-normal plant conditions.

Le système d'alarmes doit en principe:

- afficher les informations d'alarmes, pour aider l'opérateur à comprendre la situation de défaut qui se développe sans être surchargé d'informations;
- permettre à l'opérateur de supprimer les informations non pertinentes avec la certitude que les informations pertinentes et importantes soient présentées d'une façon adaptée à la capacité de compréhension de l'opérateur;
- permettre à l'opérateur de faire la distinction 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.

Il convient que le système d'alarmes possède:

- des fonctions de traitement, pour donner à l'opérateur l'information la plus représentative des 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, une documentation de procédure, par exemple une fiche d'alarmes ou une procédure de conduite, doit être prévue pour expliquer à l'opérateur les raisons probables de l'alarme et les actions correctrices qu'il a à mener.

Pour expliquer l'importance de combinaisons particulières d'un signal d'alarme, il est recommandé d'utiliser un système d'aide informatique. Voir A.4.6.4 pour des exigences complémentaires et le traitement des alarmes.

b) Affichage des alarmes

L'affichage des alarmes sur verrines ou sur écran de visualisation doit répondre aux exigences suivantes:

- une alarme doit être présentée dans la zone de la salle de commande où l'opérateur dispose des moyens nécessaires pour déclencher les actions correctrices;
- toute nouvelle alarme doit déclencher un signal auditif et un clignotement de verrine ou de marqueur sur écran;
- une alarme peut être acquittée après qu'il en soit pris connaissance;
- si une alarme est acquittée, cet état doit être indiqué pour s'assurer que son existence n'est pas oubliée;
- lorsque la cause est éliminée, l'affichage d'alarmes doit être remis dans le mode normal manuellement ou automatiquement.

4.6.5 Système support de l'opérateur

Afin d'améliorer la sûreté de la centrale, sa disponibilité et sa manœuvrabilité, des fonctions support de l'opérateur telles les fonctions de surveillance et d'affichage des paramètres de sûreté, les fonctions de diagnostic, les fonctions de guide opérateur basées sur les symptômes et les événements, les fonctions de test automatique en fonctionnement doivent en principe être prévues. Elles doivent autant que possible être totalement intégrées dans la conception d'ensemble de la salle de commande.

The alarm system should:

- display alarm information to enable the operator to understand the fault situation as it develops, and to avoid information overload;
- 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 finished and alarms which cannot be cancelled without the intervention of the maintenance service.

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 identify easily 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 of the alarm and the corrective actions required.

It is recommended that computer based operator aids are used for explaining the importance of particular combinations of alarm signal. See A.4.6.4 on additional requirements and alarm processing.

b) Display of alarms

The display of alarms on alarm-fascias or on VDUs shall meet the following requirements:

- an alarm shall be annunciated in the control room section where the operator has the necessary means for initiating corrective actions;
- any new alarm shall start an audible warning and flash a fascia light or VDU marker;
- an alarm may be steadied after it has been acknowledged;
- the steadied alarm shall be indicated to ensure that its existence is not forgotten;
- when the cause of alarm is eliminated, the alarm display shall be returned to the normal mode manually or automatically.

4.6.5 Operator support systems

In order to enhance plant safety, availability and operability, operator support functions such as safety parameter displays and surveillance functions, plant diagnosis functions, symptom-based and event-based operator guide functions, and functions for automatic on-power test, should be provided. So far as practicable such functions should be fully integrated into the overall design of the control room.

4.7 Commandes

4.7.1 Fonctions de commande

Ce paragraphe traite des spécifications fonctionnelles et des facteurs humains pour les commandes utilisées pour les conduites manuelles et en secours de commandes automatiques dans les situations normales et anormales. Cependant, les spécifications fonctionnelles des fonctions de commande, incluses dans le système de contrôle-commande, sortent du domaine d'application de cette norme.

4.7.2 Commandes

Les commandes doivent être conçues pour assurer une conduite aisée et pour réduire les erreurs de l'opérateur.

a) Moyens de commande

Les caractéristiques mécaniques des moyens de commande, tels que la taille, la pression de commande, la force de commande, le retour tactile, etc., doivent respecter les capacités humaines et les caractéristiques spécifiées dans la base de données anthropométriques.

b) Considérations ergonomiques

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 de la population attendue des opérateurs.

Les commandes doivent respecter les exigences ci-après:

- pour réduire les erreurs d'opérateur, les mouvements des commandes doivent en principe être conformes aux stéréotypes de population;
- les codages de couleur, de forme et de taille utilisés, les mouvements des commandes ainsi que le choix des commandes pour des fonctions de commande similaires doivent être cohérents;
- le rangement des commandes en catégories doit être proportionné à leur importance pour la sûreté. Voir A.4.7.1.

c) Prévention contre une activation erronée

Pour éviter un événement provoqué par l'homme, une action erronée sur les commandes doit être réduite en utilisant des moyens tels qu'une localisation convenable des commandes, l'utilisation de structures fixes de protection, des couvercles ou barrières mobiles, des commandes verrouillables, l'application de priorités d'actions ou une combinaison de ces moyens, ainsi que des considérations ergonomiques. Voir A.4.7.1 et A.4.7.2.

d) Fonctions d'aide informatisée

Une aide informatisée doit, si possible, être introduite dans les commandes pour aider l'opérateur à éviter des actions erronées, grâce à des séquences ou des verrouillages logiques de commandes ou à un guide opérateur avec un système d'affichage informatisé, etc.

4.7 Controls

4.7.1 Control functions

This sub-clause 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.

4.7.2 Controls

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

a) Control elements

Mechanical characteristics of control elements, such as size, operating pressure or force, tactile feedback, etc., shall meet human capabilities and characteristics specified in the anthropometric data base.

b) Ergonomic consideration

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

Controls shall meet the following requirements:

- to minimize operator error, control movements should conform to population stereotypes;
- consistency shall be kept for colour, shape and size codings, control movements, as well as the selection of controls for similar control functions;
- categorization of controls shall be commensurate to their importance to safety. See A.4.7.1.

c) Prevention of erroneous activation

To prevent a human-induced event, erroneous activation of controls shall be minimized by means such as locating controls at proper positions, use of fixed protective structures, movable covers or guards, interlocking controls, application of priority of actuation or their combinations as well as ergonomic considerations. See A.4.7.1 and A.4.7.2.

d) Computer aided functions

Computer aided functions should be introduced for controls, where possible, as operator aids to prevent erroneous actuation, by means of a sequential or logical actuation interlock, or an operator guide with a computer aided display system, etc.

4.8 *Intégration commandes-afficheurs*

Les commandes et leurs afficheurs associés doivent être correctement intégrés pour garantir la conduite effective de la centrale par l'équipe de salle de commande.

L'intégration commandes-afficheurs doit être conforme à la méthode proposée pour la conduite de la centrale, comme indiqué dans les analyses faites en 3.1 et 3.5.

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

- les moyens de commande doivent en principe être situés près des afficheurs associés. Il y a lieu qu'une action sur une commande produise un changement compatible sur l'afficheur associé;
- la forme adoptée pour une commande doit être cohérente avec celle de l'afficheur associé;
- le regroupement des commandes et de leurs afficheurs associés doit refléter le besoin d'atteindre les objectifs du système et doit être en accord avec le modèle mental des utilisateurs du système;
- lorsqu'une séquence d'utilisation est un facteur clé, l'organisation des commandes et des afficheurs doit refléter les relations causes-effets.
- l'organisation des commandes doit être adaptée à tous les groupes stéréotypes de la population des utilisateurs;
- les formes de codage utilisées pour les afficheurs et leurs commandes associées doivent être totalement cohérentes. Voir A.4.8.1 sur les systèmes informatisés.

4.9 *Systèmes de communication*

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

Des dispositions pour un système de communication non orale tel que le système de facsimilé ou les liaisons informatiques sont souhaitables entre la salle de commande et d'autres centres d'information afin d'améliorer la disponibilité et la sûreté de la centrale.

4.9.1 *Systèmes de communication orale*

1) Communications internes au site

- a) Pour les communications générales dans les conditions de fonctionnement normal, un système téléphonique avec un nombre suffisant de postes doit être installé. Voir A.4.9.1 a) pour les spécifications sur le système téléphonique de la salle de commande.
- b) Pour communiquer en situation accidentelle avec des points de commande et des installations de conduite supplémentaires importants pour la sûreté, un système téléphonique spécifique particulier doit être installé. Voir A.4.9.1 a) sur ce système téléphonique.
- c) Un système de sonorisation doit être prévu pour s'adresser au personnel sur le site dans toutes les conditions d'exploitation de la centrale.

4.8 *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 3.1 and 3.5.

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 form of control adopted shall be consistent with the form of associated information display;
- the grouping of controls and their associated displays shall reflect the need to achieve system objectives and shall be consistent with the user's mental model of the system;
- where sequence of use is a key factor, the organization of controls and displays shall reflect cause/effect relationships;
- the organization of controls shall embody any user population stereotype groupings;
- the form of codes used for displays and their associated controls shall be entirely consistent. See A.4.8.1 on computer based systems.

4.9 *Communication system*

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

Provision of non-verbal communication system 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.

4.9.1 *Verbal communication systems*

1) On-site communications

- a) For general communication under normal operational conditions a telephone system with a necessary number of extensions shall be installed. See A.4.9.1 a) on specifications of the control room telephone system.
- b) For communication in accident condition to supplementary operating facilities and control points which are important to safety, a separate directly wired telephone system shall be installed where appropriate. See A.4.9.1 a) on specifications of the directly wired telephone system.
- c) A public address system shall be provided to address on-site personnel under any plant conditions.

d) Pour une utilisation pendant la maintenance, les essais ou les réparations, une communication par radio avec la salle de commande, utilisant des transmetteurs mobiles, doit être prévue, à moins que tous les points locaux concernés puissent être atteints de façon suffisamment fiable par d'autres moyens.

Les aspects d'interférences radioélectriques doivent être pris en compte dans la conception, le câblage, la localisation et les essais du système de contrôle-commande.

Pour réduire de telles interférences, la gamme de fréquences et la puissance maximale de sortie de ces matériels doivent être limitées et spécifiées pour chaque pays.

Les zones où les transmetteurs ne peuvent pas être utilisés, telle la salle des matériels de commande, doivent être identifiées.

2) Communications avec l'extérieur du site

a) Pour les communications avec l'extérieur du site, destinées au personnel exploitant, aux secours, aux institutions publiques ou gouvernementales, un système de communications spécifique doit en principe être prévu. Le type et l'importance de ce système doivent en principe être spécifiés en fonction des conditions locales. Quelques numéros d'appel de postes, particulièrement celui de la salle de commande ne doivent pas être connus du public.

b) Des liaisons minimales avec l'extérieur doivent être prévues avec les organisations et personnels nécessaires. Une liste de ces organisations et personnels est donnée en A.4.9.1 b). Les liaisons importantes doivent être redondantes et diversifiées et peuvent être soit le téléphone soit un système radio.

3) Aménagement local

La salle de commande principale doit être aussi conçue comme un centre de communication de la centrale pour la conduite normale et dans les premiers moments d'un accident.

Les systèmes doivent être conçus en accord avec les besoins d'environnement locaux lors de leur utilisation.

4.9.2 *Systèmes de communication non orale*

Il est souhaitable de disposer:

- d'un système de télévision pour surveiller le plancher de service du réacteur et le groupe turbo-alternateur;
- d'un système de facsimilé;
- de liaisons informatiques,

entre la salle de commande et les centres d'information. On doit pouvoir en principe se connecter par des liaisons informatiques aux centres de crise dans les situations accidentelles. Voir A.4.9.2.

4.10 *Autres exigences*

4.10.1 *Utilisation de calculateurs*

Les calculateurs qui sont prévus pour accroître les capacités de l'interface homme/machine doivent respecter les exigences suivantes:

a) Les calculateurs ne doivent conduire à aucune perte de fonctions de sûreté, même lorsqu'ils tombent en panne.

d) 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 the I & C systems.

To minimize such interference, the frequency range and the maximum output power of these transmitters shall be limited and specified in each country.

Areas where transmitters may not be used, such as the control equipment room, shall be identified.

2) Off-site communications

a) For communication to the off-site station operating authority, emergency, governmental and public institutions, an exclusive communication system should be designed. The type and size of this system should be specified according to the local conditions. Some of the extensions call numbers, especially one in the control room, shall not be known to the public.

b) The minimum connections off-site shall be provided with necessary organisations and personnel. A list of such organizations and personnel is given in A.4.9.1 b). Important connections shall have redundant and diverse systems and may consist of one telephone and one radio system.

3) Local arrangement

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.

The systems shall be designed according to the relevant local environmental needs during their use.

4.9.2 *Non-verbal communication systems*

Non-verbal communication systems may be provided such as:

- a television system for monitoring the reactor operating floor and turbogenerator status;
- telefacsimile system;
- data links for computer,

between the control room and information centres. The data links should also provide a possible connection with emergency facilities during an emergency condition. See A.4.9.2.

4.10 *Other requirements*

4.10.1 *Utilization of computers*

Computers which are provided to enhance the man/machine interface capability shall meet the following requirements:

a) Failures of the computer system shall not lead to any loss of safety function of the plant.

- b) Le système informatique doit être conçu pour ne pas provoquer ou nécessiter de déclenchement de la centrale si une défaillance unique sur un calculateur survenait. Il faut prendre soin de réduire les conséquences des défauts de mode commun.
- c) Des modifications à la fois dans le logiciel et le matériel après l'installation initiale doivent en principe être facilement réalisables. Voir 4.6.2.
- d) La conception doit en principe inclure des considérations sur la facilité de vérification et de validation, non seulement du matériel, mais également du logiciel.
- e) Le calculateur doit en principe être suffisamment rapide pour remplir les fonctions nécessaires et respecter les exigences des facteurs humains, en matière d'affichage de caractères ou d'images sur écran.

La partie informatique du système de conduite intégré incluant le système de contrôle-commande, les systèmes d'affichage et de support opérateur dans la salle de commande peut consister en un calculateur central. Mais, dans ce cas, des mesures suffisantes doivent être prises pour éviter les défauts de mode commun causés par un fonctionnement erroné ou par une défaillance de ce calculateur.

Il est souhaitable d'utiliser un système ayant des structures hiérarchiques et en partie redondantes pour les fonctions importantes, afin d'améliorer la fiabilité et la maintenabilité du système.

4.10.2 Alimentations de puissance

L'ensemble des sources de puissance alimentant la salle de commande doit avoir une fiabilité et une disponibilité en accord avec les autres exigences du système de contrôle-commande, du système de sûreté et des systèmes liés à la sûreté. Les systèmes importants pour la sûreté en salle de commande, qui sont requis comme devant être disponibles pour être utilisés à tout instant en fonctionnement normal ou en conditions accidentelles, doivent être reliés à des sources de puissance non interruptibles.

4.10.3 Qualification

Un programme de qualification doit être prévu pour confirmer que les matériels et les systèmes liés à la sûreté en salle de commande sont capables de remplir de façon continue les performances de conception requises (par exemple étendue de mesure, précision, réponse) pour leurs fonctions, dans les conditions d'environnement susceptibles d'exister au moment 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 remplacements en temps utile, si nécessaire.

4.10.4 Maintenabilité

Le matériel doit être conçu de façon que la surveillance et la maintenance soient facilitées et qu'en cas de défaillance, le diagnostic, la réparation ou le remplacement soient aisés.

La contribution du temps de réparation dans 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 les bases de conception de chaque système particulier. La connaissance des moyens de détection de l'apparition d'un défaut, par exemple par des tests sur le système en fonctionnement, doit faire partie de cette évaluation.

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

- b) The computer system shall be designed not to cause or require plant trip following a single failure of the computer. Care shall be taken to minimize the consequence of common mode failure.
- c) Modification of both hardware and software after initial installation should be simple to carry out. See 4.6.2.
- d) Design should include consideration of the ease of verification and validation not only of hardware but also of software.
- e) The computer system should be fast enough to perform necessary functions and to meet human factors requirements for displaying information on VDUs.

The computerized part of the integrated operating system including I & C system, display system and operator support system in the control room, may consist of one computer system only. But in this case, sufficient measures shall be taken to prevent common mode failure caused by erroneous operation or failure of the computer.

It is desirable to use a distributed system having hierarchical and partly redundant structures for the important functions to improve system reliability and maintainability.

4.10.2 *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 safety related system. 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-interruptable power supplies.

4.10.3 *Qualification*

A qualification programme shall be provided to confirm that safety-related equipments 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.

4.10.4 *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 bases of each particular system. Knowledge of the means of detecting that a failure has occurred, e.g. a power 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.

4.10.5 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 également inclure des considérations sur les facilités de réparation et les pièces de rechange.

