NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
62241

Première édition
First edition
2004-11

Centrales nucléaires de puissance – Salle de commande principale – Fonctions et présentation des alarmes

Nuclear power plants – Main control room – Alarm functions and presentation

Numéro de référence
Reference number
CEI/IEC 62241:2004

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions 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.

Informations supplémentaires sur les publications de la CEI

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 cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI (www.iec.ch)**
- **Catalogue des publications de la CEI**

  Le catalogue en ligne sur le site web de la CEI (www.iec.ch/searchpub) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.
- **IEC Just Published**

  Ce résumé des dernières publications parues (www.iec.ch/online_news/justpub) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.
- **Service clients**

  Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

  Email: custserv@iec.ch
  Tél: +41 22 919 02 11
  Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. 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.

Further information on IEC publications

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 this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. 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 also available from the following:

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.
- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.
- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
62241

Première édition
First edition
2004-11

Centrales nucléaires de puissance – Salle de commande principale – Fonctions et présentation des alarmes

Nuclear power plants – Main control room – Alarm functions and presentation

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE X

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLE DE COMMANDE PRINCIPALE – FONCTIONS ET PRÉSENTATION DES ALARMES

AVANT-PROPOS

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

La Norme internationale CEI 62241 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/540/FDIS	45A/546/RVD

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – MAIN CONTROL ROOM – ALARM FUNCTIONS AND PRESENTATION

FOREWORD

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

International Standard IEC 62241 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/540/FDIS	45A/546/RVD

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

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

La présente Norme internationale complète le paragraphe 4.6.4 de la CEI 60964:1989, ainsi elle remplace les recommandations données dans l'Annexe A, en A.4.6.4, de la CEI 60964.

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

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

This International Standard supplements 4.6.4 of IEC 60964:1989 and therefore supersedes the guidance given in A.4.6.4 of Annex A of IEC 60964.

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

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

INTRODUCTION

Contexte technique, questions importantes et structure de la norme

La CEI 60964:1989 fut développée pour fournir des exigences applicables à la conception des Salles de Commande (SdC) des centrales nucléaires. Dans cette première édition de la CEI 60964 qui a été largement utilisée dans le domaine de l'industrie nucléaire, le sujet des systèmes d'alarme était traité dans un article d'une page. Prenant en compte le retour d'expérience, collecté mondialement, sur le sujet, il est apparu nécessaire d'avoir une norme complète et détaillée sur les systèmes d'alarme.

La présente Norme est applicable à la conception des nouvelles salles de commande de centrales nucléaires conformes à la CEI 60964 dont les travaux débutent après la publication de la présente norme. Elle est une référence pour les mises à niveau et la modernisation des salles de commande existantes. Si on souhaite l'appliquer pour les salles de commandes secondaires ou locales, il convient de prêter une attention particulière à l'identification des zones concernées.

Position de la présente norme dans la collection de normes du SC 45A de la CEI

La CEI 62241 qui est un document de troisième niveau traitant spécifiquement des systèmes d'alarme, sera directement référencée par la deuxième édition de la CEI 60964 (à l'étude).

Pour plus de détails sur la collection de normes du SC 45A de la CEI voir ci-dessous la « Description de la structure de la collection des normes du SC 45A de la CEI ».

Recommandations et limites relatives à l'application de cette norme

La présente norme complète le paragraphe 4.6.4 de la CEI 60964:1989, ainsi elle remplace les recommandations données dans l'Annexe A, en A.4.6.4, de la CEI 60964.

Pour la catégorisation des systèmes d'alarme, le classement de sûreté de la CEI 61226 doit être utilisé dans cette norme.

Description de la structure de la collection des normes du SC 45A de la CEI et relations avec les documents de la CEI et ceux d'autres organisations (AIEA, ISO)

Le document de niveau supérieur de la collection de normes produites par le SC 45A de la CEI est la CEI 61513. Cette norme traite des exigences relatives aux systèmes et équipements d'instrumentation et de contrôle commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires, et structure la collection de normes du SC 45A de la CEI.

La CEI 61513 fait directement référence aux autres normes du SC 45A de la CEI traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, les défaillances de cause commune, les aspects logiciels et les aspects matériels relatifs aux systèmes informatisés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la CEI 61513, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de la CEI qui ne sont pas référencées directement par la CEI 61513, sont relatives à des matériels particuliers, à des méthodes ou à des activités spécifiques. Généralement ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

INTRODUCTION

Technical background, main issues and organisation of the standard

IEC 60964:1989 was developed to supply requirements relevant for the design of Control Rooms (CR) of nuclear power plants. In this first edition of IEC 60964 which has been used extensively within the nuclear industry, the subject of alarm systems was tackled in a one page clause. Considering the return of experience gathered worldwide on the subject, it appeared that a comprehensive standard on alarm systems was needed.

This standard is for application to the design of new main control rooms of nuclear power plants conforming to IEC 60964, where work is initiated after the publication of this standard. It serves as a reference for upgrading and modernizing existing control rooms. If it is desired to apply it to supplementary and local control rooms, special attention should be given to identifying the areas affected.

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

IEC 62241 will be directly referenced by the second edition of IEC 60964 (under consideration) and is the third level document specifically tackling the topic of alarm systems.

For more details on the structure of the IEC SC 45A series of standards, see below the “Description of the structure of the IEC SC 45A series of standards”.

Recommendations and limitations regarding the application of this standard

This Standard supplements Subclause 4.6.4 of IEC 60964:1989 and therefore supersedes the guidance given in A.4.6.4 of Annex A of IEC 60964 Ed.1.0.

For the categorization of alarm systems, the safety classification of IEC 61226 should be taken into account.

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

The top level document of the IEC SC 45A series of standards is IEC 61513. It provides general requirements for instrumentation and control systems and equipment (I&C systems) that are used to perform functions important to safety in nuclear power plants (NPPs). IEC 61513 structures the IEC SC 45A series of standards.

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

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

Un quatrième niveau qui est une extension de la collection de normes du SC 45A de la CEI correspond aux rapports techniques qui ne sont pas des documents normatifs.

La CEI 61513 a adopté un format de présentation similaire à celui de la CEI 61508, avec un cycle de vie et de sûreté global, un cycle de vie et de sûreté des systèmes; elle fournit une interprétation des exigences générales des parties 1, 2 et 4 de la CEI 61508 pour le secteur nucléaire. La conformité à la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 pour l'application au secteur nucléaire. Dans ce cadre, la CEI 60880 et la CEI 62138 correspondent à la partie 3 de la CEI 61508 pour l'application au secteur nucléaire.

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA 50-C-QA pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de la CEI sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier le guide NS-R-1 et le guide NS-G-1.3[1]. La terminologie et les définitions utilisées dans les normes produites par le SC 45A de la CEI sont conformes à celles utilisées par l'AIEA.

---

1 Guide NS-R-1: *Safety of Nuclear Power Plants: Design – Requirements*

Guide NS-G-1.3: *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants – Safety Guide*

A fourth level extending the IEC SC 45A series of standards corresponds to the Technical Reports which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety series IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework and provides an interpretation of the general requirements of IEC 61508, parts 1, 2 and 4, for the nuclear application sector. Compliance with this standard will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In this framework, IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 refers to ISO as well as to IAEA 50-C-QA for topics related to quality assurance.

The IEC SC 45A series of standards consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of nuclear power plants and in the IAEA safety series, in particular the Requirements NS-R-1 and the Safety Guide NS-G-1.3[1]. The terminology and definitions used by IEC SC 45A standards are consistent with those used by the IAEA.

---

1 Requirements NS-R-1: *Safety of Nuclear Power Plants: Design*

Safety Guide NS-G-1.3: *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

CENTRALES NUCLÉAIRES DE PUISSANCE – SALLE DE COMMANDE PRINCIPALE – FONCTIONS ET PRÉSENTATION DES ALARMES

1 Domaine d'application et objet

La présente Norme internationale fournit les exigences fonctionnelles applicables aux systèmes d'alarme des salles de commande principales des centrales nucléaires de puissance. Elle donne les définitions des termes utilisés pour les fonctions d'alarme. Elle établit aussi les exigences relatives aux facteurs humains ainsi que les lignes directrices pour la conception de la présentation des alarmes dans la salle principale de commande des centrales nucléaires.

NOTE Les fonctions d'alarme peuvent être mises en œuvre sur un système dédié (système d'alarme) ou, ce qui est préférable, être partie intégrante du système d'IHM (Interface Homme Machine) de la salle de commande principale.

Elle spécifie les fonctions d'alarme et en particulier les fonctions de sélection et de définition du signal d'alarme original, traitement des signaux d'alarme (par exemple, traitement séquentiel des événements, détermination dynamique et statique des priorités), traitement d'affichage des alarmes (par exemple, suppression des alarmes) et utilisation des dispositifs d'affichage associés (par exemple, les unités de visualisation, les tableaux d'alarme conventionnels, les synoptiques muraux), avec séquences d'acquittement et de remise à zéro, et autres sujets associés.

Beaucoup d'alarmes apparaissent simultanément hors conditions de fonctionnement normal de la centrale nucléaire et lors des phases transitoires. Pour cette raison, on doit prêter, aux fonctions d'alarme de la salle de commande principale des centrales nucléaires, une attention particulière en ce qui concerne les facteurs humains et la configuration du système, afin d'éviter aux opérateurs toutes confusions et leur fournir l'information appropriée. Ainsi le domaine d'application couvre les fonctions d'alarme spéciales basées sur les facteurs humains pour la surveillance et l'exploitation des centrales nucléaires. Il ne couvre pas les fonctions d'alarme spécifiques, telles que les systèmes de protection incendie ou de sécurité.

L'objet de cette norme est d'établir au niveau international une base commune de compréhension des bases sous jacentes à la conception fonctionnelle des systèmes d'alarme des salles de commande, couvrant les exigences fonctionnelles correspondantes, les exigences liées aux facteurs humains et les recommandations de conception des fonctions d'alarme et de présentation des alarmes pour la salle de commande principale des centrales nucléaires.

Ainsi cette norme vise à donner les orientations qui permettent de minimiser les problèmes qui ont pu survenir par le passé, tels que: les omissions d'alarmes importantes, les retards dans la détection d'alarmes importantes, l'augmentation de la charge de travail qui peut avoir un impact sur les autres activités d'exploitation, le manque d'attention concernant les alarmes fréquemment activées, dites «alarmes perturbatrices» et la confusion associée à l'incompréhension des relations entre alarmes et entre les importances relatives des alarmes.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

NUCLEAR POWER PLANTS – MAIN CONTROL ROOM – ALARM FUNCTIONS AND PRESENTATION

1 Scope and object

This International Standard provides the functional requirements for the alarm systems in the main control room of nuclear power plants. It gives definitions of the terms used for alarm functions. It also establishes the human factors requirements and the design guidelines for alarm presentation for the main control room of nuclear power plants.

NOTE The alarm functions can be implemented in a dedicated system (alarm system) or preferably be an integrated part of the main control room HMI (Human-Machine Interface) system.

It specifies the alarm functions including those for the selection and definition of original alarm signals, alarm signal processing (e.g., event sequence processing, static and dynamic prioritisation), alarm display processing (e.g., alarm suppression) and the use of associated display devices (e.g., Visual Display Unit (VDU), conventional alarm fascia, mural display), with acknowledge and reset sequences, and other related matters.

Under abnormal conditions or plant transient conditions in the nuclear power plant, many alarms occur simultaneously. For this reason, the alarm functions of the main control room of nuclear power plants require special considerations for human factors engineering and system configuration, to avoid operator misunderstandings and to provide the operator with adequate information. Therefore, the scope includes special alarm functions based on human factors for monitoring and operation of nuclear power plants. It does not cover specific alarm systems, such as the fire alarm and security alarm systems.

The object of this Standard is to establish a common international understanding of the underlying functional design basis of alarm systems for control rooms, covering the corresponding functional requirements, the human factors requirements and design guidelines for the alarm functions and alarm presentation for the main control room of nuclear power plants.

This Standard therefore aims to give guidance to reduce problems which have been experienced in the past: omission of important alarms, delay in detecting important alarms, increased workload that may affect the performance of other operational activities, inattention to frequently activated alarms known as ‘nuisance alarms,’ and confusion associated with the misunderstanding of the relationships among alarms and of the importance of alarms.

2 Normative references

The following referenced documents are necessary for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

CEI 61226, *Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Classification*

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

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

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

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans la CEI 60964, ainsi que les suivants, s'appliquent.

NOTE Lorsqu'un même terme est défini dans la CEI 60964 et dans la présente norme, c'est la définition de la présente norme qui s'applique.

3.1
alarme
élément informatif relatif au diagnostic, au pronostique ou à une recommandation, qui est utilisé pour alerter l'opérateur et pour attirer son attention sur une déviation du procédé ou d'un système

NOTE L'information particulière fournie par les alarmes couvre l'existence d'anomalies pour lesquelles une action corrective pourrait être nécessaire, la cause et les conséquences potentielles de l'anomalie, l'état général de la centrale, l'action corrective correspondant à l'anomalie et le retour de l'action corrective.

Deux types de déviation peuvent être distingués:

– non prévue – Déviations du procédé indésirable et défaillance de matériels;

– prévue – Déviations relatives aux conditions du procédé ou aux états des matériels qui sont les réponses prévues, mais qui peuvent être indicatives de conditions indésirables pour la centrale.

3.2
acquittement d'alarme
action à effectuer par l'opérateur pour montrer qu'il a pris connaissance d'une alarme qui lui a été présentée

3.3
avalanche d'alarmes
situation où un grand nombre d'alarmes apparaissent dans un laps de temps court à une vitesse dépassant les capacités de l'opérateur à les prendre en compte

3.4
code d'alarme
méthode de mise en valeur auditive ou visuelle d'un élément important, dans le but d'attirer l'attention de l'opérateur sur cet élément

3.5
contrôle d'alarme
ensemble de fonctions de contrôle de présentation des alarmes qui aide l'opérateur à prendre connaissance correctement et en temps utile de l'état des alarmes

NOTE L'acquittement d'alarme, la suppression des signaux sonores, la remise à zéro sont des exemples typiques de contrôle d'alarmes.

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

IEC 61226, *Nuclear power plants – Instrumentation and control systems important for safety – Classification*

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

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60964, as well as the following definitions, apply.

NOTE When the same term is defined in IEC 60964 and in this standard, the definition given in this standard applies.

3.1
alarm
item of diagnostic, prognostic, or guidance information, which is used to alert the operator and to draw his or her attention to a process or system deviation

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

Two types of deviation may be recognised:

– unplanned – undesirable process deviations and equipment faults;

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

3.2
alarm acknowledgement
action, which operators are required to carry out to show that they have recognized an alarm presented to them

3.3
alarm avalanche
condition where a large number of alarms appear within a short time at a rate exceeding the operator's capacity to take them into account

3.4
alarm coding
method of highlighting an object of concern visually or audibly, with the intention of drawing the operator's attention to the object

3.5
alarm control
set of alarm presentation control functions, which support the operators in recognizing alarm status correctly and in a timely manner

NOTE Alarm acknowledgement, silence, and reset are typical examples of alarm control.

3.6
traitement d'affichage des alarmes
mécanismes ou fonctions de traitement des signaux d'alarme qui sont utilisés dans le traitement ou l'amélioration de la présentation des alarmes, par exemple: regroupement d'alarmes, suppression d'alarme

NOTE Le traitement d'affichage des alarmes traite les alarmes identifiées par la logique de traitement des signaux d'alarme (q.v.).

3.7
tableau d'alarme
affichage d'alarmes constitué d'un ensemble de verrines d'alarme

3.8
filtrage ou réduction des alarmes
mécanisme ou fonction de traitement des signaux d'alarme dont le but est de réduire le nombre des alarmes destinées à l'opérateur

NOTE Les termes filtrage ou réduction sont des termes génériques.

3.9
génération d'alarme
mécanisme ou fonction de traitement des signaux d'alarme utilisé pour produire une alarme à partir d'une combinaison logique prédéfinie de signaux d'alarme et d'autres signaux binaires (par exemple: signaux d'état d'un composant)

NOTE Voir aussi logique de traitement des signaux d'alarme.

3.10
légende d'alarme
légende identifiant une alarme

3.11
message d'alarme
texte d'alarme identifiant une alarme, typiquement utilisé par les affichages intégrant des unités de visualisation

NOTE Il peut être associé à de l'information complémentaire, telle que l'heure d'activation de l'alarme, le seuil et la tendance d'évolution du procédé correspondant. Il est aussi utilisable pour former une annonce sonore verbale, représentant une alarme qui peut être associée à une recommandation ou à de l'information supplémentaire.

3.12
définition de l'ordre de priorité des alarmes
mécanisme ou fonction de traitement des signaux d'alarme qui affecte les alarmes à des groupes d'une importance prioritaire différente

NOTE La priorité peut être définie à l'avance ou déterminée de façon dynamique suivant les conditions de la centrale. Voir aussi logique de traitement des signaux d'alarme (q.v.).

3.13
enregistrement d'alarme
méthode basée sur l'utilisation de moyens d'enregistrement permanents tels que, des imprimantes, des supports magnétiques long terme ou des enregistrements optiques, pour garantir l'identité et l'heure d'apparition et de disparition de chaque alarme et signal d'alarme, qui peuvent être disponibles pour les études et les analyses différées

3.14
signal d'alarme
signal binaire du système d'alarme traité pour produire une alarme. Ces signaux peuvent être des signaux bruts provenant de l'installation ou de systèmes d'I&C

3.6
alarm display processing
alarm signal processing functions or mechanisms, which are used in controlling or enhancing alarm presentation, for example, grouped alarms, alarm suppression

NOTE The alarm display processing operates on the alarms identified by the alarm signal processing (q.v.) logic.

3.7
alarm fascia
alarm display consisting of a set of alarm tiles

3.8
alarm reduction or filtering
alarm signal processing function or mechanism which has the aim of reducing the number of alarms for operator attention

NOTE Filtering or reduction are generic terms.

3.9
alarm generation
alarm signal processing function or mechanism, which is used to generate an alarm based on a logical combination of pre-defined alarm signals and non-alarm binary signals (e.g., component status signals)

NOTE See also under alarm signal processing logic.

3.10
alarm legend
caption identifying an alarm

3.11
alarm message
alarm phrase identifying an alarm, which is used typically in VDU-based alarm displays

NOTE It may be associated with supplemental information such as the time of alarm activation, the threshold, and the trend of a corresponding process. It is also used to mean a string of speech-based audible announcements, representing an alarm, which may be associated with guidance or other supplemental information.

3.12
alarm prioritisation
alarm signal processing function or mechanism, which categorizes alarms into groups of different priorities of importance

NOTE The priority may be defined beforehand or determined dynamically from plant conditions. See also under alarm signal processing (q.v.) logic.

3.13
alarm recording
method ensuring that the identity and time of appearance and clearing of each alarm and alarm signal can be available for off-line study and analysis, using a permanent record such as printout or long-term magnetic or optical recording

3.14
alarm signal
binary signal taken into the alarm system, which is processed to provide an alarm. These signals may be raw signals from the plant or from the I&C systems

3.15
traitement des signaux d'alarme
mécanisme ou logique qui traite les signaux d'alarme (q.v.), avant que les alarmes soient identifiées et passées au système de traitement d'affichage des alarmes (q.v.) pour être affichées aux opérateurs

NOTE Le traitement des signaux d'alarme peut être utilisé pour valider les signaux d'alarme, générer les alarmes, réduire le nombre d'alarmes et fixer l'ordre de priorité des alarmes.

3.16
validation des signaux d'alarme
mécanisme ou fonction du traitement des signaux d'alarme qui détermine si un signal d'alarme représente correctement l'état du procédé ou d'un système correspondant

3.17
suppression des alarmes sonores
action qui permet d'arrêter une indication ou un avertissement auditif associé à une alarme

3.18
suppression des alarmes
fonction de présentation des alarmes qui éteint l'allumage ou évite l'affichage de messages d'alarme sans signification opérationnelle courante

NOTE L'état d'une alarme supprimée peut encore être déterminé par d'autres moyens.

3.19
système d'alarme
système conçu pour alerter les opérateurs de la présence d'une anomalie (par exemple une déviation du procédé), pour laquelle une action corrective pourrait être nécessaire

NOTE Normalement, un système d'alarme est une partie intégrée des systèmes d'I&C, particulièrement des systèmes d'I&C numériques, mais il peut aussi correspondre à un ensemble de matériels séparés, comme dans le cas des systèmes d'I&C câblés.

3.20
seuil d'alarme
valeur du procédé ou état d'un système qui est utilisé comme référence pour activer un signal d'alarme

NOTE Aussi appelé limite d'alarme ou point de consigne d'alarme.

3.21
verrine d'alarme
unité d'affichage d'alarme constituée d'une légende d'alarme gravée sur une verrine qui est éclairée par derrière lorsque la condition de l'alarme est présente

3.22
alerte
acte d'avertissement des opérateurs par des moyens visuels et auditifs pour attirer l'attention de ceux-ci

3.23
panneau éteint
objectif de conception d'un affichage d'alarme, consistant à n'afficher aucune alarme lorsque les conditions de la centrale sont normales et saines

3.24
indicateur de discordance
affichage pour lequel un indicateur de contacteur ou un contacteur de contrôle d'un matériel est éclairé tant que l'état est différent du dernier état ordonné par le contacteur ou indiqué par ce contacteur

3.15
alarm signal processing
logic or mechanisms which operate on the alarm signals (q.v.), before alarms are identified and passed to alarm display processing (q.v.) to be displayed to operators

NOTE Alarm signal processing may be used to validate alarm signals, generate alarms, reduce alarms, or prioritise alarms.

3.16
alarm signal validation
alarm signal processing function or mechanism, which determines whether an alarm signal is correctly representing a corresponding process or system status

3.17
alarm silence
action, which is made to stop an audible cue or warning associated with an alarm

3.18
alarm suppression
alarm presentation function, which switches off the illumination or prevents display of the messages of alarms with no current operational significance

NOTE The state of suppressed alarms can still be determined by other means.

3.19
alarm system
system designed to alert the operators to the existence of an anomaly (i.e., a system or process deviation), for which corrective action might be needed

NOTE Normally, an alarm system is an integral part of I&C systems, especially computerized I&C systems, but it may also be a separate set of equipment as found in hardwired I&C systems.

3.20
alarm threshold
process value or system state, which is used as a reference for activating an alarm signal

NOTE Also called alarm limit or alarm setpoint.

3.21
alarm tile
alarm display unit which consists of an engraved legend shown on a tile and lit from behind when its alarm condition is present

3.22
alerting
act of warning by means of visual and audible signals, which is intended to draw the operators' attention

3.23
dark-board
for alarm display, a design goal that, for normal healthy plant conditions, no alarms are shown

3.24
discrepancy indicator
display in which an indicator switch or a switch controlling an equipment item shows an illumination when the state is different from the last state ordered by that switch or shown by that switch

3.25
codage dynamique des alarmes
mécanisme ou fonction de traitement de l'affichage des alarmes utilisé pour changer dynamiquement le code des alarmes (par exemple couleur de présentation des alarmes)

NOTE L'utilisation dans une fenêtre d'alarme de plusieurs couleurs de présentation en cohérence avec la détermination dynamique des priorités est un exemple de codage dynamique des alarmes.

3.26
première alarme
alarme qui indique le premier initiateur déclencheur associé à un ensemble d'alarmes

NOTE Souvent utilisé comme premier signal entraînant le déclenchement du système de protection réacteur ou des systèmes de sûreté. Aussi appelé alarme «première cause».

3.27
alarme groupée
alarme définie comme une combinaison logique de plusieurs alarmes

NOTE Habituellement on utilise un simple «OU» logique pour produire une alarme groupée. Parfois elles sont appelées «alarmes partagées».

3.28
groupage
groupe d'alarmes en termes de propriétés fonctionnelles ou physiques

NOTE Disposer d'un groupe d'alarmes pour un endroit, d'une façon distincte est un exemple de groupage physique.

3.29
navigation
fonction d'aide à l'opérateur lui permettant de localiser la position de l'information recherchée dans un système d'information intégrant des unités de visualisation et qui permet aussi de s'orienter pour la sélection des affichages

3.30
alarme perturbatrice
alarme qui passe cycliquement de l'état présent à l'état disparu et qui distrait ou dérange le personnel présent en salle de commande

NOTE Appelée aussi «alarme répétitive».

3.31
rallumage clignotant
action de faire clignoter une légende d'alarme ou de la présenter à nouveau avec un symbole clignotant sur une unité de visualisation, lorsqu'elle a été à nouveau activée après avoir été effacée, ou pour indiquer qu'une alarme groupée est réactivée par une nouvelle alarme

3.32
remise à zéro
fonction de contrôle des alarmes utilisée pour ramener le système d'alarme à un état prédéfini en enlevant les alarmes effacées de l'affichage

3.33
rappel
fonction de présentation d'alarme utilisée pour indiquer que la condition associée à une alarme a disparu

3.34
alarme en attente
alarme présente qui a été acquittée

3.25
dynamic alarm coding
alarm display processing function or mechanism, which is used to dynamically change alarm coding (e.g. alarm presentation colour)

NOTE Lighting an alarm window with different colours in accordance with dynamically determined priorities is an example of dynamic display coding.

