

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

61839

Première édition
First edition
2000-07

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

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



Numéro de référence
Reference number
CEI/IEC 61839:2000

Numéros des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000.

Publications consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

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 dans le Catalogue de la CEI.

Les renseignements relatifs à des questions à l'étude et des travaux en cours entrepris par le comité technique qui a établi cette publication, ainsi que la liste des publications établies, se trouvent dans les documents ci-dessous:

- «Site web» de la CEI*
- **Catalogue des publications de la CEI**
Publié annuellement et mis à jour régulièrement
(Catalogue en ligne)*
- **Bulletin de la CEI**
Disponible à la fois au «site web» de la CEI* et comme périodique imprimé

Terminologie, symboles graphiques et littéraux

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 60050: *Vocabulaire Electrotechnique International* (VEI).

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera la CEI 60027: *Symboles littéraux à utiliser en électrotechnique*, la CEI 60417: *Symboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles*, et la CEI 60617: *Symboles graphiques pour schémas*.

* Voir adresse «site web» sur la page de titre.

Numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series.

Consolidated publications

Consolidated versions of some IEC publications including amendments are available. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

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 in the IEC catalogue.

Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is to be found at the following IEC sources:

- **IEC web site***
- **Catalogue of IEC publications**
Published yearly with regular updates
(On-line catalogue)*
- **IEC Bulletin**
Available both at the IEC web site* and as a printed periodical

Terminology, graphical and letter symbols

For general terminology, readers are referred to IEC 60050: *International Electrotechnical Vocabulary* (IEV).

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications IEC 60027: *Letter symbols to be used in electrical technology*, IEC 60417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets* and IEC 60617: *Graphical symbols for diagrams*.

* See web site address on title page.

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

61839

Première édition
First edition
2000-07

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

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

© IEC 2000 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.

International Electrotechnical Commission
Telefax: +41 22 919 0300

3, rue de Varembé Geneva, Switzerland
e-mail: inmail@iec.ch IEC web site <http://www.iec.ch>



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

R

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

SOMMAIRE

	Pages
AVANT-PROPOS	4
Articles	
1 Domaine d'application et objet.....	6
2 Références normatives.....	6
3 Définitions.....	6
4 Processus d'analyse fonctionnelle et d'affectation des fonctions	8
4.1 Description générale	8
4.1.1 Analyse fonctionnelle.....	8
4.1.2 Affectation des fonctions	10
4.2 Equipe technique de base pour l'AF et AF	10
5 Analyse fonctionnelle	12
5.1 Généralités	12
5.2 Identification des fonctions.....	12
5.3 Identification des informations de base et des exigences de traitement.....	14
5.3.1 Analyse des fonctions individuelles.....	14
5.3.2 Identification des exigences temporelles et des événements représentatifs	16
6 Affectation des fonctions	18
6.1 Généralités	18
6.2 Analyse des fonctions de commande.....	18
6.2.1 Identification des unités fonctionnelles.....	18
6.2.2 Caractérisation des fonctions de commande.....	18
6.2.3 Identification des éléments caractéristiques des fonctions de commande... ..	20
6.3 Etablissement des critères d'affectation.....	20
6.3.1 Eléments caractéristiques et capacités de l'homme et de la machine	22
6.3.2 Législation nationale, règles et directives légales nationales et internationales.....	26
6.3.3 Règles et principes des exploitants et des vendeurs	26
6.4 Processus d'affectation	26
Annexe A (informative) Exemples de décomposition en objectifs et sous-objectifs.....	34
Annexe B (informative) Début d'une analyse fonctionnelle d'une centrale REP (réacteur à eau pressurisée)	36
Bibliographie	38
Figure 1 – Illustration des activités de AF et AF décrits dans la CEI 60964	30
Tableau 1 – L'homme et la machine dans le domaine fonctionnel et dans le domaine physique.....	32
Tableau 2 – Affectation des fonctions à l'homme ou à la machine – Structure de base	32

CONTENTS

	Page
FOREWORD	5
Clause	
1 Scope and object	7
2 Normative references	7
3 Definitions	7
4 Process of functional analysis and assignment	9
4.1 General description	9
4.1.1 Functional analysis	9
4.1.2 Assignment of functions	11
4.2 Basic technical team for FA and A	11
5 Functional analysis	13
5.1 General	13
5.2 Identification of functions	13
5.3 Identification of basic information and processing requirements	15
5.3.1 Individual function analysis	15
5.3.2 Identification of time requirements and representative events	17
6 Assignment of functions	19
6.1 General	19
6.2 Control function analysis	19
6.2.1 Identifying functional units	19
6.2.2 Characterising the control functions	19
6.2.3 Identifying control function characteristics measurements	21
6.3 Development of assignment criteria	21
6.3.1 Characteristic measurement and man-machine capabilities	23
6.3.2 National law, national and international legal rules and guides	27
6.3.3 Utility and vendors' rules and policies	27
6.4 Assignment process	27
Annex A (informative) Examples of decomposition of goals and subgoals	35
Annex B (informative) Beginning of PWR (pressurized water reactor) functional analysis	37
Bibliography	39
Figure 1 – Illustrated FA and A activities given in IEC 60964	31
Table 1 – Humans and machines in the functional domain and in the physical domain	33
Table 2 – Assignment of functions to humans and machines – Basic structure	33

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – CONCEPTION DES SALLES DE COMMANDE – ANALYSE FONCTIONNELLE ET AFFECTATION DES FONCTIONS

AVANT-PROPOS

- 1) La CEI (Commission Electrotechnique Internationale) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI, entre autres activités, publie des Normes internationales. Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux intéressés sont représentés dans chaque comité d'études.
- 3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
- 4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61839 a été établie par le sous-comité 45A: Instrumentation des réacteurs, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Cette norme doit être lue conjointement avec la CEI 60964.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/382/FDIS	45A/389/RVD

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

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 3.

Les annexes A et B sont données uniquement à titre d'information.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2006. A cette date, la publication sera

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**NUCLEAR POWER PLANTS –
DESIGN OF CONTROL ROOMS –
FUNCTIONAL ANALYSIS AND ASSIGNMENT**

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61839 has been prepared by subcommittee 45A: Reactor instrumentation, of IEC technical committee 45: Nuclear instrumentation.

This standard shall be read in conjunction with IEC 60964.

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

FDIS	Report on voting
45A/382/FDIS	45A/389/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

Annexes A and B are for information only.

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be

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

CENTRALES NUCLÉAIRES DE PUISSANCE – CONCEPTION DES SALLES DE COMMANDE – ANALYSE FONCTIONNELLE ET AFFECTATION DES FONCTIONS

1 Domaine d'application et objet

La présente Norme internationale définit les procédures d'analyse fonctionnelle et d'affectation des fonctions (AF et AF, quelquefois appelées «allocation des fonctions») applicables à la conception du système de salle de commande dans les centrales nucléaires et donne des règles pour établir des critères applicables à l'affectation des fonctions.

La présente norme est un complément de la CEI 60964, relative à la conception des salles de commande des centrales nucléaires de puissance.

Le but de la présente norme est d'établir des exigences spécifiques pour effectuer l'analyse fonctionnelle et l'affectation des fonctions requises en 3.1 et 3.2 de la CEI 60964, et de ce fait se substitue aux directives données en A.3.1 et A.3.2 de la CEI 60964.

La présente norme s'applique à la conception de nouvelles salles de commande ou à des rénovations (renouvellement ou modifications de la conception) apportées à des salles de commande existantes. Dans ce dernier cas, il est nécessaire d'user de prudence dans l'identification des zones affectées indirectement et directement par les modifications.

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Norme internationale. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de l'ISO et de la CEI possèdent les registres des Normes internationales en vigueur.