4.10.6 Testabilité

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

5 Vérification et validation du système intégré de salle de commande

La conception initiale d'un système intégré de salle de commande qui inclut 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 constituants du système de salle de commande, c'est-à-dire la structure de l'équipe, les procédures de conduite et le programme de formation, les procédures d'évaluation et les critères doivent en principe être développés séparément ou bien se référer aux normes nationales et guides appropriés disponibles (voir le Guide de sûreté de l'AIEA, série 50-SG-0).

5.1 Vérification du système de salle de commande

A cette étape de la conception du système de salle de commande, la vérification est une revue normale de conception - une partie des procédures d'assurance de qualité - qui garantit la prise en compte correcte des spécifications fonctionnelles et des autres informations techniques dans le concept proposé du système de salle de commande.

5.1.1 Processus

Le processus développé pour la vérification doit inclure les phases de préparation, d'évaluation et de correction. A cette étape, l'évaluation doit inclure les procédures de conduite et le programme de formation qui ont été prévus séparément comme indiqué à la figure 2 (voir A.3.3.1 et A.3.3.3 (1) pour plus de détails).

5.1.2 Critères généraux d'évaluation 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.

Il faut en particulier que:

- a) les spécifications fonctionnelles de l'interface homme/machine respectent les critères de conception, ainsi que les normes, règlements et directives s'y rapportant, et incluent correctement la conception des commandes, afficheurs et autres appareils et composants de salle de commande;
- b) la formation donne aux opérateurs les moyens d'acquérir la compréhension correcte des fonctions de l'interface homme/machine et des procédures de conduite;
- c) le programme de formation tienne compte correctement des procédures de conduite.

4.10.5 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.

4.10.6 Testability

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

5 Verification and validation of the integrated control room system

Upon completion of the initial conceptual design of an integrated control room system including the arrangements for control room staffing, the man/machine interface, the operating procedures and the training programme, its adequacy shall be verified and validated. In subsequent sub-clauses, the process and general evaluation criteria of verification and validation are specified for the man/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 Guide 50-SG-0 series).

5.1 Control room system verification

The verification at this stage of the control room system design is a normal design review - a part of quality assurance procedures - which assures the correct incorporation of functional specifications and other technical information into the proposed control room system concept.

5.1.1 Process

The process developed for the verification shall include preparation, evaluation and resolution phases. Evaluation shall be made in this stage including the operating procedures and the training programme which have been provided separately as shown in Figure 2 (see A.3.3.1 and A.3.3.3 (1) for further details).

5.1.2 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.

In particular, it shall meet the following criteria:

- a) the functional specifications of the man/machine interface meet design criteria as well as relevant regulations, standards and guidelines, and shall be correctly incorporated into controls, displays and other control room devices and component design;
- b) the training shall enable operators to acquire the correct understanding of the functions of the man/machine interface and the operating procedures;
- c) the training programme shall correctly incorporate the operating procedures.

5.2 Validation du système de salle de commande

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 sur les caractéristiques dynamiques du système proposé une fois intégré.

5.2.1 Processus

Le processus développé pour la validation doit inclure les phases de préparation, d'évaluation et de correction (voir A.3.3.1 et A.3.3.3 (2) pour plus de détails).

La préparation est menée de façon semblable à celle concernant la répartition des fonctions (voir 3.4), mais l'expertise de conduite est particulièrement importante à cette étape.

Un modèle de salle de commande approprié permettant l'évaluation des caractéristiques dynamiques du système proposé doit en principe être développé. 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.

Plusieurs mesures de performance doivent en principe être réalisées pour permettre une évaluation redondante. La cohérence qualitative et quantitative des mesures de performance interdépendantes doit être examinée pour confirmer les résultats de l'évaluation.

Dans l'évaluation de l'influence des facteurs d'environnement, les facteurs individuels, aussi bien qu'une combinaison réaliste de ces facteurs, doivent être considérés.

Afin de minimiser l'apparition de défauts de conception durant l'implémentation réelle du concept de projet, le programme de validation doit en principe inclure la trame du programme de recette.

Les critères d'évaluation doivent être cohérents avec les règlements, normes, directives, etc., existants qui s'y rapportent.

5.2.2 Critères généraux d'évaluation pour la validation du système intégré

Les critères d'évaluation doivent permettre d'évaluer les interactions entre l'interface homme/machine et les autres constituants de la salle de commande, c'est-à-dire la structure de l'équipe de salle de commande, les procédures de conduite et le programme de formation, aussi bien que l'interface homme/machine. Pour les points d'interaction détaillés, se référer à la figure 1.

Les critères généraux suivants doivent être respectés:

- a) Les séquences fonctionnelles composées de fonctions affectées à l'équipe de salle de commande et aux automatismes doivent être mutuellement cohérentes et complètes.
- b) La philosophie de conduite exprimée dans les exigences fonctionnelles doit être appliquée de façon cohérente à toutes les fonctions de commande, de telle sorte que les sous-systèmes ayant des caractéristiques de fonctionnement semblables puissent être conduits de façon identique.
- c) Les tâches assignées à l'équipe de salle de commande doivent rester dans les limites des capacités humaines. Les tâches exigeant des traitements rapides, lents ou complexes, de commande ou de traitement de l'information, ne doivent pas être laissées aux opérateurs.
- d) Des marges importantes (par exemple pour les contraintes de temps) doivent en principe être laissées aux opérateurs pour couvrir les variations humaines naturelles.

5.2 *Control room system validation*

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.

5.2.1 *Process*

The process developed for the validation shall include preparation, evaluation and resolution phases (see A.3.3.1 and A.3.3.3 (2) for further details).

Preparation for validation is made in a similar manner to the validation of functional assignment (see 3.4), but operational expertise is particularly important in 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 full scale mock-up can 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.

In the assessment of the influence of the environmental factors, the individual factors, as well as any realistic combination of them, shall be considered.

In order to minimize the occurrence of design deficiencies during actual implementation of the design concept, the validation programme should incorporate the framework of a commissioning test.

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

5.2.2 *General evaluation criteria for integrated system validation*

Criteria shall be defined for the evaluation of the interactions between the man/machine interface and other control room constituents, e.g. the control room staff structure, the operating procedures and training programme, as well as the man/machine interface itself. Refer to Figure 1 for detailed interaction points.

Evaluation criteria are as follows:

- a) Functional sequences composed of functions assigned to the control room staff and to automation together shall be mutually consistent and complete.
- b) The operating philosophy expressed in the functional requirements shall be applied to all the control functions consistently, so that subsystems with similar operating characteristics can be operated similarly.
- c) Tasks assigned to the control room staff shall be within the limitations of human capabilities. Tasks requiring quick, slow or complex controlling and information processing shall not be left for operators.
- d) Ample margins, e.g. time constraints, should be left to operators to allow for natural human variability.

e) Les performances des perceptions des opérateurs doivent respecter les capacités humaines reconnues de sensibilité, dans les domaines de la vision, de l'audition, du toucher, des vibrations, etc.

f) Les performances motrices des opérateurs doivent respecter les capacités humaines de motricité reconnues, caractérisées par les mouvements, les manipulations, la force physique, les portées et l'endurance.

g) Les performances mentales des opérateurs doivent respecter les variations de leur capacité dues aux différents niveaux de vigilance et de fatigue dans les domaines:

- du traitement d'informations;
- de la perception;
- de la mémorisation (à court et long terme);
- de la capacité de se souvenir (à court et long terme).

h) Les performances des opérateurs doivent respecter leur capacité à travailler dans un environnement physique, caractérisé par:

- une pression, température et humidité inconfortables;
- un éclairage inapproprié (niveau, contraste, éblouissement, etc.);
- des bruits irritants et les propriétés acoustiques de la salle de commande;
- la présence de produits toxiques et de rayonnements.

i) Il doit être possible de remplir les tâches affectées à chacun des membres de l'équipe sans créer de surcharge excédant les limites reconnues des capacités d'un opérateur normal.

j) Toutes les informations dont un opérateur a besoin pour remplir ses tâches durant les différentes phases de conduite et les transitoires doivent être accessibles de façon simple, et les commandes nécessaires doivent être prévues. Dans le cas d'une commande manuelle, un retour d'informations adéquat aux opérateurs concernant le comportement du système réel doit être prévu.

k) Si des écrans de visualisation sont spécifiés, l'information doit être accessible avec un minimum de recherche. L'information sur différentes variables nécessaires simultanément doit, si possible, être affichée simultanément sur le même écran. Le système d'affichage doit en principe comporter une zone d'affichage suffisante et une résolution qui permette d'obtenir des images stables et facilement lisibles. Les claviers et autres dispositifs de fonctionnement doivent en principe permettre une conduite simple et fiable du système d'information. La conception des images doit en principe être conforme aux normes reconnues et permettre la lisibilité et la compréhension des informations présentées aux opérateurs.

l) Les procédures de conduite doivent être compatibles avec les exigences de l'interface homme/machine et les temps de réponse prévus. Les procédures de conduite doivent couvrir toutes les tâches et séquences fonctionnelles prévues dans la salle de commande. Les descriptions de procédures doivent être correctes, complètes et facilement interprétables.

m) Le système interface homme/machine doit être capable de fournir les informations suffisantes requises pour les installations situées à l'extérieur de la salle de commande.

n) Le programme de formation doit être compatible avec les exigences des interfaces homme/machine et des procédures. Il doit fournir aux opérateurs les connaissances et les réflexes nécessaires pour une conduite sûre et fiable de la centrale, y compris la maîtrise des événements imprévus.

o) Les exigences concernant l'équipe de salle de commande doivent être cohérentes avec ce qui est nécessaire pour une conduite sûre et fiable, et compatibles à la fois avec les procédures de conduite et le programme de formation.

e) Operator's perceptual performance shall be within recognized limits of the human sensory capabilities in the areas of vision, audition, touch and vibration, etc.

f) Operator's motor performance shall be within recognized human motor capabilities characterized by moving, reaching, manipulating, physical strength and endurance.

g) Operator's mental performance shall be within the variation of their capabilities due to different levels of vigilance and fatigue in the areas of:

- information processing;
- perception;
- information retention (short term/long term);
- memory volume capacity (short term/long term).

h) The operator's performance required shall be within his ability to work under an adverse environment characterized by:

- abnormal temperature, humidity, pressure;
- abnormal illumination (level, contrast, glare, etc.);
- abnormal noise and acoustic properties of the control room;
- toxins and radiation.

i) It shall be possible to perform the tasks assigned to the individual operators without creating workloads exceeding recognized limits of the capabilities of the normal operator.

j) All the information an operator needs to perform the assigned tasks during the different operational states and state transitions, shall be accessible in a simple way and the necessary controls shall be provided. In case of manual control, adequate feedback information to the operators concerning the behaviour of the actual system shall be provided.

k) Information shall be accessible with a minimum of search if VDU's are specified. Information on different variables needed in the same time should be displayed simultaneously on the same VDU, if possible. The display system should have sufficient display area and resolution to allow for stable and easily legible images. Keyboards and other operating devices should support simple and reliable operation of the information system. The design of the display formats should conform to recognized standards and shall support the readability and understandability of the information presented to the operators.

l) Operating procedures shall be compatible with the requirements for man/machine interfaces and the expected plant responses, and the operating procedures shall cover all the anticipated tasks and functional sequences performed in the control room. The descriptions of the procedures shall be correct, complete and consistent and easily interpreted.

m) The man/machine interface system shall be able to provide sufficient information required from facilities outside the control room.

n) The training programme shall be compatible with the requirements for procedures and man/machine interface, and the training programme shall provide the operators with the skills and knowledge necessary for safe and reliable operation of the plant including the handling of unplanned events.

o) The control room staffing shall be consistent with the requirements for safe and reliable operation and compatible with both the operating procedures and the training programme.

p) La communication entre l'équipe de salle de commande et les opérateurs locaux, ainsi qu'avec le personnel de la centrale se trouvant à l'extérieur des installations de la salle de commande, doit être facilement réalisable.

q) Il faut prouver que les systèmes supports des opérateurs peuvent améliorer les capacités potentielles des opérateurs sans créer d'effets secondaires imprévus pouvant être la cause d'obstacles implicites aux activités de prise de décision de l'opérateur (par exemple la surveillance et la démarche intellectuelle).

Withdrawing
IECNORM.COM: Click to view the full PDF of IEC 60964:1989

- p) The communication between the control room staff and both local operators and plant personnel stationed outside the control room facilities shall be easily carried out.
- q) It shall be demonstrated that operator support systems can enhance operator's potential capabilities without generating unforeseen side effects which might bring about implicit obstacles to operator's decision-making activities, e.g. monitoring and high-level mental processing.
-

Withdrawing
IECNORM.COM: Click to view the full PDF of IEC 60964:1989

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

(Les flèches indiquent les flux de conception et d'information)