3.26
first-up alarm
alarm which indicates the first initiation triggering an associated set of alarms

NOTE Often used for the first signal causing the actuation of the reactor protection system or safety systems. Also known as 'first-out' alarm.

3.27
grouped alarm
alarm, which is defined as a logical combination of several alarms

NOTE Usually simple 'OR' logic is used to generate a grouped alarm. Sometimes called a 'shared alarm.'

3.28
grouping
group of alarms in terms of physical or functional properties

NOTE Laying out a group of alarms in a certain place in a distinctive manner is an example of physical grouping.

3.29
navigation
function, which supports the operators in locating the position of desired information in a VDU-based information system, and also in guiding the selection of displays

3.30
nuisance alarm
alarm which repeatedly cycles between the alarmed and cleared states and leads to control room distraction or annoyance

NOTE Also called a 'repeating alarm.'

3.31
reflash
action of flashing an alarm legend or of presenting it again with a flashing symbol on a VDU, when it has been activated again after it has cleared, or to indicate that a grouped alarm is reactivated by a new alarm

3.32
reset
alarm control function, which is used to return the alarm system to a pre-defined state by removing cleared alarms from display

3.33
ringback
alarm presentation function, which is used to indicate that an alarm condition has been cleared

3.34
standing alarm
alarm which is present and has been acknowledged

3.35
telop
message court ou symbole souvent à contenu numérique, présenté à la première ou à la dernière ligne des unités de visualisation pour orienter l'utilisateur vers un autre affichage ou pour informer l'utilisateur, par exemple du nombre d'alarmes présentes exceptionnel

4 Explications de fond

4.1 Problèmes liés aux systèmes d'alarme

Les systèmes d'alarme de mauvaise qualité sont connus pour être parfois à l'origine de problèmes liés aux facteurs humains qui peuvent être critiques pour la disponibilité et la sûreté des centrales. Typiquement ces problèmes de facteurs humains comprennent:

– l'omission d'alarmes importantes;

– le retard dans la détection d'alarmes importantes;

– l'augmentation de la charge de travail qui peut avoir un impact négatif sur les autres activités d'exploitation;

– le manque d'attention concernant les alarmes fréquemment activées;

– les confusions associées à l'incompréhension des relations entre les alarmes et de l'importance particulière de chaque alarme;

– le retard dans la présentation des alarmes, alors que l'opérateur sait pertinemment que l'état de la centrale a changé; ceci entraînant une perte de confiance de l'opérateur dans l'intégrité des alarmes.

Les éléments suivants sont reconnus comme étant des causes majeures de problèmes de facteurs humains:

– Activation d'un grand nombre d'alarmes lors d'un transitoire et l'opérateur ne peut répondre immédiatement. Ce problème est connu sous le nom «d'avalanche d'alarmes». De plus, beaucoup de ces alarmes ne possèdent pas nécessairement une valeur opérationnelle, mais dépendent d'autres alarmes ayant une signification plus importante.

– Alarmes perturbatrices ou alarmes permanentes.

– Alarmes activées directement par des conditions d'exploitation normales.

– Activation d'un grand nombre d'alarmes durant un arrêt de tranche ou due aux travaux de maintenance ou aux essais périodiques.

– Style d'exploitation. Afin de faire face aux difficultés liées aux facteurs humains, des opérateurs ont tendance à adopter un style d'exploitation propre. Par exemple, certains opérateurs n'essaient pas d'acquitter les alarmes immédiatement après un transitoire. Ceci les soulage du problème de la surcharge de travail, mais cela peut aussi retarder la détection de problèmes importants.

– Limitations des systèmes d'alarme existants en ce qui concerne le traitement des signaux d'alarme et l'affichage des alarmes.

De façon plus fondamentale, ces problèmes peuvent être minimisés si les concepteurs veillent aux points suivants:

– une définition claire de la valeur opérationnelle de chaque alarme dans une condition donnée;

– l'ensemble des relations dynamiques entre alarmes;

– la mise en œuvre de méthodes adaptées pour la logique de traitement des signaux d'alarme et le traitement d'affichage des alarmes.

L'objectif principal de cette norme est d'atténuer l'effet de ces problèmes de facteurs humains par l'identification précise et la mise en oeuvre des exigences et des recommandations fonctionnelles données par cette norme.

L'Annexe A fournit des informations supplémentaires.

3.35
telop
short message or a symbol, often with a numerical content, presented at the foot or heading line of a VDU display to direct the user to another display or to inform the user of some information such as the number of outstanding alarms

4 Background explanations

4.1 Problems of alarm systems

Poor alarm system design is known to sometimes cause human factor problems, which may be critical to plant availability and safety. Typical human factor problems involve the following:

– omission of important alarms;
– delay in detecting important alarms;
– increased workload that may affect the performance of other operational activities;
– inattention to frequently activated alarms;
– confusion associated with the misunderstanding of the relationships between alarms and of the importance of each alarm;
– delay in presentation of alarms when the operators know a plant change has occurred, causing loss of operator belief in the integrity of the alarms.

It is known that the following are the major causes of these human factor problems:

– A large number of alarms are activated in a transient, and operators cannot acknowledge them immediately. This problem is known as ‘alarm avalanche’. In addition, many of these alarms do not necessarily possess operational value but are dependent on other alarms of higher significance.
– Nuisance alarms and standing alarms.
– Alarms activated as a direct result of normal operating conditions.
– Large numbers of alarms activated during a plant outage or due to maintenance work, or to periodic testing.
– Operating styles. In order to cope with human factors difficulties, operators tend to create their own operating styles. For instance, some operators do not try to acknowledge alarms soon after a transient. This alleviates the problem of increased workload, but may cause delay in detecting important alarms.
– Limitations of existing alarm system designs for alarm signal processing and alarm display processing.

More fundamentally, these problems can be diminished if all system designers attend to the following:

– the operational value of each alarm at a given condition is clearly defined;
– the dynamic relationships among alarms;
– the implementation of suitable alarm signal processing logic and alarm display processing methods.

A primary intention of this standard is to alleviate these human factors problems through the clear identification of the functional requirements and the recommendations on their implementation given by this standard.

Annex A shows supplementary information.

4.2 Eléments de conception fonctionnelle

La Figure 1 présente la configuration conceptuelle des éléments qui, dans cette norme, constituent la conception fonctionnelle des systèmes d'alarme. Les configurations réelles des matériels et du logiciel peuvent être différentes et dépendre des configurations des systèmes d'I&C, des choix des concepteurs ou autres.

Dans cette norme, les cinq principaux éléments de conception des alarmes considérés sont:

– la définition d'alarme;
– le traitement des signaux d'alarme;
– le traitement de l'affichage des alarmes;
– la gestion et contrôle des alarmes;
– l'intégration de la commande d'affichage et de la présentation des alarmes.

4.3 Autres éléments

Cette norme couvre aussi les éléments de conception fonctionnelle importants suivants:

– fiabilité;
– essais;
– maintenabilité;
– enregistrement;
– Procédures de Réponse aux Alarmes (PRA).

4.2 Functional design elements

Figure 1 presents a conceptual configuration of elements that constitute the functional design of alarm systems, within the scope of this Standard. The actual hardware or software configuration may be different depending on the configurations of I&C systems, designers' choices, or others.

This standard considers the following five major elements of alarm system design:

– alarm definition;
– alarm signal processing;
– alarm display processing;
– alarm control and management;
– alarm presentation and display-control integration.

4.3 Other elements

Other important functional design elements of the alarm system, which this standard covers include the following:

– reliability;
– testing;
– maintainability;
– recording;
– Alarm Response Procedures (ARP).

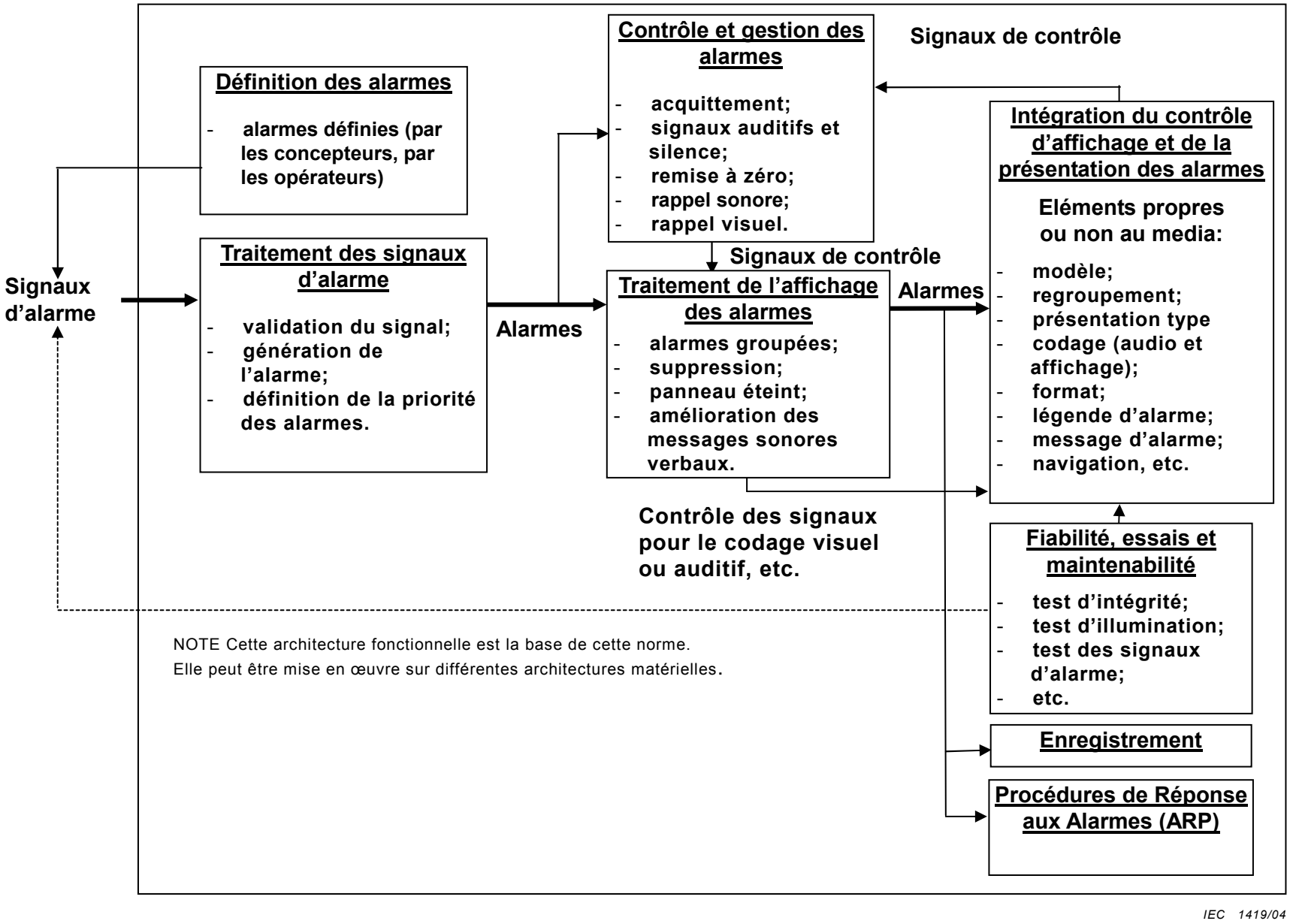


Figure 1 – Eléments de conception fonctionnelle du système d'alarme

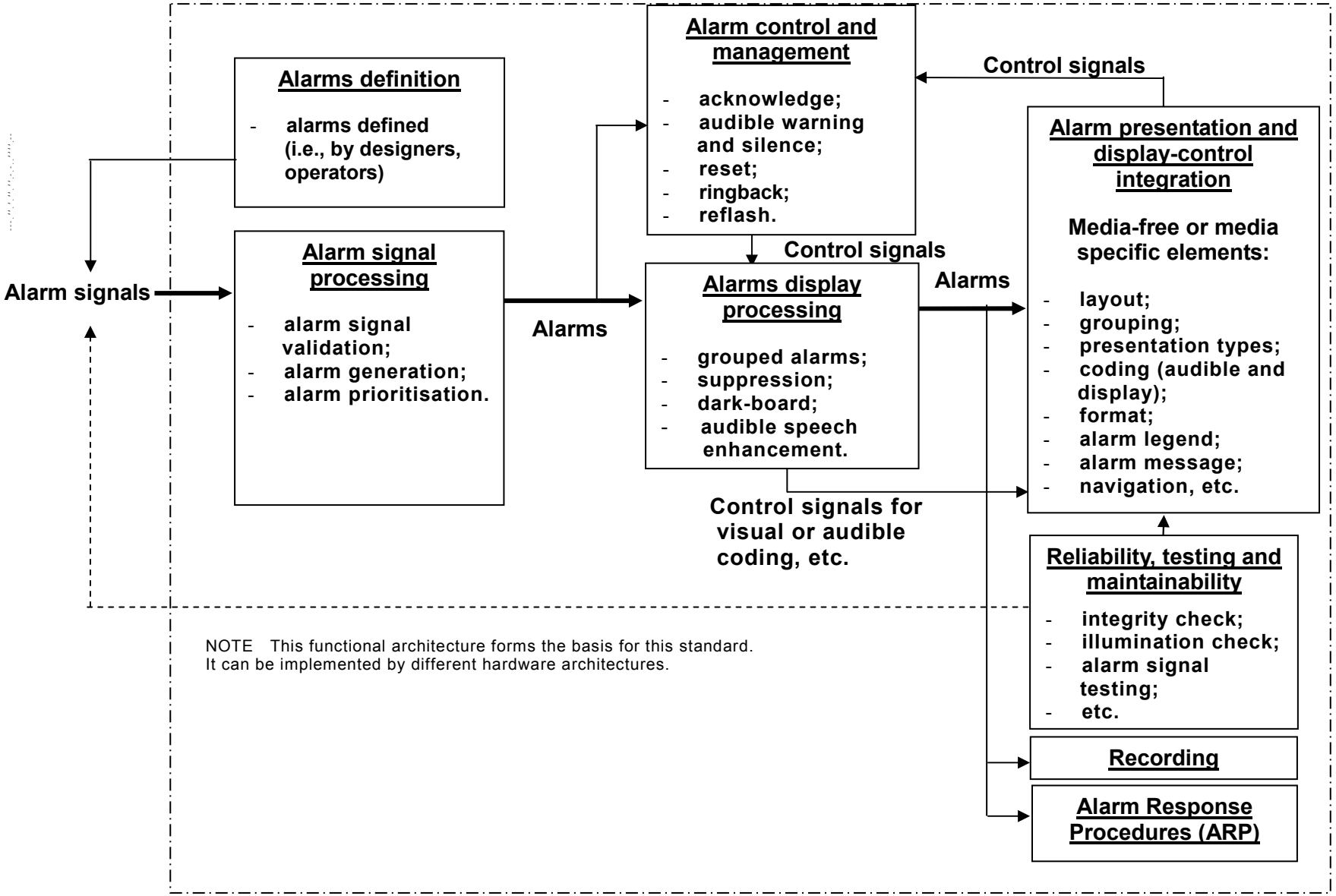


Figure 1 – Alarm system functional design elements

5 Exigences fonctionnelles de base

5.1 Fonctions d'alarme

Le système d'alarme doit détecter les changements indésirables de la centrale pour en déduire les alarmes à fournir au traitement d'affichage des alarmes et à l'affichage des alarmes en utilisant le traitement des signaux d'alarme.

Les alarmes doivent donner de façon appropriée l'alerte aux opérateurs, ainsi que l'indication sur l'origine de la mise en question de la sûreté ou de l'accident, de la perturbation de la centrale, des défaillances de la centrale ou de matériels ou d'autres événements, qui pourraient empêcher d'atteindre les objectifs opérationnels. Plus particulièrement, les fonctions d'alarme doivent présenter au minimum les caractéristiques de base suivantes:

– alerter l'opérateur sur l'existence d'états anormaux pour que les actions correctives souhaitables puissent être lancées;
– informer l'opérateur des fautes, des perturbations et des événements non attendus dans la centrale, entraînant un changement d'état ou de statut des systèmes de tranche;
– guider l'opérateur vers l'information nécessaire pour un diagnostic futur et la compréhension de l'événement signalé, afin de l'assister dans la planification et l'exécution des actions correctives;
– confirmer à l'opérateur la situation globale de la centrale.

Il convient que la conception du système de présentation globale des alarmes prenne en compte les fonctions complémentaires suivantes:

– fournir à l'opérateur l'information sur les causes et les conséquences de l'événement annoncé;
– diriger l'opérateur vers les points d'entrée du système global d'information de la salle de commande;
– fournir à l'opérateur les références appropriées aux procédures d'exploitation.

De plus on doit faire attention à minimiser les éléments distrayant l'attention de l'opérateur, le nombre d'alarmes perturbatrices et la charge de travail de l'opérateur qui sont dus au système d'alarme lui-même. Les exigences de performance propres au système d'alarme doivent être identifiées.

Les paragraphes suivants définissent les exigences fonctionnelles de base nécessaires pour assurer les fonctions principales données ci-dessus, et les paragraphes qui suivent, fournissent des recommandations détaillées pour chaque fonction.

5.2 Signaux d'alarme

5.2.1 Généralités

Les signaux d'alarme, habituellement correspondant à des entrées TOR ou des détections de seuils relatives à des entrées analogiques, sont utilisés par les traitements de génération et d'affichage, pour satisfaire aux fonctions exigées par 5.1. La définition des signaux d'alarme peut être donnée par les concepteurs responsable de la centrale, cependant si ces signaux doivent toujours représenter des alarmes et toujours être affichés lorsqu'ils sont présents, des problèmes de facteurs humains liés à la non prise en compte d'alarmes importantes et d'avalanche d'alarmes sont probables. Le traitement de ces signaux définissant les alarmes, et ensuite le traitement de celles-ci par des méthodes d'affichage appropriées, est donc nécessaire.

5 Basic functional requirements

5.1 Alarm functions

The alarm system shall detect undesirable changes in the plant to derive alarms using subsequent alarm signal processing for alarm display processing and alarm display.

Alarms shall give the operator adequate warning and indication of the onset of a safety challenge or accident, a plant disturbance, plant or equipment failure or other events, which could prevent operating goals from being achieved. More specifically, the alarm functions shall provide at least the following fundamental features:

– alert the operator to the existence of abnormal states so that suitable corrective action can be started;
– inform the operator about faults, disturbances and unexpected events in the plant leading to a change of state or status of plant systems;
– guide the operator to the information which is needed for further diagnosis and understanding of the announced event, to assist in planning and execution of corrective actions;
– confirm the overall plant situation to the operator.

The design of the overall alarm presentation system should take into account the following supplementary functions:

– provide the operator with information on causes and consequences of the announced events;
– direct the operator to entry points in the total control room information system;
– provide the operator with suitable references to the operating procedures.

Additionally, consideration shall be given to minimize distraction, nuisance alarms and operator workload due to the alarm system itself. Performance requirements shall be identified for the alarm system.

The following subclauses define the basic functional requirements needed to meet the primary functions given above, and later subclauses give detailed recommendations for each function.

5.2 Alarm signals

5.2.1 General

Alarm signals, normally provided by two-state inputs and threshold detection on analogue inputs, are used for the alarm signal generation and display processing to meet the functions required by 5.1. The definition of alarm signals may be made by the responsible plant designers, but if these signals are assumed always to represent alarms and are always displayed when they occur, the human factors problems associated with missing important alarms and alarm avalanche can be expected. The processing of those alarm signals to define alarms, and their further processing for suitable methods of display is therefore necessary.

5.2.2 Exigences de base relatives aux signaux d'alarme

On doit démontrer que les alarmes ainsi que l'information support fournies pour une centrale ont une couverture et une étendue suffisante pour être appropriées sur le plan fonctionnel et cohérentes sur le plan technique.

Il est recommandé que la définition des alarmes résulte d'une analyse fonctionnelle conforme à la CEI 61839.

Toutes les alarmes nécessaires à une exploitation efficace et sûre doivent être fournies par le systèmes d'alarme.

Il convient que les signaux d'alarme comprennent des indications sur l'état de la centrale et l'état des moyens de commande, afin d'assurer une logique de traitement d'alarme correcte durant la maintenance, les périodes de mise hors service de la centrale, les arrêts de tranche et autres conditions.

Le détail de ces exigences est donné à l'Article 6.

5.3 Traitement des signaux d'alarme

5.3.1 Généralités

Le traitement des signaux d'alarme est nécessaire pour obtenir à partir de signaux d'alarme en entrée, l'information d'alarme valide. Seules les conditions réelles pour lesquelles l'action ou l'attention des opérateurs est requise sont des alarmes. Ainsi le traitement des signaux d'alarme est nécessaire pour identifier ces conditions et, de cette façon, simplifier les activités opérateur nécessaires. Les signaux d'alarme doivent être validés pour éviter l'utilisation de signaux défectueux. L'état opérationnel de la centrale et les autres conditions d'alarme présentes au moment où apparaît ou disparaît le signal d'alarme sont pris en compte par la logique et le traitement nécessaire à l'élaboration des alarmes à partir des signaux d'alarme.

5.3.2 Exigences de base relatives au traitement des signaux d'alarme

Les caractéristiques d'une condition d'alarme réelle peuvent être définies comme l'indication de la présence d'un ou de plusieurs des éléments suivants:

– condition de perturbation fonctionnelle de la centrale, telle que l'action de l'opérateur à partir de la salle de commande est nécessaire immédiatement ou dans un laps de temps court;
– action automatique en cours, contrôlant ou limitant les conséquences de conditions excessives ou dangereuses perturbant la centrale;
– condition de défaillance matérielle, nécessitant ou indiquant une action de maintenance ou une intervention locale pour restaurer un service ou une fonction matérielle nécessaire.

Il convient de soigneusement passer en revue les autres conditions qui peuvent être indiquées par les signaux d'alarme avant de les inclure dans la catégorie des alarmes réelles nécessaires en salle de commande.

On doit constituer une base technique, à utiliser systématiquement, pour l'identification des signaux d'alarme les plus importants. Cela peut être fait par incorporation de toutes ou de certaines des fonctions suivantes:

– validation du signal d'alarme;
– génération et réduction d'alarme;
– définition de la priorité des alarmes.

5.2.2 Basic alarm signal requirements

The alarms and supporting information provided for a plant shall be shown to have sufficient extent and coverage to be operationally appropriate and technically consistent.

The definition of alarms should be the result of a functional analysis according to IEC 61839.

All alarms necessary for safe and effective operation shall be provided by the alarm system.

Alarm signals should include indications of plant state and of control switch states, to allow for suitable alarm processing logic covering maintenance, plant outage, plant shutdown and other conditions.

Details of these requirements are given in Clause 6.

5.3 Alarm signal processing

5.3.1 General

Alarm signal processing is needed to derive valid alarm information from the alarm signals as its input. Only real conditions for which some operator action or attention is required are alarms. Processing of alarm signals is therefore needed to identify those conditions and thereby to simplify the activities required by the operator. The alarm signals need validation to avoid the use of failed signals. The plant operating state and the other alarm conditions existing at the time an alarm signal appears or clears are involved in the logic and processing necessary to generate the alarms from the alarm signals.

5.3.2 Basic alarm signal processing requirements

The characteristics of a true alarm condition can be defined as indications of one or more of the following:

– a functional disturbance of the plant conditions, such that operator action from the control room is needed immediately or within a short time scale;
– an automatic action which is taking place, controlling or mitigating an excessive or dangerous plant disturbance of conditions;
– an equipment failure condition, requiring or indicating a maintenance action or local-to-plant action to restore a service or necessary equipment function.

Other conditions, which can be indicated by alarm signals should be reviewed carefully before they are included in the class of true alarms needed in the control room.

A systematic technical basis for identifying the more important alarm signals shall be achieved. This may be done by incorporation of all or some of the following functions:

– alarm signal validation;
– alarm generation and reduction;
– alarm prioritisation.

Le traitement des signaux d'alarme doit, à partir des signaux d'alarme, identifier les conditions particulières qui indiquent une alarme réelle, avant que le traitement d'affichage des alarmes ne soit réalisé.

Le détail de ces exigences est donné à l'Article 7.

5.4 Traitement d'affichage des alarmes

5.4.1 Généralités

Le traitement d'affichage des alarmes peut contribuer à l'optimisation de la perception des alarmes par l'opérateur en affichant celles-ci clairement, en les groupant, en supprimant les alarmes perturbatrices, en permettant une suppression sélective des alarmes persistantes et en utilisant pour l'affichage des alarmes un code couleur ou autre. La répartition spatiale des panneaux ou des verrines d'alarme peut être utilisée. Le but est de réduire le nombre d'alarmes affichées à celles essentielles à une exploitation sûre et efficace pour chaque condition opérationnelle.