CEI 60964:1989, *Conception des salles de commande des centrales nucléaires de puissance*

CEI 61771:1995, *Centrales nucléaires de puissance – Salle de commande principale – Vérification et validation de la conception*

3 Définitions

Pour les besoins de la présente Norme internationale, les définitions données dans la CEI 60964 et les suivantes s'appliquent:

3.1

conditions accidentelles

ensemble de conditions identifiées dans les rapports d'analyse de sûreté ou de transitoire et/ou dans les procédures de conduite accidentelles

3.2

affectation des fonctions

répartition des fonctions parmi les constituants humains et automatisés d'un système

NUCLEAR POWER PLANTS – DESIGN OF CONTROL ROOMS – FUNCTIONAL ANALYSIS AND ASSIGNMENT

1 Scope and object

This International Standard specifies functional analysis and assignment procedures (FA and A, sometimes called allocation of functions) for the design of the control-room system for nuclear power plants and gives rules for developing criteria for the assignment of functions.

This standard supplements IEC 60964, which applies to the design of the control-room for nuclear power plants.

The purpose of this standard is to provide specific requirements for carrying out the functional analysis and assignment required in 3.1 and 3.2 of IEC 60964, and therefore supersedes the guidance given in A.3.1 and A.3.2 of IEC 60964.

This standard is applicable to the design of new control-rooms or to backfits (design renewal and design modifications) to existing control-rooms. In the latter case, particular caution is to be exercised to identify areas indirectly affected as well as those directly affected.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60964:1989, *Design for control rooms of nuclear power plants*

IEC 61771:1995, *Nuclear power plants – Main control-room – Verification and validation of design*

3 Definitions

For the purpose of this International Standard, the definitions given in IEC 60964 and the following definitions apply:

3.1

accident conditions

set of conditions identified in the safety or transient analysis reports and/or in the emergency operating procedures

3.2

functional assignment

distribution of functions among the human and automated constituents of a system

3.3

interface homme/machine, IHM

interface entre l'équipe de conduite d'une part, les systèmes 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» (voir «Interface homme/machine» dans la CEI 60964)

3.4

évaluation probabiliste de sûreté (EPS)

approche méthodologique d'identification des séquences d'accident pouvant être issues d'un large spectre d'événements initiateurs; elle inclut la détermination systématique et réaliste des fréquences et des conséquences des accidents

3.5

fonction de commande

actions de commande exécutées par un homme ou une machine pour atteindre un objectif fonctionnel et comprenant l'acquisition et le traitement d'information associés ¹⁾

3.6

tâches

actions de commande exécutées par l'homme pour atteindre un objectif fonctionnel ¹⁾

4 Processus d'analyse fonctionnelle et d'affectation des fonctions

4.1 Description générale

Le processus d'analyse fonctionnelle et d'affectation des fonctions est requis à l'article 3 de la CEI 60964 comme première étape de conception d'une salle de commande (voir figure 1). Il a pour objet, d'abord, d'identifier toutes les fonctions nécessaires pour exploiter la centrale, puis d'affecter les fonctions à l'homme ou à la machine.

Deux étapes essentielles sont requises:

- a) l'analyse fonctionnelle;
- b) l'affectation des fonctions.

Elles sont respectivement définies aux articles 5 et 6 de la présente norme.

4.1.1 Analyse fonctionnelle

L'identification des fonctions (voir 5.2) est obtenue d'abord par une définition des objectifs généraux ou fondamentaux de l'exploitation de la centrale, c'est-à-dire une production d'électricité sûre et efficace, une protection du public contre les risques de rejets radioactifs, puis par une décomposition des fonctions de haut niveau – permettant à ces objectifs d'être atteints – en une hiérarchie de fonctions dont la base sera constituée des fonctions de commande qui doivent être affectées à l'homme ou à la machine. L'analyse fonctionnelle globale d'une centrale nucléaire est un moyen pour identifier toutes les fonctions accomplies depuis la salle de commande.

La base de données statique des fonctions des différents niveaux obtenue lors de l'étape précédente est complétée par la détermination du flux d'informations opérationnelles de base et des exigences de traitement pour l'exploitation de la centrale (voir 5.3.1).

¹⁾ Cette définition s'écarte de celle donnée dans la CEI 60964, mais reflète l'usage actuel.

3.3

human machine interface, HMI

interface between operating staff and I and C system and computer systems linked with the plant. The interface includes displays, controls, and the Operator Support System interface (see man/machine interface in IEC 60964)

3.4

probabilistic risk assessment (PRA)

methodological approach to identify accident sequences that can follow from a broad range of initiating events; it includes the systematic and realistic determination of accident frequencies and consequences

3.5

control function

control actions performed by humans or machines for the accomplishment of a functional goal including the associated information acquisition and processing ¹⁾

3.6

tasks

control actions performed by humans for the accomplishment of a functional goal ¹⁾

4 Process of functional analysis and assignment

4.1 General description

The process of functional analysis and assignment is required in clause 3 of IEC 60964 as a first step for the design of a control-room (see figure 1). It aims initially to identify all of the functions required to operate the plant, then to assign the functions to humans or to machines.

Two basic steps are required:

- a) functional analysis;
- b) assignment of functions.

They are defined respectively in clauses 5 and 6 of this standard.

4.1.1 Functional analysis

The identification of the functions (see 5.2) is obtained initially by defining general or fundamental objectives of the plant operation, i.e. safe and effective generation of electrical power, protection of the public from radiological hazards, then by breaking down the top-level functions, allowing those objectives to be fulfilled, into a hierarchy of functions where the lowest set of functions are the control functions which must then be assigned to humans or to machines. The general nuclear power plant functional analysis is a means to the identification of all the functions achieved from the main control-room.

The static database of functions of different levels, obtained in the previous step, is completed by the determination of the basic operational information flow and processing requirements for plant operation (see 5.3.1).

¹⁾ This definition deviates from IEC 60964 but reflects current use.

L'étape suivante de l'analyse est l'introduction d'exigences temporelles par la prise en compte d'un nombre suffisant d'événements de la base de conception et de situations d'exploitation de la centrale (normales, anormales et accidentelles) (voir 5.3.2). De cette façon, tous les éléments nécessaires à l'identification des fonctions associées à la salle de commande sont identifiés.

4.1.2 Affectation des fonctions

L'affectation des fonctions est une répartition des fonctions parmi les constituants humains et automatisés d'un système.

Tout d'abord, une caractérisation des fonctions identifiées est à conduire pour

- a) regrouper méthodiquement, si nécessaire, les fonctions définies (voir 6.2.1);
- b) identifier et définir en détail toutes les actions nécessaires à l'accomplissement des fonctions (voir 6.2.2);
- c) identifier les éléments caractéristiques types des fonctions (voir 6.2.3).

Ensuite, l'affectation des fonctions peut être assurée sur la base d'un ensemble prédéfini de critères d'affectation (voir 6.3).

Affecter des fonctions à l'homme signifie les réaliser par des commandes manuelles, par une démarche intellectuelle ou par leurs combinaisons. Affecter des fonctions à la machine signifie les réaliser par voie d'automatismes. Par conséquent, dans le domaine fonctionnel, «machine» désigne les automatismes, tandis que «homme» désigne l'équipe de la salle de commande. Voir tableau 1.

Le terme «machine» couvre un ensemble de matériels qui incluent le système de contrôle-commande et le système support de l'opérateur.

Il convient de noter que les systèmes manuels de réglage, les moyens de commandes et de présentation d'informations, qui font partie du système de contrôle-commande, sont nécessaires pour permettre à l'équipe de la salle de commande de remplir les fonctions qui lui sont assignées.

La vérification et la validation (V et V) de l'affectation des fonctions sont hors du domaine d'application de la présente norme et relèvent de la CEI 61771.

NOTE La conception de la centrale et l'analyse des fonctions et des tâches qui en résulte sont limitées aux événements, scénarios prévus et aux combinaisons prévus d'événements et de défaillances. Des fonctions peuvent s'avérer nécessaires pour le diagnostic et la gestion de situations d'exploitation imprévues; cela est évidemment du ressort de l'équipe de conduite et est alors en dehors du domaine d'application de la présente norme.