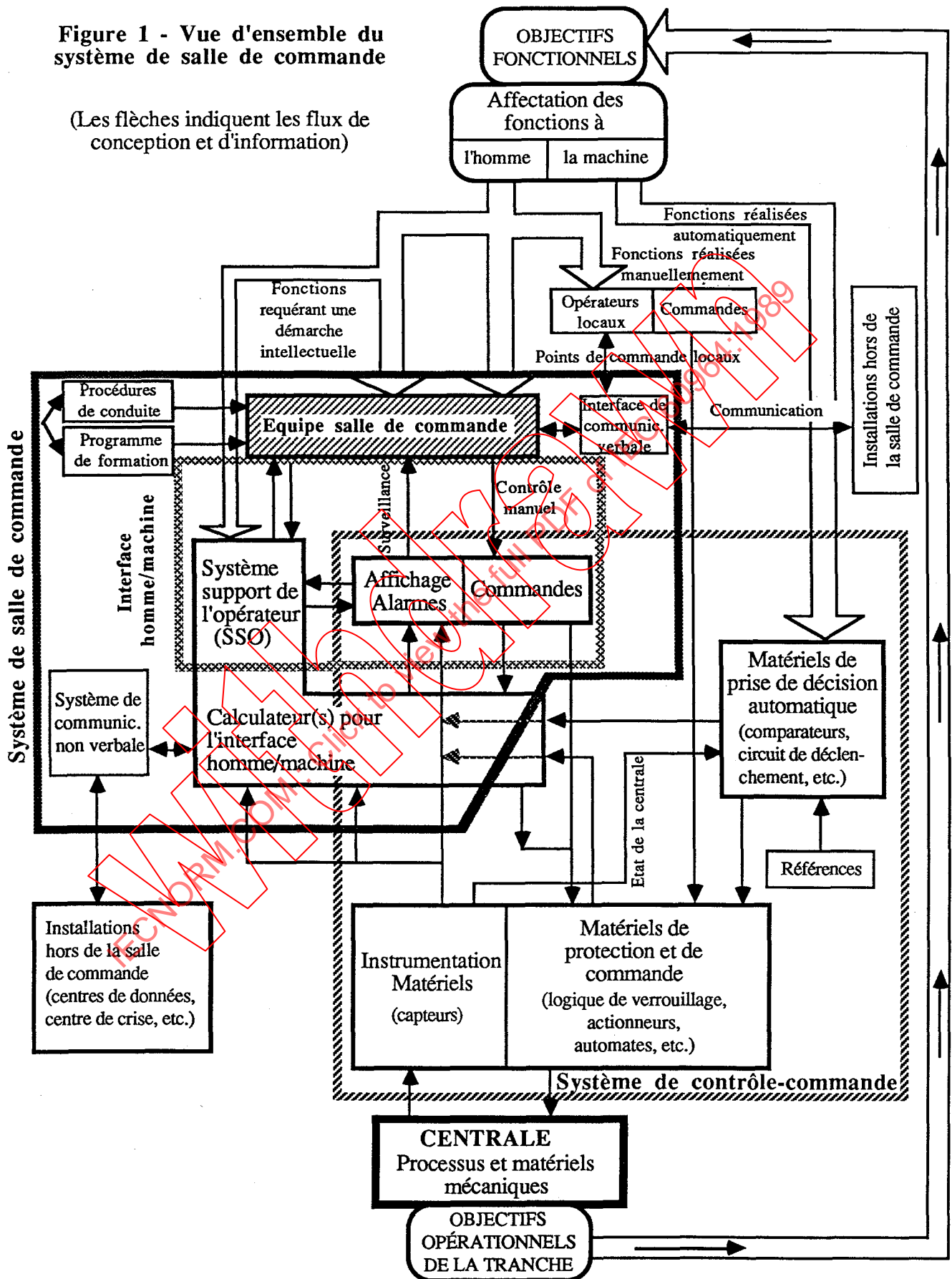
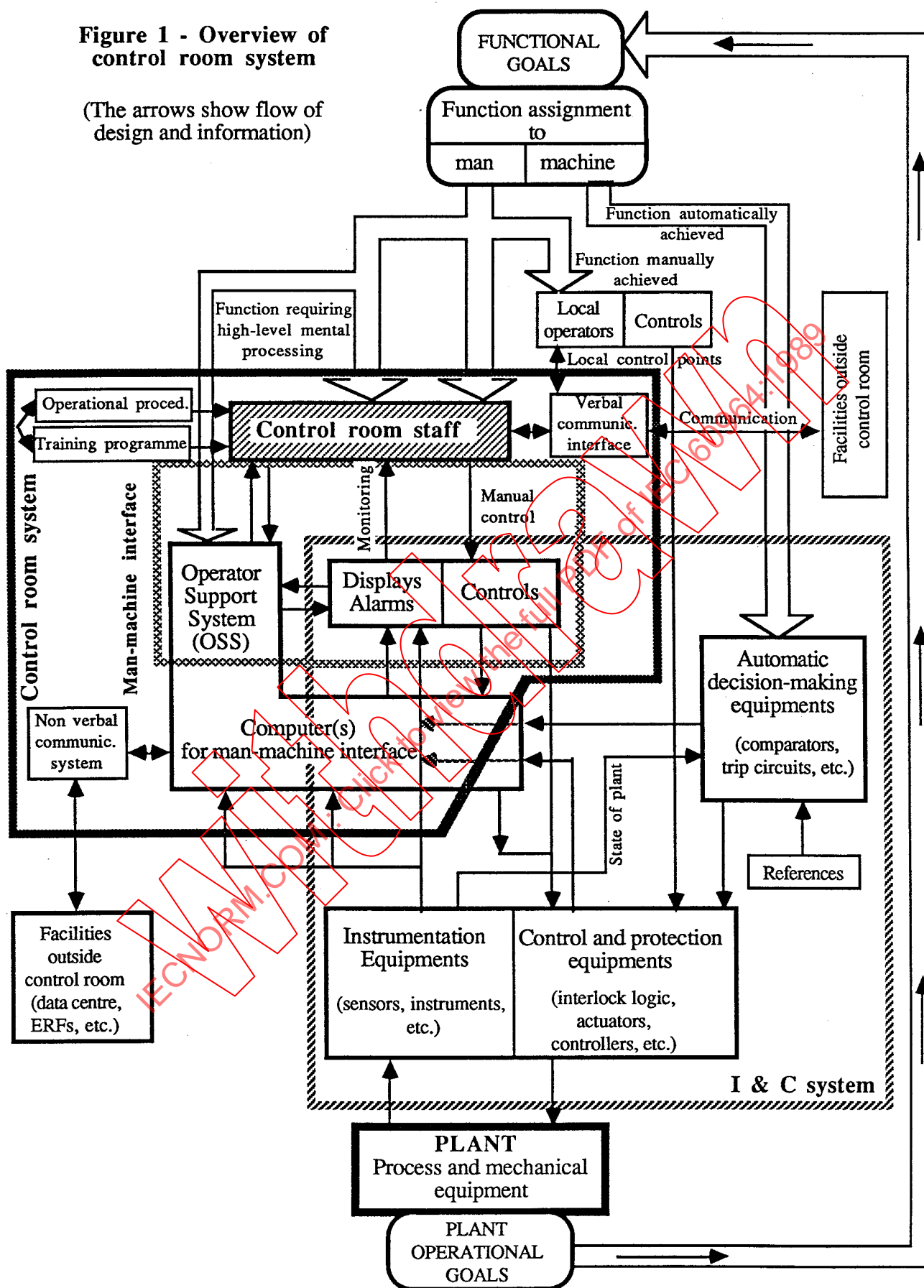
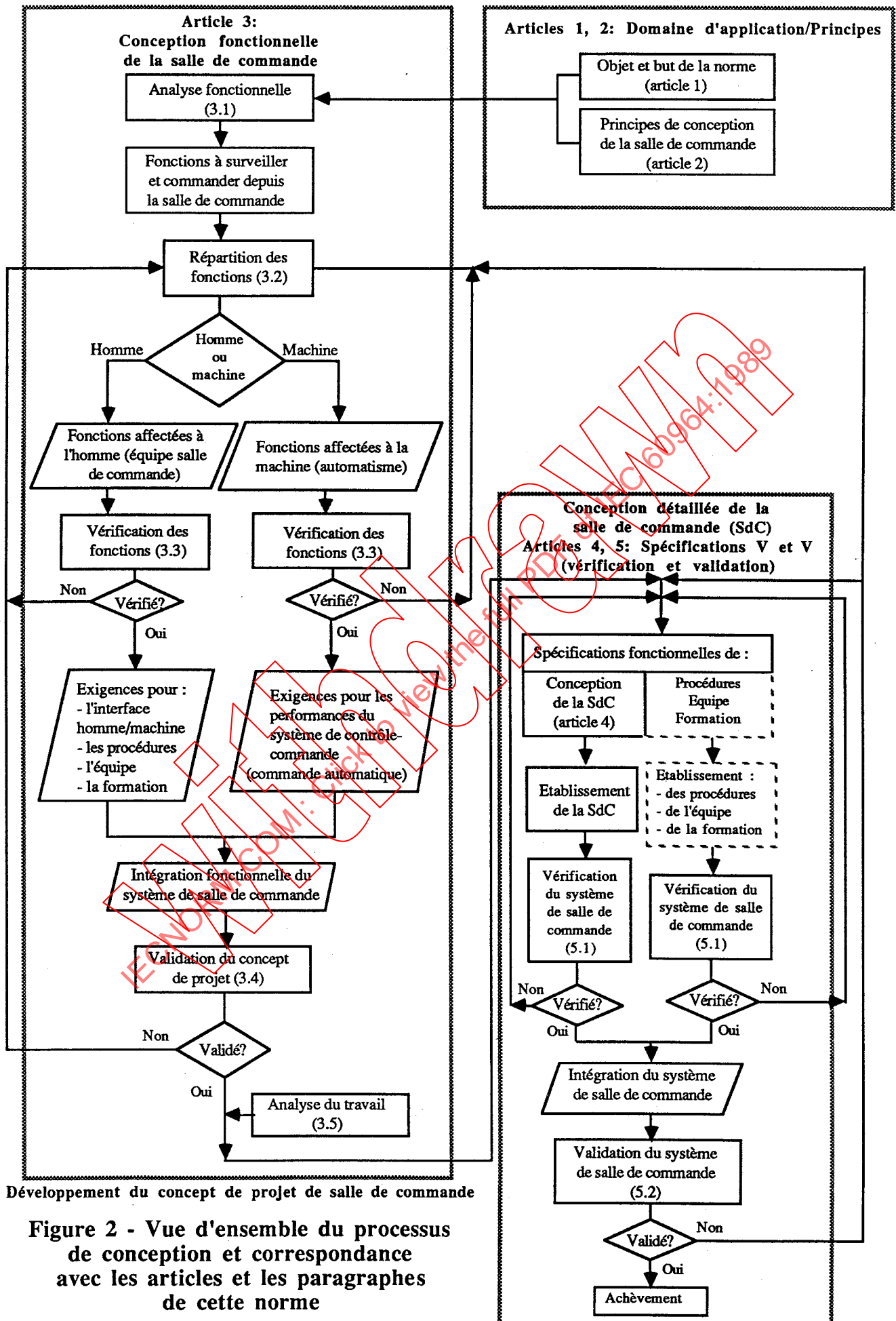
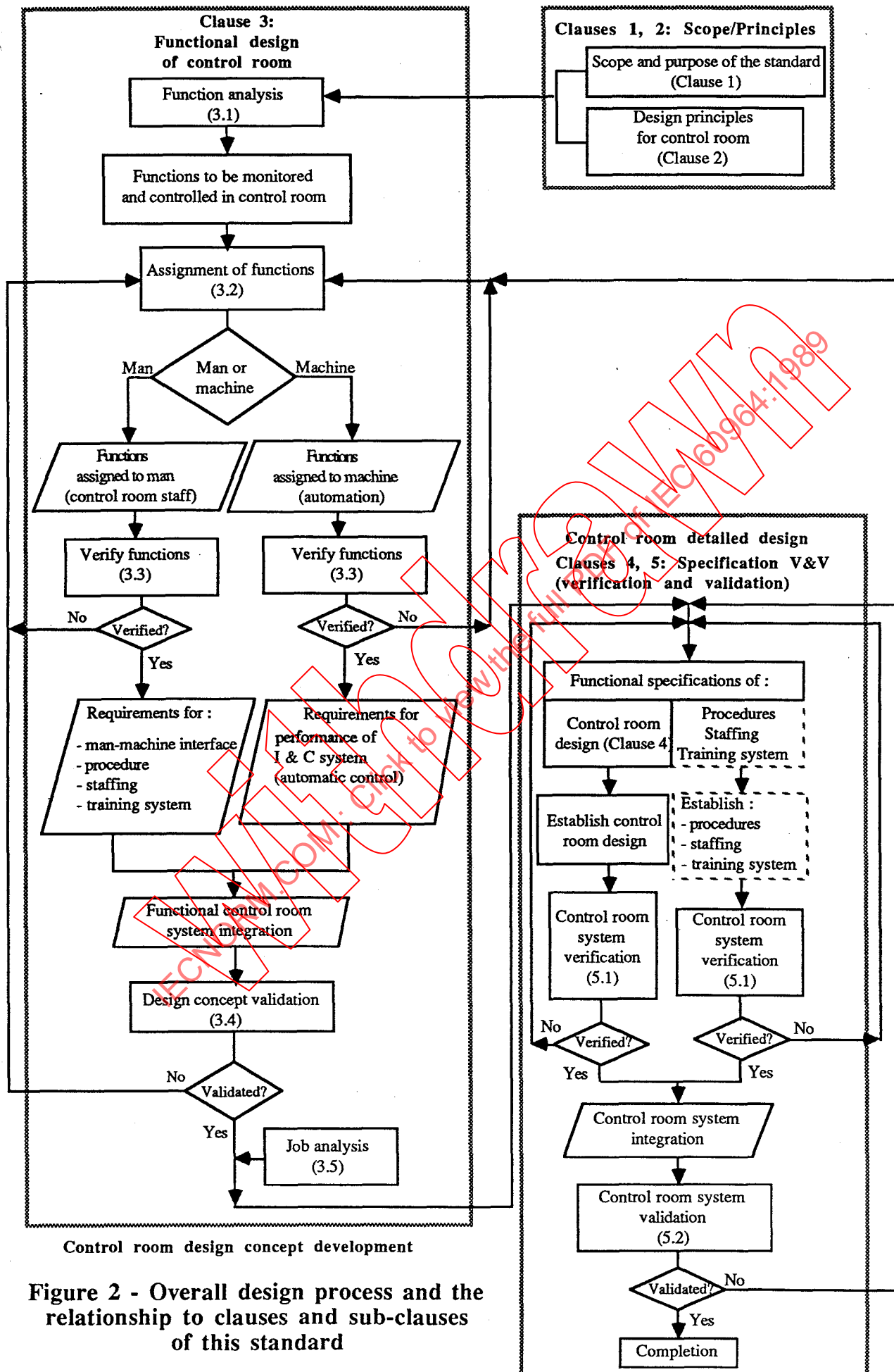


Figure 1 - Overview of control room system

(The arrows show flow of design and information)







SOMMAIRE DE L'ANNEXE A

GUIDE DE CONCEPTION DES SALLES DE COMMANDE

Articles	Pages
A.1 Domaine d'application et but de l'annexe	62
A.1.1 Domaine d'application	62
A.1.2 But	62
A.1.3 Application	62
A.1.4 Explication des concepts et des termes utilisés dans la norme	62
A.2 Principes de conception de la salle de commande	68
A.3 Conception fonctionnelle de la salle de commande	70
A.3.1 Analyse fonctionnelle	70
A.3.2 Répartition des fonctions	74
A.3.3 Vérification et validation de la répartition des fonctions et du système intégré de salle de commande	80
A.3.4 Systèmes d'instrumentation et de contrôle	88
A.3.5 Analyse du travail	92
A.4 Spécifications fonctionnelles de conception	94
A.4.1 Données fondamentales de conception sur les facteurs humains	94
A.4.2 Localisation, environnement et protection	98
A.4.3 Espaces et configuration	102
A.4.4 Agencement des panneaux	104
A.4.5 Aides à la localisation	104
A.4.6 Système d'information	112
A.4.7 Commandes	122
A.4.8 Intégration des commandes et des moyens d'information	124
A.4.9 Systèmes de communication	126
A.5 Vérification et validation du système intégré de salle de commande	128

CONTENTS OF APPENDIX A

DESIGN GUIDE FOR CONTROL ROOMS

Clause	Page
A.1 Scope and purpose of the appendix	63
A.1.1 Scope	63
A.1.2 Purpose	63
A.1.3 Application	63
A.1.4 Explanation of concepts and terms used in the standard	63
A.2 Design principles for control room	69
A.3 Functional design of control room	71
A.3.1 Functional analysis	71
A.3.2 Assignment of functions	75
A.3.3 Verification and validation of the function assignment and the integrated control room system	81
A.3.4 I & C systems	89
A.3.5 Job analysis	93
A.4 Functional design specification	95
A4.1 Fundamental design data of human factors	95
A.4.2 Location, environment and protection	99
A.4.3 Space and configuration	103
A.4.4 Panel layout	105
A4.5 Location aids	105
A.4.6 Information system	113
A.4.7 Controls	123
A.4.8 Control-display integration	125
A.4.9 Communication system	127
A.5 Verification and validation of the integrated control room system	129

ANNEXE A

GUIDE DE CONCEPTION DES SALLES DE COMMANDE

A.1 Domaine d'application et but de l'annexe

A.1.1 *Domaine d'application*

La présente annexe est un guide qui fournit des informations supplémentaires nécessaires à la conception des salles de commande, ces informations n'étant pas comprises dans la norme.

A.1.2 *But*

La norme sur la conception des salles de commande fournit la trame principale de conception des salles de commande et contient uniquement les exigences fondamentales de conception. Le but de cette annexe est de fournir des informations supplémentaires qui incluent des principes philosophiques et méthodologiques, des explications et recommandations et des spécifications détaillées pour la conception des salles de commande.

A.1.3 *Application*

Cette annexe est établie pour fournir des informations supplémentaires. Elle est applicable aux salles de commande de conception nouvelle dont la conception débutera après la parution de cette norme. Si l'on désire l'appliquer aux centrales existantes ou en projet, des précautions particulières sont à prendre en ce qui concerne des facteurs tels que le niveau d'automatisme.

A.1.4 *Explication des concepts et des termes utilisés dans la norme*

A.1.4.1 *Le système de salle de commande*

L'ensemble "interface homme/machine, équipe de conduite, procédures de conduite, programme de formation, matériels ou installations associées" est appelé système de "salle de commande" et est représenté sur la figure 1. Dans les paragraphes ci-après, les fonctions des constituants du système de salle de commande et leurs relations sont explicitées.

Il y a deux objectifs opérationnels majeurs pour la centrale, la production maîtrisée d'électricité et la prévention des rejets de radioactivité dans l'environnement. Un certain nombre d'objectifs fonctionnels doivent être satisfaits pour obtenir les objectifs opérationnels de la centrale. Ils sont satisfaits pour le contrôle du processus au travers de l'utilisation contrôlée des ressources de la centrale, par exemple les systèmes mécaniques (ici, "contrôle" se réfère à la fois à la commande et à la protection).

Il y a essentiellement deux manières de contrôler les systèmes de la centrale, automatiquement et manuellement (commande manuelle locale et commande à distance). Les systèmes supportant les commandes automatiques et les commandes manuelles à distance sont appelés systèmes de commande et de sûreté; ils font partie du système de contrôle-commande, et comprennent les actionneurs, les capteurs et les autres matériels.

Les actions automatiques requièrent de la part de l'équipe de salle de commande, de surveiller leur exécution correcte au travers de moyens d'affichage et d'effectuer des commandes manuelles qui incluent des commandes en secours des automatismes, des remises à zéro, etc.

Les commandes manuelles à distance exigent une intervention de l'équipe de salle de commande au travers de moyens de commande et d'afficheurs localisés dans la salle de commande principale.

APPENDIX A

DESIGN GUIDE FOR CONTROL ROOMS

A.1 Scope and purpose of the appendix

A.1.1 Scope

This appendix is a guide to provide the supplementary information necessary in the design of control rooms, which is not contained in the standard.

A.1.2 Purpose

The design standard for control rooms forms the main basis for control room design and covers only fundamental requirements for the design. The purpose of this appendix is to provide supplementary information which include points of philosophy and methodology, explanations and detailed recommendations and specifications for the control room design.

A.1.3 Application

This appendix is provided to give supplementary information. It is intended to apply to new control rooms whose design is initiated after the publication of this standard. If it is desired to apply it to existing plants or designs, special caution shall be used concerning factors such as automation level.

A.1.4 Explanation of concepts and terms used in the standard

A.1.4.1 The control room system

An integration of the man/machine interface, control room staff, operating procedures, training programme, and associated equipments and facilities is called a control room system - a shaded area in Figure 1. In subsequent sub-clauses, functions and interrelationship of these control room system constituents are explained.