5.4.2 Exigences de base relatives au traitement d'affichage des alarmes

Le traitement d'affichage des alarmes doit être utilisé pour faciliter l'identification de l'importance des alarmes par les opérateurs. Il convient qu'il mette en oeuvre les fonctions pour:

– afficher la légende d'une alarme ou d'un message, lorsque l'alarme est détectée, avec un allumage clignotant ou un symbole associé et une alerte sonore;
– afficher et gérer une avalanche d'alarmes;
– gérer les alarmes persistantes;
– gérer les alarmes perturbatrices;
– grouper les alarmes par secteur de tranche ou suivant d'autres caractéristiques;
– afficher et enregistrer les alarmes avec leurs heures d'apparition et de disparition.

Le détail des méthodes permettant de réaliser ces fonctions est donné à l'Article 8.

5.5 Gestion et contrôle des alarmes

5.5.1 Généralités

La gestion et le contrôle des alarmes comprennent les fonctions associées à l'acquittement des alarmes, l'alerte sonore, les fonctions de réinitialisation des panneaux d'alarmes et des pages des unités de visualisation, ainsi que celles de sélection des affichages particuliers sur les unités de visualisation. Les méthodes d'affichage où les alarmes sont rallumées lorsqu'elles se répètent (rallumage clignotant), ou sont représentées à nouveau si elles disparaissent (rappel) impliquent un moyen de contrôle.

5.5.2 Exigences de base relatives à la gestion et au contrôle des alarmes

La présentation des alarmes doit être contrôlée par des fonctions conçues pour assurer que l'opérateur a bien noté chacune des alarmes. Il convient de fournir les fonctions de contrôle des alarmes suivantes:

– arrêt de l'alerte sonore lorsque les alarmes apparaissent;
– acquittement de chacune des alarmes lorsqu'elle apparaît;
– rappel pour indiquer la disparition d'alarme;
– remise à zéro pour effacer les alarmes disparues;
– rallumage clignotant lorsqu'une alarme déjà affichée apparaît à nouveau.

Le détail des méthodes permettant de réaliser ces fonctions est donné à l'Article 9.

The alarm signal processing shall identify from the alarm signals the specific conditions which indicate a true alarm, before the alarm display processing takes place.

Details of these requirements are given in Clause 7.

5.4 Alarm display processing

5.4.1 General

Alarm display processing can contribute to optimize the operators' perception of alarms by displaying alarms clearly, grouping alarms, suppressing nuisance alarms, allowing selective suppression of standing alarms, and coding the display by colour or otherwise. Spatial grouping of alarm fascias and alarm tiles can be used. The aim is to reduce the number of alarms shown in each operating condition to those essential to safe and effective operation.

5.4.2 Basic alarm display processing requirements

Alarm display processing shall be used to facilitate the identification of the importance of alarms by the operators. It should be able to provide functions for:

– display of the alarm legend or message when the alarm is detected, with a flashing illumination or associated symbol and an audible warning;
– alarm avalanche handling and display;
– handling of standing alarms;
– handling of nuisance alarms;
– grouping of alarms by plant section or other characteristic;
– display and recording of alarms with time of appearance and clearing.

Details of methods to achieve these functions are given in Clause 8.

5.5 Alarm control and management

5.5.1 General

Alarm control and management includes those functions associated with alarm acknowledgement, the audible warning, those to reset alarm fascias or VDU pages and those to select specific display functions on VDUs. Display methods where alarms are reflashed if they repeat (reflash), or are presented again if they clear (ringback) involve controls.

5.5.2 Basic alarm control and management requirements

The alarm presentations shall be controlled with functions designed to ensure that the operators have noticed each alarm. The following alarm control functions should be provided:

– silence the audible warning when alarms appear;
– acknowledge each alarm when it appears;
– ringback to indicate when an alarm clears;
– reset to remove cleared alarms;
– reflash where an alarm already on display appears again.

Details of methods to achieve these functions are given in Clause 9.

5.6 Intégration de la présentation des alarmes et de la commande d'affichage

5.6.1 Généralités

Une approche intégrée de la présentation des alarmes comme partie du système d'information global, origine des décisions et des commandes, est nécessaire aux opérateurs pour que soient atteints les objectifs de fonctionnement et de sûreté de la centrale. Les méthodes de présentation des alarmes comprennent les panneaux conventionnels et les verrines d'alarme, les unités de visualisation, les grands écrans et les synoptiques muraux. Le choix de la méthode, le modèle des affichages, le fonctionnement et la commande de l'affichage des alarmes, les légendes ou les messages des alarmes, et les méthodes détaillées d'affichage lorsque des unités de visualisation sont employées, nécessitent une attention particulière concernant leur clarté et leur facilité de mise en œuvre.

5.6.2 Exigences de base relatives à l'intégration de la présentation des alarmes et de la commande d'affichage

Les types de présentation physique des messages d'alarme, leurs dispositions et leurs regroupements doivent être soigneusement conçus, conjointement avec les fonctions et les techniques répertoriées de 5.3 à 5.5, pour mettre en oeuvre les fonctions et satisfaire aux exigences définies en 5.1.

En particulier, il convient que la méthode de présentation des alarmes garantisse que la fonctionnalité de base du système soit maintenue dans les conditions d'alarme les plus chargées, c'est-à-dire que les alarmes exigeant une action immédiate de l'opérateur ou indiquant une menace pour une fonction de sûreté critique (alarme de haute priorité) soient présentées de façon à favoriser une détection rapide et une compréhension de la part de l'opérateur dans toutes les conditions de charge d'alarmes. En conséquence, les exigences générales sont les suivantes:

– il convient de réserver un endroit pour l'affichage des alarmes de haute priorité;
– étant donné un moyen d'affichage, il convient de regrouper préférablement ces alarmes par fonction ou par système de tranche ou suivant une autre organisation logique.

En outre, la conception doit prendre en compte de façon appropriée les caractéristiques de présentation détaillée suivantes:

– codage;
– caractéristiques de présentation (par exemple, format d'affichage);
– clarté et cohérence des légendes et messages;
– moyens de navigation.

Le détail des méthodes permettant de réaliser ces fonctions est donné à l'Article 10.

5.7 Facteurs humains

La conception du système d'alarme doit être cohérente avec les normes et les conventions utilisées pour les autres interfaces homme-machine. Elle doit être aussi cohérente avec les procédures d'exploitation applicables. Ainsi, les concepteurs ne doivent pas définir les alarmes de façon isolée, mais comme partie intégrante de l'ensemble du système d'information, en prêtant une attention toute particulière aux intérêts de l'exploitation et aux facteurs humains.

Les éléments spécifiques nécessitant une attention particulière comprennent les suivants:

– contenu informatif et couverture;
– terminologie et abréviation, par exemple, clarté et cohérence de la présentation de l'information pour les présentations utilisant des unités de visualisation et des verrines d'alarme;

5.6 Alarm presentation and display-control integration

5.6.1 General

The operators need an integrated approach to the alarm presentation as part of the total information system and as the starting point for decisions and control, to achieve the safety and operational goals of the plant. The methods of alarm presentation include conventional fascias and tiles, VDUs, large screens and mural display panels. The choice of method, the layout of the displays, the operation of the controls over the alarm displays, the alarm legends or messages, and the detailed methods of display when VDU methods are used need careful attention for clarity and operability.

5.6.2 Basic alarm presentation and display-control integration requirements

The physical presentation types of the alarm messages, their layout and grouping shall be carefully designed, in conjunction with the functions and techniques listed in 5.3 to 5.5, to implement the functions and meet the requirements defined in 5.1.

In particular, the alarm presentation method should ensure that the basic system functionality is maintained under high alarm loading conditions, i.e., that the alarms requiring immediate operator action or indicating a threat to plant critical safety functions (high priority alarms) shall be presented in a manner that supports rapid detection and understanding by the operators under all alarm loading conditions. Consequent general requirements are:

– spatial dedication should be provided for the high priority alarms;
– alarms within a given display medium should be grouped, preferably by function, or by plant system or other logical organisation.

Furthermore, the design shall suitably address the following detailed presentation characteristics:

– coding;
– presentation properties (e.g. display format);
– clarity and consistency of legend, messages;
– navigation means.

Details of methods to achieve these functions are given in Clause 10.

5.7 Human factors

The design of the alarm system shall be consistent with standards and conventions of other human-machine interfaces. It shall also be consistent with relevant operating procedures. Therefore designers shall define alarms not in isolation but as an integral part of the overall information system with due consideration of the interests of operation and of human factors.

Specific elements of concern involve the following:

– information contents and coverage;
– terminology and abbreviations, for example, clarity and consistency of information presentation for VDU-based presentation and alarm tiles;

– codage et autres conventions et normes de facteurs humains, par exemple, cohérence du codage pour la présentation utilisant des unités de visualisation et des verrines d'alarme.

Les recommandations et les critères liés aux facteurs humains doivent être spécifiés dans le but de concevoir le système d'alarme et doivent être systématiquement appliqués. Il convient de faire référence aux normes et guides relatifs aux facteurs humains.

L'attention de l'équipe de conception de la salle de commande principale doit se porter de façon appropriée sur la conception du système d'alarme. On peut nommer un coordinateur pour la conception du système d'alarme. On doit couvrir les facteurs humains et considérer les problèmes de sûreté de façon appropriée.

Durant la conception, il convient de sélectionner une méthode de base pour attirer l'attention des opérateurs sur les alarmes et acquitter les actions nécessaires. Il est recommandé que ce soit une liste de messages d'alarme, afin d'assurer une identification non ambiguë et un enregistrement. Il convient d'utiliser les mêmes symboles et les mêmes conventions pour la liste des messages d'alarme et les diagrammes et les schémas procédés, en plus des conditions indiquées, pour signaler les changements d'état des alarmes (de l'état actif ou effacé à partir d'un autre état).

5.8 Evaluation

Une évaluation des performances doit être réalisée, conformément à la CEI 61771, pour assurer que les performances du système prévues sont effectivement atteintes. En particulier les conditions d'avalanche de référence doivent être identifiées et le système doit être capable de transmettre ces alarmes à l'opérateur dans un laps de temps spécifié.

6 Définition de la conception des alarmes

6.1 Généralités

La fonction d'alarme doit être classée conformément à la CEI 61226. L'Annexe G donne des exemples de points à prendre en considération dans la catégorisation des alarmes, qui déterminent la classe de matériel à utiliser pour les mettre en œuvre.

Il convient de définir très tôt dans la conception de la centrale, l'étendue des alarmes, les sources d'information, et les principes sur lesquels elles doivent être identifiées et fournies. Lors des revues de modernisation, l'étendue des alarmes devra avoir été déterminée dans la conception originale. Il convient qu'une revue assure la cohérence avec les principes de conception d'origine, et il est recommandé que celle-ci prenne en compte les nouvelles sources d'information liées à la révision en fonction de principes clairement identifiés.

Il convient que les principes applicables à l'information nécessaire à la définition des alarmes soient basés sur une fourniture suffisante de signaux afin de surveiller les points suivants:

– état des fonctions critiques de sûreté;
– dangers possibles pour le personnel;
– endommagement ou défaillance des matériels liés aux fonctions de sûreté;
– conditions de la centrale ayant un impact sur l'atteinte des objectifs opérationnels.

NOTE Pour les fonctions critiques représentatives, voir A.3.1.1 de la CEI 60964, qui en fournit une liste comprenant la réactivité, l'inventaire en eau, l'évacuation de la chaleur résiduelle, la source froide, l'intégrité du système de refroidissement du réacteur, l'intégrité de l'enceinte de confinement ou voir les guides AIEA.

– coding and other human factors standards and conventions, for example consistency of coding for VDU-based presentation and alarm tiles.

Human factors criteria and guidelines shall be specified for the purpose of designing the alarm system, and shall be systematically applied. Reference should be made to appropriate human factors standards and guidelines.

Alarm system design shall be properly focussed in the MCR (Main Control Room) design team. An alarm system design co-ordinator may be nominated. Suitable human factors coverage and proper consideration of safety issues shall be ensured.

During design, a primary method of drawing the alarms to the operators' attention, and requiring the acknowledge action, should be selected. This should normally be the listing of alarm messages, to ensure unambiguous identification and recording. The same symbols and conventions should be used both for alarm message lists and for process diagrams and mimics, in addition to the indicated condition, to indicate changes in the alarm state (to the active or cleared state from the other state).

5.8 Evaluation

A performance evaluation shall be conducted in accordance with IEC 61771 to ensure that the intended system performances are effectively achieved. In particular, a reference avalanche condition shall be identified, and the system shall be able to transmit those alarms to the operator within a specified delay time.

6 Design definition of alarms

6.1 General

The alarm function shall be classified in accordance with IEC 61226. Annex G gives examples of points to consider in the categorization of alarms, which then determine the class of the equipment used to implement them.

The extent of alarms, the information sources, and the principles on which they are to be identified and provided should be defined early in the design of the plant. For reviews to identify refit requirements, the extent of alarms will be determined in the original design. The review should ensure consistency with the principles of the original design, and include new information sources following clearly identified revision principles.

The principles on which information is needed for alarm definition should be based on ensuring sufficient signals are provided to monitor the following:

– the state of critical safety functions;
– possible personnel hazards;
– damage to or failure of equipment with a safety function;
– plant conditions affecting the achievement of operational goals.

NOTE For representative critical safety functions, see A.3.1.1 of IEC 60964, which lists these as reactivity, coolant inventory, core heat removal, heat sink, reactor coolant system integrity, containment vessel integrity, or see the IAEA guides.

6.2 Alarmes principales

Les fonctions d'alarme doivent être mises en œuvre dans des matériels d'I&C compatibles avec leur classement de sûreté. Si, pour des fonctions générales d'alarme, le matériel utilisé n'est pas compatible avec le plus haut niveau de sûreté requis, il peut être nécessaire d'affecter un sous ensemble d'alarmes à un matériel de classe de sûreté supérieure, pour supporter les fonctions de:

– fonctionnement sûr et continu de la centrale en état stable durant la période où le système principal informatisé ou le système d'alarme intégré sont indisponibles;
– mise et maintien en arrêt sûr de la centrale si une des alarmes principales apparaît durant la période où le système principal informatisé ou le système d'alarme intégré sont indisponibles;
– vérification et confirmation que l'arrêt sûr a été atteint.

Ceci doit s'appliquer sauf s'il a été démontré que le système principal informatisé ou un autre système d'alarme intégré avait une fiabilité suffisante pour garantir qu'une exploitation et un arrêt sûrs étaient toujours assurés.

6.3 Alarmes nécessaires

Il convient de définir et justifier le besoin d'alarmes et leur importance sur la base de prévisions d'exploitation et pas uniquement sur celles d'un concepteur d'un système individuel. Il est recommandé de fournir à la logique de traitement des signaux d'alarme, des signaux d'alarme pour produire des alarmes pour le système de présentation des alarmes, pour les conditions suivantes:

– mesures des paramètres relatifs à l'exploitation continue de la centrale ou qui sont critiques pour la sûreté de celle-ci et qui sont comparés à des seuils afin de détecter les conditions anormales;
– mesures des paramètres qui comparés à plusieurs seuils permettent de détecter les écarts par rapport aux conditions stabilisées ou qui permettent de détecter le développement de conditions anormales telles que l'arrêt d'urgence de la centrale ou l'injection de sûreté;
– état électrique ou mécanique anormal des matériels, tels que vannes, pompes ou autres équipements;
– échec d'une action automatique ou d'une séquence incomplète d'actions (par exemple, autosurveillance des fonctions automatiques, surveillance en ligne des séquences automatiques ou de mécanismes de commande: «alarmes attendues mais non apparues»);
– discordance entre l'état attendu et l'état réel de la centrale (par exemple, un système régulé en boucle fermée ne produit pas le résultat escompté, un disjoncteur ne se ferme pas lorsque l'interrupteur de commande a été manœuvré pour le fermer);
– anomalies et défaillances de systèmes numériques ou d'autres systèmes d'instrumentation, des systèmes de traitement d'alarmes et d'affichage, des systèmes de commande et de protection, et résultat des fonctions d'autodiagnostic;
– plus particulièrement, la perte d'une partie de l'alimentation du système informatisé, la perte de la redondance d'un système informatisé et la perte totale de ce système ou d'un autre système principal fournissant des alarmes.

Il est recommandé que les signaux qui ne doivent pas être pris en compte par l'opérateur ou auxquels il ne doit pas répondre, ne soient pas des alarmes en salle de commande principale.

Le système d'alarme doit présenter des réserves de ressources et de moyens pour évoluer.

L'Annexe B indique les origines types des signaux d'alarme.

6.2 Key alarms

Alarm functions shall be implemented in I&C equipment compatible with their safety classification. If, for general alarm functions, equipment is used that is not compatible with the highest safety class needed, it may be necessary that a subset of alarms be additionally assigned to a higher equipment class, to support the functions of:

– continued safe operation of the plant in a steady state during unavailability of the station computer or integrated alarm system;

– safe shutdown operations of the plant if one of the key alarms appears during unavailability of the station computer or integrated alarm system;

– verifying and confirming a safe shutdown has been achieved.

This shall apply unless the station computer system or other integrated alarm system has been shown to have sufficient reliability to ensure safe operation and shutdown can always be achieved.

6.3 Alarms needed

The need for alarms and their importance should be defined and rationalized from an operational perspective, not just from an individual system designer perspective alone. Conditions, which should provide alarm signals needed by the alarm signal processing logic to produce alarms for alarm presentation, include the following:

– parameter measurements, that are related to continuation of plant operation, or which are critical for plant safety, checked against thresholds for abnormal conditions;

– parameter measurements checked against several thresholds to detect a deviation from normal steady conditions, or to detect the development of abnormal conditions such as plant trip and safety injection;

– abnormal status of electrical or mechanical equipment, such as valves, pumps and other equipment;

– failure of an automatic action or sequence, or incomplete action (e.g. the self-surveillance of automatic functions, or the run-time monitoring of automatic sequences or of drives: ‘expected but failed to occur alarms’);

– discrepancy between the requested state and the actual state of a plant system (e.g. the closed loop control system did not produce the expected result, the circuit-breaker failed to close when the control switch was operated to close it);

– anomalies and failures of computer-based and other instrumentation, alarm processing and display systems and of control and protection systems, and the result of self diagnostic functions;

– specifically, loss of a section of the computer system input power, loss of computer system redundancy and total loss of the computer-based system, or other main system providing alarms.

Signals which operators do not need to take into account or to respond to should not be alarms of the main control room.

The alarm system shall have spare capacity and facilities to make changes.

Annex B gives typical sources of alarm signals.

7 Traitement des signaux d'alarme

7.1 Généralités

Il est recommandé que le traitement des signaux d'alarme assure que seules les alarmes valides et pertinentes sont choisies pour être présentées en temps réel, et que l'apparition d'alarmes non pertinentes soit limitée quelles que soient les conditions de la centrale.

Il convient que le traitement des signaux d'alarme assure que les alarmes sont correctement détectées et enregistrées lorsqu'elles sont apparues.

7.2 Validation des signaux d'alarme

Il convient de valider en ligne les signaux d'entrée et les capteurs pour assurer que des informations intempestives ne sont pas utilisées pour produire des alarmes dues à des défaillances matérielles des signaux d'entrée d'alarme ou de capteurs.

Les méthodes appropriées de validation en ligne des signaux analogiques peuvent comprendre la vérification de l'acceptabilité de la valeur dans les plages électrique et de mesure. Les méthodes de validation en ligne pour les contacts ou les signaux «tout ou rien» peuvent comprendre des matériels de détection de défauts de circuit incluant la détection des défauts de mise à la terre et des méthodes de filtrage des pertes des contacts.

Il convient d'indiquer à l'affichage, par des marquages ou d'autres moyens, que les alarmes et les informations liées à n'importe quelle entrée défectueuse ou n'importe quel matériel défaillant, sont défectueuses.

7.3 Traitement de génération et de réduction des alarmes

7.3.1 Exigences pour le traitement de génération et de réduction des alarmes

Il convient d'utiliser la logique de traitement des signaux d'alarme pour générer les alarmes et les limiter ou en réduire le nombre à celles importantes pour l'exploitation, en utilisant des fonctions incluant:

– l'identification du mode de fonctionnement, de maintenance ou d'arrêt et l'utilisation de cette information pour affecter un signal d'alarme à une méthode d'affichage d'alarme ou d'information;

– la définition des priorités, en utilisant les signaux d'alarme et les alarmes générées, par un traitement de détermination d'un niveau de priorité fixé à l'avance, ou de détermination dynamique d'un niveau de priorité ou d'une priorité relative comparée aux autres alarmes;

– la réduction des signaux d'alarme pour ne retenir que les alarmes ayant une signification opérationnelle courante;

– les méthodes de traitement de réduction du nombre d'alarmes, lorsque des conditions d'avalanche apparaissent lors des arrêts d'urgence ou autrement.

Au niveau de la conception, les points suivants concernant la génération d'alarmes doivent être satisfaits:

– les signaux d'alarme et autres signaux utilisés pour générer de nouvelles alarmes doivent être clairement identifiés;

– la définition de la méthode ou de la logique de génération des alarmes doit être documentée et connue des concepteurs et des utilisateurs;

– il convient de réduire par des techniques de traitement des alarmes, le nombre de messages d'alarme présentés hors conditions normales aux opérateurs, et ceci pour soutenir leur aptitude à détecter et à comprendre les alarmes qui sont importantes pour les conditions de la centrale et à agir dans le temps imparti;

– il convient d'utiliser la suppression, la réduction et la définition des priorités des alarmes.

7 Alarm signal processing

7.1 General

Alarm signal processing should ensure that only valid and relevant alarms are chosen for presentation in real time, and that the occurrence of irrelevant alarms should be limited under all plant conditions.

Alarm signal processing should ensure that alarms are properly detected and recorded to have appeared.

7.2 Alarm signal validation

Sensor and input signals should be validated on-line to ensure that spurious information is not used to generate alarms due to sensor or alarm signal input equipment failure.

Suitable methods for on-line validation of analogue signals may include electrical and measured value checks of acceptable range. Methods for on-line validation of contact and two-state signals may include equipment to detect circuit faults including incorrect earth isolation and contact debounce filtering methods.

The alarms and information dependent on any defective input or input equipment failure should be indicated as defective when they are displayed, by marks or by other means.

7.3 Alarm generation and reduction processing

7.3.1 Requirements for alarm generation and reduction processing

Alarm signal processing logic should be used to generate the alarms and limit or reduce the number to those of operational importance by functions that include:

– identification of the operating, maintenance or shutdown mode and use of this to assign an alarm signal to an information or alarm display method;

– assignment of priority using the alarm signals and the generated alarms, by processing to determine either a previously fixed priority level, a dynamic determination of priority level or a relative priority compared to other alarms;

– reduction of the alarm signals to retain only the alarms of current operational significance;

– methods of alarm number reduction processing when alarm avalanche conditions appear at plant major trips or otherwise.

When the design requires alarm generation, the following shall be met:

– alarm signals and other signals used to generate new alarms shall be clearly identified;

– the definition of the method or the logic for generating alarms shall be documented and known to designers and users;

– the number of alarm messages presented to the operators during off-normal conditions should be reduced by alarm processing techniques to support the operators ability to detect, understand, and act upon all alarms that are important to the plant condition within the necessary time;

– alarm suppression, reduction and prioritisation processing should be used.

Le traitement des signaux d'alarme peut être utilisé pour définir des alarmes ou les grouper à partir des signaux d'alarme ou pour réduire le nombre d'alarmes. La logique peut utiliser des ET, OU, NON, avec des retards ou d'autres opérateurs logiques définis, pour générer ou grouper des alarmes ou pour identifier la priorité d'une alarme. La logique de traitement d'alarme peut être utilisée pour décider du classement ou non d'un signal d'alarme pour le traitement d'affichage, en association avec l'état opérationnel de la centrale ou les conditions des autres signaux d'alarme. Les méthodes qui ont été utilisées sont décrites en Annexe C.

7.3.2 Définition des priorités des alarmes

L'objectif de la définition des priorités des alarmes est de guider l'opérateur pour déterminer l'importance relative de l'alarme. Il est recommandé de ne pas se baser sur la définition des priorités pour supprimer les alarmes, car cela élimine des changements opérationnels pertinents, nécessaires à l'opérateur, pour maintenir son attention et comprendre les changements affectant la centrale.

La définition des priorités peut être réalisée en affectant chaque alarme à un des niveaux de priorité. Il convient d'adopter un nombre réduit de niveaux de priorité afin d'éviter toute confusion (c'est-à-dire entre 3 et 5 niveaux).

La définition de la priorité des alarmes peut faire partie du traitement des signaux d'alarme. Il convient que le déterminant principal de la priorité des alarmes soit le caractère de gravité de la condition ou des conséquences. La priorité d'une alarme peut être fixée dans la conception ou déterminée dynamiquement.