4.2 Equipe technique de base pour l'AF et AF

En général, il convient que l'équipe technique de base pour l'analyse fonctionnelle et l'affectation des fonctions inclue les domaines d'expertise suivants:

- ingénierie des systèmes nucléaires et non nucléaires;
- analyses des systèmes;
- conception des systèmes de contrôle et de commande (CC);
- conception des systèmes informatiques et d'information;
- ingénierie des facteurs humains;
- exploitation de centrale;
- élaboration des procédures de conduites normale et accidentelle.

Dans la suite, cette équipe technique est désignée par «le concepteur».

The next step of the analysis is the introduction of time requirements, taking into account a sufficient number of basic design events and plant conditions (normal, abnormal and accident conditions) (see 5.3.2). In this way, all of the elements needed for the identification of the functions associated with the control-room are identified.

4.1.2 Assignment of functions

Functional assignment is a distribution of functions between the human and automated constituents of a system.

As a first step, a characterisation of the identified functions is to be performed to

- a) methodically group, if necessary, the defined functions (see 6.2.1);
- b) identify and define in detail all the actions needed for the accomplishment of the functions (see 6.2.2);
- c) identify typical function characteristic measurements (see 6.2.3).

Then, the functional assignment can be provided on the basis of a pre-defined set of assignment criteria (see 6.3).

Assigning functions to humans means achieving them by manual control, monitoring, high-level mental processing, or their combinations. The assignment of functions to machines means achieving them by automation. Therefore, machine in the functional domain signifies automation, while human in the functional domain signifies the control-room staff. See table 1.

The term machine covers a number of hardware entities which include the I and C system and the operator support system.

It should be noted that manual control systems, controls and displays which are part of the I and C system are needed to enable the control-room staff to achieve functions assigned to them.

The verification and validation (V and V) of the functional assignment is outside the scope of this standard; refer to IEC 61771.

NOTE The design of a plant and the resulting analysis of functions and tasks are limited to the anticipated events, scenarios and anticipated combinations of events and failures. There may be a need for functions for the diagnosis and handling of unforeseen operating situations, which is obviously to be handled by the operating staff, which is then outside the scope of this standard.

4.2 Basic technical team for FA and A

In general, a basic technical team for FA and A should include the following areas of expertise:

- nuclear and non-nuclear systems engineering;
- systems analysis;
- instrumentation and control (I and C) systems design;
- information and computer systems design;
- human factor engineering;
- plant operation;
- development of normal operation and emergency procedures.

In the following, this technical team is called the “designer”.

5 Analyse fonctionnelle

5.1 Généralités

Le processus d'analyse fonctionnelle doit inclure les deux étapes suivantes:

- identification des fonctions;
- identification du flux d'informations et des exigences de traitement.

5.2 Identification des fonctions

Le but de l'identification des fonctions de commande est d'assurer que l'IHM affectée à ces fonctions en sera un support correct. Par exemple, il faut que la conception de l'IHM en salle de commande fasse en sorte que toutes les informations et commandes associées aux fonctions de sûreté soient à la fois présentes et convenablement présentées à l'opérateur.

L'identification des fonctions de commande nécessaires doit être basée sur une décomposition fonctionnelle générale de la centrale nucléaire. Dans la suite, les grandes lignes d'une méthode strictement hiérarchique sont tracées. Cette décomposition doit être obtenue en présentant les résultats des études de conception d'ensemble de la centrale de manière hiérarchique en liaison avec les objectifs opérationnels de la centrale:

- a) l'objectif de sûreté (limitation des rejets radioactifs dans l'environnement), et
- b) l'objectif de disponibilité (production maîtrisée d'électricité).

Ces objectifs doivent être développés de façon plus approfondie en sous-objectifs pour produire une structure d'objectifs hiérarchisés, c'est-à-dire un ensemble de relations entre des objectifs et des sous-objectifs fonctionnels structurés hiérarchiquement.

En ce qui concerne la structure d'objectifs hiérarchisés mentionnés ci-dessus, toutes les fonctions de la centrale nécessaires pour atteindre ces objectifs et sous-objectifs doivent être identifiées. Il convient que l'identification des fonctions résulte directement de l'identification des objectifs. En principe, les termes «objectif» et «fonction» sont interchangeables. Cependant, aux niveaux supérieurs de la structure hiérarchique, la vision conceptuelle de la centrale est appréhendée et mieux exprimée en termes d'«objectifs» alors qu'aux niveaux inférieurs faire référence à une «fonction» en tant qu'activité ou rôle rempli par l'homme ou par des systèmes automatiques (définition de la CEI 60964) est plus approprié.

Le concepteur doit tout d'abord subdiviser chacune de ces fonctions et élaborer un ensemble de règles afin d'identifier le moment où l'analyse hiérarchique a abouti à un niveau suffisant de détail. La décomposition d'une fonction peut être typiquement stoppée quand

- a) la fonction ne comprend plus de fonction de commande, par exemple une fonction purement mécanique;
- b) le niveau de maîtrise de fonctions individuelles, de paramètres ou d'actionneurs est atteint.

Les règles définies doivent assurer que les fonctions de bas niveau forment un ensemble complet, sont individualisées et décrites en termes fonctionnels, ou que le processus peut être arrêté quand les fonctions détaillées ont été obtenues et que les constituants importants de la structure ont été identifiés.

Dans tous les cas, le niveau final de décomposition doit permettre la mise à disposition de l'information nécessaire à l'étape suivante de conception (voir paragraphes suivants). Il se peut que quelques itérations soient nécessaires pour atteindre ce niveau final.

Au sommet, la structure hiérarchique obtenue aura les objectifs fonctionnels, au milieu, des fonctions de type système, et à la base, des fonctions de commande détaillées devant être affectées à l'homme ou à la machine.

5 Functional analysis

5.1 General

The functional analysis process shall include the following two steps:

- identification of functions;
- identification of information flow and processing requirements.

5.2 Identification of functions

The purpose of identifying control functions is to assure that the HMI allocated to these functions will support them correctly. As an example, the control-room HMI design must ensure that all signals and controls associated with safety functions are both present and clearly displayed to the operator.

The identification of control functions needed shall be based on a general nuclear power plant functional decomposition. In the following, a strictly hierarchical method is outlined. This decomposition shall be obtained by presenting the results of the overall plant design in a hierarchical manner, with the plant operational goals:

- a) safety goal (prevent activity release to the environment); and
- b) availability goal (controlled generation of electricity).

These goals shall be developed further as subgoals, producing a hierarchical goal structure, i.e. a relationship between functional goals and subgoals structured in a hierarchical order.

With regard to the hierarchical goal structure above, all plant functions to achieve these goals and subgoals shall be identified. The function identification should follow immediately from goal identification. In principle, the terms "goal" and "function" are interchangeable. However, at higher levels of the hierarchy, the plant design concept is considered and better expressed in terms of goals, when at lower levels it is more appropriate to refer to a function as an activity or role performed by a human or automated systems (definition in IEC 60964).

The designer shall subdivide each of these functions successively and develop a set of rules to identify when the hierarchical analysis is completed to a sufficient level of detail. The decomposition of a function can be typically stopped when

- a) the function does not contain a control function any more, for example purely mechanical;
- b) the level of controlling individual functions, parameters or actuators is reached.

The defined rules shall ensure that the bottom-level functions form a complete set, itemised and stated in functional terms, or the process can be stopped where detailed functions are obtained and the important constituents of the structure have been identified.

In any case, the final level of decomposition shall allow the provision of the information needed for the next design step (see following paragraphs). Some iteration could be necessary to reach this final level.

The resultant hierarchy will have the functional goals at the top, system-level functions in the middle and detailed control functions at the bottom level, to be assigned to humans or machines.