There are two major plant operational goals: controlled generation of electricity and prevention of release of radioactivity to the environment. A number of functional goals shall be satisfied to achieve the plant operational goals. They are satisfied by controlling ("controlling" refers to control and protection) plant processes through controlled utilization of plant resources, e.g. mechanical plant.

There are, essentially, two ways of controlling the plant systems: automatic control and manual control which includes remote and local manual control. Hardware systems implementing automatic control and remote manual control are called control and safety systems, a part of the I & C system, and include actuators, sensors, and other hardware devices.

Operation of automatic control requires the control room staff to monitor its action through the displays, and to take manual control, which includes back-up control, reset, etc.

Operation of remote manual control requires the intervention of the control room staff through controls and displays located in the main control room.

Les commandes et les afficheurs, qui font également partie du système de contrôle-commande, constituent l'interface physique avec l'équipe de salle de commande (voir figure 1), et sont ainsi appelés interface homme/machine.

Les commandes manuelles locales sont effectuées localement - en des lieux extérieurs à la salle de commande principale - par des opérateurs locaux depuis des installations de commande locales, etc., sur demande de l'équipe de salle de commande. Des instructions sont données au travers de l'interface de communication.

Outre les commandes automatiques, les commandes manuelles et la surveillance¹ associée, une démarche intellectuelle est demandée à l'équipe de salle de commande (par exemple l'interprétation de multiples lectures, l'élaboration de stratégie basée sur la connaissance).

Des efforts intensifs ont été ou sont faits pour développer des systèmes supports de l'opérateur utilisant des calculateurs pour aider aux démarches intellectuelles. Il y a différents types de systèmes supports de l'opérateur disponibles, par exemple des systèmes de diagnostic, des systèmes d'aide à la conduite et d'aide à l'application des procédures.

L'équipe de salle de commande peut avoir différentes sortes d'interfaces avec ces systèmes, depuis le simple retour d'information unidirectionnel au travers d'afficheurs, jusqu'à la communication bidirectionnelle de haut niveau au travers de matériels appropriés. Le système support de l'opérateur est classé dans la catégorie des interfaces homme/machine.

Les communications avec le personnel de la centrale ou l'équipe de direction se trouvant dans les installations situées à l'extérieur de la salle de commande principale peuvent être réalisées au travers de l'interface de communication.

¹ Le terme "surveillance" se réfère à des tâches telles que le contrôle d'un niveau ou d'un état.

The controls and displays, which are also a part of I & C system, have a physical interface with the control room staff, as shown in Figure 1, and, therefore, they are called the man/machine interface.

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

Besides automatic control, manual control and associated monitoring¹, 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.

Extensive efforts have been, and are being made to develop computer-based operator support systems to aid the high-level mental processing. There are various types of operator support systems available, e.g. diagnostic systems, operation consulting systems, procedure synthesizers.

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 described as a man-machine interface.

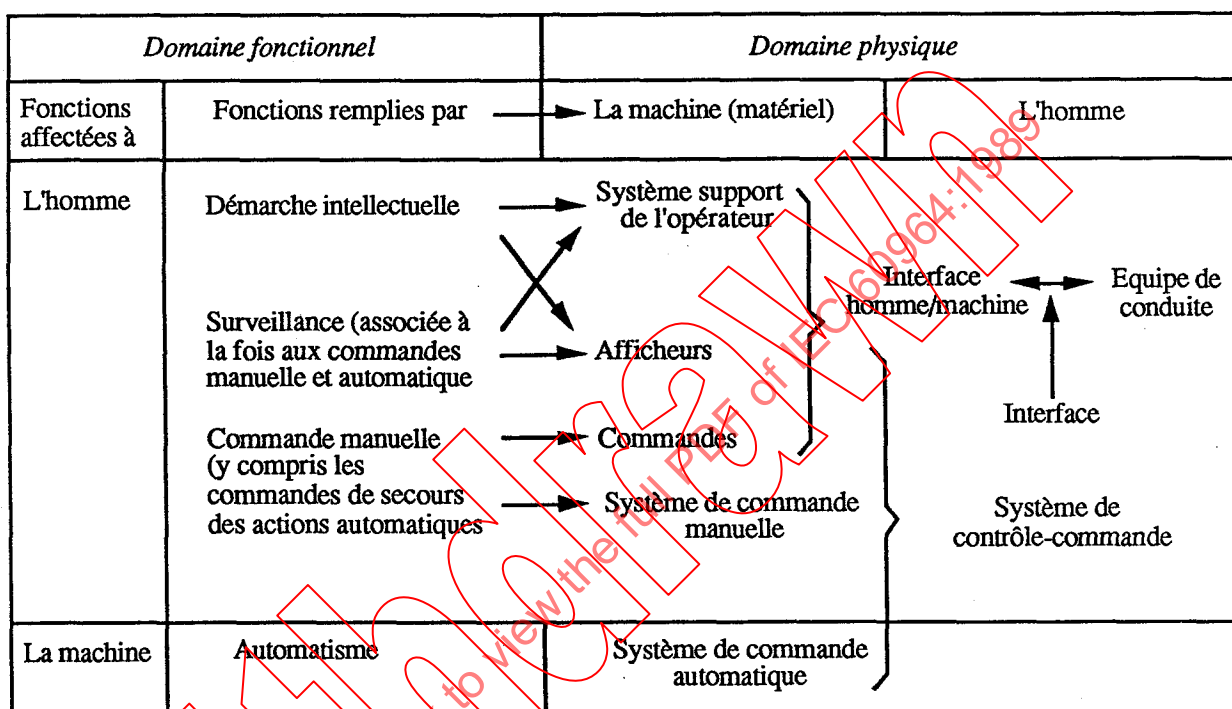
Communication with plant personnel and managerial staff stationed outside the main control room can be made through the communication interface.

¹ The term "monitoring" refers to simple tasks such as level checking, status checking.

A.1.4.2 Homme et machine

Affecter des fonctions à la machine signifie les remplir par un automatisme. Par conséquent, dans le domaine fonctionnel, "machine" symbolise l'automatisation, tandis que "homme" symbolise l'équipe de salle de commande (ensemble d'opérateurs). Affecter des fonctions à l'homme signifie les remplir soit par des commandes manuelles, soit par la surveillance, soit par une démarche intellectuelle ou par leur combinaison (voir tableau A.1).

Tableau A.1 - L'homme et la machine dans le domaine fonctionnel et dans le domaine physique



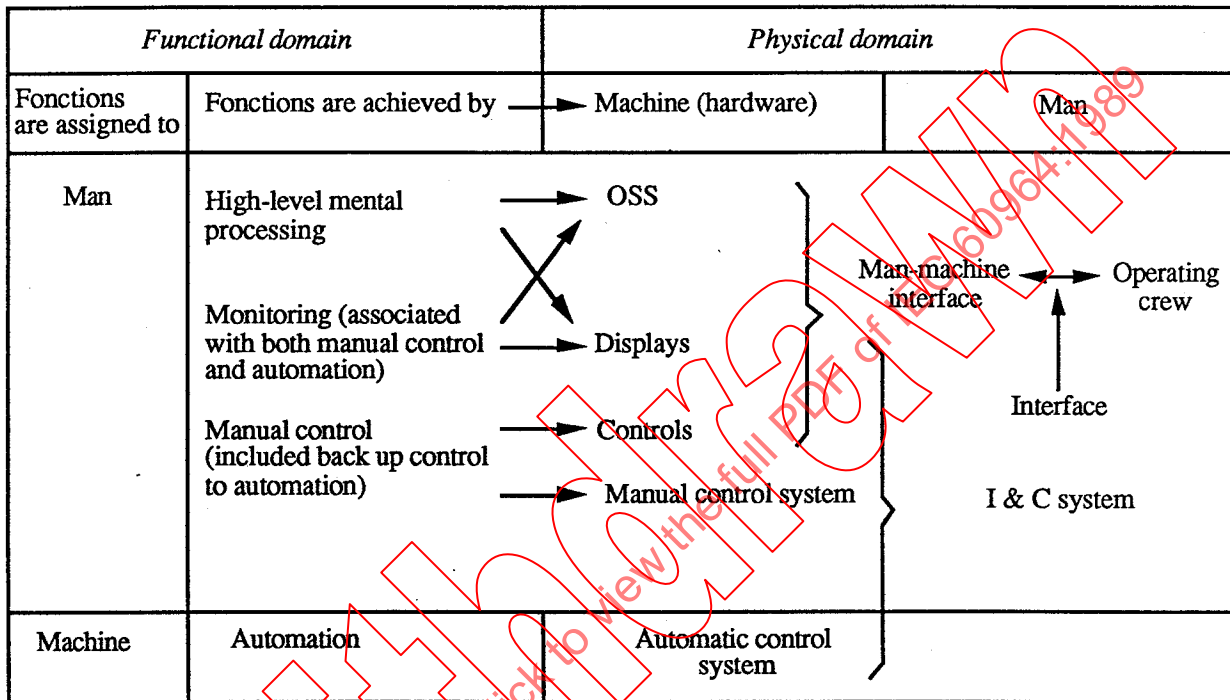
Le terme "machine" couvre un ensemble de matériels qui incluent le système de contrôle-commande et le système support de l'opérateur. Il y a lieu de remarquer que les systèmes manuels de réglage, les moyens de commande et de présentation d'information, qui font partie du système de contrôle-commande, permettent à l'équipe de salle de commande de remplir les fonctions qui lui sont assignées.

Ces notions spécifiées dans la norme sont présentées dans le tableau A.2.

A.1.4.2 Man and machine

The assignment of functions to machine means to achieve them by automation. Therefore, "machine" in the functional domain signifies automation, while, "man" in functional domain, signifies the control room staff. Assigning functions to man means to achieve them by either manual control, monitoring, high-level mental processing, or their combinations (see Table A.1).

Table A.1 - Man and machine in functional domain and physical domain



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

Items specified in the standard are shown in Table A.2.

A.2 Principes de conception de la salle de commande

Les principes de conception de la salle de commande figurent à l'article 2, comme base de conception.

On peut également se référer, dans le domaine de la sûreté, aux guides de sûreté AIEA figurant dans le programme NUSS.

Tableau A.2 - Notions spécifiées dans la norme

Notion	Exigences	Critères de V et V
<i>Domaine fonctionnel</i> (1) Homme/machine (2) Commande à distance / Commande locale (3) Fonctions ou tâches à assurer par le système support de l'opérateur (SSO) (4) Procédures de conduite Programme de formation et structure de l'équipe salle de commande	Oui (3.1 et 3.2) Oui (3.1 et 3.2) Oui (3.1 et 3.2) Oui mais seulement les exigences d'interface	Oui (3.1 et 3.4) Oui (3.3 et 3.4) Oui (3.3 et 3.4) Oui mais seulement les exigences d'interface
<i>Domaine physique</i> (1) Conception fonctionnelle du système de contrôle-commande (2) Conception fonctionnelle de l'interface homme/machine (3) Procédures de conduite Formation et structure de l'équipe de salle de commande	Hors norme Oui (article 4) Hors norme	Hors norme Oui (5.1 et 5.2) Oui mais seulement en tant que système intégré salle de commande (5.1 et 5.2)

A.2 Design principles for control room

Design principles for the control room are provided in Clause 2.

IAEA Safety Guides provided in the NUSS programme can also be referred to in the safety area.

Table A.2 - Items specified in the standard

Item	Requirements	V & V criteria
<i>Functional domain</i>		
(1) Man/machine	Yes (3.1 and 3.2)	Yes (3.1 and 3.4)
(2) Remote control/Local control	Yes (3.1 and 3.2)	Yes (3.3 and 3.4)
(3) Functions or tasks to be supported by operator support system (OSS)	Yes (3.1 and 3.2)	Yes (3.3 and 3.4)
(4) Operational procedures Training programme and criteria structure of control room staff	Yes but only interface requirements	Yes but only interface requirements
<i>Physical domain</i>		
(1) Function design of I & C system	Out of this standard	Out of this standard
(2) Function design of man/machine interface	Yes (Clause 4)	Yes (5.1 and 5.2)
(3) Operational procedures Training system and structure of control room staff	Out of this standard	Yes but only as an integrated control room system (5.1 and 5.2)

A.3 Conception fonctionnelle de la salle de commande

A.3.1 Analyse fonctionnelle

A.3.1.1 Identification des fonctions

Ainsi qu'il est spécifié en 3.1, l'analyse des fonctions débute par l'établissement d'une structure d'objectifs hiérarchisés.

Puisque les finalités de la conception d'une centrale nucléaire sont la production contrôlée d'électricité (objectif de disponibilité) et la limitation des rejets radioactifs dans l'environnement (objectif de sûreté), ces objectifs peuvent être placés au sommet de la hiérarchie à établir.

En premier lieu, il convient que le concepteur analyse quelles sont les dispositions essentielles à respecter pour atteindre chacun de ces objectifs.

L'objectif de disponibilité a ainsi quatre sous-objectifs:

- Amener la centrale jusqu'à un état opérationnel en puissance (démarrage et montée en puissance).
- Contrôler la chaudière dans les différents modes de fonctionnement normaux (c'est-à-dire fonctionnement en base, suivi de charge, etc.).
- Convertir l'énergie produite par la chaudière en électricité et conduire la centrale avec l'efficacité et la disponibilité la plus élevées possible.
- Contrôler l'arrêt du réacteur et le rechargement du combustible.

Le concepteur doit aussi identifier les fonctions essentielles pour chacun de ces sous-objectifs. Elles sont habituellement appelées fonctions critiques de disponibilité, puisque la perte de ces fonctions modifie le maintien en puissance, et de ce fait, affecte la disponibilité de la centrale.

Par exemple, pour le deuxième sous-objectif (la fourniture de vapeur nucléaire), on identifie les fonctions suivantes:

- contrôle de la puissance nucléaire;
- contrôle de la distribution de flux neutronique;
- contrôle de l'inventaire en eau;
- contrôle de l'évacuation de chaleur du cœur;
- contrôle de la source froide;
- contrôle du groupe turbo-alternateur;
- maintien de l'intégrité du système de refroidissement du réacteur.

Par rapport à l'objectif de sûreté, trois barrières physiques sont réalisées pour éviter les rejets de radioactivité: la gaine du combustible, le système de refroidissement du réacteur et l'enceinte de confinement.

Les procédures de conduite visent à maintenir l'intégrité de chacune de ces barrières pour atteindre l'objectif de sûreté en conditions accidentelles. Le concepteur identifie alors les fonctions essentielles au maintien de l'intégrité des barrières.

A.3 Functional design of control room

A.3.1 Functional analysis

A.3.1.1 Identification of functions

As specified in 3.1, the functional analysis starts with the development of hierarchical goal structures.

Since the ultimate purposes of the plant are controlled generation of electricity (availability goal) and prevention of activity release to the environment (safety goal), these are the goals to be placed at the top of the hierarchy.

First, the designer should analyze the essential design considerations made to achieve each of these goals.

For the availability goal, there are four sub-goals:

- Bring the plant to an operational state at power (start-up operation, initial power increase).
- Control nuclear steam supply under various normal operational modes (e.g. steady power operation, load follow operation, etc.).
- Convert nuclear steam supply of energy to electricity and operate plant with the highest practicable efficiency and availability.
- Shut-down and refuelling.

The designer should identify essential functions for each of these sub-goals. They are usually called critical availability functions, since the loss of these functions will change the maintenance of power operation thereby affecting the plant availability.

For instance, the following are identified for the second sub-goal (e.g. for control of nuclear steam supply):

- control nuclear power;
- control neutron flux distribution;
- control coolant inventory;
- control core heat removal;
- control heat sink;
- control turbine generator system;
- maintain reactor coolant system performance.

For the safety goal, there are generally three physical barriers implemented to prevent activity release: fuel clad, boundary of reactor coolant system and containment vessel.

The operating procedures are intended to maintain the integrity of these barriers to achieve the safety goal under accident conditions. The designer, then, identifies essential functions that support the maintenance of the barrier integrity.

Les fonctions critiques de sûreté les plus importantes sont les suivantes:

- contrôle de la réactivité en sous-criticalité (maintien de la sous-criticalité);
- maintien de l'inventaire en eau;
- maintien de l'évacuation de chaleur du cœur;
- maintien de la source froide;
- maintien de l'intégrité du système de refroidissement du réacteur;
- maintien de l'intégrité de l'enceinte de confinement.

La perte de ces fonctions dans un accident peut mettre la centrale dans un état critique qui remet en question le plan de sûreté.

NOTE - Bien que le déclenchement ne soit pas une opération normale, il doit être en principe considéré dans le deuxième sous-groupe défini ci-dessus (par exemple le contrôle du fonctionnement de la chaudière).