Les méthodes suivantes peuvent être utilisées pour affecter les priorités:

– Priorité fixe basée sur le degré d'importance statique propre à l'alarme. Les alarmes sont classées par leur degré d'importance propre, fondé sur l'impact sur la centrale, la possibilité de rejets de matériaux radioactifs, et l'urgence des actions demandées à l'opérateur.
– Priorité dynamique basée sur le degré d'importance dynamique de l'alarme. L'importance des alarmes est déterminée dynamiquement par la logique de traitement des signaux d'alarme en utilisant les relations entre les signaux d'alarme générés et les conditions d'exploitation de la centrale (par exemple, en exploitation normale ou incidentelle ou accidentelle). A cet instant les alarmes importantes et les alarmes moins importantes sont distinguées en utilisant des niveaux de priorité.

La priorité fixe est simple, mais elle peut ne pas assurer une affectation optimale des priorités dans tous les états de tranche. La priorité dynamique peut amener à une élaboration plus précise des priorités. Cependant, il y a le risque que malgré un effort d'ingénierie important on ne puisse atteindre un niveau de cohérence satisfaisant.

a) Priorité fixe

   Lorsque des priorités fixes sont utilisées, la priorité d'une alarme peut être définie lors de la conception à un des niveaux suivants, haut, moyen, bas et cette priorité est utilisée en permanence et conditionne la méthode d'affichage.

   La priorité de certaines alarmes peut être fixée par des exigences réglementaires ou autres, pour être toujours à un niveau défini, et il convient que la logique de génération des alarmes permette de satisfaire à de telles exigences. Les priorités peuvent se situer à trois niveaux:

   – au plus haut niveau de priorité, alarmes nécessitant l'exécution de procédures d'exploitation postaccidentelle spéciales ou l'entrée dans un mode d'exploitation postaccidentel;
   – alarmes indiquant une réduction de la disponibilité d'un système de sûreté;
   – autres alarmes.

Alarm signal processing may be used to form or group alarms from the alarm signals, or to reduce the number of alarms. The logic may use AND, OR and NOT logic with time delays, or other defined logic, to generate an alarm, to group alarms or to identify the priority of an alarm. Alarm processing logic may be used to decide to class or not to class an alarm signal as an alarm for display processing, by association with the plant operating state or the condition of other alarm signals. Methods which have been used are described in Annex C.

7.3.2 Alarm prioritisation

The purpose of prioritising alarms is to provide guidance to operators in determining relative alarm importance. Prioritisation should not be the basis for alarm suppression since it then removes operationally relevant plant changes that operators need, to maintain awareness of plant changes.

Prioritisation may be realised by assigning each alarm to one of several priority levels. The number of priority levels should be kept low to avoid confusion (for example in the range 3 to 5 levels).

Alarm priority determination may be part of alarm signal processing. The primary determinant of alarm priority should be condition seriousness or consequence. The priority of an alarm may be fixed in design or determined dynamically.

The following methods of assigning priority may be used:

– Fixed priority based on the degree of static importance specific to the alarm. Alarms are classified by the degree of importance specific to each alarm based on the impact on the plant, possible discharge of radioactive materials, and the urgency of actions required by operators.
– Dynamic priority based on the degree of dynamic importance of the alarm. The degree of importance of alarms is dynamically determined by the alarm signal processing logic, using the relationship between alarm signals generated and current plant operation (e.g. during normal operation, at abnormality, and at accident). Important alarms and less important alarms at that point in time are distinguished by using the priority levels.

Fixed priority is simple but may not represent an optimal assignment of priority in all plant states. Dynamic priority may lead to more accurate priorities. However there is a risk that, in spite of very high engineering effort, satisfactory consistency is not obtained.

a) Fixed priority

   When fixed priority is used, the priority of an alarm may be defined in design at one of several levels, such as high, medium, low, and this priority is used at all times to condition the method of display.

   The priority of some alarms may be fixed by regulatory requirements or otherwise, to be always at some defined level, and the alarm generation logic should allow for such requirements. Priorities may be at three levels:

   – alarms needing the performance of specific post-accident operating procedures or the entry to a post-accident operating mode, at highest priority;
   – alarms indicating a reduction of availability of the safety system;
   – other alarms.

b) Priorité dynamique

Lorsque la priorité dynamique est utilisée, il convient que le schéma de définition de la priorité dynamique soit capable d'identifier dynamiquement les alarmes pertinentes de haute ou basse importance, comparées aux autres alarmes, ou dans des conditions données de la centrale qui peuvent évoluer dans le temps. Le fondement de la pertinence peut s'appuyer sur les éléments suivants:

– degré d'urgence de l'action corrective à initier;

– degré de gravité de la condition, objet de l'alarme, relativement à son impact sur les conditions de la centrale.

Le degré de gravité peut être défini à la conception, mais l'urgence relative des actions correctives à prendre dépend normalement du contexte opérationnel, aussi il convient de le déterminer de façon dynamique. La définition des priorités dynamiques de l'importance peut être faite en trois étapes, fondée sur les conséquences de la défaillance, comme suit:

Groupe d'alarmes 1	Alarme demandant à l'opérateur de réaliser des opérations d'exploitation données.
Groupe d'alarmes 2	Alarme demandant à l'opérateur de confirmer la situation de la centrale.
Groupe d'alarmes 3	Alarme qui ne demande pas nécessairement à l'opérateur de réaliser une action ou une confirmation.

Des informations complémentaires sur les méthodes qui ont été utilisées pour la génération des alarmes et l'affectation dynamique et relative des priorités, le filtrage et la réduction des alarmes sont données en Annexes C, D et E.

7.4 Traitement de la séquence des évènements et du retard

Il est recommandé que le système d'alarme intègre la possibilité d'appliquer des filtres temporels et des retards sur les signaux d'alarme pour permettre le filtrage du bruit sur les signaux et pour éliminer les alarmes momentanées indésirables.

Les retards peuvent être utilisés dans les traitements de génération et de réduction d'alarmes, ainsi que pour la surveillance des séquences d'évènements. Des exemples d'utilisation de logiques temporelles sont:

– l'utilisation de conditions pour la présentation ou la définition de priorité de certaines alarmes durant une avalanche, jusqu'à ce que les conditions de tranche soient stabilisées;

– les limites de temps associées au processus de démarrage ou d'arrêt de matériel de tranche, tels qu'une pompe, pour identifier un mauvais fonctionnement de celui-ci;

– les limites de temps associées à la réalisation des séquences automatiques d'exploitation pour confirmer que le déroulement des évènements est correct ou pour prévenir en cas de défaillance.

Des éléments d'information complémentaires sont fournis par l'Annexe E.

7.5 Traitement du premier défaut

Comme aide au diagnostic et à l'analyse des causes originelles, il convient de mettre en place des dispositifs pour identifier les événements initiateurs associés à l'arrêt d'urgence automatique de la centrale, par l'utilisation de l'alarme premier défaut.

b) Dynamic priority

When dynamic priority is used, the dynamic alarm prioritisation scheme should be able to dynamically identify relevant alarms of high or low importance compared to other alarms or in given plant conditions, which may change over time. The basis of the relevance may involve the following:

– degree of urgency of the corrective action to be taken;

– degree of seriousness of the alarmed condition relative to its effect on plant conditions.

The degree of seriousness may be defined in the design, but the relative urgency of the corrective action to be taken normally depends on operational contexts, hence it should be determined in a dynamic manner. Dynamic prioritisation of importance may be made in three stages, based on the consequences of failure, as follows:

Alarm group 1	Alarm that requires the operator to make corresponding operations.
Alarm group 2	Alarm that requires the operator to confirm the plant situation.
Alarm group 3	Alarm that does not necessarily require the operator to make corresponding operations or confirmation.

Further information on methods which have been used for alarm generation, dynamic and relative priority assignment, filtering and reduction is given in Annexes C, D and E.

7.4 Event sequence and time delay processing

The alarm system should incorporate the capability to apply time filtering and time delays to the alarm signals to allow filtering of noise signals and to eliminate unneeded momentary alarms.

Time delays may be used in alarm generation and reduction processing, and for monitoring event sequences. Examples of the use of timing logic include:

– conditioning the presentation or priority of some alarms during an alarm avalanche, until plant conditions have stabilised;

– time limits on the starting or shut down progress of a plant item such as a pump to identify faulty operation;

– time limits on the operation of an automatic sequence of operations to confirm events are taking the correct path or to provide warnings of failures.

More information is given in Annex E.

7.5 First-out processing

As an aid to diagnostic procedures and root cause analysis, provision should be made for identifying the initiating event associated with automatic plant trips through the use of first-out alarms.

8 Traitement d'affichage des alarmes

8.1 Généralités

Les alarmes doivent être affichées lorsqu'elles sont détectées et la légende de l'alarme ou le message doit être présenté sur un moyen adapté (voir 10.1.2). Lorsqu'une alarme est affichée pour la première fois, elle doit être associée à une légende clignotante ou à un symbole clignotant, jusqu'à ce qu'elle soit acquittée (voir 9.4) et il est recommandé qu'elle soit accompagnée par une alerte sonore (voir 9.2) qui devrait retentir jusqu'à ce qu'on l'arrête.

Lorsqu'une alarme est effacée sur un panneau ou sur une verrine, sa légende peut être soit effacée du premier coup, soit rester allumée jusqu'à ce que la commande de remise à zéro soit passée (voir 9.6), ou faire l'objet d'une action de rappel (voir 9.5). Il est recommandé que la conception identifie laquelle de ces actions doit être réalisée pour chaque alarme, et inclue un symbole distinctif dans la légende pour indiquer cela.

Quand une alarme s'efface de l'affichage d'une unité de visualisation, il convient de fournir un moyen qui montre de façon non ambiguë que son état est maintenant effacé. D'autres méthodes peuvent être utilisées, mais il convient de faire attention.

Les méthodes réduisant les risques de confusion comprennent:

– le retrait du message des listes seulement lorsqu'il est affiché et visible, par une action de gestion et de contrôle des alarmes directe de la part de l'opérateur;
– le réarrangement ou le regroupement des messages qui peuvent apparaître sur un affichage après disparition de l'alarme, seulement par une action de gestion et de contrôle des alarmes directe de la part de l'opérateur, et non par des méthodes automatiques.

Il est recommandé que le traitement d'affichage des alarmes soit fondé sur des méthodes techniques systématiques et cohérentes avec le traitement logique des alarmes, qui doivent être utilisées pour la commande de la présentation des alarmes.

8.2 Alarmes groupées

Les alarmes groupées peuvent être utilisées pour le regroupement logique en un message ou en une légende de plusieurs signaux d'alarme; des logiques ET, OU, NON, des temporisations peuvent être utilisées pour cela.

Chaque signal d'alarme individuel doit être relié à l'alarme groupée et un moyen doit être fourni pour accéder à chaque signal d'alarme individuel à partir de l'alarme groupée.

Il est recommandé de ne combiner des alarmes que si l'action corrective est essentiellement la même pour toutes ces alarmes. On peut former des groupes à partir:

– des alarmes relatives à une même condition sur des composants redondants qui ont chacun des indicateurs séparés et proches;
– de toutes les alarmes d'un système ou d'un composant tenant compte du fait qu'elles aient toutes le même degré d'urgence et la même importance;
– de toutes les alarmes d'un système pour lequel l'action correspond à l'envoi en local d'un opérateur pour investiguer plus avant;
– des alarmes de synthèse, faisant une somme d'alarmes à entrée simple disponibles ailleurs en salle de commande.

8 Alarm display processing

8.1 General

Alarms shall be displayed when they are detected and the alarm legend or message shall be shown on a suitable medium (see 10.1.2). When an alarm is initially displayed, it shall have an associated flashing legend or flashing symbol until it is acknowledged (see 9.4) and should be accompanied with the initiation of an audible warning (see 9.2) which should sound until silenced.

When an alarm clears on a fascia or tile, its legend may either be cleared at once or be left illuminated until a reset control is operated (see 9.6), or have an associated ringback action (see 9.5). The design should identify which of these actions is to be taken for each alarm, and should include a distinguishing symbol in the legend to indicate this.

When an alarm clears from a VDU (visual display unit) based display, a means should be provided to show unambiguously that its state is now clear. Alternative methods may be used but care should be taken.

Methods which reduce the risk of confusion include:

– removing messages from lists only when the messages are on display and visible and by a direct operator alarm control and management action;
– re-ordering or closing up the messages which can appear on display after alarms have cleared only by a direct operator alarm control and management action, not by automatic methods.

The alarm display processing should be based on systematic and consistent technical methods for the logical processing of alarms, which are to be used for controlling alarm presentation.

8.2 Grouped alarms

Grouped alarms may be used for logical groupings to a single message or legend of several alarm signals, and logic for AND, OR, NOT and time delay may be used for this.

Each individual alarm signal shall be related to the grouped alarm, and means shall be provided to access each individual alarm signal from the grouped alarm.

Alarms should only be combined in a group if the corrective action is essentially the same for all of them. Groups may be formed from:

– alarms for the same condition on redundant components which each have separate indicators in close proximity;
– all alarms on a given system or component provided that they all have the same relative urgency and importance;
– all alarms of a system for which the action is to dispatch an operator to the local scene to investigate further;
– alarms that summarize single-input alarms available elsewhere in the control room.

8.3 Suppression d'alarme

8.3.1 Suppression

Les alarmes peuvent être supprimées automatiquement par le traitement de l'affichage des alarmes ou par des actions manuelles. Il convient de définir clairement les critères utilisés pour la suppression automatique. Les méthodes automatiques peuvent comprendre:

– la réduction du statut d'une alarme persistante à celui d'information, alors que celle-ci est présente et a été acquittée pour un temps défini;

– la réduction de la priorité d'une alarme produite par les fonctions de traitement à celle d'une information ou d'un état;

– le retard d'affichage d'une alarme pour permettre à l'opérateur de porter son attention sur les alarmes de plus haute importance, par exemple en condition d'avalanche d'alarmes;

– l'identification de signaux d'alarme défectueux par un processus de validation, utilisée pour supprimer les alarmes associées produites par les fonctions de traitement;

– la suppression des alarmes d'un matériel qui est consigné hors service.

Il convient de mettre à disposition des moyens manuels de suppression d'alarme par sélection de l'alarme et par identification de la fonction de suppression demandée.

Des moyens permettant la vérification, l'enregistrement, le retour en service et la confirmation des alarmes supprimées doivent être mis à disposition. L'utilisation d'écrans d'unité de visualisation peut permettre ceci efficacement.

Les informations présentées par les systèmes d'alarme doivent être cohérentes. La suppression d'alarmes sur un affichage, alors que les mêmes alarmes sont présentées sur un affichage équivalent, doit être empêchée au niveau de la conception, car ceci est opérationnellement incohérent et peut potentiellement induire en erreur l'opérateur essayant de se représenter mentalement l'état réel de la centrale.

8.3.2 Alarmes perturbatrices

Il convient de fournir à l'opérateur les moyens de commande de suppression des alarmes répétitives et qui le perturbent. Après suppression et jusqu'au retour de service, il convient que les signaux d'alarme en cause n'entraînent pas de modifications des affichages, mais il est recommandé que leurs états puissent être accessibles sur requête par l'opérateur.

8.3.3 Alarmes persistantes

Afin d'éviter de maintenir un nombre excessif d'alarmes dans les listes d'affichage sur les unités de visualisation, il convient qu'une méthode de retrait des alarmes persistantes de ces listes soit fournie. Il est recommandé que cela permette à l'opérateur de sélectionner une alarme ou un groupe d'alarmes et de pouvoir en commander le retrait dans des listes d'alarmes persistantes ou dans d'autres enregistrements de ces alarmes. La condition des signaux d'alarme concernés doit rester opérationnelle pour que, si l'alarme disparaît ou disparaît et revient, ces états soient identifiés sur les affichages.

8.4 Présentation panneau éteint

Il convient de réaliser une présentation panneau éteint en exploitation à pleine puissance et celle-ci est aussi recommandée pour tous les états à puissance réduite. Il est recommandé que le critère de base soit qu'un nombre minimal d'alarmes soient présentées, ceci étant cohérent avec les objectifs de sûreté et de disponibilité. Cela s'applique également pour les méthodes spécifiques aux panneaux d'alarmes, aux verrines, aux synoptiques et aux unités de visualisation.

8.3 Alarm suppression

8.3.1 Suppression

Alarms may be suppressed automatically by alarm display processing, or by manual actions. Criteria used for automatic suppression should be defined clearly. Automatic methods may include:

– reducing the status of a standing alarm which has been present and acknowledged for a defined time to that of information;

– reducing the priority of an alarm produced by the processing functions to that of information or status;

– delay before display of an alarm to allow operator attention to alarms of higher importance, for example under alarm avalanche conditions;

– identification of a defective alarm signal by validation processes, used to cause suppression of the associated alarms produced by processing functions;

– suppression of alarms from equipment which is tagged out.

Manual means should be provided to suppress alarms by selection of the alarm and identification of the suppression function required.

Means shall be provided to enable the checking, recording, return to service and confirmation of suppressed alarms. The use of VDU information screens allows this effectively.

Information presented in alarm systems shall be consistent. Suppressing alarms in one display while showing the same alarms in another similar presentation shall be prevented in the design since it is operationally inconsistent and is likely to result in operator errors in interpreting the true plant status.

8.3.2 Nuisance alarms

A means should be provided under operator control to suppress alarms, which repeat and are a nuisance. After suppression and until return to service, the alarm signals concerned should not cause any change to the displays, but their state should be accessible by the operator on request.

8.3.3 Standing alarms

A method of removing standing alarms from lists for display on VDU's should be provided, to avoid retaining excessive numbers of alarms in display lists. This should allow operator selection of the alarm or of a set of alarms, and controlled removal to lists of standing alarms or other records of those alarms. The condition of the alarm signals concerned shall remain operable, so that if the alarm clears, or clears and then returns, those states are identified on the displays.

8.4 Dark-board presentation

Dark-board presentation should be achieved for full power operation and is recommended for all lower power plant states. The basic criterion is that a minimum number of alarms should be presented, consistent with operating goals of safety and availability. This applies equally to alarm fascias, tiles in panels, large screen and VDU methods of display.

9 Gestion et commande des alarmes

9.1 Généralités

Il convient que les commandes des alarmes soient cohérentes avec l'ensemble des types de présentation des alarmes (par exemple, panneaux d'alarmes, verrines, unité de visualisation, synoptiques, etc.).

Il convient que les moyens de commande des alarmes soient facilement distinguables les uns des autres (par exemple, boutons, menus des unités de visualisation, boutons à cliquer, etc.) – en termes de formes, couleurs, tailles etc. – pour que la probabilité d'une manipulation accidentelle d'une mauvaise commande soit minimisée. Les recommandations générales sont les suivantes:

– il convient de fournir des commandes séparées pour arrêter le signal sonore, pour l'acquittement, pour la remise à zéro;
– il convient que les commandes des alarmes fassent l'objet d'un codage distinct pour en faciliter la reconnaissance;
– il convient que chaque ensemble de commandes d'alarmes remplisse les mêmes fonctions, dans les emplacements comparables;
– il convient que la conception des commandes d'alarmes ne permette pas à l'opérateur de s'affranchir des contrôles.

Il est recommandé qu'une séquence standard de commandes d'alarmes soit suivie sur tous les moyens de présentation (par exemple, en même temps sur les panneaux d'alarmes et les affichages de l'ordinateur d'alarme).

Voir Figures 2 et 3 pour des séquences typiques de gestion et de commande d'alarmes.

9.2 Signal sonore et son arrêt

9.2.1 Logique du signal sonore et de son arrêt

Lorsqu'une alarme est initialement affichée, un signal sonore doit être émis, jusqu'à ce que la commande d'arrêt de celui-ci ou la commande d'acquittement soit actionnée manuellement ou automatiquement. Si l'alarme disparaît et apparaît de nouveau, il convient que le signal sonore soit à nouveau réactivé, en fonction de l'intervalle de réapparition de l'alarme.

Il est recommandé que la conception de la logique d'activation du signal sonore prenne en compte les situations où de nombreuses alarmes apparaissent dans un laps de temps court, afin d'éviter que le signal sonore n'irrite l'opérateur.

A l'exception de l'arrêt du signal sonore par sa commande d'arrêt, qui est conçue pour être opérationnelle pendant des périodes prédéterminées, il convient qu'il ne soit pas possible de mettre celui-ci hors service manuellement.

9.2.2 Code sonore

Les sons d'alerte ne doivent pas être masqués par l'ambiance sonore prévisible et il convient qu'ils soient facilement distinguables des signaux sonores des autres systèmes, tels que celui de sécurité de la centrale, de l'alerte d'évacuation liée aux rayonnements, de l'alerte incendie ou ceux relatifs à des dangers similaires. Un niveau sonore situé à 10 dB au dessus du niveau de bruit d'ambiance est généralement considéré comme approprié. Il convient que le niveau du signal sonore soit ajustable dans une plage spécifique.

Le niveau sonore ou la fréquence de répétition peuvent être différents suivant l'importance de l'alerte (par exemple, alarme, annonce d'évènements).

9 Alarm control and management

9.1 General

Alarm controls should be consistent for all types of alarm presentation (e.g., alarm fascia, alarm tile, VDU display, large panel displays, etc.).

Alarm controls (e.g., buttons, VDU menus, mouse click targets etc.) should be easily distinguishable from each other – in terms of shape, colour, size, etc. – so that the probability of accidentally manipulating a wrong control can be minimized. General recommendations are as follows:

– separate controls should be provided for silence, acknowledgment, reset;
– alarm controls should be distinctively coded for easy recognition;
– each set of alarm controls should have the functions in the same relative locations;
– alarm control designs should not allow the operator to defeat the control.

A standard alarm control sequence should be followed for any presentation means (e.g., both for alarm fascias and for computer alarm displays).

See Figures 2 and 3 for typical alarm control and management sequences.

9.2 Audible warning and silence

9.2.1 Audible warning and silence logic

When an alarm is initially displayed, an audible warning shall sound until either the silence control or the acknowledge control is operated manually or automatically. If the alarm clears and then appears again, the audible warning should be sounded again, depending on the interval before it reappears.

The design of the logic for the initiation of the sound should take into account situations where many alarms are appearing in a short timescale, to prevent the warning irritating the operators.

Except for use of the silence control, which may be designed to be effective for predetermined periods, a manual disable of the audible warning should not be possible.

9.2.2 Audible coding

The warning sounds shall not be masked by the anticipated ambient noise and should be easily distinguishable from the audible signal associated with other systems such as the plant security, radiation evacuation warnings, fire and similar hazard warnings. A sound level 10 dB above the average ambient noise is generally considered adequate. The adjustment of the audible signal level should be possible in a specific range.

The sound level or repeating rate may differ according to the importance of the alerted situation (e.g., alarm, event announcement).

Plusieurs sons différents, distinguables par l'opérateur, peuvent être employés pour représenter la priorité de l'alarme. Il est recommandé, qu'au total, pas plus de cinq signaux sonores ne soient utilisés en salle de commande, afin d'éviter toutes confusions à l'opérateur.

9.3 Clignotement et rallumage clignotant

Il convient qu'un signal visuel clignotant soit prévu pour toutes les alarmes et soit activé lorsque la condition d'alarme apparaît. Le clignotement des messages complets sur les unités de visualisation n'est pas recommandé.

Un clignotement avec une fréquence de 1 Hz à 5 Hz peut être utilisé. Un clignotement plus rapide peut être utilisé pour indiquer qu'une séquence automatique d'exploitation n'a pas avancé ou ne s'est pas terminée correctement. Il convient que tous les clignotements des verrines et panneaux soient synchronisés par rapport à tous les états clignotants utilisés en salle de commande.

Le rallumage clignotant est une fonction automatique de la gestion d'alarmes, qui est utilisée pour produire à nouveau un message d'alarme, si celui-ci réapparaît après disparition ou après avoir été acquitté.

La fonction rallumage clignotant doit être fournie pour toutes les alarmes groupées. Une alarme groupée doit être rallumée de façon clignotante si l'un quelconque des signaux d'alarme, utilisé pour la générer, change d'état, indiquant une condition moins sûre.

Il convient de présenter une alarme affichée sur une unité de visualisation avec un nouveau symbole clignotant, si elle réapparaît après avoir disparu (et lorsqu'elle est encore présente dans les listes d'alarmes tenues à jour et non encore remises à zéro), mais seulement si le message est encore visible sur l'affichage. Autrement, il convient de présenter directement l'alarme nouvellement réapparue, ou de l'indiquer par un telop sur un affichage en cours de visualisation.

9.4 Acquittement

Une fonction de commande d'acquittement doit être mise à disposition pour chaque ensemble d'alarmes, comme celles des panneaux d'alarmes, ou celles des groupes de verrines ou pour agir sur les alarmes présentées sur des unités de visualisation voisines.

Il convient d'arrêter le clignotement de l'alarme et de maintenir un allumage fixe à un niveau constant après l'acquittement. L'acquittement peut aussi être utilisé pour arrêter directement le signal sonore.

Il est recommandé que l'acquittement ne soit possible que des endroits et aux moments où la ou les alarmes correspondantes sont visibles par l'opérateur. La commande d'acquittement ne doit pas permettre d'acquitter des alarmes qui ne sont pas affichées, ou des alarmes qui sont cachées derrière d'autres formats d'affichage d'unités de visualisation.