Il peut être noté que, même si sûreté et disponibilité forment des points d'entrée séparés dans la décomposition fonctionnelle, ils convergent souvent sur des fonctions communes (sauf pour des objectifs spécifiques tels que l'intégrité du confinement). En conséquence, il est admis, pour cette analyse spécifique seulement, que les objectifs de sûreté et de disponibilité soient pris en compte ensemble.

Dans le cas d'une nouvelle conception de centrale, ce processus «du haut vers le bas» est conduit collectivement pour tous les systèmes de la centrale (c'est-à-dire systèmes mécaniques, systèmes électriques, etc.). Il convient alors que cette décomposition d'objectifs généraux en fonctions destinées à être affectées à l'homme ou à la machine fasse partie du processus d'ensemble de conception de la centrale et ne soit pas exclusivement réalisée pour la conception de la salle de commande. Cela devrait permettre une prise en compte de la conception de la salle de commande à un stade précoce de la conception de la centrale et éviter des itérations.

Les principes et critères utilisés lors de l'analyse doivent être documentés.

Il convient de remarquer qu'une décomposition strictement hiérarchique des fonctions n'est pas la seule voie d'organisation et de représentation d'une centrale. Selon les objectifs de conception, il est admis que d'autres représentations fonctionnelles soient mieux adaptées. Des exemples de décomposition fonctionnelle sont donnés aux annexes A et B.

5.3 Identification des informations de base et des exigences de traitement

L'étape suivante de l'analyse fonctionnelle est l'identification des informations de base et des exigences de traitement nécessaires à la réalisation des fonctions de commande définies à l'étape précédente.

Tout d'abord, chaque fonction est analysée individuellement, puis les fonctions sont prises en compte collectivement, selon les besoins de réponse à des événements spécifiques de la centrale, pour identifier des exigences temporelles.

5.3.1 Analyse des fonctions individuelles

Pour chaque fonction de commande, le concepteur doit identifier

- les paramètres observables indiquant l'état de la centrale et/ou agissant comme données d'entrée de la fonction;
- les actions réalisées par la fonction et les équipements impliqués;
- les valeurs de référence requises pour vérifier l'exécution de la fonction;
- l'importance pour la sûreté (c'est-à-dire la classification de sûreté).

Le concepteur doit aussi identifier

- comment déterminer le fonctionnement correct de la fonction;
- quelles solutions de remplacement sont disponibles lorsque l'on perd le fonctionnement correct, et comment on peut choisir parmi elles. Ici les solutions de remplacement se réfèrent à des fonctions qui peuvent venir en appui d'une fonction d'un niveau fonctionnel plus élevé à la place de la fonction analysée. Par exemple, on peut choisir parmi plusieurs circuits redondants d'évacuation de la chaleur selon les conditions de la centrale;
- les modes de fonctionnement de la centrale quand la fonction est requise (par exemple de l'arrêt jusqu'au fonctionnement à pleine puissance);
- les états de la centrale lorsque la fonction est requise (par exemple fonctionnement normal, fonctionnement anormal, accidents);
- les fonctions support (par exemple alimentation en air ou en électricité).

It should be noted that, even if safety and availability form separate entry points to the functional breakdown, they often converge on common functions (except for specific objectives such as containment integrity). As a result, availability and safety objectives may be considered together for this particular analysis only.

In the case of a new plant design, this top-down process is performed commonly for all plant systems (i.e. fluid systems, electric systems, etc.). This decomposition of overall goals into functions subjected to assignment to humans or machines should then be a part of the overall plant design process, and not be performed exclusively for the control-room design. This would allow the control-room design to be considered at an early stage of the plant design and avoid iterations.

The principles and criteria used in the analysis shall be documented.

It should be noted that a strictly hierarchical decomposition of functions is not the only choice for plant organisation and representation. Depending on the design objectives, other function representations may be more suitable. Examples of function decomposition are given in annexes A and B.

5.3 Identification of basic information and processing requirements

The next step in the functional analysis is to identify the basic information and processing requirements needed for the accomplishment of each control function defined in the previous step.

Firstly, each function is analysed individually, and then functions are collectively considered as needed in response to specific plant events to identify time requirements.

5.3.1 Individual function analysis

For each control function, the designer shall identify the following:

- observable parameters which will indicate the plant status and/or will act as a function input;
- actions performed by the function and involved equipment;
- performance measures required to check the achievement of the function;
- safety relevance (i.e. safety classification).

The designer shall also identify

- how to determine correct operation 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 analysed. For instance, several redundant heat removal paths could be chosen depending on plant conditions;
- plant operation modes when the function is required (for example, shutdown through full power operation);
- plant states when the function is required (for example, normal operation, abnormal operation, accidents);
- the supporting functions (for example, air or electrical power supply).

A ce stade, il convient que l'approche soit générale et ne se réfère pas à une mise en œuvre spécifique ou à un niveau d'implication de l'opérateur. Si, pour des raisons technologiques ou d'autres raisons, des choix ont déjà été faits, ils doivent être explicitement identifiés et documentés.

Lors de l'identification des valeurs de référence permettant de garantir la réalisation de la fonction, il est parfois judicieux d'utiliser des informations se rapportant aux événements de la base de conception. Il est optimal de disposer de valeurs de référence basées sur une approche physique. Par exemple, une des valeurs relatives à l'évacuation de la chaleur du cœur peut être déterminée par une information sur les matériaux utilisés pour la gaine du combustible, comme 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.

5.3.2 Identification des exigences temporelles et des événements représentatifs

Le concepteur doit inclure dans l'analyse tous les événements représentatifs, de façon à couvrir convenablement les fonctions associées à la structure fonctionnelle hiérarchique, et à définir les caractéristiques temporelles. L'analyse permettra d'identifier la vitesse à laquelle l'influence d'un événement peut se propager dans la hiérarchie et quelles fonctions de niveau supérieur sont affectées. En conséquence, des exigences relatives aux contraintes temporelles liées à l'accomplissement de fonctions spécifiques doivent être définies.

Pour cela, les scénarios suivants doivent être analysés:

- a) toutes les séquences d'exploitation comme les opérations de démarrage et le fonctionnement normal;
- b) tous les événements de la base de conception cités dans le rapport d'analyse de sûreté (par exemple APRP (accident de perte de réfrigérant primaire), perte de l'alimentation électrique en courant alternatif, etc.);
- c) les événements hors dimensionnement, comme la fusion du cœur, les explosions de vapeur, etc. (conditions d'accident grave) lorsque cela est requis.

Dans cette analyse, les événements qui imposent les exigences les plus sévères en termes de temps d'action et de fiabilité doivent être identifiés. Il convient d'examiner ceux qui suivent:

- les événements qui, dans la conception de la centrale, devraient suivre un arrêt automatique ou une sollicitation de la sauvegarde du réacteur;
- les événements requérant des conduites estimées subjectivement difficiles en termes de complexité d'interprétation de données ou de rapidité d'action de commande;
- les événements requérant la plus grande certitude d'une réponse correcte, par exemple dans certaines situations accidentelles;
- les événements importants en termes d'analyse probabiliste de sûreté;
- les événements pour lesquels un arrêt automatique de la centrale est hautement probable à moins qu'une action corrective ne soit exécutée à temps;
- les événements dont la probabilité d'occurrence est grande;
- les événements correspondant à la perte d'une fonction spécifique.

At this stage the approach should be general and not refer to a specific implementation or level of human involvement. If, for technological or other reasons, choices have already been made, they shall be explicitly identified and documented.

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

5.3.2 Identification of time requirements and representative events

The designer shall include in the analysis all representative events, to cover adequately the functions associated with the hierarchical functional structure, and to define time-dependent characteristics. The analysis will allow the identification of the speed at which the influence of an event may propagate along the hierarchy and at which higher-level functions are influenced. Consequently, requirements shall be defined for the timing needed to accomplish specific functions.

For this the following scenarios shall be analysed:

- a) all operational sequences such as start-up and normal power operations;
- b) all design basis events given in the safety analysis report (for example, LOCA (loss of coolant accident), loss of a.c. power, etc.);
- c) beyond design events, such as core fusion, steam explosions, etc. (severe accident conditions) when required.