Après l'identification des fonctions critiques (fonctions critiques de sûreté et de disponibilité), le concepteur peut décomposer chacune de ces fonctions.

Par exemple, pour les réacteurs à eau sous pression, la première fonction critique identifiée ci-dessus peut être décomposée selon les sous-fonctions suivantes:

- maintien de toutes les barres de commande enfoncées;
- maintien d'une concentration chimique suffisante dans le poison liquide servant à la commande de la compensation.

Le concepteur pourrait continuer la décomposition jusqu'à ce qu'il n'y ait plus de décomposition possible. Cependant, il peut s'arrêter lorsqu'il a pu obtenir des sous-fonctions suffisamment détaillées et lorsque les constituants du système important pour l'analyse ont été identifiés.

La hiérarchie obtenue aura, au sommet, les fonctions de plus haut niveau d'abstraction, au milieu, des fonctions au niveau système et, à la base, des matériels détaillés ou des fonctions au niveau composants.

A.3.1.2 Flux d'informations et exigences de traitement

L'étape suivante de l'analyse fonctionnelle est l'identification des exigences de traitement et des informations pour chacune des fonctions identifiées dans les étapes précédentes.

Pour chaque fonction, il y a lieu que le concepteur identifie:

- les paramètres observables indiquant l'état de la centrale;
- les commandes et les éléments de référence pour remplir cette fonction.

Il convient également que le concepteur sache:

- comment déterminer le fonctionnement correct de chaque fonction;
- quelles solutions de remplacement sont disponibles lorsque l'on perd ce fonctionnement correct et comment on peut choisir parmi elles.

Ici, ces solutions de remplacement se réfèrent à des fonctions qui peuvent se situer à un niveau fonctionnel plus élevé que celui de la fonction analysée. Par exemple, on peut trouver plusieurs chemins redondants d'évacuation de la chaleur, qui sont choisis de façon interchangeable selon les conditions de la centrale.

The most essential critical safety functions are as follows:

- control reactivity below critical (maintain sub-criticality);
- maintain coolant inventory;
- maintain core heat removal;
- maintain heat sink;
- maintain reactor coolant system integrity;
- maintain containment vessel integrity.

The loss of these functions in an accident conditions may result in severely degraded plant conditions that challenge the plant safety.

NOTE - Although electric load shut-down is not a normal operation, it should be considered under the second sub-goal defined above (e.g. control of nuclear steam supply).

After identifying the critical functions (i.e. critical safety functions and critical availability functions), the designer can decompose each of the critical functions.

For example, in the case of PWRs, the first critical function identified above can be subdivided into sub-functions as follows:

- maintain all control rods fully inserted in the core;
- maintain sufficient concentrations of chemical poison shim-control liquid.

The designer should continue the decomposition until further decomposition is impossible. However, it can be stopped where detailed sub-functions could be obtained and the important constituents of the systems have been identified for the analysis.

The resultant hierarchy will have the abstract high-level functions at the top, system-level functions in the middle, and detailed equipment- or component-level functions at the bottom levels.

A.3.1.2 Information flow and processing requirements

The next step of the functional analysis is the identification of information and processing requirements for each of the functions identified in the previous step.

For each function, the designer should identify the following:

- observable parameter which will indicate the plant status;
- control process and performance measures required to achieve the function.

The designer should also identify:

- how to determine correct discharge of the function;
- what alternatives are available if correct functioning is lost and how alternatives can be chosen.

Here, alternatives refer to functions that can support a higher level function in place of the function being analyzed. For instance, several redundant heat removal paths could be chosen depending on the plant conditions.

A ce stade, l'approche doit en principe être générale et ne pas se référer à une implantation spécifique ni impliquer l'opérateur.

Lors de l'identification des valeurs de référence permettant de garantir la réalisation de la fonction, il est parfois souhaitable d'utiliser des informations se rapportant aux événements de référence. Il est souhaitable de disposer de valeurs de référence basées sur une approche physique. Ainsi, une de ces valeurs, pour l'évacuation de la chaleur du cœur, peut être déterminée par une information sur les matériaux utilisés pour la gaine du combustible, par exemple la température de fusion. Cependant, toutes les valeurs de référence ne peuvent être déterminées de cette façon. Parfois, on doit se contenter d'une information obtenue lors des analyses d'accident. Une sélection d'événements est spécifiée en 3.1.2.

Bien que le concepteur ait à identifier un ensemble d'événements représentatifs les mieux adaptés aux objectifs de conception, il peut considérer la liste ci-après comme étant une sélection caractéristique.

a) Événements liés à la sûreté

- accident de perte de refroidissement;
- brèches dans les conduites de vapeur principales;
- brèches dans l'alimentation en eau (réacteurs à eau sous pression);
- rupture d'un tube de générateur de vapeur (réacteurs à eau sous pression);
- pertes de toutes les sources d'alimentation électriques en courant alternatif.

b) Événements liés à la disponibilité

- défaut de capteur du système de contrôle (par exemple système de contrôle d'alimentation en eau des réacteurs à eau sous pression).

Le concepteur doit en principe choisir des événements qui couvrent uniquement les fonctions analysées. Il doit en principe savoir que la perte de certaines fonctions est équivalente à l'apparition d'un certain événement et pouvoir montrer comment cela peut affecter des fonctions de niveau plus élevé, par une propagation dans la hiérarchie des fonctions du bas vers le haut.

A.3.2 Répartition des fonctions

La répartition des fonctions comporte trois phases:

- l'analyse des tâches;
- l'établissement des critères de répartition;
- la répartition.

A.3.2.1 Analyse des tâches

En utilisant la base de données établie lors de l'analyse des fonctions (c'est-à-dire les flux d'informations et les exigences de traitements), le concepteur procède à une analyse des tâches. Le but de cette analyse est d'identifier le contenu détaillé de chaque tâche et ses éléments caractéristiques.

En premier lieu, le concepteur doit en principe regrouper les sous-fonctions si étroitement liées qu'elles peuvent être traitées comme une unité. Ces sous-fonctions peuvent également être structurées hiérarchiquement. De telles unités peuvent être divisées en deux groupes.

Un groupe consiste en unités fonctionnelles dont le fonctionnement simultané est une condition essentielle pour remplir une fonction de plus haut niveau. Un autre groupe consiste en unités fonctionnelles qui sont des fonctions support de remplacement pour une fonction de plus haut niveau ou dont le fonctionnement n'est pas une condition indispensable à la réalisation d'une fonction de plus haut niveau.

At this stage, the approach should be general and not refer to a specific implementation or level of human involvement.

When identifying performance measures that ensure the achievement of a function, it is sometimes advisable to utilize information on design basis events. It is ideal to develop performance measures based upon a truly physical approach. For instance, one of the performance measures for the core heat removal can be determined from the knowledge of the materials used for the fuel cladding such as for example melting temperature. However, not all the performance measures can be determined this way. Sometimes, one has to rely on information obtained from accident analysis. Guidelines for event selection are specified in 3.1.2.

Although each designer should identify a set of representative events best fitted to his design purposes, the following is a typical selection:

a) Safety-related

- loss of coolant accident;
- main steamline break;
- feedwater line break (PWR);
- steam generator tube rupture (PWR);
- loss of all AC power.

b) Availability-related

- failure of control system sensor (e.g. feedwater control system of PWR).

The designer should select events that can cover the range of functions being analyzed. The designer should know that the loss of a certain function is equivalent to the occurrence of a certain event, and can see how it may affect higher level functions by propagating through the hierarchy from bottom to top.

A.3.2 Assignment of functions

The function assignment consists of three phases:

- task analysis;
- development of assignment criteria;
- assignment.

A.3.2.1 Task analysis

Using the data base developed in the function analysis (i.e. information flow and processing requirements), the designer conducts a task analysis. The purpose of task analysis is to identify the detailed components of a task and its characteristic measures.

First, the designer should define an integration of such sub-functions as are closely related so that they can be treated as a unit. These may also have hierarchical structures. Such units can be divided into two groups.

One consists of function units whose common achievement is an essential condition for the accomplishment of a higher level function. Another group consists of functional units which are alternative supporting functions to a higher level function or whose accomplishment is not necessarily a requisite condition for a higher level function.

En second lieu, le concepteur doit en principe identifier, pour chacune de ces sous-fonctions regroupées, les éléments suivants (c'est-à-dire le contenu d'une tâche):

- l'enchaînement logique conduisant à sa réalisation (Pourquoi est-elle requise?);
- les actions de commande nécessaires à sa réalisation (Comment peut-elle être obtenue?);
- les paramètres nécessaires aux actions de commande;
- les critères permettant d'évaluer le résultat des actions de commande;
- les paramètres nécessaires à cette évaluation;
- les critères d'évaluation;
- les critères de choix des solutions de remplacement.

Il convient de remarquer que l'ensemble des paramètres identifiés ci-dessus constitue la base de regroupement des paramètres. Il constitue également la base de regroupement des moyens de présentation d'information et de commandes.

En troisième lieu, le concepteur doit identifier les éléments caractéristiques et définir plusieurs classes pour chaque élément. Les éléments caractéristiques doivent en principe être objectifs (par exemple temps, précisions), mais peuvent inclure des éléments subjectifs. Ils doivent également inclure des éléments qualitatifs, tels que ceux relatifs aux prises de décision. Le concepteur doit en principe y inclure les éléments suivants:

- la charge;
- la précision;
- les facteurs temps (vitesse, marge et contrainte de temps);
- la complexité des enchaînements logiques;
- les types et complexités des prises de décision (par exemple la reconnaissance de formes);
- les conséquences de la perte d'une fonction et les facteurs temps associés.

Il est conseillé au concepteur de contacter les experts en psychologie cognitive, aussi bien que les concepteurs de systèmes pour établir des éléments caractéristiques pertinents. Le concepteur classe alors chaque tâche par rapport à ces éléments caractéristiques.

A.3.2.2 *Etablissement des critères de répartition*

Parallèlement à l'analyse des tâches, le concepteur doit en principe développer des critères de prise de décision pour la répartition des fonctions:

- par l'homme ou par la machine;
- par des commandes manuelles à distance ou des commandes manuelles locales;
- par des systèmes supports de l'opérateur.

La base de ces critères doit être cohérente avec celle des éléments caractéristiques.

a) Critères de répartition des fonctions entre l'homme ou la machine

Les critères de répartition des fonctions entre l'homme ou la machine doivent en principe être fondés en premier lieu sur les éléments caractéristiques suivants:

- la charge;
- la précision;
- les facteurs temps;
- la complexité des enchaînements logiques;
- les types et complexités des prises de décisions.

Une structure de base des critères est présentée dans le tableau A.3.

Second, the designer should identify the following for each of these integrated sub-functions (i.e. contents of a task):

- logical requirements for its accomplishment (Why its accomplishment is required);
- control actions necessary for its accomplishment (How it can be accomplished);
- parameters necessary for control action;
- criteria for evaluating the result of control actions;
- parameters necessary for the evaluation;
- evaluation criteria;
- criteria for choosing alternatives.

It should be noted that the above identified parameter set forms the basis for parameter grouping. It also forms the basis for display and control layout grouping.

Third, the designer should identify characteristic measurements and define several classes for each measurement. The characteristic measurements should be objective (e.g. time, rate), but may include subjectively scaled ones. They should also include qualitative measurements to assist decision-making. The designer should consider the following characteristics:

- load;
- accuracy;
- time factors (e.g. rate, time margin/constraint);
- complexity of action logic;
- types and complexities of decision-making (e.g. pattern recognition);
- impacts resulted from the loss of function and associated time factors.

It is advisable for the designer to consult experts on cognitive psychology as well as system designers to develop relevant characteristic measurements. The designer, then, classifies each task for all the characteristic measurements.

A.3.2.2 Development of assignment criteria

In parallel with the task analysis, the designer should develop criteria for the decision points of the function assignment:

- to man or machine;
- to remote manual control or local manual control;
- to operator support systems.

The basis for the criteria shall be consistent with that for the characteristic measurements.

a) Criteria for function assignment to man or machine

Criteria for assignment of functions to man or machine should be based primarily on the following characteristics factors:

- load;
- accuracy;
- time factors;
- complexity of action logic;
- types and complexities of decision-makings.

A basic structure for the criteria is presented in Table A.3.

b) Critères de répartition des fonctions entre commandes manuelles à distance et commandes manuelles locales

Les critères de répartition des fonctions entre commandes manuelles à distance et commandes manuelles locales doivent en principe être fondés en premier lieu sur les paramètres caractéristiques suivants:

- les facteurs temps;
- les conséquences de la perte des fonctions et facteurs temps associés.

Les fonctions pour lesquelles ce facteur temps est élevé (rapidité) et les conséquences sérieuses ne doivent pas en principe être commandées localement.

Tableau A.3 - Répartition des fonctions entre l'homme et la machine. Structure de base

Mesures caractéristiques	Répartitions	
	Homme	Machine
Charge	Modérée	Elevée, très faible
Marge temporelle	Grande	Etroite, très grande
Vitesse	Modérée	Elevée, très lente
Complexité des logiques d'action	Simple	Complexe
Type et complexité des prises de décision	Mal structuré	Bien structuré

c) Critères pour l'affectation de fonctions aux systèmes supports de l'opérateur (SSO)

Les critères pour l'affectation de fonctions aux systèmes supports de l'opérateur doivent en principe être fondés en premier lieu sur les paramètres caractéristiques suivants:

- la complexité dans la prise de décision avec des marges de temps limitées;
- l'importance de la prise de décision sur la sûreté et la disponibilité de la centrale;
- la nécessité d'accroître les capacités potentielles de l'opérateur dans les activités de prise de décision, par exemple diagnostic et démarche intellectuelle.

A.3.2.3 Répartition

Le concepteur peut conduire la répartition des fonctions en comparant les paramètres caractéristiques aux critères d'affectation. Comme spécifié dans cette norme, la répartition des fonctions est poursuivie tant que les insuffisances de conception sont identifiées lors des vérifications et validations.

b) Criteria for function assignment for remote or local manual controls

Criteria for assignment of functions to remote manual control or local manual control should be based primarily upon the following characteristic measures:

- time factors;
- impacts resulting from the loss of functions and associated time factors.

Those functions associated with quicker or higher time factors and large impacts should not be locally controlled.

Table A.3 - Assignment of functions to man and machine. Basic structure of assignment

Characteristics	Assignment	
	Man	Machine
Load	Moderate	High, very low
Time margins	Large	Small, very large
Rate	Moderate	High, very low
Complexity of action logic	Simple	Complicated
Types and complexities of decision-making	Ill-structured	Well-structured

c) Criteria for function assignment for operator support systems (OSS)

Criteria for assignment of functions to operator support system should be based primarily on the following characteristic measures:

- complexity of decision-making with limited time margins;
- importance of decision-making to the plant safety and availability;
- necessity for enhancement of operator's potential capabilities in decision-making activities, e.g. diagnostic monitoring and high-level mental processing.

A.3.2.3 Assignment

The designer can conduct the function assignment by comparing the classified characteristic measures against the assignment criteria. As specified in this standard, the function assignment continues until no design deficiencies can be identified in the verification and validation.

A.3.3 Vérification et validation de la répartition des fonctions et du système intégré de salle de commande

A.3.3.1 Aspects communs à la vérification et à la validation (V et V)

La répartition des fonctions de la salle de commande entre l'homme et la machine et la conception d'ensemble du système intégré de salle de commande sont vérifiés et validés comme indiqué à la figure 2.

1) Processus

Le processus de vérification et de validation doit en principe inclure les phases suivantes:

a) Préparation

La préparation doit en principe inclure l'identification des documents sources, l'établissement des critères d'évaluation, la constitution de l'équipe d'évaluation et la planification de l'évaluation. On doit en particulier veiller à l'exhaustivité des documents et à l'indépendance de l'équipe d'évaluation.

La préparation de la validation doit en principe inclure également une sélection d'événements représentatifs et une synthèse des séquences fonctionnelles. Une expertise opérationnelle est particulièrement importante lors de la validation du système intégré de salle de commande. En outre, l'équipe d'évaluation doit en principe être pluridisciplinaire, dans la mesure où cela est nécessaire.

b) Evaluation

L'évaluation doit être systématique et son processus doit être documenté de façon traçable. Les évaluations des fonctions affectées à l'homme et de celles affectées à la machine doivent en principe être faites en parallèle, comme indiqué sur la figure 2.

c) Correction

Toutes les erreurs identifiées lors de l'évaluation doivent être corrigées individuellement ou de façon itérative jusqu'à ce que les spécifications fonctionnelles respectent tous les critères d'évaluation. Les modifications des critères d'affectation et/ou de réaffectation des fonctions doivent être faites si une inadéquation est trouvée lors de la vérification ou de la validation, comme indiqué par les boucles d'itération de la figure 2.