9.5 Rappel

Le rappel est une fonction de gestion automatique des alarmes, qui informe l'opérateur par signaux sonores et/ou visuels qu'une condition d'alarme a disparu et que l'alarme correspondante peut être remise à zéro.

Il convient d'utiliser le rappel lorsqu'il est important d'informer explicitement l'opérateur de la disparition d'une condition qui une fois fut anormale.

Il convient d'utiliser avec précaution le rappel sur les affichages d'unités de visualisation, car il peut en résulter un nombre excessif de messages d'alarme et occasionner un masquage apparent des autres alarmes.

Several different sounds, which can be distinguished by the operator, may be used to represent the alarm priority. It is recommended that a total of not more than five different warning sounds should be made in the control room, to prevent operator confusion.

9.3 Flash and reflash

A flashing visual signal should be included for all alarms, initiated when the alarm condition appears. Flashing complete messages on VDU screens is not recommended.

A flashing rate of between 5 Hz and 1 Hz may be used. A faster flashing signal may be used to show that an automatic sequence of operations has not progressed or terminated correctly. The flash timing of alarm tiles and fascias should be synchronized for all flashing states used in the control room.

Reflash is an automatic alarm management function, which is used to generate an alarm message again if it reappears after clearing or being acknowledged.

The reflash function shall be provided for all grouped alarms. A grouped alarm shall reflash if any alarm signal used to form it changes to a state which indicates a less safe condition.

An alarm message shown on a VDU should be presented with a new flashing symbol if it appears again after clearing (and when still held in lists of alarms but not yet reset), but only if the alarm message is still on a current visible display. Otherwise it should be shown directly as a newly appearing alarm or indicated by a telop on a currently visible display.

9.4 Acknowledgement

An acknowledgement control function shall be provided for each set of alarms, such as those on an alarm fascia or group of tiles, or to act on the alarms shown on a nearby VDU.

Alarm flashing should be stopped and illumination continued at a steady level after acknowledgement. Acknowledgement may also be used to cause the silence action directly.

Acknowledgement should be possible only from locations where and when a corresponding alarm or alarms are visible to operators. The acknowledgement control shall not cause acknowledgement of alarms that are not displayed or of those alarms that are hidden behind other VDU display formats.

9.5 Ringback

Ringback is an automatic alarm management function, which informs operators by audible and/or visual means that an alarm condition has been cleared and the corresponding alarm can be reset.

Ringback should be used where it is important to inform operators explicitly of a cleared condition that had once been abnormal.

Ringback should be used with caution on VDU displays, since it can result in excessive numbers of alarm messages and can cause apparent masking of other alarms.

9.6 Remise à zéro

La commande de remise à zéro doit être mise à disposition pour chaque ensemble d'alarmes, tel que celui des panneaux d'alarmes, ou des groupes de verrines, ou pour agir sur les alarmes présentées sur les écrans d'unités de visualisation voisines.

Il convient que la commande de remise à zéro place les alarmes associées effacées dans un état spécifique défini. Ce peut être l'arrêt de l'allumage des verrines, le retrait des messages ou des symboles des listes d'alarmes ou le retrait de code sur des icônes, etc.

Il convient que la commande de remise à zéro des messages des unités de visualisation d'alarmes soit conçue de façon cohérente avec le processus utilisé pour les panneaux d'alarmes. Cela peut entraîner une remise à zéro sur les pages de messages en cours de visualisation, ou cela peut entraîner une remise à zéro d'une liste complète d'alarmes en cours de revue. Il convient que la commande de remise à zéro retire les messages des alarmes qui ont été effacées, mais il est recommandé qu'à la conception, on évite les changements importants de contenu des pages en cours de visualisation. Le retrait des messages des alarmes effacées, des parties de liste qui ne sont pas en cours de visualisation, mais qui sont en revue, peut attendre jusqu'à ce que les parties en question soient visibles afin d'éviter cet effet.

Il convient de conserver à l'affichage toutes les alarmes encore existantes dans un ensemble d'alarmes associées qui est remis à zéro.

Il convient d'utiliser une séquence de remise à zéro manuelle, lorsqu'il est important que l'opérateur vérifie qu'une alarme a disparu. Cependant, une séquence de remise à zéro automatique peut être disponible pour les opérateurs, lorsqu'ils ont à répondre à de nombreuses alarmes, ou lorsqu'il est essentiel de remettre rapidement le système à zéro.

Il convient que la fonction de remise à zéro ne soit opérationnelle que des endroits à partir desquels le personnel de la centrale sait quelles sont les alarmes qu'il remet à zéro.

9.6 Reset

A reset control function shall be provided for each set of alarms, such as those on an alarm fascia or group of tiles, or to act on the alarms shown by a nearby VDU screen.

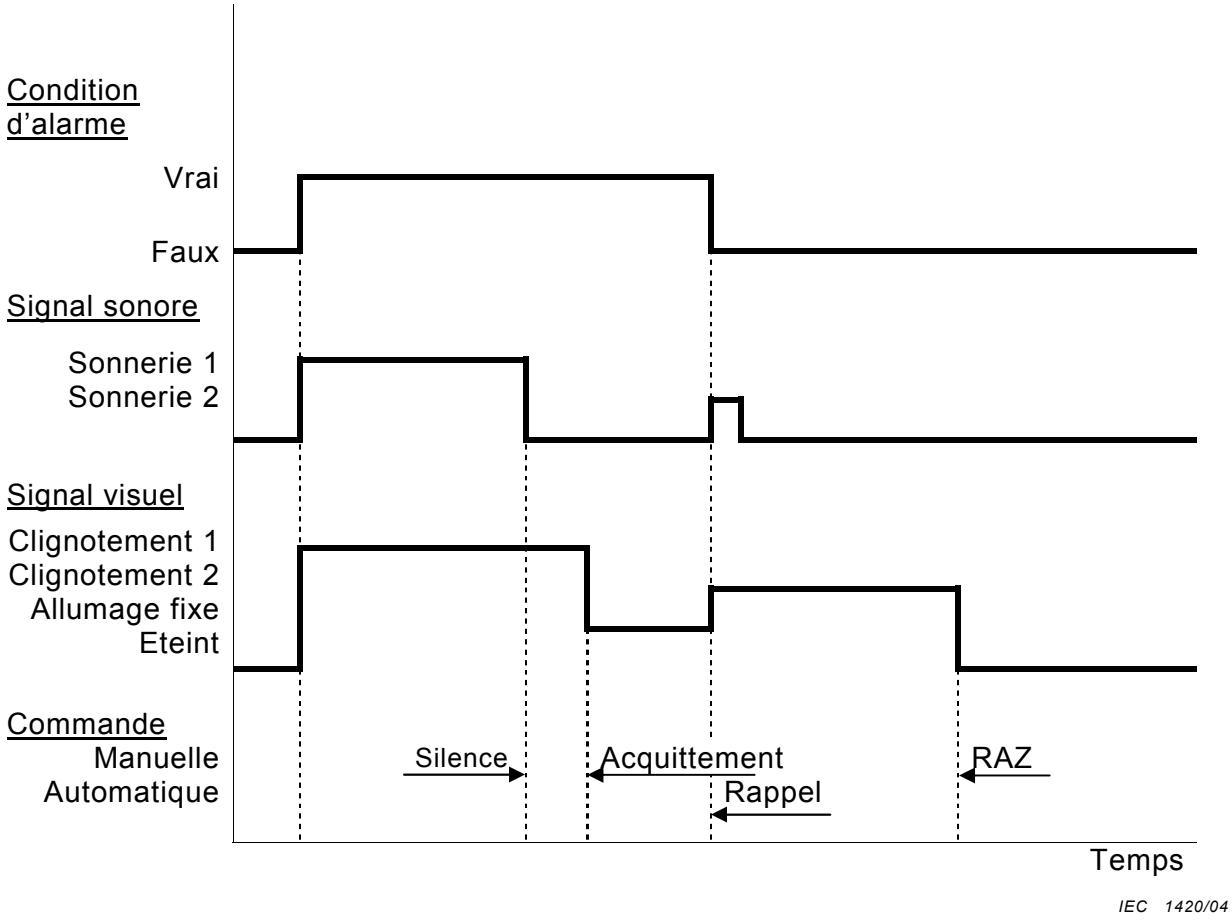
The reset control should place the associated cleared alarms in the proper defined state. This may be removal of illumination from tiles, removal of messages or symbols from alarm lists or removal of coding from icons, etc.

Reset for VDU alarm messages should be designed consistently with the process used for alarm fascias. It may cause a reset action on the page of messages currently being viewed, or a reset action on a complete list of alarms currently being reviewed. The reset action should remove messages of alarms which have been cleared, but the design should avoid major changes of the contents of pages currently being viewed. Removal of the cleared alarm messages from the sections of a list not currently being shown but under review may wait until that section is shown, to avoid this effect.

Any alarms still existing in the associated set of alarms which were reset should then remain on display.

A manual reset sequence should be used where it is important for the operator to check that an alarm has cleared. However, an automatic reset sequence may be made available where operators have to respond to numerous alarms or where it is essential to quickly reset the system.

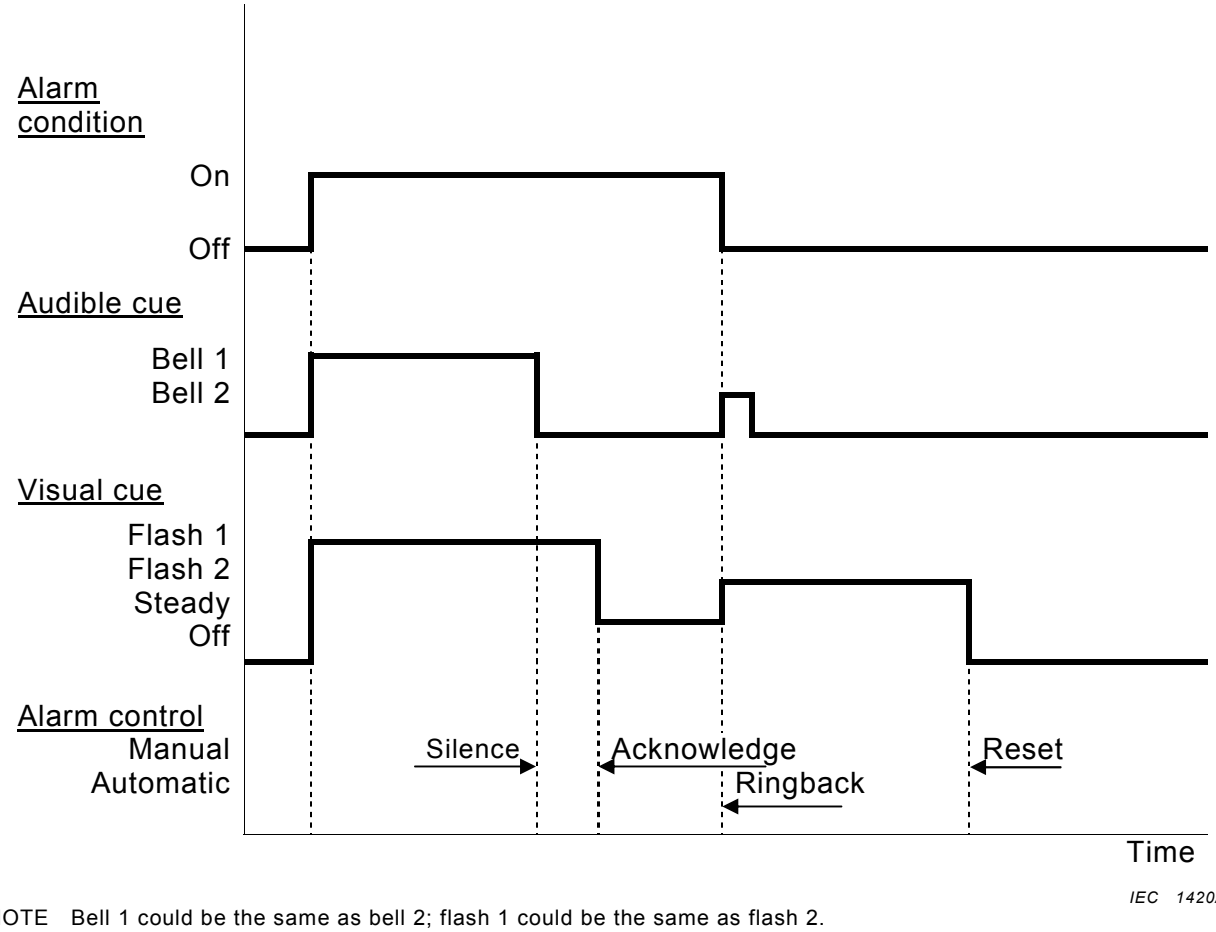
The reset function should be effective only from locations at which plant personnel know which alarm they are resetting.



RAZ Remise À Zéro.

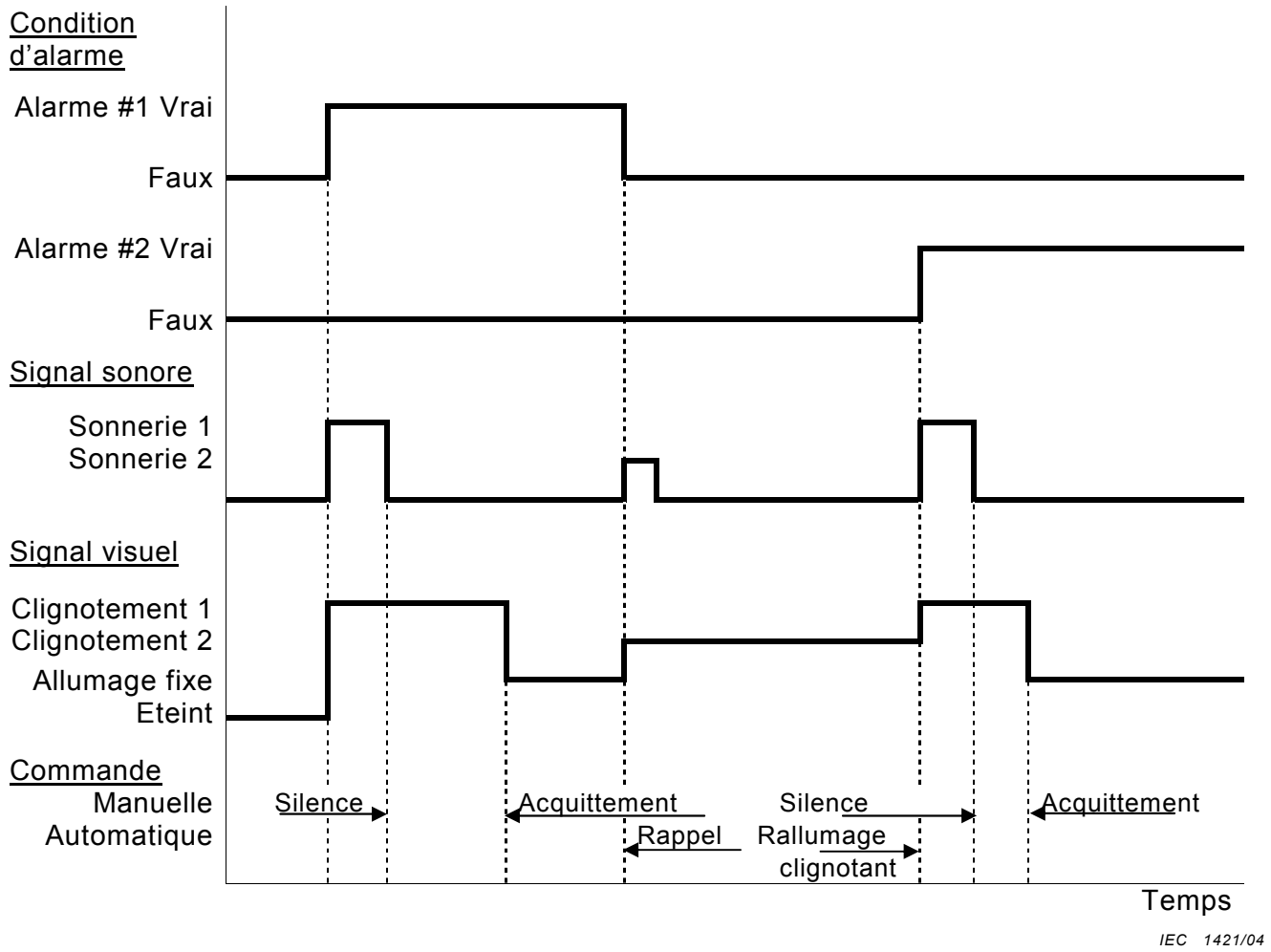
NOTE La sonnerie 1 peut être la même que la sonnerie 2; le clignotement 1 peut être le même que le clignotement 2.

Figure 2 – Séquence de commandes d'alarme typique



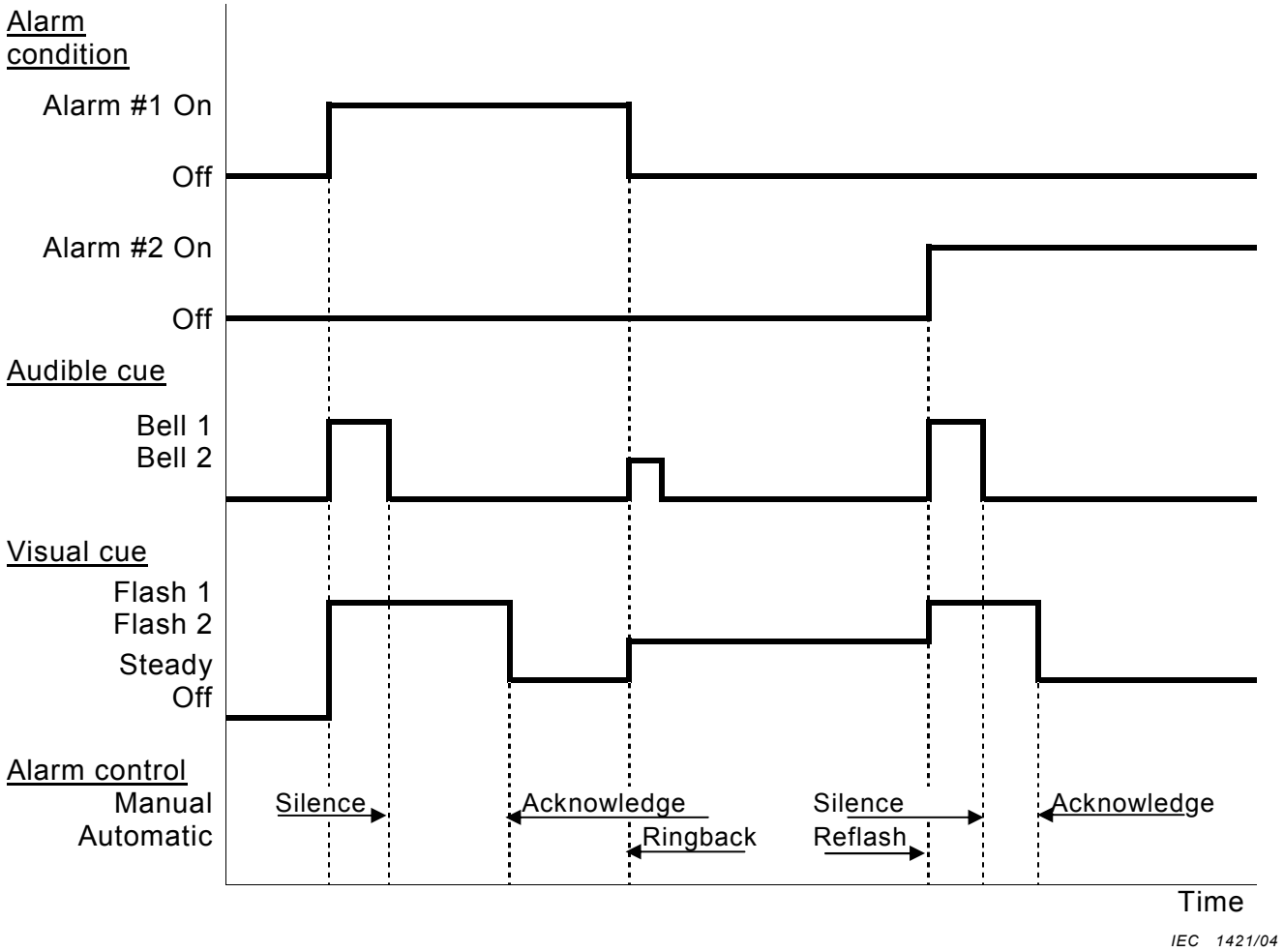
NOTE Bell 1 could be the same as bell 2; flash 1 could be the same as flash 2.

Figure 2 – Typical alarm control sequence



NOTE L'alarme #1 et l'alarme #2 sont combinées pour former une alarme groupée. Le rallumage clignotant se produit lorsque l'alarme #2 est activée. Dans cet exemple, la remise à zéro n'a pas été réalisée lorsque l'alarme #1 a été effacée.

Figure 3 – Séquence de commandes d'alarme typique pour une alarme groupée



NOTE Alarm #1 and alarm #2 are combined to form a grouped alarm. Reflash occurs when alarm #2 is activated. In this example, reset was not conducted after alarm #1 was cleared.

Figure 3 – Typical alarm control sequence for a grouped alarm

10 Intégration des commandes d'affichage et de la présentation des alarmes

10.1 Généralités

10.1.1 Fonctions

Il convient que la présentation d'alarmes mette à disposition les fonctions d'alarme décrites de 5.1 à 5.6, au moyen de traitement des signaux d'alarme et d'affichage, de modèles, de méthodes visuelle et sonore. Il convient plus particulièrement que les fonctions de présentation:

– indiquent clairement qu'une condition d'alarme existe;
– attirent l'attention de l'opérateur sur un point anormal, initialement par un signal sonore et un allumage clignotant ou par des marquages clignotants sur les affichages des unités de visualisation, pour l'inciter à évaluer la situation;
– assurent que le message décrit correctement le point anormal, avec des informations concises et non ambiguës;
– assurent que la présentation des messages se fait dans un endroit et dans un environnement adapté, de façon à faciliter l'appréciation et la décision de l'opérateur;
– indiquent clairement l'état des alarmes (c'est-à-dire, nouvelles, acquittées, effacées, supprimées);
– montrent les priorités (c'est-à-dire, l'urgence pour une action opérateur et son importance pour la sûreté de la centrale);
– montrent simplement les relations avec les autres alarmes et les matériels associés;
– assistent l'opérateur pour répondre de façon correcte à chaque alarme;
– dirigent l'attention de l'opérateur vers tous les affichages nécessaires pour vérifier ou clarifier une situation d'alarme;
– offrent un support à l'ensemble du personnel en l'aidant à prendre conscience de l'état de la centrale et de ses principales fonctions.

10.1.2 Sélection des types de présentation de base

Il convient que les types de présentation de base soient définis dès le début de la conception, en conformité avec les objectifs fonctionnels indiqués de 5.1 à 5.6. Il est recommandé de prendre en compte les méthodes de présentation d'alarmes suivantes:

– panneaux d'alarmes;
– verrines d'alarme;
– indicateurs de discordance;
– indications lumineuses;
– affichage des unités de visualisation avec des fonctions d'interrogation;
– grands écrans de présentation des unités de visualisation;
– synoptiques muraux pilotés par systèmes numériques.

Il convient que le système d'alarme soit, autant que possible, fonctionnellement intégré, et plus particulièrement, s'il utilise une combinaison de différentes méthodes de présentation, s'il est localisé dans différents endroits de la salle de commande (par exemple, unités de visualisation, écrans géants, panneaux dédiés). Ainsi, il est recommandé qu'il ne soit pas formé par la juxtaposition de deux sous systèmes indépendants ou plus, sauf choix délibéré de l'intégration fonctionnelle et opérationnelle.

10 Alarm presentation and display-control integration

10.1 General

10.1.1 Functions

The alarm presentation should provide the alarm functions of 5.1 to 5.6 by means of alarm signal and display processing, layout, visual and audible methods. More specifically, the presentation functions should:

– clearly indicate that an alarm condition exists;
– attract the operator's attention to the abnormality, to encourage operator appraisal, initially with an audible warning and flashing illumination or flashing marker on VDU displays;
– ensure the message states the abnormality properly, with concise and unambiguous information;
– ensure that the presentation of the message take place in an appropriate context and location, in order to enhance the operator's appraisal and decision making;
– clearly indicate the state of alarms (e.g., new, acknowledged, cleared, suppressed);
– show the priority (i.e., urgency for operator action and importance to plant safety);
– show simply the relationship with other alarms and related equipment;
– assist the operator to respond suitably to each alarm;
– direct the operator's attention to any need to access other displays to verify or clarify the alarm state;
– support the entire operating staff in maintaining an awareness of the state of the plant and its major functions.

10.1.2 Selection of basic presentation types

The basic types of alarm presentation should be defined early in the design, in accordance with the functional goals indicated in 5.1 to 5.6. The following methods of presenting alarms should be considered:

– alarm fascias;
– alarm tiles;
– discrepancy indicators;
– indication light;
– VDU displays with interrogation functions;
– large screen VDU presentation;
– mural display panels including those driven by computer systems.