In this analysis those events shall be identified which impose the highest requirements on timing and reliability. The following should be considered:

- events in the basic plant design which should follow a reactor trip or a safety challenge;
- events requiring operations subjectively judged to be difficult in terms of complexity of data interpretation or control speed, etc.;
- events requiring the highest certainty of correct response, for example, 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;
- events corresponding to loss of a specific function.

6 Affectation des fonctions

6.1 Généralités

L'affectation des fonctions doit être fondée sur les différentes fonctions ayant été décomposées en fonctions de commande. Le processus d'affectation est découpé en trois phases:

- analyse des fonctions de commande;
- élaboration de critères d'affectation;
- processus d'affectation.

6.2 Analyse des fonctions de commande

A l'aide de la base de données constituée lors de l'analyse fonctionnelle (c'est-à-dire flux d'informations et exigences de traitement), le concepteur doit procéder à une analyse de façon à identifier le contenu détaillé des fonctions et leurs éléments caractéristiques.

Cette analyse doit être réalisée en trois étapes.

6.2.1 Identification des unités fonctionnelles

La première étape concerne le possible réarrangement des fonctions définies en 5.2, pour les grouper convenablement selon le contexte de leur utilisation prévue et pour être en mesure ensuite de déterminer leurs éléments caractéristiques globaux. Il peut être constaté que des fonctions sont déjà liées entre elles et qu'elles peuvent être traitées comme une unité, c'est-à-dire une fonction unique.

Le concepteur doit identifier les fonctions qui doivent être exécutées ensemble pour réaliser des activités opérationnelles telles que le démarrage de la centrale, les mouvements de puissance, l'atténuation de conséquences d'événements de la base de conception. Cela devrait permettre d'identifier certains facteurs comme les contraintes de charge ou de temps, facteurs qui ne sont pas inclus dans les éléments caractéristiques des fonctions individuelles. Prises ensemble, elles seront désignées comme unité fonctionnelle.

6.2.2 Caractérisation des fonctions de commande

Dans le contexte des unités fonctionnelles, le concepteur doit identifier, pour chaque fonction de commande, les éléments suivants:

- l'enchaînement logique conduisant à sa mise en œuvre (pourquoi sa mise en œuvre est-elle requise ?);
- les actions de commande nécessaires à sa mise en œuvre (comment peut-elle être mise en œuvre ?);
- 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 de choix de solutions de remplacement.

Les paramètres identifiés dans l'analyse décrite ci-dessus constituent la base pour le choix des équipements de contrôle et de commande automatiques et/ou des dispositifs d'interface avec l'opérateur, comme les commandes et les affichages de paramètre. Cela constitue également la base de regroupement des moyens de présentation d'information et des commandes.

Un exemple de fonction de commande est donné ci-après.

6 Assignment of functions

6.1 General

The functional assignment shall be based on the different functions having been decomposed into control functions. The assignment process is split up into three phases:

- control function analysis;
- development of assignment criteria;
- assignment process.

6.2 Control function analysis

Using the database developed in the functional analysis (i.e. information flow and processing requirements) the designer shall conduct an analysis in order to identify the detailed parts of the functions and their characteristics.

This analysis shall be done in three steps.

6.2.1 Identifying functional units

The first step is related to a possible rearrangement of the functions defined in 5.2, in order to group them properly according to the context of their foreseen use and to be able then to determine their global characteristics. It can be found that some functions are already related so that they can be treated as a unit, i.e. a single function.

The designer shall identify the functions that are required to be performed together to support operational activities such as plant start-up, power manoeuvre, mitigation of basic design events. This would allow factors like work load and time constraints to be identified, which are not contained in the characteristics of the individual functions. Taken together, they will be referred to as a functional unit.

6.2.2 Characterising the control functions

The designer shall identify the following for each control function in the context of the functional units:

- the logical requirements for its implementation (why its implementation is required);
- the control actions necessary for its implementation (how it can be implemented);
- the parameters necessary for control actions;
- the criteria for evaluating the result of control actions;
- the parameters necessary for the evaluation;
- the criteria for choosing alternatives.

The parameters identified in the above analysis form the basis for the selection of automatic I and C equipment and/or interfacing devices to the operator, such as controls and parameter displays. It also provides the basis for grouping the displays and controls.

An example of a control function is as follows.

Une pompe doit être démarrée/arrêtée pour réaliser une fonction donnée basée sur certains paramètres du procédé (par exemple niveaux bas/haut dans un réservoir).

Dans ce cas, l'action de commande peut être manuelle (l'opérateur démarre/arrête la pompe sur la base d'une information de niveau et d'une procédure) ou automatique (le niveau réel est comparé aux points de consigne de démarrage/arrêt et le signal de commande requis est généré). Le paramètre de commande est le niveau dans le réservoir. Le critère d'évaluation du résultat de l'action de commande traduit que le niveau du réservoir reste dans une plage de valeurs autorisées en utilisant le niveau comme paramètre d'évaluation; les critères de remplacement pourraient être l'intensité absorbée par le moteur de la pompe, le débit de décharge, les alarmes de très bas ou très haut niveau, etc.

6.2.3 Identification des éléments caractéristiques des fonctions de commande

Le concepteur doit identifier les éléments caractéristiques des fonctions de commande et définir plusieurs classes pour chaque élément (en raison de leur niveau d'importance). En sélectionnant les différents éléments caractéristiques, des exigences de performance doivent être identifiées pour chaque fonction de commande. Le concepteur doit tenir compte à la fois de la fiabilité et de la validité de ces éléments, et leur affecter un niveau d'importance. Il convient que la sélection inclue à la fois des éléments objectifs (par exemple le temps, la rapidité) et subjectifs pour aider à la prise de décision. Lorsque des éléments subjectifs sont retenus, il convient que ceux-ci incluent des jugements basés sur des échelles de valeurs quantifiées.

Le concepteur doit au moins envisager les éléments caractéristiques suivants, tout en prenant aussi en compte la charge due aux autres fonctions de commande devant être exécutées ensemble:

- la charge de travail potentielle pour l'homme, dans tous les modes d'exploitation;
- les facteurs temporels (par exemple rapidité, marge et contrainte de temps);
- la précision et la répétabilité;
- la complexité de la logique d'enchaînement;
- les types et complexités des prises de décision (par exemple évaluation de relations non linéaires, de scénarios qui ne sont pas analysés de façon exhaustive);
- la conséquence sur l'exécution de la fonction de commande de l'événement type pendant lequel la tâche est réalisée;
- les conséquences de la perte d'une fonction et les facteurs temporels associés.

Il est conseillé au concepteur de contacter des ergonomes et des experts en psychologie appliquée avec de l'expérience dans le domaine des méthodes d'analyse de tâche et dans celui de leur application dans la conception de systèmes, aussi bien que des concepteurs de systèmes, pour établir des éléments caractéristiques pertinents. Le concepteur doit alors classer chaque fonction de commande selon les éléments caractéristiques définis.

Les principes et critères utilisés dans l'analyse doivent être documentés.

6.3 Etablissement des critères d'affectation

Parallèlement à l'analyse des fonctions de commande, le concepteur doit établir des critères de prise de décision pour l'affectation des fonctions et leur mise en œuvre:

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

A pump shall be started/stopped to accomplish a given function based on certain process parameters (for example, low/high level in a tank).

In this case, the control action can be manual (the operator starts/stops the pump based on level indication and instructions) or automatic (the actual level is compared with start/stop level setpoints and the required control signal is generated). The control parameter is the tank level. The criterion for evaluating the result of the control action involves the tank level being inside a permitted range, by using the level as an evaluation parameter; the alternative ones could be current absorption by the pump motor, discharge flow, low-low/high-high alarms, etc.