Dans le cas où des insuffisances fondamentales sont identifiées, les corrections doivent en principe être réalisées et notées avec soin, de telle sorte qu'elles n'aient pas d'effet de bord défavorables sur les concepts qui auraient été trouvés adéquats lors de l'évaluation initiale. De toute façon, la validation doit être faite de façon itérative chaque fois que l'intégration proposée du système de salle de commande est modifiée.

2) Equipe d'évaluation

Deux recommandations sont essentielles pour l'équipe d'évaluation.

En premier lieu, l'équipe doit en principe être indépendante des concepteurs impliqués dans la répartition initiale des fonctions ou dans la réalisation de l'intégration du système de salle de commande. Cependant, cela ne signifie pas d'interdire la communication avec les concepteurs; ceux-ci doivent en principe être disponibles pour des discussions et des explications.

A.3.3 Verification and validation of the function assignment and the integrated control room system

A.3.3.1 Items common to verification and validation (V & V)

The assignment of control room functions to man and machine and the overall design of integrated control room system are verified and validated as shown in Figure 2.

1) Process

The process of the V & V should include the following phases:

a) Preparation

Preparation should include identifying source documents, developing evaluation criteria, organizing an evaluation team, and scheduling the evaluation. Special attention should be paid to the completeness of the documents and the independence of the evaluation team.

It should include also selecting representative events and synthesizing functional sequences for validation. Operational expertise is particularly important in the validation of an integrated control room system. In addition, the evaluation team should be, to the extent necessary, interdisciplinary.

b) Evaluation

The evaluation shall be systematic and its process shall be documented in a traceable manner. The evaluation of the function assignment to man or to machine should be made in parallel as shown in Figure 2.

c) Resolution

Any mistakes identified in the evaluation shall be corrected individually or iteratively until the function assignment meets all the evaluation criteria. Modification of assignment criteria or reassignment of functions shall be made if any inadequacy is found in the verification or the validation as indicated by the iteration paths shown in Figure 2.

If fundamental deficiencies are identified, resolution should be carefully developed and recorded, so that no unfavourable side effects are imposed on design concepts which have been found adequate in the original evaluation. In any case, the validation shall be iteratively made when the proposed control room system integration is modified.

2) Evaluation team

There are essentially two recommendations for the evaluation team.

First, the team should be independent of designers involved in the initial function assignment or the development of control room system integration. However, this does not need to inhibit the communication with the designer; rather, they should be available for discussions and explanations.

En second lieu, l'équipe doit en principe relever des disciplines concernées. Il convient d'inclure les domaines d'expertise suivants:

- ingénierie nucléaire;
- conception architecturale et génie civil;
- analyse des systèmes;
- système de contrôle-commande;
- traitement de l'information et systèmes informatiques;
- ingénierie des facteurs humains;
- expérience en conduite et en formation.

Une expérience en conduite est nécessaire pour s'assurer que les prescriptions proposées sont réalistes. Le nombre de membres de l'équipe doit en principe être maintenu faible afin d'assurer un travail efficace. L'expertise dans des domaines non couverts par l'équipe d'évaluation doit être réalisée par la consultation d'experts en dehors de l'équipe.

A.3.3.2 Vérification et validation de la répartition des fonctions

a) Vérification de la répartition des fonctions

Comme spécifié dans cette norme, le concepteur doit vérifier l'exhaustivité de la répartition des fonctions. On doit en principe noter que ce n'est pas par la vérification, mais par la validation, que le concepteur peut s'assurer de la justesse de cette répartition qui entend assurer les performances optimales de l'homme et de la machine.

b) Validation de la répartition des fonctions

Les structures hiérarchiques basées sur des objectifs, établies lors de l'analyse des fonctions, sont fondamentalement des bases de données statiques. Le concepteur peut savoir comment chacune des fonctions peut être remplie ou non remplie en se référant aux éléments de référence définis pour chacune d'elles. Cependant, il n'est pas nécessairement évident de voir comment une suite de fonctions peut être exécutée de façon dynamique à l'occasion d'événement spécifique. La perte d'une fonction déclenche un événement: à quelle vitesse, son influence peut-elle se propager à l'intérieur de la hiérarchie et quelles fonctions de plus haut niveau peuvent être influencées? Cela dépend de la nature de l'événement et de son étendue. Les principaux buts de la validation sont d'analyser ces caractéristiques de la hiérarchie qui dépendent du temps et de s'assurer de l'adéquation de la répartition des fonctions.

A.3.3.3 Vérification et validation du système intégré de salle de commande

La vérification et la validation du système intégré de salle de commande supposent que les exigences fonctionnelles vérifiées et validées, établies conformément à l'article 3, ont été utilisées comme des entrées dans le travail de conception, et ont abouti à des spécifications détaillées pour les constructeurs et les réalisateurs de la salle de commande visée. Dans ce travail de conception, les critères et recommandations donnés à l'article 4 sont à considérer.

A cette étape du développement, la salle de commande existe en tant que concept décrit en détail par des dessins et des spécifications écrites. Au moins dans le principe, les objectifs du travail de vérification et de validation sont de vérifier les spécifications avant que le processus de réalisation ne commence. En pratique, le processus de vérification et de validation peut être étendu sur une large période de temps, à cause des différents décalages de temps entre les différentes parties du projet.

Second, the team should maintain relevant disciplines. The following expertises should be included:

- nuclear engineering;
- architectural design and civil engineering;
- systems analysis;
- I & C systems;
- information and computer systems;
- human factors engineering;
- operating experience and training.

The operating experience is needed to ensure that the proposed requirements are realistic. The number of members in the team should be kept low in order to ensure efficient work. Expertise in areas not covered by the evaluation team shall be achieved by consulting experts outside the team.

A.3.3.2 *V & V of the function assignment*

a) Verification of function assignment

As specified in this standard, the designer shall verify the completeness of the function assignment. It should be noted that it is not the verification but the validation in which the designer can assess the correctness of the function assignment that would assure the optimized performance of man and machine.

b) Validation of function assignment

The goal-oriented hierarchical structures developed in the function analysis are basically static data bases. The designer can know how each of the functions can be accomplished or cannot be accomplished by referring to performance measures defined for them. However, it is not necessarily evident how a series of functions are required to be accomplished dynamically under a specific event. The loss of a certain function initiates an event. How fast its influence may propagate along the hierarchy and which higher level functions may be influenced depend on the kind of event and its scale. The main purposes of the validation are to analyze these time-dependent characteristics of the hierarchies and to assure the adequacy of the function assignment.

A.3.3.3 *V & V of the integrated control room system*

The verification and validation of the integrated control room system assumes that the verified and validated functional requirements developed according to Clause 3 have been used as inputs for a design effort, resulting in detailed specifications for the manufacturing and construction of the desired control room. In this design work the criteria and recommendations given in Clause 4 shall be considered.

At this stage of development, the control room exists as a concept, described in detail by drawings and specifications. At least in principle the objective of the verification and validation effort is to check the specifications before the manufacturing process is started. In practice, the verification and validation process could be spread out over a period of time due to various time lags between different parts of the project.

La vérification des éléments constituant la salle de commande est obtenue par l'évaluation des spécifications de conception proposées en fonction des exigences fonctionnelles applicables, ainsi que des exigences et des critères de conception.

La validation du système intégré de salle de commande est obtenue par l'évaluation des interactions entre la salle de commande, l'opérateur, les procédures et le programme de formation pour obtenir une conduite sûre et fiable de la centrale.

1) Vérification du système intégré de salle de commande

Il y a deux principales sources d'information à utiliser pour formuler les critères de vérification:

- les exigences fonctionnelles pour la salle de commande réelle, développées conformément à l'article 3;
- les règles et critères à appliquer dans la conception des salles de commande, fournis à l'article 4.

Les critères établis à partir de ces deux sources doivent couvrir les aspects purement techniques ainsi que les aspects d'ingénierie des facteurs humains.

Ces critères sont à utiliser pour démontrer que les principes appropriés d'ingénierie des facteurs humains ainsi que les capacités techniques requises ont été incorporés dans la conception de la salle de commande.

Les exemples typiques de critères de vérification sont les suivants:

- les instruments et afficheurs prévus en salle de commande doivent présenter les paramètres pertinents du processus;
- les commandes et afficheurs doivent être disposés selon une configuration cohérente et ordonnée;
- les instruments et afficheurs en panne doivent être aisément reconnaissables comme tels;
- les postes de travail doivent être disposés de telle sorte que l'accès aux panneaux de contrôle ne soit pas entravé;
- les commandes adéquates pour le réglage de la température, de l'humidité et de la ventilation doivent être prévues;
- les commandes doivent être disposées de telle sorte que les afficheurs associés puissent être utilisés pour fournir le retour d'information.

2) Validation du système intégré de salle de commande

L'objectif de la validation du système intégré de salle de commande est de s'assurer que les interactions entre les composants du système de salle de commande sont telles que le système intégré de salle de commande se comporte d'une façon conforme à celle exigée pour une conduite sûre et fiable de la centrale. Le domaine de validation se limite dans cette norme à trois interactions bidirectionnelles possibles:

- la salle de commande et l'opérateur;
- la salle de commande et les procédures de conduite;
- la salle de commande et le programme de formation.

a) Domaine de validation

Il doit être limité en prenant en compte le fait que la salle de commande, aussi bien que les procédures de conduite et le programme de formation, à cette phase de développement, n'existent que sous forme de spécifications écrites et de plans.

The verification of the control room is performed by evaluating the proposed design specifications against the applicable functional requirements and design requirements and criteria.

The validation of the integrated control room system is performed by evaluating the interactions between the control room, the operator, the procedures and the training programme which support safe and reliable operation of the plant.

1) Verification of integrated control room system

There are two main sources of information to be used when formulating the verification criteria. These are:

- the functional requirements for the actual control room as developed according to Clause 3;
- rules and criteria to be applied in the design of the control room as given in Clause 4.

The criteria that are developed from these two sources shall cover technical aspects as well as human factor engineering aspects.

The criteria are to be used when demonstrating that proper human factor engineering principles as well as required technical abilities have been incorporated in the control room design.

Typical examples of verification criteria are:

- instruments and displays provided in the control room shall represent relevant process parameters;
- controls and displays shall be arranged in a consistent and orderly pattern;
- failed instruments and displays shall be easily recognizable as failed;
- work stations shall be arranged so that access to the control boards is not impeded;
- adequate controls for air temperature, humidity and ventilation shall be provided;
- controls shall be located so that the related displays can be used to provide feedback.

2) Validation of integrated control room system

The objective of the validation of the control room system is to determine that the interactions between the components of the control room systems are such that the integrated system behaves in the manner demanded by requirements for safe and reliable operation of the plant. The scope of the validation is limited, in this standard, to three of the possible multiple interactions:

- the control room and the operator;
- the control room and the operating procedures;
- the control room and the training programme.

a) Scope of validation

The scope of the validation shall be limited by taking into account that the control room as well as the operating procedures and the training programme at this stage of development exist as drawings and specifications.

b) Scénarios de validation

Les scénarios sont des descriptions écrites de situations opérationnelles adaptées aux méthodes de validation choisies. Ces scénarios doivent être représentatifs de la centrale réelle et doivent couvrir le fonctionnement normal, un mélange d'événements ou de défaillances multiples et des anomalies, aussi bien que des conditions d'urgence.

Les scénarios doivent décrire les conditions initiales, la séquence appropriée des réponses de la centrale et les symptômes applicables. Les chemins qu'il est prévu de suivre, lorsque la centrale sera en exploitation, doivent être fournis afin de permettre l'établissement des critères d'évaluation.

c) Sélection des méthodes de validation

Les méthodes disponibles pour la validation de la salle de commande intégrée sont:

- la méthode de la "table ronde", qui inclut une discussion approfondie des étapes de procédures concernant le scénario proposé;
- la méthode de "maquettage", où des personnes jouant le rôle d'opérateurs appliquent pas à pas les actions de la procédure, selon un scénario proposé par une équipe d'observateurs, sans agir sur des fonctions de commande réelles. Un préalable à cette méthode est une maquette, qu'il est possible de réaliser simplement avec des dessins sur des panneaux de contrôle fixés sur les murs;
- la méthode des "simulations", dans laquelle des personnes jouant le rôle d'opérateurs agissent sur les fonctions de commande réelles sur des matériels simulés, selon un scénario prédéfini en présence d'une équipe d'observateurs.

Différentes combinaisons de ces méthodes de validation peuvent être utilisées selon le domaine de validation. Par exemple, des simulateurs de tâches spécifiques ou couvrant un domaine limité peuvent être utilisés pour jouer des scénarios comportant des paramètres dépendant du temps, durant des validations de type "table ronde" ou "maquette".

d) Critères d'évaluation

Le concepteur doit développer des critères d'évaluation spécifiques pour la validation du système intégré de salle de commande. Les critères suivants sont donnés pour information.

- Salle de commande et opérateurs

- . Les verrines d'alarme, les instruments, les afficheurs spécifiés peuvent-ils être utilisés comme des moyens adéquats pour alerter l'opérateur qu'il doit accomplir une action requise?
- . Les commandes sont-elles faciles à atteindre et les afficheurs lisibles sur le panneau de commande analysé?
- . Les repères d'identification sur l'instrumentation et les commandes sont-ils suffisamment détaillés pour permettre à l'opérateur de localiser le panneau et la commande particulière sans avoir à recourir à une autre documentation?
- . Les indications permettant à l'opérateur de déterminer qu'une étape a été franchie ou qu'une condition est remplie ont-elles été prévues? Cette indication fournit-elle une information satisfaisante?
- . Si les moyens primaires de commande ou les indicateurs ne sont pas disponibles, y-a-t-il encore un moyen pour terminer l'étape commencée?
- . S'il est entendu que l'opérateur exécute une action lorsqu'un paramètre du processus atteint une certaine valeur, l'instrument concernant ce paramètre est-il lisible pour cette valeur?
- . Les échelles et les domaines de mesures de tous les instruments sont-ils appropriés à la précision de lecture requise en terme d'échelle et de résolution temporelle?

b) Validation scenarios

The scenarios are written descriptions of selected operational situations adapted to the chosen validation method. These scenarios shall be representative of the actual plant and shall cover normal operation, a mix of multiple failure events and disturbances as well as emergency conditions.

The scenarios shall describe the initial conditions, the proper sequence of plant responses and applicable symptoms. The expected paths to be followed when operating the plant shall be given in order to allow for the evaluation criteria to be addressed.

c) Selection of validation methods

The available methods for validating the integrated control room are:

- the table-top method which includes a thorough discussion of the procedural steps of the proposed operating scenario;
- the walk-through method whereby persons acting as operators conduct a step-by-step enactment of the procedural actions during a proposed scenario for an observer team without carrying out actual control functions. A prerequisite for a walk-through is a mock-up, the simplest thing being a room with the drawings for the control panels mounted on the walls;
- the simulator method whereby persons acting as operators perform actual control functions on simulated equipment during a proposed scenario in front of an observer team.

These validation methods can be used in different combinations depending on the scope of the validation. For instance, limited scope or part task simulators could be used to support the scenarios with time-dependent parameter information during table-top and walk-through validation.

d) Evaluation criteria

The designer shall develop specific evaluation criteria when validating the control room system integration. The following are given for information.

- Control room and operators

- . Could specified annunciators, instruments or plant displays be used as cues, adequate to alert the operator to perform a required action?
- . Are controls reachable and displays readable on the reviewed control room panel?
- . Are the identification labels on instrumentation and controls sufficiently detailed to permit the operator to locate the panel and the particular control without resorting to other documentation?
- . Are indications provided to allow the operator to determine that a step has been completed or that a condition has cleared? Does this indication convey the information satisfactorily?
- . If the primary cues, controls or indicators are not available, is there still some way to complete a given step?
- . If the operator is expected to take some action when a process parameter reaches a certain value, is the instrument for that parameter readable to that value?
- . Are all instrument scales and ranges appropriate to the required reading precision in terms of scale and time resolution?

- Salle de commande et procédures de conduite

- . Les actions spécifiées dans les procédures de conduite peuvent-elles être remplies dans les séquences désignées?
- . Y a-t-il d'autres voies de réussite qui ne sont pas incluses dans les procédures analysées?
- . L'action d'une procédure peut-elle être remplie en salle de commande et dans un laps de temps spécifié?
- . L'opérateur peut-il obtenir l'information nécessaire telle que requise dans la procédure, depuis l'instrumentation spécifiée dans la salle de commande?
- . Les afficheurs et les instruments spécifiés fournissent-ils l'information adéquate à l'opérateur pour choisir la procédure applicable?
- . Est-il nécessaire pour l'opérateur d'utiliser une information ou un matériel non spécifiés dans les procédures pour accomplir sa tâche?
- . Est-ce que la représentation des conditions de la centrale en salle de commande est compatible avec les descriptions de ces mêmes conditions dans les procédures?
- . L'opérateur peut-il utiliser le repérage, les abréviations, les symboles et les informations de localisation prévus dans les procédures pour trouver le matériel correct?
- . Les domaines de mesure des instruments sont-ils cohérents avec les valeurs des instruments indiquées dans les procédures?
- . L'utilisation des procédures ne constitue-t-elle pas une charge intellectuelle excessive pour les opérateurs ?
- . Les procédures de conduite en situation d'urgence sont-elles aisées à distinguer des autres procédures en salle de commande (couleur, taille, emplacement)?
- . Les procédures et la salle de commande sont-elles physiquement compatibles?
- . Y a-t-il un espace disponible en différents endroits de la salle de commande pour poser les procédures, et leur reliure permet-elle de les mettre à plat sur l'espace de travail?
- . Les procédures sont-elles trop volumineuses ou trop lourdes pour une manipulation aisée?