The alarm system should be functionally integrated as much as possible, specifically if it uses a combination of different presentation methods, placed in different zones of the main control room (e.g.: VDU, large screen, dedicated panels). That is, it should not be the juxtaposition of two (or more) independent subsystems unless with deliberate functional and operational integration.

Les panneaux d'alarmes, verrines d'alarme et indicateurs de discordance permettent d'adopter l'approche panneau éteint. Les indicateurs de discordance et les indicateurs lumineux peuvent être plus particulièrement utilisés lorsque l'approche panneau éteint n'est pas adaptée. Ceci est par exemple applicable lorsque chaque état est sûr dans des conditions données mais pas sûr dans d'autres conditions d'exploitation, telles qu'un démarrage correct ou non, ou la défaillance indésirable des caractéristiques d'une fonction de sûreté. Plusieurs centrales utilisent maintenant les affichages par unités de visualisation pour toutes les alarmes, à l'exception d'un petit nombre d'alarmes principales nécessaires en cas de défaillance grave des fonctions informatisées. Ces centrales peuvent posséder un synoptique d'ensemble, tel qu'un grand écran d'unité de visualisation ou un panneau d'affichage mural, utilisé en association avec les affichages des unités de visualisation et les fonctions de commande logicielles.

Les panneaux d'alarmes, grands écrans, synoptiques muraux et verrines d'alarme, sont à même d'alerter efficacement l'opérateur de l'occurrence d'un phénomène, par différentes affectations simultanées. Ceci permet à l'équipe de conduite de partager une compréhension commune, de reconnaître le type de situation anormale, ceci comprenant la compréhension des points anormaux dépendant de relations ou de la transmission par le site d'un certain nombre d'alarmes.

L'unité de visualisation est le principal matériel de surveillance permettant d'afficher intégralement les informations dépendantes; elle est capable d'afficher des alarmes en continuité ou seulement lorsqu'elles sont nécessaires et elle peut afficher des telops en haut ou en bas de l'écran. Elle peut aussi trier temporellement les affichages relatifs à l'apparition d'alarmes.

Ce dispositif, commun ou partagé, d'unités de visualisation peut fonctionner comme un moyen parallélisé de présentation des alarmes, en conjonction avec une autre méthode d'affichage; des zones d'affichage dynamique sur grands écrans, des affichages disponibles à différents endroits, l'utilisation jointe d'unités de visualisation et de panneaux d'alarmes, des panneaux d'ensemble ou autres moyens peuvent être utilisés pour réaliser cet objectif de présentation parallélisée.

Les caractéristiques complémentaires des panneaux d'alarmes et des affichages d'unités de visualisation peuvent être intégrées dans un système numérique qui permet au niveau de la conception de tirer avantage des points forts de chaque type de présentation. Les unités de visualisation permettent de réordonner simplement les panneaux d'alarmes pour organiser et regrouper les alarmes, tout en maintenant la distribution spatiale pour la compréhension rapide de l'opérateur. Ces systèmes d'unités de visualisation peuvent aussi fournir des affichages supports de formes parallèles de présentation interfacées avec le système de supervision globale de la centrale.

Il est recommandé que le moyen d'affichage principal des alarmes soit les unités de visualisation; l'utilisation des unités de visualisation et complémentairement des panneaux d'alarmes et des unités de visualisation sera efficace, fournissant ainsi à l'opérateur les informations appropriées. Lorsque les alarmes sont présentées en utilisant la méthode des unités de visualisation, il peut être approprié d'utiliser des symboles ou des panneaux informatifs sur les diagrammes ou des représentations pour leur affichage comme pour les messages d'alarme.

10.1.3 Disposition

La localisation et le type d'affichage des alarmes et des messages doivent garantir les points suivants:

– chaque membre de l'équipe de conduite a les alarmes dont il a besoin pour accomplir les tâches qui lui sont assignées;

– l'ensemble de l'équipe de conduite peut voir les alarmes importantes concernant l'exploitation générale de la centrale, celles ci peuvent être les alarmes principales décrites à l'Article 6.

Alarm fascias, alarm tiles and discrepancy indicators allow the dark-board approach to be used. Discrepancy indicators and indicating lights may be of special use where the dark-board approach is not suitable. This can apply for indications where each state is safe in some conditions, but unsafe in other conditions of operation, such as the correct or incorrect initiation or the undesired failure of engineered safety features. Many plants now use VDU display for all alarms except for a small number of key alarms needed if the computer functions suffer severe failure. Plants may include an extensive overview mimic panel such as large screen VDU or mural display panels used in association with VDU displays and software control functions.

Alarm fascias, large screen presentations, mural display panels and alarm tiles are able to warn operators effectively about the phenomenon with different simultaneous assignments, which has occurred. This allows them to share a common understanding and recognize abnormality patterns, including understanding abnormalities which depend on the relationship or sites of transmission of a number of alarms.

The VDU is the principal monitoring device for integrally displaying related information; it is capable of displaying alarms continually or only when needed, and can display telops at the top or bottom of the screen. It can also make time-ordered displays of the occurrence of alarms.

This common or shared VDU facility can operate as a parallel alarm presentation device, in conjunction with another display method; active display areas on large screens, displays available at several locations, joint use of VDU and fascia alarms, overview panels or other means, can be used to achieve this parallel presentation.

The complementary features of alarm fascias and VDU displays can be integrated in a computer-based alarm system, which allows the design to take advantage of the strengths of both types of presentation. VDU display allows simple rearrangement of alarms to organise and group them, while maintaining spatial dedication for rapid operator comprehension. VDU systems can also provide displays supporting the parallel form of presentation interfaced with the overall plant supervision system.

The main alarm display should normally be the VDU; the use of VDU and complementary use of fascia and VDU will be effective in providing the operator with adequate information. When alarms are presented using the VDU method, symbols or drop-down information panels on process diagrams or mimics may be appropriate for their display as well as alarm messages.

10.1.3 Layout

The location and type of alarm display and messages shall ensure the following:

– each member of the operating staff has alarms needed to perform the task assigned to him or her;

– all operating staff can see essential alarms for the overall plant operation; these may be the key alarms described in Clause 6.

Différentes structures d'équipe et différents effectifs seront nécessaires suivant les modes opératoires, par exemple normal par rapport aux urgences. Il convient que l'accès aux affichages soit possible à partir de chacune des stations de travail associées à chaque mode opératoire.

La disposition des affichages d'alarmes doit être cohérente avec la philosophie de conception d'ensemble de la salle de commande principale. Il convient d'accorder une attention toute particulière à la disposition d'affichage des alarmes de salles de commande partagées par plusieurs unités (par exemple, certaines alarmes sont dupliquées entre les unités).

La disposition de la présentation, par la familiarisation avec la localisation sur les dispositifs de présentation, doit améliorer la compréhension des messages par l'opérateur.

10.1.4 Regroupement spatial

Il convient que les règles de regroupement soient claires et cohérentes avec les habitudes des opérateurs.

Il convient que le regroupement physique des alarmes sur les panneaux de contrôle ou les regroupements associatifs par les méthodes d'affichage des unités de visualisation constituent pour l'opérateur une méthode d'accès facile pour identifier quelle fonction ou quel système de la centrale est impacté par une situation anormale.

Conformément à l'approche fonctionnelle qui constitue la base de la conception de la salle de commande (voir la CEI 61839), il convient que les alarmes soit regroupées géographiquement par fonction de la centrale, par fonction de sûreté et de disponibilité, auxquelles toutes les alarmes d'un groupe se réfèrent.

Une autre possibilité pour le regroupement spatial est de former des groupes par système élémentaire de tranche ou d'utiliser une structure logique pour organiser les alarmes. D'autres niveaux peuvent être définis pour les sous groupes, afin d'arriver à une organisation complète des alarmes. Un exemple conceptuel est donné dans l'Annexe D.

10.1.5 Format des messages et des légendes d'alarmes

Il convient que les légendes, messages ou sous titres d'alarmes, soient simples et faciles à comprendre, qu'ils utilisent une terminologie courante et traitent spécifiquement des conditions, de telle façon que l'opérateur puisse lire et comprendre les messages.

Les légendes et les messages d'alarme doivent être uniques, et identifier clairement les éléments de la centrale affectés, la nature du problème et les conditions (par exemple, paramètres procédé, matériels). Il convient que le numéro d'étiquette du signal initiateur, ou du signal dérivé, ou un code de référence unique, fasse partie du message complet de l'alarme.

Il convient que les noms des alarmes soient identiques à ceux utilisés généralement dans la centrale. Les légendes et les messages d'alarme doivent être cohérents entre toutes les alarmes.

Il convient que les légendes et les messages d'alarme suivent un schéma de rédaction systématique. Cela peut être (suivant l'ordre en langue française) – Groupe principal de tranche et identification, Groupe secondaire de tranche et identification, Condition ou paramètre, Situation anormale.

Pour une identification précise et non ambiguë d'une alarme sur une centrale nucléaire, les légendes d'alarme peuvent devenir longues et détaillées, ainsi la longueur d'un message peut apparaître comme une limitation, pour les verrines comme pour les messages d'unités de visualisation. Un total de 40 caractères alphanumériques latins et d'espaces peut être une limite imposée par le matériel, sauf si deux lignes sont utilisables pour une phrase.

Different staff structures and staff numbers will be used under different operating modes e.g. normal versus emergency. Access to alarm displays should be possible at the associated workstations for each operating mode.

The layout of alarm displays shall be consistent with the general main control room design philosophy. Special consideration should be given to the alarm display layout for a multi-unit control room (e.g. some alarms are duplicated between units).

The layout of the presentation shall be used to improve the operator's understanding of the messages through familiarity with their location on the presentation device.

10.1.4 Spatial grouping

The grouping rules should be clear and consistent with the operator's usage.

The physical grouping of alarms on the control panels, or the associative grouping through VDU display methods, should give the operator an easy access method to identify which plant function or system is affected by abnormality.

In accordance with the functional approach which constitutes the basis for control room design (see IEC 61839) alarms should be spatially grouped by plant functions, availability and safety functions, to which all the alarms in one group refer.

Other possibilities for spatial grouping are to group alarms by plant system or to use a logical structure to organise alarms. Further levels of sub-groups can be defined, to arrive at a complete alarm organisation. A conceptual example is provided in Annex D.

10.1.5 Alarm legend and message form

Alarm legends, messages or captions should be simple, easily understandable, use standard terminology, and address conditions specifically so that the operator can read and understand the messages.

Alarm legends and messages shall be unique, and clearly identify affected plant items and the nature of the defect or condition (e.g., process parameters, equipment). The tag number of the initiating signal or derived signal, or a unique code reference, should be part of the total alarm message.

Names of alarms should match those used uniformly throughout the plant. Alarm legends and messages shall be consistent over all alarms.

The alarm legends or messages should follow a systematic order of phrasing. This may be (in English language ordering) – Major plant group and identity, Minor plant group and identity, Condition or parameter, Abnormality.

Alarm legends for accurate and unambiguous identification of an alarm on a nuclear plant can become long and detailed and therefore message length can be found to be a limitation, both for tiles and VDU display. A total of about 40 Roman alphabet characters and spaces for a VDU phrase can be a constraint placed by the equipment, unless a two-line phrase is used.

A moins que l'espace à disposition pour les légendes ou les messages d'alarme ne soit strictement compté, il convient de ne pas utiliser d'abréviations. Si une légende ou un message est long, une abréviation peut être utilisée si le message reste compréhensible. Si une abréviation est utilisée, cela doit faire l'objet de règles systématiques.

Il convient de spécifier les règles d'abréviation systématiques et de les appliquer aux points suivants:

– abréviations pour les conditions courantes telles que haute pression ou bas niveau;
– identification de l'unité de la centrale, de la voie, du numéro de matériel et autres;
– versions raccourcies progressives de mots communs utilisées dans la définition des messages; une méthode possible consiste à utiliser des versions de référence de mots sans retrait, puis avec le retrait d'une et de deux voyelles.

Il convient de faire une revue systématique des messages et des légendes d'alarme définis à la conception, par des experts en facteurs humains et le personnel opérationnel, et ceci pour des raisons de compréhension et de clarté.

10.1.6 Code d'affichage

Il convient que le code d'affichage soit cohérent avec la philosophie de codage de l'installation et soit appliqué de façon systématique pour les affichages d'alarmes.

Il convient que le code d'affichage garantisse une détection et une interprétation rapide des alarmes par l'opérateur sous toutes les conditions prévalant durant l'exploitation en salle de commande.

Il convient d'utiliser des codes d'alarme (par exemple clignotement rapide ou surbrillance) pour les alarmes qui nécessitent des actions rapides de la part de l'opérateur. La définition des priorités liées à l'importance peut être codée avec des couleurs.

Par exemple, lors de la production de plusieurs alarmes, un affichage dynamique des priorités avec trois couleurs de verrine peut être utilisé pour identifier des alarmes importantes. Les alarmes qui sont tout le temps importantes, peuvent être indiquées en rouge, alors que les autres informations seraient en jaune ou vert.

Lorsqu'elle est affichée, il convient que l'opérateur saisisse rapidement la priorité d'une alarme. Les alarmes de même niveau de priorité peuvent être affichées sur une unité de visualisation particulière.

10.2 Panneau d'alarme et verrines

10.2.1 Légende d'alarme

Il convient que les légendes des panneaux d'alarmes et des verrines suivent les principes fournis en 10.1.5.

Les légendes des panneaux d'alarmes peuvent être regroupées sous un titre pour l'ensemble du panneau d'alarme, tel que l'identification de la zone de la centrale touchée. Ceci permet aux légendes des alarmes d'être raccourcies par rapport aux messages complets d'alarme.

Dans le cas du message d'une verrine d'alarme, intégrée dans une représentation ou une disposition comparable à un panneau de commande, où une reconnaissance précise peut être garantie par des modèles cognitifs ou des indicateurs topographiques, des messages simplifiés tels que «haute pression» peuvent être utilisés.

Unless the space available for alarm legends or messages is very restricted, abbreviations should not be used. If a legend or message is long, an abbreviation may be used, provided the message remains clearly understandable. If an abbreviation is used, it shall be based on systematic rules.

Systematic abbreviation rules should be specified and applied to the following:

– abbreviation of common conditions such as high pressure, low level;
– identification of plant unit, train, equipment number, and others;
– progressively shorter versions of common words used in defining messages; a possible method is using reference versions of words with removal of none, then one and then two vowels.

The alarm messages and legends defined at the design stage should be reviewed systematically for clarity and comprehension by human factors experts and by representatives of the operating staff.

10.1.6 Display coding

Display coding should be consistent with the station coding philosophy and applied systematically throughout alarm displays.

Display coding should ensure rapid detection and interpretation of alarms by the operators under all control room operating conditions.

Alarm coding (e.g., fast flashing or bright) should be used for alarms that require rapid operator action. Prioritisation of importance may be colour coded.

For example, to identify important alarms at the time of multiple alarm generation, a dynamic priority display in a three-colour tile may be used. The important alarm at any point can be shown in red, while other information is controlled to yellow or green.

When displayed, operators should be able to grasp the alarm priority easily. The alarms at each priority of importance may be displayed on an exclusive VDU screen, provided for each degree of importance.

10.2 Alarm fascia and tile

10.2.1 Alarm legend

Alarm fascia and tile legends should follow the principles given in 10.1.5.

Alarm fascia legends may be able to be grouped under a heading for the total alarm fascia group, such as the identity of the plant area affected. This allows the alarm legends to be shortened from the full alarm message.

In the case of alarm tile messages, integrated within mimic or similar layouts of panel controls, where accurate recognition may be ensured by pattern recognition or topographic cues, simplified messages such as ‘high pressure’ may be used.

10.2.2 Modèle de panneaux d'alarmes ou de verrines

Dans un panneau, il convient que l'identification d'une verrine d'alarme soit facilitée par certains moyens visant à prévenir toute erreur d'évaluation de la situation; ces moyens comprennent, l'utilisation de la disposition des verrines, les couleurs, le regroupement, le codage audio, et les alarmes groupées.

La méthode d'affichage dynamique des priorités par des verrines avec trois couleurs modifiables peut être utilisée pour faciliter l'identification de l'importance d'une alarme, lorsqu'un grand nombre d'alarmes apparaissent. Ceci empêche le masquage d'alarme et minimise les omissions ou les erreurs de reconnaissance par l'opérateur. Pour les alarmes groupées, il convient d'utiliser l'affichage sur unités de visualisation, les affichages triés temporellement et l'affichage de telop.

Les méthodes utilisant les panneaux d'alarmes peuvent mettre en oeuvre des logiques fixes pour identifier les alarmes de plus haute priorité ou les premières alarmes à apparaître dans un groupe existant, ceci sans modifier les alarmes déjà existantes.

Les panneaux d'alarmes et les verrines lumineuses peuvent être utilisés pour présenter l'état de la centrale, indiquant sa disponibilité et sa bonne exploitation. L'état du système de sûreté et de commande automatique du réacteur peut être présenté à l'aide de panneaux ou de verrines lumineuses. Le traitement des signaux sera nécessaire pour identifier l'instant où il convient d'utiliser les informations d'état pour produire une alarme. Plus d'informations sont données en Annexe E.

10.3 Affichage des listes d'alarmes sur les unités de visualisation

10.3.1 Généralités

Dans les centrales utilisant des systèmes numériques d'affichage, l'utilisation d'unités de visualisation pour l'affichage des alarmes, permet l'intégration dans la méthode d'affichage d'alarmes de nombreuses autres informations nécessaires en salle de commande. Ceci permet à l'opérateur d'accéder directement à partir des affichages d'alarmes à des affichages d'informations associées à l'état de la centrale, pour l'assister dans le diagnostic et les prises de décisions concernant les actions appropriées.

Il convient que les alarmes et les alarmes groupées présentées sur les panneaux de commande ou les verrines soient aussi affichées sur les unités de visualisation. Il est recommandé qu'il soit prévu à la conception de pouvoir présenter, à partir du message d'alarme, les signaux d'alarme utilisés pour chaque groupe, à l'aide de moyens de commande d'exploitation adaptés, tels que l'utilisation du curseur, de cliques de souris, d'utilisation d'écran tactile.

Il convient de prévoir, pour la présentation des alarmes dans des listes de messages sur les unités de visualisation, un espace de visualisation suffisant, afin de pouvoir visualiser simultanément l'ensemble des messages de haute priorité ou alors il est recommandé d'utiliser d'autres méthodes pour permettre d'avoir une vue d'ensemble et une présentation rapide des alarmes de haute priorité. La meilleure solution peut être des affichages dont la place est réservée ou des panneaux. On doit mettre en place des moyens simples pour dérouler les listes d'alarmes ou en tourner les pages, avec la possibilité d'afficher rapidement les alarmes les plus récentes.

10.3.2 Messages d'alarme affichés sur les unités de visualisation

Il convient que les messages affichés sur les unités de visualisation ou sur les grands écrans suivent les principes donnés en 10.1.5.

10.2.2 Layout of alarm fascias and tiles

The alarm tile identification within a fascia should be made easier by means which include the use of the tile layout, colour, grouping, audio-coding, and grouped alarms, aiming at preventing faulty judgment of the situation.

To make it easier to identify the degree of importance when a number of alarms appear, the dynamic priority display method by the three-colour variable tile may be used. This prevents alarm masking, and minimizes omission or faulty recognition by operators. The VDU display should be used for the grouped alarm display, time-ordered display, and telop display.

Methods using fascia displays may use fixed logic to identify the highest priority alarm or the first alarms to appear in an existing group, without altering those alarms already existing.

Alarm fascias and illuminated tiles may be used to show the status of plant, indicating its availability or correct operation. The status of the reactor automatic control and safety systems may be shown by fascias or illuminated tiles. Alarm signal processing will be necessary to identify when such status information should be used to generate an alarm. Further information is given in Annex E.

10.3 VDU alarm list display

10.3.1 General

The use of VDU displays for alarms allows the integration of the alarm display method with the display of much of the other information needed in the control room, for plants where computer-based displays are used. This allows the operator to have direct access from display of an alarm to associated displays of information on the plant state to assist in diagnosis and decision on appropriate actions.

Alarms and grouped alarms presented by alarm fascias or tiles should also be presented on VDU displays. The design should allow the details of the alarm signals used to form each grouped alarm to be shown by operation of suitable controls, such as a cursor and mouse click or touch screen operation on the alarm message.

For alarm presentations, such as VDU message lists, sufficient display area should be provided for the simultaneous viewing of all high-priority alarms or alternative methods should be used to show an overview or to allow rapid presentation of high priority alarms. Spatially dedicated displays or panels may be the best solution. Simple means to scroll or turn pages through lists of alarms shall be provided, with the ability to show quickly the most recent alarms.

10.3.2 VDU alarm messages

Messages displayed by VDU or large screens should follow the principles given in 10.1.5.

Il convient que les messages affichés sur les unités de visualisation et imprimés soient cohérents. Afin d'éviter toutes confusions à l'opérateur, il convient de dresser et de mettre à sa disposition la liste des abréviations disponibles et de leurs significations et que celle-ci soit accessible à l'écran sur requête.

Concernant la présentation des alarmes sur les écrans en séquence d'affichage d'alarmes (affichages chronologiques), il est recommandé d'indiquer les temps d'apparition et de disparition des alarmes, afin de pouvoir évaluer les alarmes, à l'aide d'autres formes de présentation (par exemple, courbes de tendance, registre des évènements).

10.3.3 Organisation des affichages d'alarmes sur les unités de visualisation

Il convient que la méthode d'affichage d'alarmes utilisant des unités de visualisation permette l'affichage de l'enregistrement chronologique des alarmes apparues. Ceci peut être fait à partir de la liste paginée des alarmes apparues récemment. La page la plus récente d'alarme – appelée ici page de tête – peut être affichée, présentant ainsi les alarmes qui viennent juste d'apparaître avec un symbole clignotant associé à leur message d'alarme. Il convient qu'on puisse rappeler des pages précédentes à l'aide de commandes adaptées.

Il est recommandé que les listes d'alarmes qui existent soient disponibles sous forme de diverses associations. Celles-ci peuvent être présentées par le biais de commandes adaptées, afin de sélectionner des types de tri ou la liste choisie en mémoire. Parmi ces listes on peut distinguer les suivantes:

– alarmes par ordre chronologique, à chaque niveau de la hiérarchie d'affichage, de la vue d'ensemble aux détails de la centrale;
– alarmes à chaque niveau de priorité;
– alarmes supprimées ou retirées de l'exploitation car classées «perturbatrices»;
– alarmes retirées des listes chronologiques qui sont connues, ont été acquittées et qui existent depuis longtemps;
– alarmes associées avec chaque élément particulier de la centrale, triées suivant le repère d'identification, un ordre propre à la centrale ou l'ordre chronologique;
– signaux d'alarme avant traitement, tels qu'ils sont en entrée du système d'alarme;
– alarmes d'un type particulier.

Les alarmes débordant de la page de tête peuvent être présentées dans les pages suivantes. On doit avoir en même temps des indications sonores et visuelles, telles que les telops, pour attirer l'attention de l'opérateur, lorsqu'il y a des alarmes non acquittées dans d'autres pages qui ne sont pas en cours de visualisation.

Les méthodes utilisant des unités de visualisation peuvent permettre une exploitation «à affichage retenu» avec une intervention ultérieure pour présenter la dernière alarme non acquittée et pour afficher les alarmes récentes non encore acquittées. Ceci peut empêcher l'écrasement automatique d'affichages lors d'opérations critiques, et permettre aux alarmes prioritaires d'être immédiatement présentées, mais aussi, permettre de garder l'avantage de l'affichage automatique rapide des alarmes de priorité normale.

Il convient que la structure de l'affichage des alarmes sur les unités de visualisation permette à l'opérateur de voir rapidement les alarmes ou les groupes d'alarmes importants, et de rechercher dans les affichages les détails des anomalies affectant la centrale.

Il est recommandé que le système d'affichage sur les unités de visualisation permette d'afficher explicitement les signaux d'alarme utilisés par la logique du système de traitement de signaux d'alarme pour produire une alarme. Il convient que cette méthode permette d'identifier les composants de toute alarme existante et il est recommandé qu'elle intègre des affichages de navigation et une méthode d'affichage pour toute la centrale. Des informations complémentaires sont fournies à l'Annexe B et dans la CEI 61772.

VDU alarm messages and printer messages should be consistent. To prevent operators from being confused, a list of available abbreviations and their expansions should be produced and made available for on-screen call-up.

For alarm presentation on screens in the form of alarm sequence displays (chronological displays), the activated and cleared time of each alarm should also be indicated to allow the alarms to be assessed in relation to other forms of presentation (e.g. trend curves, event logs).

10.3.3 VDU alarm display organization

The method of alarm display using VDUs should allow for display of the chronological record of alarms which have appeared. This may be done by a list of the more recent alarms divided into pages. The most recent page of alarms – called here the top page – may be on display normally, with the alarms, which have just appeared shown with a flashing symbol adjacent to their alarm message. Operation of suitable controls then should allow earlier pages to be shown.