6.2.3 Identifying control function characteristics measurements

The designer shall identify the control function characteristic measurements and define several classes (due to their level of importance) for each measurement. In selecting different measures, performance requirements shall be identified for each control function. The designer shall consider both the reliability and validity of the measure and allocate a level of importance to each. The selection should include both objective (for example, time, rate) and subjective measures to assist decision-making. Where subjective measures are selected, these should include quantitatively scaled judgements.

The designer shall consider, as a minimum, the following characteristics, taking also into account load due to other control functions to be performed together:

- potential human workload, under all operating modes;
- time factors (for example, rate, time margin/constraint);
- accuracy and repeatability;
- complexity of logic action;
- types and complexities of decision-making (for example, evaluation of non-linear relationships, of scenarios which are not exhaustively analysed);
- impact on the control function performance measure due to the event type in which the task is performed;
- impacts resulting from the loss of function and associated time factors.

It is advisable for the designer to consult ergonomists or applied psychologists with experience in task analysis methods and their usage in system design, as well as system designers, to develop relevant characteristic measurements. The designer finally shall classify each control function according to the defined characteristic measurements.

The principles and criteria used in the analysis shall be documented.

6.3 Development of assignment criteria

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

- to humans or machines;
- to remote manual control or local manual control.

Les critères doivent être basés sur

- les éléments caractéristiques et les capacités de l'homme et de la machine;
- la législation nationale, les règles et directives légales nationales et internationales;
- les règles et principes des exploitants et des vendeurs (expérience d'exploitation et de maintenance, aspects sociaux, etc.);
- les coûts.

6.3.1 Éléments caractéristiques et capacités de l'homme et de la machine

6.3.1.1 Critères de base

a) Critères pour l'affectation des fonctions à l'homme ou à la machine

Les critères d'affectation des fonctions à l'homme ou à la machine doivent être basés en premier lieu sur les éléments caractéristiques suivants:

- la charge de travail potentielle pour l'homme, dans tous les modes d'exploitation;
- la précision et la répétabilité;
- les facteurs temporels;
- les types et complexités des prises de décision et l'enchaînement logique requis.

Une structure de base des critères est présentée au tableau 2.

La progression rapide des capacités et des performances des systèmes de contrôle-commande fait qu'il n'y a pas de stricte distinction entre les fonctions qui seraient plus efficacement affectées à l'homme ou à la machine. Chaque nouveau projet peut nécessiter un catalogue de critères d'affectation mis à jour. De même, il convient de garder à l'esprit qu'homme et machine devraient être considérés comme des acteurs complémentaires en salle de commande.

b) Critères de mise en œuvre des fonctions par des commandes manuelles à distance ou locales

Les critères de mise en œuvre des fonctions par des commandes manuelles à distance ou locales doivent être basés en premier lieu sur les éléments caractéristiques suivants:

- les facteurs temporels;
- la facilité d'accès et le temps du déplacement;
- la disponibilité d'opérateurs locaux;
- les conséquences de la perte de fonctions et les facteurs temporels associés;
- la facilité de communication;
- la radioprotection;
- les facteurs environnementaux (chaleur, bruit);
- les dispositifs de commande locaux, nécessaires lorsque la salle de commande est évacuée.

Il convient que les fonctions pour lesquelles une réponse immédiate ou relativement rapide est requise ne soient pas commandées depuis une zone sans personnel (poste local). Une fonction automatique doit être mise en œuvre à moins qu'une action manuelle ne puisse être nettement justifiée.

Il convient également de prendre en compte les critères issus des principes généraux d'automatisation de la centrale (voir 6.3.3).

The basis for the criteria shall be

- characteristic measurement and man-machine capabilities;
- national law, national and international legal rules and guidelines;
- utility and vendors' rules and policies (operational and maintenance experience, social aspects, etc.);
- cost.

6.3.1 Characteristic measurement and man-machine capabilities

6.3.1.1 Basic criteria

a) Criteria for the assignment of functions to humans or machines

Criteria for the assignment of functions to humans or machines shall be based primarily on the following characteristic factors:

- potential human work load, under all operating modes;
- accuracy and repeatability;
- time factors;
- types and complexities of decision-making and action logic needed.

A basic structure for the criteria is presented in table 2.

The rapid development of I and C systems capabilities and capacities implies that there is no firm distinction between functions best assigned to the operator or to the machine. Each new project may need a revised catalogue of assignment criteria. It should also be kept in mind that humans and machines should be considered as having complementary roles in the control-room.

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

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

- time factors;
- ease of access and time taken;
- available local operators;
- impacts resulting from the loss of functions and associated time factors;
- ease of communication;
- exposure rates;
- environmental factors (heat, noise);
- local control measures, needed if the main control-room is evacuated.

Those functions, which require an immediate response or relatively prompt response, should not be controlled from an unmanned area (local platform). An automatic function shall be implemented unless a clear justification can be made for a manual action.

Criteria derived from general plant automation philosophy (see 6.3.3) should also be considered.

6.3.1.2 Capacités de l'opérateur

Les fonctions allouées à l'opérateur doivent distinguer celles pour lesquelles

- il effectue réellement une tâche de commande;
- il supervise un système automatique en train d'exécuter des fonctions de commande;
- il est en train de réaliser des démarches intellectuelles de haut niveau telles que des diagnostics.

Il convient que cette analyse aboutisse aux informations nécessaires à la conception de la structure du système d'information et à l'organisation fonctionnelle des ressources permettant de mener à bien chaque prise de décision et tâche de commande.

Pour chaque fonction potentielle de l'opérateur, des évaluations des capacités de traitement d'informations et de réponse effective de l'opérateur sont nécessaires. Celles-ci prennent en compte les capacités de perception pour détecter des signaux (par exemple acuité visuelle), la capacité de mémorisation et la rapidité de réaction. Pour achever l'affectation initiale, ces capacités humaines de base peuvent alors être comparées à celles requises pour accomplir chaque fonction. Il est aussi important pour le concepteur d'avoir pris connaissance du retour d'expérience d'exploitation provenant de conceptions précédentes appropriées pour identifier tout problème lié à l'exécution de la fonction par l'opérateur. Il convient que les évaluations des capacités humaines requises pour mettre en œuvre chaque fonction soient modifiées sur la base de résultats de vérification et utilisées pour reconsidérer l'affectation de la fonction aussi bien que pour fournir une définition plus détaillée des capacités requises de l'opérateur.

Si des exigences adaptées relatives au temps de réponse de l'opérateur ne peuvent être satisfaites, l'automatisation complète de la fonction de commande doit être envisagée.

Des exemples de critères d'affectation relatifs aux actions de sûreté en situation d'accident peuvent être trouvés dans les directives qui ont servi de base technique pour rédiger les procédures accidentelles de centrales précédentes possédant des caractéristiques similaires.

Il convient que les différents types de données disponibles pour l'opérateur soient groupés en se basant sur les tâches et non sur l'origine des données. Le but est d'organiser les informations provenant de différentes sources en accord avec chacune des tâches de prise de décision pour fournir à l'opérateur un système d'information à la fois complet et compatible avec ses capacités.

6.3.1.3 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 équipements, suivie par une description plus détaillée des séquences d'événements d'exploitation 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 facilitera l'évaluation des capacités à la fois de la machine et de l'homme pour accomplir chacune des tâches de prise de décision et de commande. Les capacités de traitement du système de contrôle-commande doivent finalement prendre en compte des spécifications telles que des exigences de volume, de temps de réponse et de précision auxquelles le système et/ou le matériel doivent satisfaire, aussi bien que des normes d'ingénierie du facteur humain définissant l'interface homme/machine pour chaque type de composant.

Pour réduire la probabilité d'une erreur humaine, le système de contrôle-commande doit être conçu pour maintenir la centrale à l'intérieur de limites de sûreté sans aucune action de l'opérateur pendant une période de temps spécifiée après l'initiation de certaines situations anormales de la centrale. Cette période de temps doit être reproduite dans les spécifications fonctionnelles et de fiabilité des systèmes de protection et de commande automatique.