- Salle de commande et programme de formation

- . Tous les systèmes et matériels peuvent-ils être utilisés de façon sûre et correcte avec l'instrumentation et les commandes disponibles?
- . Est-ce qu'un système ou matériel peut être utilisé de façon incorrecte à cause d'une mauvaise compréhension de ces moyens?
- . Est-ce qu'une action volontaire peut être déclenchée suite à l'apparition d'une alarme?
- . Est-ce que l'information provenant des commandes et de l'instrumentation peut être mal interprétée?
- . Est-ce que des conclusions erronées peuvent être déduites des commandes et de l'instrumentation?
- . La formation doit-elle être utilisée pour compenser une conception déficiente de la salle de commande ou des procédures?

A.3.4 Systèmes d'instrumentation et de contrôle

Bien que la vérification et la validation des systèmes de contrôle-commande soient hors du domaine d'application de cette norme, les critères d'évaluation suivants sont fournis pour information:

1) Vérification du respect d'aspects généraux

Les points suivants doivent être vérifiés:

- a) Les spécifications concernant les différents aspects du système doivent être cohérentes et conformes aux principes de base de conception relatifs à la sûreté, la fiabilité et au niveau d'automatisme.
- b) Les exigences en matière de moyens pour les tests et la mise en service du système doivent être incluses dans les exigences fonctionnelles.

- Control room and operating procedures

- . Can the actions specified in the procedures be performed in the designated sequence?
- . Are there alternative success paths that are not included in the reviewed procedure?
- . Can the procedure action be performed in the control room and within a specified time?
- . Can the operator obtain the necessary information as required in the procedures from the specified instrumentation in the control room?
- . Will the specified instruments and displays provide adequate information for the operator to select the applicable procedure?
- . Is it necessary for the operator to use information or equipment not specified in the procedures to accomplish his task?
- . Is the presentation of plant conditions in the control room compatible with the description of the same conditions in the procedures?
- . Can the operator find the correct equipment with the labelling, abbreviations, symbols and location information provided?
- . Are instrument ranges consistent with instrument values stated in the procedures?
- . Will the use of the procedures place excessive burdens on the memory of the operator?
- . Are the emergency operating procedures easy to distinguish from other procedures in the control room (colour, shape, location)?
- . Are the procedures and the control room physically compatible?
- . Is there space available in different parts of the control room to lay the procedures down and will the binding allow them to lay flat on work space?
- . Are the procedures too bulky or too heavy for convenient handling?

- Control room and training programme

- . Can all plant systems and equipment be safely and correctly operated with the available controls and instrumentation?
- . Is any plant system or equipment likely be incorrectly operated due to lack of understanding of those devices?
- . Can due action be taken in response to annunciators?
- . Can information from controls and instrumentation be misinterpreted?
- . Can erroneous conclusions be drawn from controls and instrumentation?
- . Is training used to compensate for deficient design of the control room or the procedures?

A.3.4 I & C systems

Although V & V of I & C systems is not within the scope of this standard, the following evaluation criteria are given for information:

1) Verification of fulfillment of general aspects

The following points shall be verified:

- a) The specifications for different aspects on the I & C system shall be mutually consistent and in accordance with the stated design basis principles of safety, reliability and automation level.
- b) Requirements for facilities for system testing and commissioning shall be included in the functional requirements.

- c) Les exigences relatives à la maintenabilité doivent être documentées et cohérentes avec celles relatives à la disponibilité.
- d) Les exigences relatives à la flexibilité et l'adaptabilité des fonctions de contrôle-commande proposées doivent être telles que les changements futurs concevables dans les besoins des utilisateurs puissent être satisfaits.
- e) Les fonctions affectées au système de contrôle-commande doivent satisfaire aux objectifs appropriés de l'environnement du travail, et les opérateurs ne doivent pas être exposés à des températures excessives, au bruit, aux substances toxiques, à la radioactivité, etc. Des applications requérant des tâches fastidieuses ou une force physique excessive doivent être évitées.

2) Vérification du respect des spécifications propres aux automatismes

On doit vérifier que les aspects suivants sont réalisés de façon adéquate.

- a) L'affectation des fonctions au système de contrôle-commande est cohérente avec un certain niveau d'automatisme. Ce niveau, au regard des commandes, protections, verrouillages, affichages, rapports écrits, gestion de données, communication, etc., et tenant compte des divers modes de conduite et des transitoires, doit correspondre aux objectifs exprimés pour éviter une charge excessive de l'équipe de conduite.
Le niveau d'automatisme doit être choisi en considérant les limites humaines, telles que l'inaptitude à conduire des processus très rapides, très lents ou très complexes, ou la capacité limitée de la mémoire humaine.
La possibilité de conduire à distance des systèmes pour cause d'inaccessibilité ou de localisation éloignée doit également être vérifiée.
- b) Pour chaque sous-processus, pour les interactions entre sous-processus, pour les états opérationnels et les transitoires, chaque fois que les exigences fonctionnelles en matière de rapidité ou de précision sont difficiles à respecter par l'homme, des automatismes doivent être choisis.
- c) Des automatismes pour améliorer la disponibilité et la productivité et accroître la qualité de production et la capacité d'utilisation doivent en principe être justifiés et ne doivent pas imposer des exigences impossibles sur la vitesse, la précision ou le volume des mesures, la conception du processus et des appareils, et les tâches des opérateurs. Ces exigences ne doivent pas imposer de violation aux principes de base de conception.
- d) Une instrumentation et des commandes adéquates doivent en principe être prévues pour permettre à l'opérateur de faire face de façon sûre à des événements pour lesquels les fonctions automatiques n'ont pas été prévues ou ne sont pas capables d'agir.
- e) Les spécifications de disponibilité concernant les matériels automatiques liés à la sûreté doivent être possibles et suffisantes pour respecter les réglementations de sûreté des autorités compétentes et des exploitants.

- c) The requirements for maintainability shall be documented and consistent with the requirements for availability.
- d) The requirements for flexibility and adaptability of the proposed I & C functions shall be such that conceivable future changes of the user's needs can be met.
- e) The proposed functional assignment to the I & C system shall meet appropriate goals for work environment and operators shall not be exposed to excessive temperatures, noise, toxic substances, radioactivity, etc. Applications requiring tedious work sequences or excessive physical strength shall be avoided.

2) Verification of fulfillment of specified automation aspects

It shall be verified that the following items are fulfilled adequately.

- a) The assignment of functions to the I & C system is consistent with a certain level of automation. This level, with regard to controls, protections, interlocks, displays, reports, data management, communication, etc., and with respect to various operational modes and mode transitions, shall correspond to the stated objective of avoiding excessive workload of the operating crew.
The automation level shall be selected with due regard to limitations of the human capacity, such as inability to control very fast or very slow or very complex processes or the limited capacity of the human memory.
Remote operation of the systems because of location in inaccessible or remote areas shall also be verified.
- b) For each sub-process, interaction between sub-processes, operational state and state transition, where the functional demands on operational speed or accuracy are difficult for man to meet, automated solutions shall be chosen.
- c) Automated solutions for improving availability and productivity and for enhancing product quality and capacity utilization should be justified and shall not impose impossible requirements on the speed and accuracy or volume of measurements, process and device design and operators tasks. These requirements shall not impose violations of the principles of the design basis.
- d) Adequate instrumentation and controls shall be provided to allow the operator to cope safely with events for which the automated functions are either not intended or not capable of handling.
- e) The specifications for availability on demand for safety related automatic equipment shall be practicable and sufficient to meet safety regulations of the utility and of licencing authorities .

A.3.5 Analyse du travail

Comme il est spécifié en 3.5, le but de l'analyse du travail est d'identifier les exigences fondamentales concernant la structure de l'équipe de salle de commande, les procédures de conduite et le programme de formation.

La première étape de l'analyse du travail est d'identifier les caractéristiques et le contenu des tâches attribuées à l'homme. Le concepteur peut alors définir l'organisation et le nombre d'opérateurs à l'intérieur de l'ossature de la structure de l'équipe de salle de commande requise par la réglementation ou les principes de l'exploitant.

Un opérateur ne doit pas se voir affecter des tâches qui pourraient le surcharger ou qui seraient hors du domaine de responsabilité qui lui est attribué au sein de l'équipe. Le concepteur peut ensuite identifier les communications entre opérateurs et/ou les communications entre opérateurs en salle de commande et opérateurs locaux, nécessaires à l'accomplissement des tâches.

Le concepteur peut aussi identifier les activités non opérationnelles (par exemple le rapport aux autorités) inhérentes à quelques tâches, en se référant aux documents appropriés. Ces facteurs constituent une partie des bases des processus de conduite et du programme de formation.

A.3.5 Job analysis

As specified in 3.5, the purpose of the job analysis is to identify fundamental requirements for the control room staff structure, the operating procedures and the training programme.

The first step of the job analysis is to identify the characteristics and the number of tasks assigned to man. 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/or the utility normal practice.

Each operator shall not be assigned tasks that may overload him or that are not within the scope of the responsibilities defined by the staff structure. Next, the designer can identify communications among operators and/or communications between control room operators and local operators that are necessary for the achievement of tasks.

The designer can also identify non-operational activities (e.g. reporting to authorities) inherent into some tasks by referring to appropriate documents. These factors form a part of the basis for the operating procedures and the training programme.

A.4 Spécifications fonctionnelles de conception

Cet article fournit des informations supplémentaires à l'article 4 incluant des recommandations détaillées, quelques exemples de valeurs quantitatives recommandées et des explications pour aider à la conception de l'interface homme/machine et des matériels, et pour établir une spécification détaillée du système de salle de commande.

A.4.1 Données fondamentales de conception sur les facteurs humains

A.4.1.1 Considérations anthropométriques

Les considérations anthropométriques occupent une place centrale dans la conception de l'interface homme/machine. Leur non-prise en compte dans la conception peut mettre en péril la performance du système, la sûreté de l'opérateur et/ou la disponibilité de la machine.

- a) Une base de données anthropométriques doit être établie pour la conception des panneaux de commande, des tableaux et des matériels. Une base de données préétablie peut être utilisée, mais son applicabilité à la population concernée doit être évaluée avant utilisation.
- b) La base de données anthropométriques doit constituer la base des exigences physiques pour les dimensions et la forme des commandes et des matériels associés.
- c) Les dimensions des éléments de conception ci-dessus et les rayons d'atteinte résultants, les distances de vision, les zones de vision et les angles de vision doivent être à l'intérieur des limites acceptables pour les 5 à 95 percentiles de la population des utilisateurs.
- d) Un exemple de liste de données anthropométriques à utiliser pour les limites de dimensionnement des matériels est fourni dans le tableau A.4.

Tableau A.4 - Exemples de données anthropométriques. Positions debout et assise

	Valeurs limites (cm)	
	5 percentiles	95 percentiles
	Femme adulte	Homme adulte
Debout (sans chaussures)		
Stature	152	187
Hauteur de l'œil au-dessus du sol	141	174
Hauteur de l'épaule	123	154
Hauteur du coude	95	119
Hauteur du bout du doigt	61,5	73,2
Atteinte fonctionnelle	64	88,9
Atteinte fonctionnelle étendue	73,4	99,1
Distance de l'axe du corps au bord de la console	12,7	13,5
Distance de l'œil à l'axe central du corps	7,6	8,6
Assis		
Hauteur du jarret (flexion à l'arrière du genou)	38,1	48,8
Hauteur assise au-dessus du siège (droit)	79	97,8
Hauteur assise au-dessus du siège (relâché)	77,5	95,5
Hauteur de l'œil au-dessus du siège (droit)	67,6	85,3
Hauteur de l'épaule au-dessus du siège	49,8	65,5
Hauteur du coude au-dessus du siège	16,3	28,7
Atteinte fonctionnelle	64	88,9
Atteinte fonctionnelle étendue	73,4	99,1
Hauteur libre pour les cuisses	10,4	18,8
Longueur fesse-jarret	43,4	54,6
Hauteur du genou	47	59,9
Distance de l'axe du corps au bord de la console	12,7	13,5
Distance de l'œil à l'axe central du corps	7,6	8,6

A.4 Functional design specification

This clause provides supplementary informations to Clause 4, which include detailed recommendations, some examples of quantitative figures to be recommended and explanations to aid the design of man-machine interface and equipment and to provide a detailed specification of the control room system.

A.4.1 Fundamental design data of human factors

A.4.1.1 Anthropometric consideration

Anthropometric considerations occupy a central place in man-machine interface design. Failure to account for them in the design can jeopardize system performance, operator safety, or machine availability.

- a) An anthropometric data base shall be established for the design of control panels, boards and equipment. A pre-established data base may be utilized, but its applicability to the relevant population shall be checked prior to the utilization.
- b) The anthropometric data base shall form the basis of physical requirements for the dimensions and form of control and associated equipment.
- c) The dimensions of the above design elements and resultant reach radius, viewing distance, viewing zone and viewing angle shall be within acceptable limits, typically for the 5th to 95th percentile of the user population.
- d) An example of anthropometric data list to be prepared for setting limits for equipment dimensions is given in Table A.4.

Table A.4 - Examples of anthropometric data. Standing and sitting

	Bounding measurements (cm)	
	5th percentile	95th percentile
<i>Standing (without shoes)</i>	Adult female	Adult male
Stature	152	187
Eye height from floor	141	174
Shoulder height	123	154
Elbow height	95	119
Fingertip height	61,5	73,2
Functional reach	64	88,9
Extended functional reach	73,4	99,1
Dist. from axis of body to leading edge of console	12,7	13,5
Eye distance forward of central axis of body	7,6	8,6
<i>Sitting</i>		
Popliteal height (bent at back of knee)	38,1	48,8
Sitting height above seat surface (erect)	79	97,8
Sitting height above seat surface (relaxed)	77,5	95,5
Eye height above seat, sitting erect	67,6	85,3
Shoulder height above seat surface	49,8	65,5
Elbow height above seat surface	16,3	28,7
Functional reach	64	88,9
Extended functional reach	73,4	99,1
Thigh clearance height	10,4	18,8
Buttock-popliteal length	43,4	54,6
Knee height	47	59,9
Dist. from axis of body to leading edge of console	12,7	13,5
Eye distance forward of central axis of body	7,6	8,6

A.4.1.2 Stéréotypes de population

L'interface de la salle de commande doit être conçue en prenant en considération les stéréotypes de population.

Une base de stéréotype de population doit être établie pour les aspects suivants:

- mouvements des commandes;
- mouvements des index d'afficheurs ou équivalents;
- signification des couleurs.

Un exemple de stéréotype de réponse pour les commandes est montré à la figure A.1.