Lists of alarms which exist should be available in various associations. These may be shown by operation of suitable controls to select the type of ordering or the chosen list held in the computer memory. The lists may include the following:

– alarms in chronological order, at each level of a display hierarchy from overview to plant detail;
– alarms at each priority level;
– alarms suppressed or removed from operation due to ‘nuisance’ initiations;
– alarms removed from any chronological list which are known, acknowledged and have existed for long periods;
– alarms which are associated with each specific plant item, in tag identity order, a plant based order or in chronological order;
– alarm signals before alarm signal processing and as inputs to the alarm system;
– alarms of a specific type.

Alarms overflowed from the top page may be presented on subsequent pages. Especially, if unacknowledged alarms are contained in other pages, which are not currently on display, both audible and visual indications such as a telop shall be given to draw the operator’s attention to the existence of unacknowledged alarms on other pages or displays.

Methods using computer-based VDU systems may allow operation of a ‘Display hold’ with a later operation of a control to show the ‘Last unacknowledged alarm’ to display the most recent alarm not yet acknowledged. This can prevent automatic display override in critical operations, and then allow the priority alarm to be immediately shown, but also keep the advantage of rapid automatic display of priority alarms normally.

The VDU display of alarms should include a structure to allow the operator to see quickly the most important alarms or alarm groups, and to track through the displays to find the detail of the plant anomaly.

The VDU system of display should allow explicit display of alarm signals used to form alarms by the alarm signal processing logic. This method should allow the components of any existing alarm to be identified, and should be integrated with display navigation and the display method for the whole plant. Further information is given in Annex B and IEC 61772.

Les méthodes basées sur les unités de visualisation doivent intégrer des écrans d'interrogation. Les exemples de méthodes suivants peuvent être retenus:

– sélection par le curseur ou par la souris d'une alarme groupée pour obtenir une fenêtre présentant les composants d'alarme formant le groupe;
– sélection par la souris d'une valeur affichée pour avoir une fenêtre avec les seuils d'alarme et l'état des signaux;
– sélection par la souris d'un message d'alarme pour accéder directement à un affichage associé à la condition de la centrale;
– sélection par la souris d'une alarme pour obtenir un menu et lancer une séquence de commandes, telle que la suppression d'alarmes persistantes ou perturbatrices, ou pour revenir à un service;
– entrée clavier de critères de recherche, tels que l'identité d'une alarme sélectionnée, le type codé identifiant d'un instrument ou d'un composant de la centrale, pour obtenir une impression de toutes les alarmes recherchées.

D'autres méthodes de sélection que la souris et le curseur peuvent être utilisées, telles que le clavier à interrupteur multipositionnel, le clavier ou l'écran tactile pour sélectionner le message d'alarme ou le signal concerné.

10.3.4 Formats et modèle des affichages d'alarmes

Il est recommandé que de courts indicateurs visuels (par exemple, telops) indiquent sur tous les écrans des unités de visualisation que des alarmes sont présentes, et ceci peut être fait dans la bordure haute ou basse de chaque écran. Ces messages peuvent indiquer le nombre d'alarmes présentes qui n'ont pas encore été acquittées, l'identité de l'écran d'unité de visualisation sur lesquels les alarmes peuvent être visualisées ou des pointeurs équivalents. Ces indicateurs visuels doivent être mis à jour à intervalles réguliers, par exemple, toutes les secondes et lorsque des alarmes sont présentées ou acquittées.

Afin de minimiser les possibilités de confusion entre deux lignes adjacentes, une séparation (par exemple une ligne de blancs ou une ligne horizontale) peut être insérée toutes les quatre ou cinq lignes dans les affichages de messages sur les unités de visualisation.

10.3.5 Commande

Il convient d'intégrer le contrôle du fonctionnement des unités de visualisation d'alarmes dans le contrôle du fonctionnement de toutes les unités de visualisation du système numérique complet de la centrale. Il est recommandé que les moyens de commande soient robustes, fiables, durables et adaptés à l'environnement de la salle de commande d'une centrale. Il convient que les séquences de commandes soient courtes et de préférence lancées «en appuyant sur une touche» pour tous les objectifs. Les méthodes appropriées sont entre autres les suivantes:

– boutons poussoirs et interrupteurs proches de chaque unité de visualisation;
– claviers alphanumériques standards ou spécifiquement conçus proches de chaque unité de visualisation;
– boule roulante, curseur ou souris et menus ou zones à cliquer sur les unités de visualisation.

Il convient de minimiser autant que possible le nombre d'opérations pour appeler un écran, et il est recommandé de limiter ce nombre à deux opérations ou moins. Il est aussi recommandé de pouvoir appeler par une action simple, un écran associé, à partir d'un signet de renvoi ou d'une commande. Des recommandations concernant la conception des affichages sont données dans la CEI 61772.

VDU methods shall allow for interrogation displays. Examples of methods which may be used include:

– mouse or cursor click on a grouped alarm message to provide a window showing the alarm components making up the group;
– click on a displayed value to give a window of the alarm threshold and state of the signal;
– click on an alarm message to provide a direct display transfer to the associated display of plant condition;
– click on an alarm message to provide a menu and initiate a control sequence such as suppression of a nuisance or standing alarm or return to service;
– keyboard entry of a search condition, such as the selected alarm identity, plant item or the instrument type coded identity, to give a printout of all associated alarms.

Other methods of selection than the mouse or the cursor may be used, such as a multi-position switch, keyboard or touch screen to select the alarm message or signal concerned.

10.3.4 Alarm display layout and formats

Brief visual clues (e.g., telops) that alarms are present should be shown on all VDU screens, and this may be at the bottom or top edge of each screen. These may show the number of alarms which are presented or not yet acknowledged, VDU screen identity for which alarms should be viewed or similar pointers. These visual clues shall be updated at regular times such as every second and when alarms are shown or acknowledged.

To reduce confusion between two adjacent message lines, a separation (e.g., blank row or horizontal line) may be inserted every four or five lines in VDU alarm message display.

10.3.5 Control

The control of VDU alarms operations should be integrated with the control of all VDUs for the complete computer system. The controls should be robust, reliable, long life items and suitable for a process plant control room environment. Control sequences should be short, and preferably ‘one touch’ in operation for any objective. Methods, which are suitable, include:

– hardware pushbuttons and switches adjacent to each VDU;
– standard alphabetical or specially designed keyboards near each VDU;
– roller ball, cursor or mouse click on menus or target areas of VDU displays.

The number of operations to call up a required screen should be minimized as far as possible and two actions or less is recommended. It should also be possible to call up related screens by a single action of the related screen request button or control. Guidance is given on display design in IEC 61772.

10.4 Annonce sonore

Les annonces sonores, comprenant les messages verbaux, peuvent être utilisées pour attirer l'attention de l'opérateur, de façon qu'il ne rate pas l'évènement annoncé par alarme.

Le message verbal est un moyen approprié pour présenter les informations liées aux interfaces, et il peut être avantageux d'utiliser les messages verbaux pour la présentation des alarmes informatives. Par contre l'utilisation des seuls messages verbaux pour les alarmes informatives n'est pas recommandée. Il est recommandé d'éviter l'utilisation abusive des annonces sonores car cela peut distraire ou irriter le personnel de conduite.

11 Fiabilité, essais et maintenabilité

11.1 Fiabilité

Il est recommandé que la fiabilité d'un système intégré d'alarme soit cohérente avec le rôle de sûreté assuré par la fonction réalisée. Il convient que la défaillance unique d'un tel système ne conduise pas à des défaillances multiples au niveau des alarmes. Il est recommandé d'avoir un niveau de redondance adapté et des fonctions d'autodiagnostic pour la détection des défaillances.

Lorsque les alarmes sont présentées sur une unité de visualisation principale, il est recommandé que les opérateurs puissent avoir accès aux alarmes de plusieurs autres unités de visualisation.

11.2 Essais

Il convient, après installation sur site, de tester chaque opération sur les alarmes, en même temps du côté du terminal du système d'alarme et du côté des appareils initiateurs. Cela est nécessaire pour garantir que les alarmes sont opérationnelles avant le début de la mise en exploitation.

Une commande doit être prévue pour essayer l'allumage des panneaux d'alarmes et des verrines, et il est recommandé de disposer d'une méthode pour essayer la fonction clignotement.

Il est recommandé que chaque alarme affichée par une méthode utilisant des unités de visualisation soit présentée durant la mise en service pour montrer qu'elle est affichée correctement, avec le bon titre, le bon traitement logique et les informations associées. Ceci peut être fait par essais se recouvrant, pour montrer de façon séparée que l'appareil initiateur fonctionne correctement en entrée du matériel d'alarme et que l'alarme est correctement présentée en fonction de ces entrées.

Chaque alarme importante pour la sûreté doit être testée sur site à partir des appareils initiateurs pour montrer que l'alarme est correctement présentée et il convient de conserver les enregistrements d'essai.

Durant la mise en service du système, le système d'alarme installé doit être testé pour démontrer que toutes les fonctions du traitement des signaux d'alarme et du traitement de l'affichage des alarmes sont satisfaisantes. Il convient de réaliser un essai pour montrer que tous les signaux d'alarmes d'un groupe nombreux apparus en un laps de temps court ont été détectés et mémorisés correctement et que les alarmes associées ont été produites et affichées. (Un essai adapté peut être fait par méthode de simulation ou d'injection de signal pour produire les centaines de signaux d'alarme en quelques secondes, avec vérification du système de sortie par exemple.)

10.4 Audible annunciation

Audible annunciation including speech annunciation may be used to attract the operators' attention, so that they do not miss the event announced by the alarm.

Speech is an acceptable medium for presenting interface-related information, and there may be advantages associated with using speech for presenting alarm information as well. However, using speech alone for presenting alarm information is not recommended. The extensive use of speech should be avoided since this could prove a distraction or irritation to the operating staff.

11 Reliability, testing, and maintainability

11.1 Reliability

The reliability of an integrated alarm system should be consistent with the importance to safety of the alarm functions performed. Single failure of such a system should not lead to multiple failure of alarms. Appropriate redundancy and self-diagnosis functions to detect failures of the system are recommended.

Where alarms are presented on a VDU as the primary display, the operators shall be able to access the alarms from more than one VDU.

11.2 Testing

The operation of each alarm should be tested on site after installation, both from the terminals of the alarm system equipment and from the initiation devices. This is necessary to ensure all the alarms are in full working order before plant operation is attempted.

A control shall be provided to test the illuminations of alarm fascias or tiles and a method should allow the flashing function to be tested.

Each alarm displayed using a VDU method should be shown during commissioning to be displayed correctly, with the correct title, logic processing and associated information. This may be done by overlap testing to show separately that the initiation device operates correctly at the input to the alarm equipment and that the correct alarm is shown from those inputs.

Each alarm important to safety shall be tested on site from the initiating devices to show that the correct alarm is shown, and the test records should be preserved.

During system commissioning, the installed alarm system shall be tested to demonstrate that all the functions of alarm signal processing and alarm display processing are satisfactory. A test should be done to show that all of a large group of alarm signals raised over a short time are detected and memorised correctly, and the associated alarms generated and displayed. (A suitable test may be done by simulation or signal injection methods to raise several hundred alarm signals in a period of a few seconds, with checks of the system output, for example.)

11.3 Maintenabilité

Il convient de concevoir le système d'alarme de telle façon que les activités de maintenance puissent être réalisées en ayant un minimum d'interférence avec les activités opérateur. Lors du retrait d'une alarme, les éléments suivants doivent être pris en compte:

- Indication d'alarme hors service – il convient que la mise hors service complète d'une alarme nécessite l'inhibition des signaux initiateurs des indicateurs sonores et visuels pour cette alarme seulement. En outre, il convient que les indicateurs pour la reconnaissance rapide d'une alarme hors service ou inhibée soient conçus avec le système.
- Indication de défaillance du système d'alarme – il convient que les opérateurs soient alertés rapidement avec des indications détaillées sur l'emplacement de la défaillance du système d'alarme ou de ses sous composants principaux.

Concernant les verrines ou les panneaux d'alarmes, les éléments suivants doivent être pris en compte:

- Durée d'allumage longue – si, en fonctionnement normal, il faut qu'une verrine d'alarme ou un panneau soit allumé pour une période longue du fait de réparations ou de remplacements de matériel, il convient qu'elle soit identifiée de façon particulière par des moyens adaptés afin qu'elle soit reconnue durant cette période et contrôlée par des procédures administratives.
- Cabochon de remplacement des verrines – si le remplacement d'une ampoule nécessite le retrait de la verrine avec sa légende, il est recommandé d'avoir un moyen de garantir que la verrine est replacée au bon endroit.
- Prévention des risques – le remplacement d'une ampoule ne doit pas présenter de risques de chocs électriques.
- Aide à l'opérateur pour le remplacement des ampoules – il convient de fournir les aides opérateur si nécessaire pour le remplacement des ampoules.

12 Enregistrement des alarmes

Afin de pouvoir les analyser ultérieurement, toutes les alarmes importantes pour la sûreté doivent être enregistrées. Les enregistrements peuvent être imprimés directement, ou après un stockage intermédiaire, ou conservés sur des supports mémoire adaptés, tels que des disques magnétiques, des bandes, des moyens optiques, à écriture unique et à lectures multiples, avec des possibilités d'interrogation, d'affichage et d'impression. Il convient de mettre à disposition les moyens de recherche et de sélection partielle des enregistrements ou de l'historique des signaux d'alarme.

Il est recommandé qu'il soit possible d'imprimer les enregistrements d'alarmes et les signaux d'alarme qui ont changé d'état, et de faire des impressions de l'historique des alarmes et des signaux d'alarme pour des systèmes de la centrale donnés.

L'enregistrement de l'information relative aux alarmes doit inclure les informations temporelles propres à celles-ci ainsi que les séquences d'apparition et de disparition d'alarmes associées aux séquences relatives aux autres signaux binaires et aux évolutions analogiques.

Certaines centrales peuvent avoir des systèmes d'enregistrement rapide des séquences événementielles, capables de discerner des basculements d'interrupteur de 10 ms ou moins, et de les mémoriser suite à une défaillance électrique majeure.

11.3 Maintainability

The alarm system should be designed so that maintenance activities can be performed on the alarms with minimal interference with the activities of the operators. On removal of an alarm from service, the following shall be taken into account:

– Out of service alarm indication – taking an alarm out of service completely should require disabling of the associated initiation of visual and audio signals of that alarm only. Furthermore, cues for prompt recognition of an out-of-service or tagged out alarm should be designed into the system.

– Alarm system failure indication – the operators should be given prompt warning with detailed location indication of a failure of the alarm system or its major subcomponents.

For an alarm tile or fascia, the following shall be taken into account:

– Extended duration illumination – if an alarm tile or fascia must be 'ON' for an extended period during normal operations because of equipment repair or replacement, it should be distinctively coded by any suitable means for positive recognition during this period, and controlled by administrative procedures.

– Tile cover replacement – if a lamp replacement requires legend tile removal, there should be a way to ensure that the tile is replaced in the correct location.

– Hazard avoidance – lamp replacement shall not pose an electrical shock hazard.

– Operator aids for lamp replacement – operator aids should be provided if needed for lamp replacement.

12 Alarm recording

For purposes of later analysis, all alarms important to safety shall be recorded. Recording may be by printout directly or after buffer storage, or by suitable storage systems such as magnetic disc, tape or an optical write-once-read-many times (worm) medium, with facilities to interrogate the record for display or printout. Facilities to search for and to select sections of the record or specific alarm signal histories should be provided.

It should be possible to print the record of alarms and alarm signals that have changed state, and to make printouts of the history of alarms and alarm signals for selected plant systems.

The recording of alarm information shall include the time and the sequence of alarm appearance and disappearance together with the sequence of other binary signals and analogue trends.

Some plants may include a rapid sequence of events recording system, able to discriminate switch-gear events to within 10 ms or faster, and to record them, following a major electrical fault.

13 Procédures de Réponse aux Alarmes (PRA)

13.1 Généralités

Il convient qu'une PRA soit disponible pour chaque alarme.

Il convient que l'opérateur ait accès aux PRA de l'endroit où il lit les messages d'alarme.

Les informations contenues dans les PRA doivent être cohérentes avec les informations présentées sur les panneaux de commande, dans le système d'alarme, dans les procédures d'étalonnage et de réglage des points de consigne de l'I&C, dans les documents de contrôle qui fixent les points de consigne (par exemple, spécifications techniques, analyses accidentelles), ainsi que dans les autres procédures de la centrale et les autres documents techniques.

13.2 Contenu

Il est recommandé que les PRA contiennent les informations suivantes:

– le groupe ou système fonctionnel auquel l'alarme appartient;
– le message, la légende ou le texte exact de l'alarme;
– l'origine de l'alarme (par exemple, le ou les capteurs émettant le signal, la logique de validation ou le traitement du signal, et l'actionneur ou l'équipement pour les alarmes référençant un diagramme schématique sur lequel l'actionneur peut être trouvé);
– les seuils d'alarmes;
– les priorités (importance de sûreté);
– les causes sous jacentes probables de l'alarme (par exemple, bas niveau d'eau – débit d'alimentation défaillant à long terme);
– les actions opérateur nécessaires immédiatement, incluant les actions réalisées par l'opérateur pour confirmer l'existence de la condition d'alarme;
– les actions se déclenchant automatiquement lorsqu'une alarme survient (et dont il convient que l'opérateur vérifie l'exécution);
– le suivi des actions;
– les références pertinentes;
– des informations relatives au diagnostic nécessaires pour l'identification de la cause de l'alarme;
– des indications sur le comportement futur de l'installation.

13.3 Format

Il convient que le format soit conforme aux points suivants:

– identification correcte de la PRA sur chaque page de la procédure;
– identification correcte des éléments importants;
– informations sur les catégories au même endroit sur chaque page aisément localisables;
– présentation de l'information cohérente tout au long de la PRA;
– minimisation de la nécessité pour l'opérateur de changer de page pour avoir l'information qui lui est nécessaire.

13 Alarm Response Procedures (ARP)

13.1 General

ARP should be available for each and every alarm.

The operators should have access to ARP from the location at which the alarm messages are read.

Information in ARP shall be consistent with information on control boards, in the alarm system, in I&C procedures used to calibrate alarm setpoints, in controlling documents that determine setpoints (e.g., technical specifications and accident analyses), and in other plant procedures and technical documents.

13.2 Contents

ARP is recommended to contain the following information:

– the system/functional group to which the alarm belongs;
– the exact alarm message, text or legend;
– the alarm source (i.e., the sensor or sensors sending the signal, including processing or signal validation logic, and the actuating device or devices for the alarm with a reference to a schematic diagram on which such devices can be found);
– alarm thresholds;
– priority (safety importance);
– potential underlying causes for the alarm (e.g., low water level – feed flow deficiency in the long term);
– required immediate operator action, including actions the operator can take to confirm the existence of the alarm condition;
– actions which occur automatically when the alarm occurs (and which the operator should verify as having taken place);
– follow-up actions;
– pertinent references;
– diagnostic hints needed to identify the cause of the alarm;
– indication of future plant behaviour.

13.3 Format

The format of ARP should satisfy the following:

– ARP identified on each page of the procedure is identified suitably;
– important items are identified suitably;
– information categories in the same position on each page are easy to locate;
– information throughout ARP is presented consistently;
– the need for operators to page back and forth to obtain the information is minimized.

Annexe A
(informative)

Problèmes des systèmes d'alarmes

Les exemples donnés dans ces annexes sont basés sur un retour d'expérience.

A.1 Débit d'alarmes et de changements d'information normal et en cas d'avalanche

Pour une centrale, un taux de plusieurs centaines de changements de signaux d'information par jour est considéré comme normal et permet de prévoir le nombre d'alarmes produites; les systèmes d'alarme acceptent couramment cette charge. Lors des arrêts d'urgence ou des évènements majeurs, les signaux d'entrée qui produisent les alarmes peuvent changer très rapidement, formant une avalanche ou un flot de changements. Les centrales qui n'avaient pas mis en œuvre des logiques adaptées ont fait face à des problèmes de mémorisation et de traitement de ce flot d'informations. Dans ces conditions, les opérateurs de centrale peuvent aussi avoir à faire face à une surcharge d'information, si la production des alarmes à partir de ces informations n'a pas été soigneusement conçue.

Il a été montré que, concernant l'information relative aux alarmes affichées sur les unités de visualisation, les opérateurs ne peuvent pas lire plus vite qu'un titre d'alarme toutes les 10 s, et que l'analyse des conséquences d'une alarme affichée prend beaucoup plus de temps (plusieurs minutes). Ainsi les procédés de production d'alarmes doivent être conçus pour identifier les alarmes qui nécessitent une action positive, pour les présenter de façon à ne pas dépasser les capacités de perception des opérateurs et pour que la situation reste sous leur contrôle, même lors de taux élevé de changement des informations d'entrée utilisées pour produire les alarmes.

Lors des arrêts d'urgence provoqués au niveau du réacteur, de la centrale ou d'un système électrique, des centrales nucléaires ont du faire face à l'apparition d'un millier de changements d'informations en quelques secondes. Plus de 200 changements à la minute peuvent continuer à apparaître, pendant plusieurs minutes et plusieurs fois pendant l'heure qui suit l'arrêt d'urgence.

Une discrimination temporelle de 200 ms pour les changements d'informations et d'alarmes est appropriée pour les alarmes générales de la centrale, par contre un pas de temps de 10 ms peut être nécessaire pour les séquences d'événements liés aux systèmes d'interrupteurs.

A.2 Alarmes perturbatrices

Avec les systèmes numériques d'alarme, des centrales nucléaires ont du faire face à des problèmes dus à des signaux initiateurs défaillants, à des seuils ou à des valeurs d'hystérésis incorrects entraînant la production et disparition d'alarmes répétitives. Ces changements perturbateurs apparaissent typiquement avec des périodes variant de 10 s à 10 min. L'étude des journaux d'enregistrement des changements de signaux permet d'identifier ces problèmes. La maintenance dans la centrale des contacts défectueux et la correction des signaux de seuil et de leurs hystérésis peuvent réduire le problème. Ceci n'est pas toujours suffisant pour réduire la charge des perturbations sur les opérateurs. Il est habituellement relativement simple, dans les systèmes numérisés, de mettre en œuvre les méthodes nécessaires pour supprimer de telles alarmes, de les enregistrer dans des journaux et de rétablir le service lorsque la source de perturbations est corrigée.

Annex A
(informative)

Problems of alarm systems

The examples given in these annexes are based on real experience.

A.1 Normal and avalanche rates of alarm and information change

A normal rate of appearance of information signals used to derive alarms can be several hundred signal changes per day for a nuclear plant, which can usually be handled by the alarm systems. At plant trips and major changes, the input information signals used to generate alarms can change very rapidly for many signals, in an 'avalanche' or 'flood' of changes. Plants which have not included suitable logic, have experienced problems in memorizing and processing this flood of information. In these conditions, plants can also have problems of information overload to the operator unless alarms are carefully determined from the information.

It has been shown that operators cannot read VDU information on alarms faster than about one alarm title every 10 s, and their analysis of the implication of alarms which existe takes far longer (several minutes) per alarm. Therefore, the alarm generation processes need to be designed to identify the alarms which need a positive action, and present them in a way which does not overload the operators' perceptive ability, and which remains under their control, even at high rates of change of the input information used to generate the alarms.

At major reactor, plant or electrical trips, nuclear plants have experienced rates of appearance of changed information of about 1 000 changes appearing in a period of a few seconds. Changes can continue to appear at over 200 changes per minute, several times and for minutes at a time, for up to an hour after a trip.

A time resolution for information and alarm changes of about 200 ms is suitable for general plant alarms, but resolution of 10 ms can be needed for special switchgear sequence-of-events systems.

A.2 Nuisance alarms

In computer-based alarm systems, plants have experienced problems due to faulty initiation signals, incorrect thresholds or hysteresis settings which can cause alarms to be generated and cleared repeatedly. These nuisance changes occur typically at intervals of 10 s to 10 min. Study of the logs of the signal changes is used to identify problems. Maintenance of defective plant contacts and correction of threshold signals and their hysteresis can reduce the problem. This is not always sufficient to reduce the nuisance load on the operators. For computer-based systems, methods to suppress such alarms, to log them and to return them to service when the source of the nuisance is corrected are usually necessary and relatively simple to implement.

Annexe B
(informative)

Origine de l'information des signaux utilisés pour produire les alarmes

Les signaux d'information utilisés comme signaux d'alarme, traités par la logique de traitement des signaux d'alarme pour produire les alarmes pour le traitement d'affichage des alarmes peuvent avoir, dans les centrales nucléaires, les origines suivantes:

– signaux de contacts, tels que les relais, les contacts auxiliaires des interrupteurs ou boîtiers de fin de course;

– sorties logiques du relayage, détecteurs de proximité, enregistreurs de position de vanne, thermostats;

– signaux analogiques vérifiés par rapport à des limites hautes et des limites basses (par exemple, consignes de seuil avec hystérésis);

– sélecteurs et commandes de position, sélecteurs auto/manu, qui conditionnent l'information;

– conditions du système de sûreté et de protection, produites par le système de sûreté ou autrement par les signaux logiques dépendant du niveau de flux, de blocages et d'états opérationnels;

– calculs sur les signaux analogiques, avec détection d'erreurs, telles qu'une mesure individuelle de température de sortie de cœur hors limites comparée aux canaux de mesure voisins;

– calculs utilisant en même temps des signaux analogiques et des signaux d'état, tels que les détecteurs de position de barre identifiant une barre non alignée dans un groupe;

– états internes d'un calculateur ou d'une logique, produits directement ou indirectement par des conditions de la centrale;

– regroupement ou autres logiques portant sur des états ou des alarmes pour produire d'autres alarmes.