6.3.1.2 Operator capabilities

The functions assigned to the operator shall distinguish between those where

- he is actually performing a control task;
- he is supervising an automatic system that is performing the control function;
- 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 organisation of resources to perform each decision-making and control task.

For each potential operator function, estimates of basic human information handling and physical response capabilities are needed. These include perceptual capabilities for detecting signals (for example, visualization), memory capacity and speed of response. To complete the initial allocation, these basic human capabilities can then be compared to those required to implement each function. It is also important for the designer to have consulted operating experience with relevant predecessor designs to identify any problems with human operations. The estimates of human capabilities required to implement each function should be modified on the basis of 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.

If adequate requirements concerning operator response time cannot be fulfilled, complete automation of the control function shall be considered.

Sources of assignment criteria related to safety tasks in accident conditions can be found in the emergency procedure guidelines of preceding designs, with similar plant characteristics, which served as technical bases for issuing emergency procedures for accident management.

The various types of data available to the operator should be grouped on the basis of the tasks and not on the sources of data. The purpose is to organise the information from various sources with respect to each decision-making task to provide a comprehensive information system for the operator within his capabilities.

6.3.1.3 I and C system processing capabilities

Analysis of instrumentation 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 human/machine interface requirements for each task. The purpose is to organise the machine information and capabilities with respect to the tasks defined for operator interaction.

This organisation 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 and C system shall 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 shall be designed to keep the plant within safe limits without any operator action during a specified period of time after initiation of certain abnormal conditions of the plant. This period of time shall be reflected in the functional and reliability requirements of the automatic protection and control systems.

Des exemples de critères de définition du temps de réponse recommandé pour les actions opérateur peuvent être trouvés dans la publication ANSI/ANS 58.8 ou dans différentes réglementations nationales (règles des 10 min ou 30 min).

6.3.2 Législation nationale, règles et directives légales nationales et internationales

La législation nationale peut comprendre certaines exigences de conception, exprimées lors de l'approbation préliminaire de la conception. De telles exigences peuvent être spécifiques au pays ou être issues de règles internationales, par exemple des codes pour la sûreté des centrales nucléaires ou des guides de sûreté de l'AIEA.

6.3.3 Règles et principes des exploitants et des vendeurs

Les critères qui s'appliquent à la conception générale de la centrale, les principes d'automatisation et les attributions du personnel de la centrale sont des questions importantes, devant être typiquement traitées dès le début, dans le cadre de la phase de définition du projet de la centrale; ils peuvent être utilisés comme données d'entrée au processus d'affectation.

La constitution du personnel de la salle de commande à partir d'opérateurs bien formés et entraînés est un facteur important pour l'efficacité de l'exploitation et donc pour l'économie de la centrale. Les aspects relatifs aux principes de conduite de l'exploitant pour des centrales nucléaires sont décrits en 2.6 de la CEI 60964.

6.4 Processus d'affectation

Le processus d'affectation doit commencer par l'identification des fonctions de commande pour lesquelles l'automatisation est obligatoire et de celles pour lesquelles la maîtrise par l'opérateur est obligatoire. Cela est normalement possible en tenant compte de la réglementation, de principes préexistants et de jugements évidents sur les limitations des performances humaines et sur celles des machines. Par exemple, l'affectation à la machine est obligatoire lorsqu'un environnement hostile exclut la présence d'un homme ou que le temps de réaction requis dépasse les capacités humaines.

Il convient que le processus d'affectation fournisse des données d'entrée pour la définition précise des automatismes de la centrale et pour la rédaction des procédures de conduite (conduite normale, conduite accidentelle).

Le processus d'affectation est une tâche plus exigeante pour les fonctions dont une affectation obligatoire n'a pas été identifiée. Dans ce cas, les objectifs, tels qu'ils sont formulés dans l'analyse fonctionnelle, doivent être confrontés aux capacités de l'homme et de la machine en mettant en œuvre les critères élaborés en 6.3.1.

Le concepteur doit conduire l'affectation des fonctions en comparant les éléments classés caractérisant les fonctions de commande aux critères d'affectation. L'affectation des fonctions doit se poursuivre jusqu'à ce qu'aucune insuffisance de conception ne puisse être identifiée lors des phases de vérification et de validation menées conformément à la CEI 61771.

Des directives complémentaires peuvent être trouvées dans la publication de l'AIEA TECDOC 668. Une proposition de manière de faire est d'affecter les fonctions à une des quatre catégories suivantes:

- fonctions qui doivent être automatisées;
- fonctions qu'il serait mieux d'automatiser;
- fonctions qu'il convient d'assurer par l'homme;
- fonctions qu'il convient de partager.

Examples of design criteria for the recommended delay period for the operator's actions can be found in ANSI/ANS 58.8 or in various national regulations (10 min, 30 min rules).

6.3.2 National law, national and international legal rules and guides

National law can include certain design requirements, expressed in the preliminary design approval. Such requirements can be specific for the country or they may be based on international rules, for example IAEA safety codes of practice or safety guides.

6.3.3 Utility and vendors' rules and policies

Criteria that apply to general plant design, automation philosophy and roles of station staff are main issues, typically to be defined upfront, as a part of the plant project definition phase; they can be used as inputs to the assignment process.

Control-room staffing with well-educated and trained operators is an important factor for the plant efficiency of operation and hence for the plant economy. Aspects of utility operating principles for nuclear power plants are described in 2.6 of IEC 60964.

6.4 Assignment process

The assignment process shall begin with the identification of those control functions for which automation is mandatory and those for which human control is mandatory. This can normally be made by considering regulations, policy, and obvious assessment on human performance limitations or machine limitations. For instance, allocation is mandatory to a machine when a hostile environment precludes the presence of a human or when the required reaction time exceeds human capability.

The assignment process should provide inputs for the detailed design of plant automation and for the issue of plant operation procedures (operation manual, emergency procedures).

The assignment process is a more demanding task for the functions for which no mandatory allocation is identified. In this case, the goals, as expressed in the functional analysis, shall be matched against the capabilities of humans and machines, using the criteria developed under 6.3.1.

The designer shall conduct the functional assignment by comparing the classified control function characteristic measures against the assignment criteria. The functional assignment shall continue until no design deficiencies can be identified in the verification and validation phase, according to IEC 61771.

Further guidance can be found in IAEA TECDOC 668. A suggested way is to assign the functions to one of the following four categories:

- functions which must be automated;
- functions which are better automated;
- functions which should be given to humans;
- functions which should be shared.

Enfin, les fonctions pour lesquelles un partage des tâches entre l'homme et la machine est nécessaire peuvent être identifiées. En général, même si une fonction de commande est automatisée, quelques tâches à faire par l'homme restent nécessaires (par exemple vérification du déroulement correct de la fonction en position AUTO, surveillance du secours, conduite manuelle si l'automatisme défaille).

Le processus d'affectation étant itératif, toutes les affectations, y compris celles considérées comme obligatoires, doivent être vérifiées en tenant compte des facteurs d'influence économiques et technologiques et de la cohérence entre le rôle de l'opérateur défini a priori (voir 6.3) et celui issu du processus d'affectation. En conséquence, des itérations complémentaires pourraient être nécessaires.

Les principes et critères utilisés dans l'analyse doivent être documentés et doivent tenir compte d'éléments qui concernent les capacités et les limitations à la fois de l'équipe de la salle de commande et du système d'automatisme.

IECNORM.COM : Click to view the full PDF of IEC 61839:2000

Finally, functions can be identified for which a sharing of tasks between humans and machines is needed. In general, even if a control function is automated, some human tasks are still required (for example, verification of correct AUTO function, monitoring back-up, manual control if automatism fails).

The assignment process being iterative, all the allocations, also those defined as mandatory, shall be checked, taking into account economic and technological influencing factors and consistency between the a priori defined operator's role (see 6.3) and the role resulting from the allocation process. As a result, further iterations could be needed.