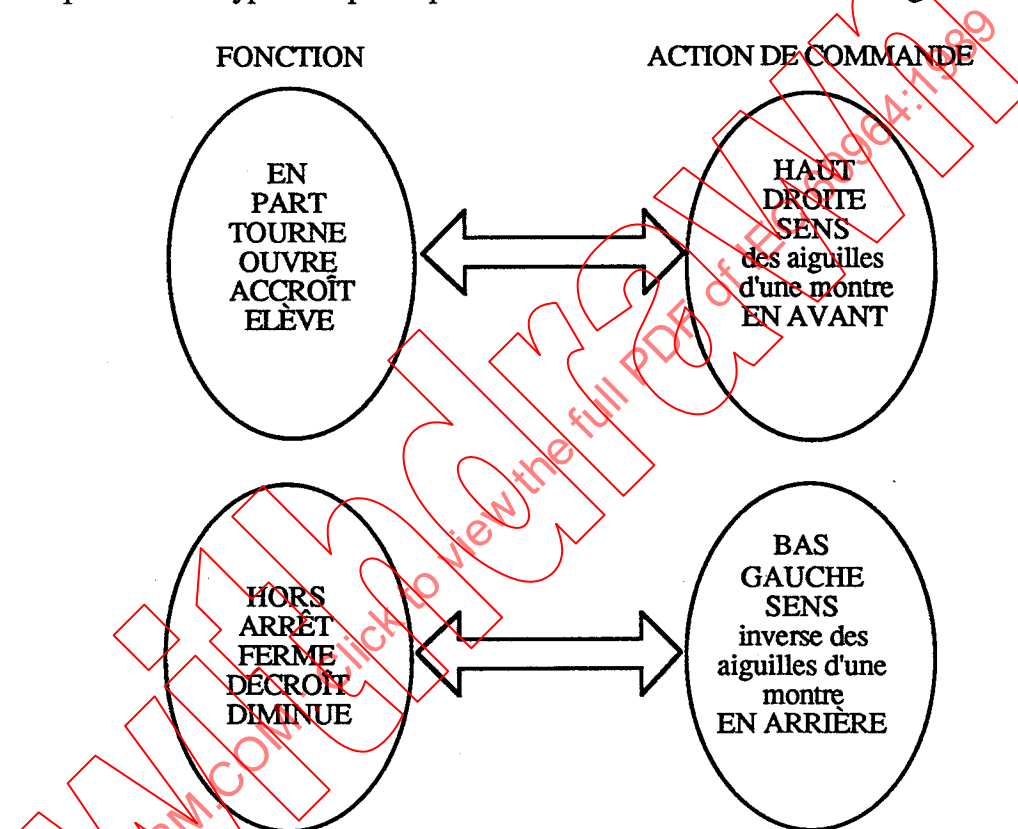


Figure A.1 - Exemple de stéréotype de réponse pour les commandes

A.4.1.3 Aptitudes et caractéristiques visuelles et auditives

La base de données de conception sur les aptitudes et caractéristiques auditives et visuelles doit être réalisée en incluant les paramètres dont les valeurs caractéristiques sont les suivantes:

a) Aspects auditifs

- domaine de fréquences: 200 Hz à 5 000 Hz;
- domaine de fréquences optimal: 500 Hz à 3 000 Hz;
- niveaux d'intensité: entre 60 dB et 90 dB;
- bruit ambiant maximal: 45 dB;
- différence minimale d'intensité avec le bruit ambiant: 10 dB;
- intensité des signaux d'urgence: 90 dB à 100 dB.

A.4.1.2 Population stereotypes

The control room interface shall be designed with due consideration of population stereotypes.

A basis of population stereotypes shall be established for the following:

- movement of controls;
- movement of display pointer and equivalents;
- meaning of colours.

An example of stereotype response of controls is shown in Figure A.1.

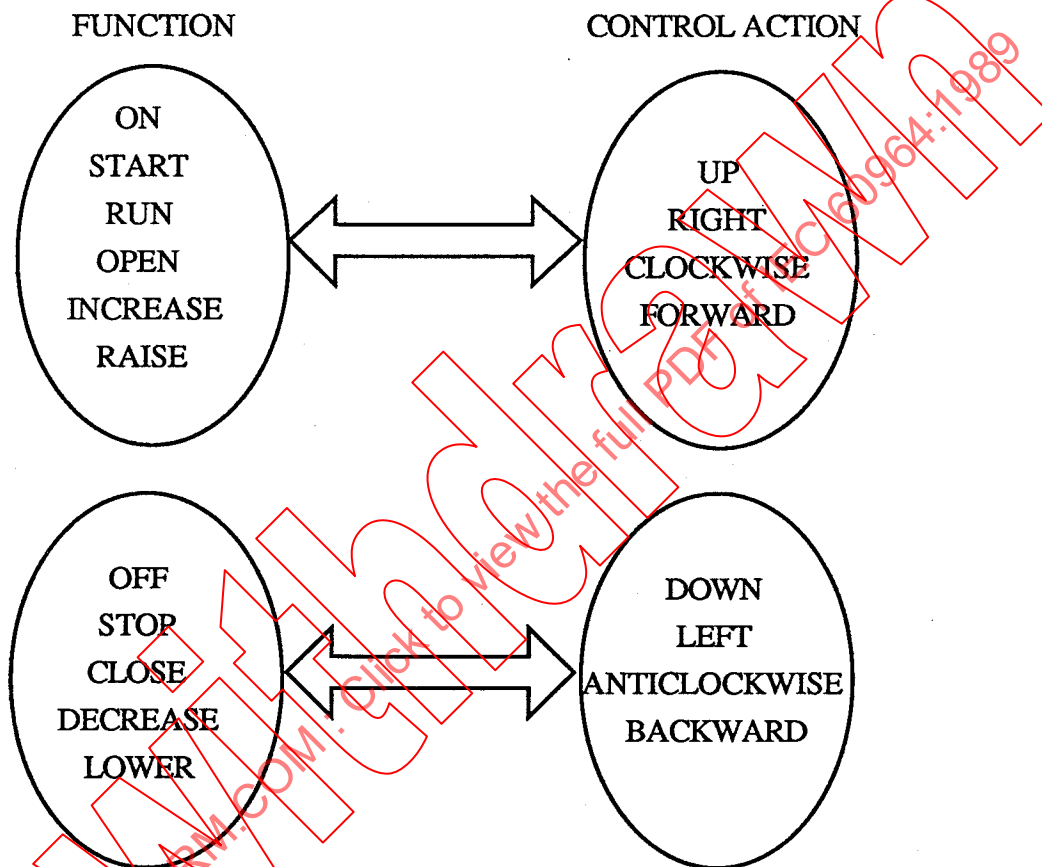


Figure A.1 - An example of stereotype of controls

A.4.1.3 Auditory and visual capabilities and characteristics

Design data base on auditory and visual capabilities and characteristics shall be provided including the following items:

a) Auditory

- range of frequency: 200 Hz to 5 000 Hz;
- range of optimum frequency: 500 Hz to 3 000 Hz;
- levels of intensity: between 60 dB and 90 dB;
- maximum ambient noise: 45 dB;
- minimum difference of intensity to the ambient noise: 10 dB;
- intensity of emergency signal: 90 dB to 100 dB.

b) Aspects visuels

- niveaux d'éclairage:

minimal: 200 lx
maximal: 750 lx

- uniformité de l'éclairage (ratio): pas moins de 0,5

- éclairage incident sur les écrans de visualisation:

minimal: 50 lx
maximal: 100 lx

- angles de vision minimal des caractères et symboles: 15 min

- angle de vue minimal entre l'axe visuel et la façade des afficheurs: 45 degrés

- niveau d'éclairage minimal de secours: 200 lx

A.4.1.4 *Aptitude humaine au traitement de l'information*

Les bases de données de conception sur l'aptitude humaine à traiter l'information doivent être établies, par exemple avec les modèles de charge, de précision, de vitesse, de temps de réponse et de prise de décision, telles la reconnaissance de formes ou l'analyse de textes.

Quelques exemples de ces données sont:

a) Le temps moyen d'appel d'une image ou de son équivalent doit être en principe inférieur à 2 s et il est souhaitable qu'il soit inférieur à 1 s. Le temps de mise à jour d'une donnée sur une telle image doit être aussi en principe inférieur à 2 s et il est souhaitable qu'il soit inférieur à 1 s. Le temps d'affichage doit dépendre en principe de la quantité d'informations sur l'image et du format.

b) Une présentation de type analogique est meilleure pour les lectures de contrôle lorsqu'il faut déterminer des limites, une vitesse ou un changement de direction et une comparaison de données, et quand il y a une échelle de temps pour les courbes et les estimations. Les affichages alphanumériques sont appropriés pour des comparaisons.

c) Lorsque des valeurs discrètes ou des comparaisons sont requises, une présentation numérique est perçue environ quatre fois plus vite qu'une représentation analogique et le taux d'erreur associé est de 1/20.

Les critères de sélection pour les types de présentation d'information analogique ou numérique doivent être en principe également prévus.

A.4.1.5 *Facteurs d'environnement*

Les données concernant les exigences d'environnement pour les opérateurs en salle de commande doivent être en principe prévues pour les conditions normales et anormales de la centrale. Ces données doivent en principe se référer aux spécifications d'environnement de la salle de commande principale indiquée en A.4.2.2.

A.4.2 *Localisation, environnement et protection*

A.4.2.1 *Localisation*

En ce qui concerne les exigences de sûreté, l'emplacement de la salle de commande doit être tel qu'elle ne soit pas affectée par les conséquences d'accidents de la centrale, tels que des missiles, des rayonnements, le feu, etc., que les opérateurs pourront y accéder facilement pour toutes les conditions d'exploitation de la centrale, et qu'ils pourront l'évacuer si elle devenait inhabitable.

b) Visual

- levels of illumination:

minimum: 200 lx
maximum: 750 lx

- uniformity of illumination (ratio): not less than 0,5

- incident illumination to VDU screen:

minimum: 50 lx
maximum: 100 lx

- minimum visual angle of characters and symbols: 15 min

- minimum viewing angle between the line of sight and the face of display: 45 degrees

- minimum emergency illumination: 200 lx

A.4.1.4 Human ability to process information

The design base on human capabilities and characteristics of information processing shall also be provided such as for load, accuracy, rate, time delay and decision-making patterns, e.g. pattern recognition or text search.

Some examples of these data are as follows:

a) An average call-up time of visual display or equivalents should be less than 2 s ideally less than 1 s. Data update time of such a display should also be less than 2 s but it should match the human capability and interval of the measurement. Display time should depend on information quantity and the format.

b) Analogue type presentation is superior for check readings, where relation to set limits is to be determined or rate and change of direction, data comparison. Analogue presentation is superior when a time scale is introduced, using trend and predictive displays. Alphanumeric displays are suitable for making comparisons.

c) Where numerical value or comparisons are required, digital presentation is perceived about four times faster than that of the analogue and the associated error rate is about 1/20.

Selection criteria for presentation of types of information, by analogue or digital, should also be provided.

A.4.1.5 Environmental factors

Data on environmental requirements for operators in the control room should be provided for both normal and abnormal conditions of the plant. The data should be used to provide the environmental specifications of the main control room shown in A.4.2.2.

A.4.2 Location, environment and protection

A.4.2.1 Location

As a safety requirement, the control room shall be located where it will not be affected by the consequences of plant internal hazards such as missile, radiation, fire, etc., and where operators can easily gain access under all the plant conditions and escape from it if it becomes uninhabitable.

A.4.2.2 Environnement

Afin de maintenir un environnement de la salle de commande adapté aux opérateurs pour qu'ils remplissent leurs tâches, les exigences ci-après doivent être respectées *a minima* :

a) Climatisation

La salle de commande doit être climatisée. La conception du système de ventilation doit inclure des mesures appropriées aux conditions accidentelles pour la centrale.

b) Eclairage

Dans la conception d'éclairage de la salle de commande principale, une attention spéciale doit être en principe portée sur l'uniformité, les ombres, l'éblouissement, les réflexions et le suréclairage. Quelques données sont fournies en A.4.1.3.

Un système d'éclairage de secours doit fournir continuellement l'éclairage nécessaire pour remplir les tâches, même en cas de défaillance du système normal.

c) Environnement sonore

L'environnement sonore de la salle de commande doit être conçu en prenant en considération une base de données pertinente sur les capacités et les caractéristiques auditives de l'homme fournies en A.4.1.3.

Le bruit de fond en salle de commande doit être minimisé et ne doit pas en principe excéder 45 dB.

A.4.2.3 Protections

a) Protection incendie

On doit faire en principe attention à utiliser uniquement des matériaux non inflammables. La zone de la salle de commande doit être équipée avec des systèmes de protection et de lutte contre le feu.

Les matériels électriques en salle de commande doivent, autant que possible, être conçus pour ne provoquer ni entretenir aucun feu.

Les câbles et appareils de coupure associés à la salle de commande doivent être protégés contre les conséquences d'un incendie. L'isolation des câbles et les matériaux des gaines doivent en principe être de type non propagateur de flamme et respecter les critères d'essais nationaux en matière de propagation de la flamme et concernant le choix des matériaux, lorsqu'ils sont applicables.

b) Protection contre les rayonnements

L'équipe de salle de commande doit en principe être protégée contre les rayonnements directs pour toutes les situations accidentelles. Les gaines d'arrivée d'air doivent être équipées d'un système de surveillance de la radioactivité. Si les circonstances l'exigent, le système de ventilation de la salle de commande doit pouvoir être isolé. L'équipe doit pouvoir disposer d'appareils respiratoires.

c) Protection contre les missiles

La conception de la salle de commande doit inclure une évaluation et une protection contre les missiles d'origine interne ou externe à la salle de commande. Un guide pour la protection contre les missiles figure dans le Guide de sûreté 50-SG-D4 de l'AIEA.

A.4.2.2 Environment

In order to maintain the environment of the control room suitable for the operators to perform their tasks, the following minimum requirements shall be satisfied :

a) Air conditioning

The control room shall be air conditioned. The ventilation system design shall include measures to cope with accident conditions on the plant.

b) Illumination

In the design of the lighting system in the main control room, special attention should be given to uniformity, shadows, glare, reflections and high-lighting. Some data are provided in A.4.1.3.

An emergency lighting system shall continuously provide illumination necessary for task performance even on failure of the normal system.

c) Auditory environment

Auditory environment of the control room shall be designed considering a relevant data base on human auditory capability and characteristics shown in A.4.1.3.

Background noise in the control room should be minimized and should not exceed 45 dB.

A.4.2.3 Protection

a) Fire protection

Attention should be given to using nonflammable materials only. The control room area shall be equipped with fire detection and fire fighting systems.

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. A guide for the protection from the missiles is given in the IAEA Safety Guide 50-SG-D4.

d) Protection contre les séismes

Les matériels en salle de commande liés aux fonctions de sûreté, le système de climatisation et les systèmes d'éclairage de secours doivent être conçus sur la même base sismique que les matériels de contrôle-commande importants pour la sûreté.

e) Protection contre les actes de sabotage

Des mesures doivent en principe être prises pour restreindre l'accès en salle de commande et la protéger contre les sabotages.

Le plan de sécurité doit être conforme aux exigences de la réglementation de chaque pays.

A.4.3 *Espaces et configuration*

A.4.3.1 *Espaces*

Comme il est mentionné en 4.3.1, des emplacements suffisants doivent en principe être prévus, tels que des zones de travail, des endroits pour écrire et des meubles de rangement pour stocker les documents.

- Les zones de travail nécessitant une présence permanente doivent être conçues pour un travail assis et un siège adéquat doit être prévu, ce siège doit en principe permettre aussi de travailler en position debout.
- Quand l'écriture et l'accès à la documentation font partie des tâches normales de la salle de commande, des emplacements adéquats pour écrire doivent être prévus.
- Des espaces de stockage pour les documents doivent aussi être prévus près du poste de travail pour éviter que les documents soient laissés sur les consoles, les pupitres, etc.
- De l'espace peut être prévu pour des réaménagements qui pourraient être réalisés ultérieurement.

A.4.3.2 *Configuration dans la salle de commande*

a) Regroupement des zones de travail

- La surface de la salle de commande doit être théoriquement divisée en zones de travail où chaque opérateur a toutes les commandes et les indications requises pour effectuer les tâches qui lui sont assignées lors des différentes conditions de fonctionnement, comprenant le démarrage, le fonctionnement normal, l'arrêt et les situations d'urgence.
- La configuration doit en principe minimiser les interférences entre les tâches de l'opérateur.

b) Tableaux de commande et aménagement

L'aménagement des panneaux de commande, pupitres et tableaux de la salle de commande doit être tel que:

- chaque opérateur ait un espace suffisant entre ces éléments, etc., lui permettant d'avoir un accès immédiat et direct à l'information et aux commandes en rapport avec ses tâches;
- les conflits entre les trajets des différents opérateurs soient réduits;
- la coordination et la communication entre les opérateurs soient faciles;
- les reflets soient minimisés.

Si plus d'une rangée de panneaux ou de tableaux de commande est inévitable, les indications et les commandes sur les panneaux non directement situés en face de l'opérateur doivent être limitées à celles n'exigeant pas une action immédiate ou continue.

d) Earthquake protection

The control room equipment related to safety functions, the air-conditioning system and emergency illumination systems shall be designed on the same seismic basis as the safety I & C equipments important to plant safety.

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.

A.4.3 *Space and configuration*

A.4.3.1 *Space*

As mentioned in 4.3.1, space should be provided where necessary for such needs as 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 standing operations.
- Where writing and access to documentation form normal part of 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 backfitting that might be required in the future.

A.4.3.2 *Configuration within the control room*

a) Grouping of operating areas

- The control room area shall be ideally divided into operating areas where each operator has all the controls and indications required to perform the tasks assigned to him in various operating conditions including start up, normal operation, shut-down and emergencies.
- The configuration should minimize interference between operator tasks.

b) Control boards and arrangement

The arrangement of control panels, desks and boards in the control room shall be such as to:

- allow each operator to have sufficient space between the panels, etc., for immediate and direct access to the information and controls pertinent to his tasks;
- minimize conflicting paths for the various operators;
- facilitate communications and coordinations between the operators;
- minimize reflections.

If more than one row of panels or control boards is provided, the indications and controls on the panels not directly in front of the operator shall be restricted to those not requiring immediate or continuous action.