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

IECNORM.COM : Click to view the full PDF of IEC 61839:2000

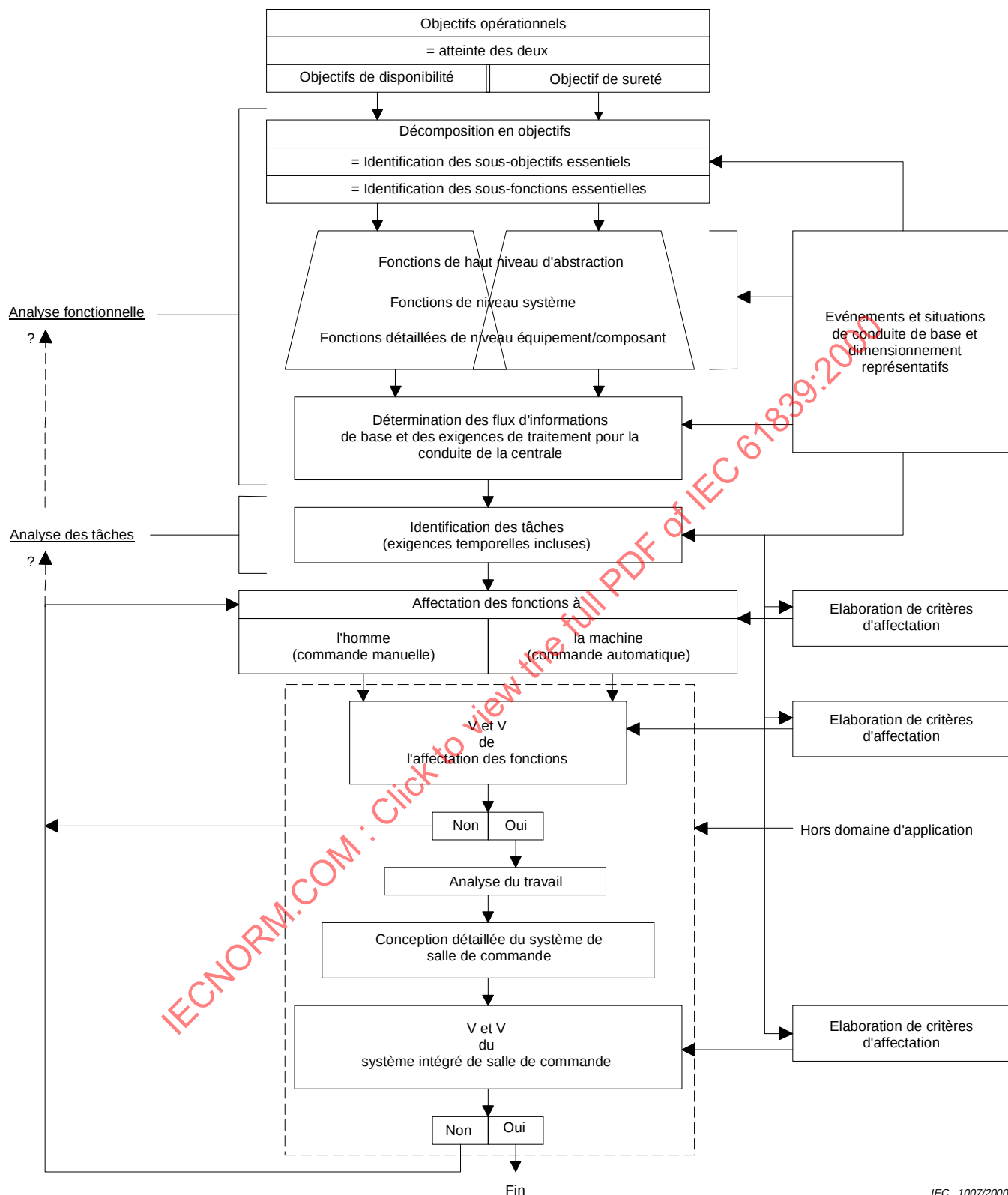


Figure 1 – Illustration des activités de AF et AT décrits dans la CEI 60964

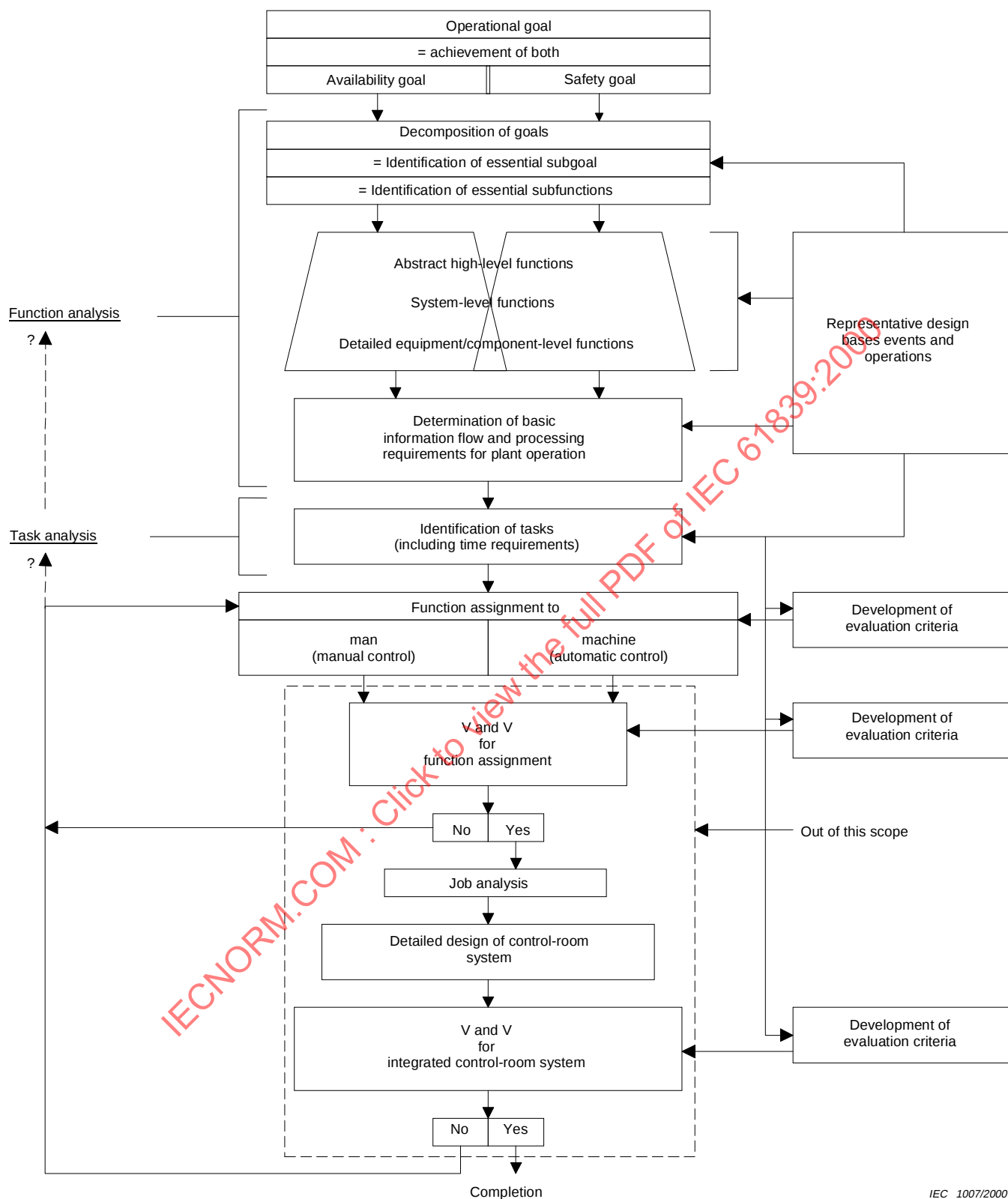


Figure 1 – Illustrated FA and A activities given in IEC 60964