Typiquement, environ 10 000 signaux analogiques et 10 000 signaux TOR (tout-ou-rien) peuvent correspondre à une centrale nucléaire équipée d'un réacteur et d'une turbine, ce qui produit au moins 20 000 libellés d'alarme possibles.

Annex B
(informative)

Information sources for signals used to generate alarms

Information signals used as alarm signals, processed by alarm signal processing logic to generate alarms for alarm display processing are provided on nuclear plants from sources which include the following:

– contact signals, such as relays, switchgear auxiliary contacts or limit switches;
– solid state logic outputs, proximity detectors, valve states, temperature switches;
– analogue signals checked against high or low limits (i.e., thresholds with hysteresis settings);
– control and selector switch states, auto/manual selectors, which condition the information;
– safety and protection system conditions, processed by the safety system or otherwise with logic signals depending on flux level, operational vetoes and operational state;
– calculations on analogue signals, with detection of anomalies, such as an individual reactor core outlet temperature out of limits compared to the channels near it;
– calculations using both analogue and status signals, such as detection of a control rod in the operating group not in line with the group;
– internal computer or logic states, derived directly or indirectly from plant conditions;
– grouping or other logic on states and alarms to generate other alarms.

A typical nuclear plant unit with one reactor and turbine may have about 10 000 analogue signals and at least 10 000 contact and two-state signals, resulting in at least 20 000 possible alarm titles.

Annexe C
(informative)

Exemples de traitement logique des alarmes et de définition dynamique des priorités

C.1 Méthodes de logique de traitement d'alarmes

Parmi les méthodes qui ont été employées avec succès on trouve les suivantes:

– La logique peut être définie pour les systèmes de sûreté d'alarme, où tous les ensembles redondants du système de sûreté d'alarme peuvent apparaître ensemble. Un regroupement logique simple peut être efficacement utilisé. Un conditionnement logique plus complexe utilisant les verrouillages liés aux niveaux de puissance basse et intermédiaire, les signaux de demande et de compte rendu d'action des arrêts d'urgence et des fonctions de sûreté d'urgence avec d'autres signaux, peut être défini, pour permettre un mode d'exploitation sur une base continue. Certaines centrales ont mis à disposition des opérateurs, des positionneurs pour indiquer à la logique un mode d'exploitation. Le mode d'exploitation est alors utilisé par une logique Booléenne adaptée pour contrôler les suppressions d'alarmes et le partage des alarmes du système de sûreté avec les autres affichages d'alarmes. Des logiques équivalentes de regroupement, utilisant un composant temporel, ont été développées pour identifier les conditions d'arrêt d'urgence et le fonctionnement redondant de sûreté des centrales, pour vérifier qu'aucune centrale n'a démarré lorsque cela doit en être ainsi.

– La logique d'alarme peut être définie en utilisant les opérateurs logiques standards (ET, OU, NON, temporisation, etc.) qui sont mis en œuvre par les logiciels, pour filtrer les alarmes et déterminer à partir d'un état postulé (par exemple, de la pleine puissance à l'arrêt) et des conditions d'alarme, quelles alarmes doivent être montrées ou supprimées et quelles sont les priorités. Il convient de considérer la logique dynamiquement, et ne pas se limiter aux conditions statiques, pour que les changements affectant à tout instant les alarmes courantes ou l'absence d'une alarme attendue soient pris en compte pour réaliser une détermination logique et cohérente des conditions.

– La logique d'alarme peut être basée sur la signification relative de deux alarmes coexistantes, cette signification étant définie lors de la conception ou issue de l'expérience du site en exploitation. Lorsqu'une alarme apparaît, le système numérique vérifie les alarmes associées à la nouvelle alarme à l'aide d'une base de données d'alarmes associées. S'il n'y a pas d'alarme associée présente, la nouvelle alarme est classée comme significative et est présentée avec un haut niveau de priorité ou de signification. Si une alarme associée existe , et donc a déjà été affichée auparavant, alors la nouvelle alarme est classée avec une signification basse, et n'est pas affichée comme une alerte mais seulement comme une information.

Une logique utilisant des temporisations logicielles peut être développée pour contrôler une avalanche d'alarmes due à un arrêt d'urgence de la centrale ou à des pertes électriques.

C.2 Définition dynamique des priorités

C.2.1 Définition des priorités par les relations cause-conséquence

Les alarmes qui sont identifiées comme des causes principales peuvent être considérées comme de la plus haute priorité.

Annex C
(informative)

Examples of alarm processing logic and dynamic prioritisation

C.1 Methods for alarm processing logic

Methods, which have been used successfully, include the following:

– Logic may be defined for the safety system alarms, where each redundant set of safety system alarms may appear together. Simple grouping logic may be used effectively. More complex conditioning logic using the low power and intermediate power level interlocks, the trip or ESF demanded and the trip or ESF actuated signals, together with other signals, may be defined to derive an operating mode on a continuous basis. Some plants have used an operator switch to define an operating mode to the logic. The operating mode has then been used with suitable Boolean logic to control the alarm suppression and alarm sharing of safety system and other alarm displays. Similar grouping logic with a time component has been developed for identification of reactor trip conditions and operation of the redundant safety plant, to identify that plant has not started when it should have done so.

– Alarm logic may be defined using standard logic gates (AND, OR, NOT, timer, etc.) which are implemented in software, to filter alarms and to determine from a postulated plant state (i.e., full power through shutdown) and alarm condition, which alarms are to be shown or suppressed and at what priority. The logic should be considered in a dynamic manner, and not limited to static conditions, so that changes to the alarms existing at any time or failure of an expected alarm to appear will still cause consistent conditions to be determined by the logic.

– Alarm logic may be based on the relative significance of two co-existing alarms, with significance judged in design or added from site experience. When an alarm appears, the computer checks the alarms associated with the new alarm using a database of associated alarms. If no associated alarm exists, the new alarm is classed as significant and shown with high priority or significance. If an associated alarm already exists, and therefore has been displayed earlier, then the new alarm is classed with low significance, and not displayed as a warning but as information only.

Logic may be developed to control alarm avalanche due to major plant or electrical trips based on software timers.

C.2 Dynamic prioritisation

C.2.1 Prioritisation by cause-consequence relation

Alarms which are identified as major causes can be considered of higher priority.

Par exemple, si l'arrêt d'une pompe entraîne l'activation de «l'alarme arrêt de la pompe», «l'alarme perte du débit» ou «l'alarme bas niveau», «l'alarme arrêt de la pompe» est considérée comme celle de plus haute priorité, car elle est la cause première et les autres ne sont qu'entraînées par celle-ci.

Ce schéma cause/conséquence présente un inconvénient pour les opérateurs qui sont moins concernés par les causes, que par les conséquences qu'ils doivent gérer. Aussi le choix de la bonne priorité des alarmes liées aux conséquences dépend de l'ordre et du type des actions que les opérateurs doivent réaliser. Si l'action principale consiste à corriger les causes, et que la cause principale est clairement identifiée, il convient de donner la priorité la plus haute à l'alarme de la cause principale. Il peut même alors être approprié de supprimer les alarmes relatives aux conséquences, plutôt que de baisser leurs priorités.

C.2.2 Définition des priorités par l'importance de gravité – alarmes à seuils multiples

Pour un paramètre, qui a plusieurs alarmes à seuil, une alarme qui indique la condition la plus pénalisante est considérée comme celle de plus haute priorité.

Par exemple, une «alarme très bas niveau» est considérée comme de plus haute importance qu'une «alarme de bas niveau».

C.2.3 Définition des priorités par le contenu d'information

Les alarmes qui sont les conséquences naturelles d'actions les précédant (par exemple, arrêt d'urgence de la centrale) et qui indiquent que l'état des matériels est normal sont considérées comme fournissant une information d'état (par exemple, déviations prévues) plutôt que comme des anormalités (par exemple, déviations non prévues). Elles peuvent être considérées comme de plus bas niveau et il est recommandé de ne pas les considérer comme des alarmes véritables.

For instance, if a pump trip has caused activation of the ‘pump trip alarm,’ ‘loss of flow alarm,’ or ‘low level alarm,’ the ‘pump trip alarm’ is considered of higher priority since it is the root-cause and others are induced by it.

This scheme of cause/consequence has the disadvantage that operators may be more concerned with the consequences they have to compensate for than the causes. So the choice for the right priority of the consequential alarms therefore depends on the order and type of actions the operators are expected to perform. If the main action is to correct the cause, and the root cause is clearly identified, the higher priority should be given to the root cause alarm. It may then even be more appropriate to suppress the consequence alarms, instead of reducing their priority.

C.2.2 Prioritisation by importance of severity – multiple-threshold alarms

For a parameter, which has several alarm thresholds, an alarm which indicates the most severe condition is considered to be of higher priority.

For instance, a ‘low-low level alarm’ is considered of higher priority than a ‘low level alarm.’

C.2.3 Prioritisation by information content

Alarms that are natural consequences of some preceding actions (e.g., plant trip) and indicate that the corresponding equipment status is normal are considered to be providing status information (i.e. planned deviations) rather than abnormality (i.e. unplanned deviations). They can be considered of lower priority and should not be considered as true alarms.

Annexe D
(informative)

Exemple conceptuel de regroupement et de catégorisation des alarmes

Comme la centrale est généralement analysée et représentée en termes d'ensembles de fonctions qu'il faut contrôler (voir la CEI 61839), de façon à refléter les critères de conception de la production d'énergie électrique, tout en garantissant un comportement sûr du procédé physique, l'architecture cohérente d'un système d'alarme revient à organiser les alarmes de façon à refléter la structure fonctionnelle de la centrale.

Ainsi, les alarmes peuvent être regroupées par fonction de la centrale, et en descendant plus bas, par procédé, par système, par composant, etc., créant une hiérarchie pouvant être utilisée pour la définition des priorités et/ou pour la présentation:

Fonctions de la centrale => Procédés => Systèmes => Composants => Composants Supports.

Cette hiérarchie permet aux opérateurs de distinguer entre les différentes catégories d'alarmes:

– messages relatifs aux violations des principaux objectifs des fonctions de la centrale;
– messages relatifs aux dérangements des mécanismes procédés contrôlant une fonction;
– messages relatifs aux anormalités constatées dans les systèmes physiques conçus pour réaliser les mécanismes précédents;
– messages relatifs aux défaillances de matériels individuels au sein de ces systèmes;
– messages relatifs aux défaillances de systèmes auxiliaires.

Le plus haut niveau de regroupement est lié aux fonctions de la centrale; les fonctions suivantes sont des fonctions de contrôle typiques d'un Réacteur à Eau Pressurisée (REP):

– contrôle de la réactivité;
– contrôle de l'inventaire en eau du réacteur;
– contrôle de la turbine;
– contrôle de la distribution électrique, etc.

Chaque fonction de tranche est contrôlée par les actions de plusieurs mécanismes procédé; par exemple, un changement de pression réacteur peut être obtenu soit en modifiant la température réacteur, soit en modifiant la masse d'eau dans le pressuriseur, soit en modifiant le taux de transformation vapeur en liquide dans le pressuriseur, etc. Suivant la topologie décrite précédemment, ceci correspond au second niveau d'organisation des alarmes, à savoir le niveau procédés.

Un ou plusieurs systèmes physiques sont généralement mis en œuvre comme moyen de commande afin de gérer de tels mécanismes de procédé; par exemple, l'addition d'eau au système primaire peut être faite soit par le système d'appoint en eau du circuit primaire, soit par l'injection de sûreté, suivant les situations particulières. Suivant le type de structure spécifiée ci dessus, cela représente le troisième niveau d'organisation des alarmes, à savoir le niveau systèmes.

Un certain nombre de composants (pompes, réchauffeurs, vannes, ventilateurs, etc.) sont mis en œuvre au niveau de chaque système physique pour atteindre les objectifs visés par le système; le fonctionnement de ces composants est, à son tour, supporté par un ensemble de systèmes auxiliaires qui permettent aux différents composants de fonctionner correctement

Annex D
(informative)

Conceptual example of alarm grouping and categorisation

As the plant itself is generally analysed and represented in terms of a set of functions that must be controlled (see IEC 61839), in order to reflect the overall design criteria of producing electrical energy while ensuring a safe behaviour of the physical processes, a consistent alarm system architecture organises alarms so as to mirror the functional structure of the plant.

Alarms can therefore be grouped by plant functions and, going deeper, by processes, systems, components, etc., creating a hierarchy that can be used for prioritisation and/or presentation:

Plant functions => Processes => Systems => Components => Component supports.

This hierarchy allows operators to distinguish between several categories of alarms:

– messages relative to the violation of the plant functions' main goals;
– messages relative to disturbances in the mechanisms of the processes controlling the function;
– messages relative to abnormalities within physical systems designed to provide the above mechanisms;
– messages relative to failure of pieces of equipment within those systems;
– messages relative to a fault within the ancillary systems.

The highest grouping level is related to plant functions; some typical control functions of a Pressurised Water Reactor (PWR) are, for instance:

– reactivity control;
– reactor coolant inventory control;
– turbine control;
– electrical power distribution control, etc.

Each plant function is controlled through the action of several process mechanisms; for example, a change in the reactor pressure can be obtained either by changing the reactor temperature, or by modifying the amount of reactor water mass in the pressuriser, or by changing the steam-to-liquid water ratio in the pressuriser, etc. According to the above described topology, this is a second level of organising the alarms, i.e. in terms of processes.

One or more physical systems are generally provided to supply control means for the management of such process mechanisms; for example, addition of water to the primary system may be accomplished by either a reactor make-up water system, or by safety injection systems, according to the specific situation. According to the type of structure specified above, this represents a third level of organising alarms, i.e. in terms of systems.

In the context of each physical system, a number of components (pumps, heaters, valves, fans, etc.) operate to achieve the system's desired goals; the operation of these components is, in turn, supported by a set of ancillary systems which allow proper component performance

(par exemple, disponibilité de l'énergie électrique, de l'air comprimé, de l'eau de refroidissement, etc.). Ces deux domaines supplémentaires (composants et supports) forment d'autres niveaux d'organisation des alarmes, le niveau de composants et de composants supports des systèmes.

En conséquence, le format du système d'alarme ainsi structuré permet à l'opérateur d'observer les anomalies dans un contexte significatif, réduisant la charge liée à la sélection des informations importantes, lui permettant ainsi de les intégrer et d'en interpréter les résultats. Par exemple, si l'action d'un système auxiliaire, pour certaines raisons, dévie du comportement attendu, l'opérateur (au moyen d'une présentation appropriée) peut voir la perturbation associée dans le contexte opérationnel d'un composant donné, appartenant à un système particulier, qui participe en support à la mise en œuvre d'un certain procédé nécessaire pour commander une fonction particulière de la centrale.

Simultanément, alors qu'une alarme devient active, l'opérateur peut détecter au premier coup d'œil (ce qui est toujours le cas lorsque la présentation est structurée correctement), quelle fonction de la centrale est l'objet d'une perturbation procédé (par exemple, contrôle de la pression primaire: pression diminuant anormalement); alors il/elle peut savoir quel système est à l'origine de ce problème particulier (par exemple, système pressuriseur), et finalement quel est le composant ou le système auxiliaire touché (par exemple, fuite de la soupape de décharge du pressuriseur XXYY). Grâce au regroupement original, et avec l'aide du choix de présentation, on peut mettre immédiatement à disposition de l'opérateur une somme toujours plus importante d'informations significatives.

(for example, availability of electrical power, compressed air, cooling water, etc.). These two additional fields (components and their supports) form further levels of organising alarms, i.e. in terms of components and component support systems.

The resulting format of the alarm system structured in this manner consequently allows the operator to observe abnormalities in a very meaningful context, reducing the burden of selecting important information, integrating it and interpreting the results. For instance, if the action of an ancillary system is, for some reason, deviating from the expected behaviour, the operator (by means of a suitable presentation) can see the associated disturbance in the context of the operation of a given component, belonging to a specific system, which supports the performance of a certain process necessary to control a particular plant function.

At the same time, when an alarm becomes active, the operator can detect at a first glance (always if the presentation is properly structured), which plant function is the object of a particular process disturbance (e.g.: reactor coolant pressure control: pressure abnormally decreasing); then he/she can know which is the physical system originating the particular abnormality (e.g.: pressuriser system), and eventually which is the affected component and/or ancillary system (e.g.: pressuriser relief valve XXYY leaking). Thanks to the original grouping, and with the help of the presentation choice, increasing levels of meaningful information could be immediately available to operators.

Annexe E
(informative)

Eléments de base concernant la nécessité de distinguer entre les alarmes et l'information d'état

Généralement les systèmes d'alarme présentent trois différents types de données procédé en centrale:

– Données concernant ce qui est inquiétant ou anormal (par exemple, un message d'alarme réel indiquant aussi précisément que possible, la nature de l'anomalie).
– Données concernant ce que les systèmes automatisés (commande et protection) sont en train de faire (par exemple, démarrage de l'injection de sûreté – ce qui n'est pas une condition anormale, car l'injection de sûreté est conçue pour intervenir dans certain cas, si bien que son fonctionnement dans ces conditions est normal, c'est-à-dire, est attendu).
– Données concernant le fonctionnement en régime permanent de systèmes complexes (par exemple, aptitude des systèmes de sauvegarde à fonctionner). Ces messages, aussi, n'indiquent pas des anomalies, mais sont plutôt des confirmations pour l'opérateur qui se trouve dans des situations où l'activation (normale), telle que prévue à la conception, est demandée.

Généralement, le système d'alarme fournit deux types d'informations sur la base des distinctions précédentes:

– informations sur des situations non prévues;
– informations sur des situations prévues.

Ces deux types d'informations doivent être considérés différemment, car ils sont complémentaires: l'affichage de messages d'anomalie et l'affichage de messages qui ne sont pas liés à des anormalités, mais qui se rapporte à l'état d'un système important; dans les salles de commande classiques, les messages du second type sont très souvent utilisés et assimilés à des alarmes, car l'intervention, par exemple, du système de sauvegarde est associée à l'apparition d'une condition accidentelle. Le contenu informatif des messages d'état est important pour les opérateurs, mais leur fonction ne relève pas à proprement parler du système d'alarme. En conséquence la première exigence concernant la conception d'un système d'alarme est la suivante:

L'objectif de cette exigence est d'être complètement conforme au critère «panneau éteint», qui exige que le panneau d'affichage d'alarme soit éteint (aucun message d'alarme présent) lorsque la centrale fonctionne normalement, avec l'ensemble des systèmes dans leur configuration prévue. Les manquements dans l'application de ce concept sont les prémisses d'une surcharge potentielle des tâches opérateurs.

Annex E
(informative)

Material for the need of distinction between alarm and status information

Three different types of plant process data are typically presented by alarm systems:

– Data about what is alarming or abnormal (i.e. a true alarm message stating, as precisely as possible, the nature of the abnormality).
– Data about what the automatic systems (control and protection systems) are doing (e.g.: safety injection initiated – this is not an abnormal condition, because the safety injection is designed to intervene in certain situations; as such, its operation, in those conditions, is normal, i.e. what is expected).
– Data about the steady-state status of complex systems (e.g.: the pre-actuation readiness of a safeguard system to operate). These messages also do not indicate abnormalities but are rather confirmations for the operator in situations demanding their designed-for (normal) activation.

On the basis of the above distinctions, the alarm system typically provides two types of information:

– information about unplanned situations;
– information about planned situations.

These two types of information are to be distinctly considered, because they are complementary: display of abnormality messages and display of messages that do not include abnormalities, but refer to the status of some important system; in traditional control rooms the second type of message used very frequently to be assimilated to alarms, since the intervention, for instance, of a safeguard system was associated with the onset of a faulted condition. The information content of status messages is also important for operators, but the function is not properly speaking one coming from the alarm system. Consequently, the first requirement for alarm system design is the following:

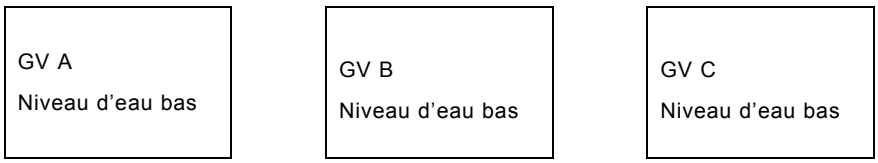
The goal of this requirement is to fully comply with the dark board criterion, which requires the alarm display panel to be unlit (no alarm messages present) when the plant is operating normally, with all systems in their expected configuration. Failure in the application of this concept creates the premises for a potential operator's task overload.

Annexe F
(informative)

Exemple de disposition des verrines

Les panneaux d'alarmes sont généralement situés sur la partie supérieure des pupitres.

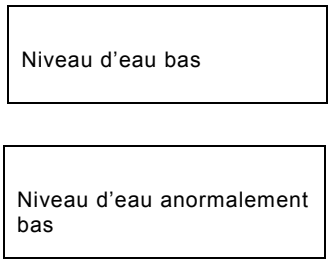
Les alarmes similaires dans un système sont rangées de la gauche vers la droite dans l'ordre alphabétique. Voir la Figure F.1.



IEC 1422/04

Figure F.1 – Modèle horizontal pour les verrines d'un système redondant

Afin d'indiquer la progression des alarmes dans un même système, haut-bas, vers le haut-vers le bas, etc., celles-ci sont rangées dans un ordre décroissant. Pour les cas ne correspondant pas à cela, les alarmes avec le plus haut degré d'importance sont placées en haut. Voir la Figure F.2.



IEC 1423/04

Figure F.2 – Modèle vertical pour les verrines d'un ensemble d'alarmes d'une importance différente

Si la transmission d'éléments constitutifs d'alarmes, qui ont habituellement le même degré d'utilisation et qui appartiennent au même système, varie d'un paramètre, alors la disposition suivra le principe suivant, du haut vers le bas, pression, niveau d'eau, température et débit.

Annex F
(informative)

Example of arrangement of alarm tiles

Alarm fascias are typically provided on the uppermost layer of the board.

Similar alarms within the same system are arranged from left to right in alphabetical order. See Figure F.1.

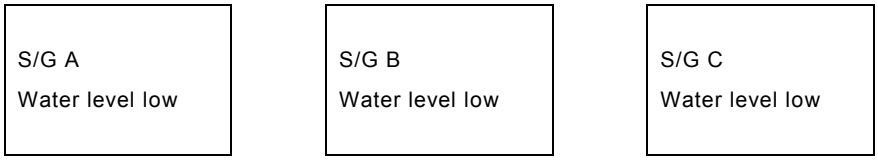


Figure F.1 – A horizontal layout of alarm tiles for redundant components

To indicate the progress of alarms within the same system, high-low, up-down, etc. are arranged in the top-bottom order. In the cases that do not correspond to this, the alarms with the higher degree of importance are placed on the top. See Figure F.2.

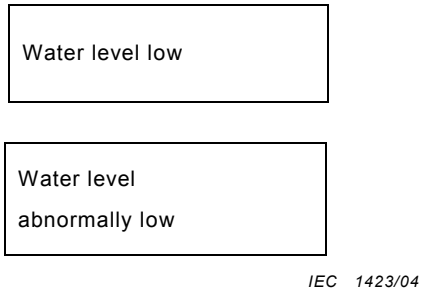


Figure F.2 – A vertical layout of alarm tiles for a set of alarms with different importance

If transmission elements of alarms that have the same degree of normal use and belong to the same system vary by parameter, arrangement will be made, in principle, from top to bottom in the order of pressure, water level, temperature, and flow rate.

Annexe G
(informative)

Exemples de points à considérer pour la catégorisation des alarmes

Les alarmes se situent normalement en catégorie C ou sont non classées au sens de la CEI 61226. Cependant, certaines alarmes peuvent être affectées à des catégories supérieures.

Les facteurs suivants peuvent être considérés pour la catégorisation des alarmes:

a) Il peut y avoir quelques alarmes liées à des conditions rares et qui sont nécessaires à la sûreté. Il convient de les considérer avec l'enchaînement dans le temps des actions opérateur.

b) Il peut y avoir certaines alarmes qui demandent la réalisation de certaines actions manuelles après une demande d'arrêt d'urgence pour garantir l'arrêt du réacteur. Il convient de les considérer avec l'enchaînement dans le temps des actions opérateur.

c) Il y a généralement des alarmes qui alertent l'opérateur que le système de sûreté, les fonctions techniques de sûreté ou leurs systèmes supports sont partiellement indisponibles ou défaillants ou n'ont pas fonctionné comme demandé.

d) Il peut y avoir des alarmes supports de la sûreté ou qui réduisent la fréquence des conditions défectueuses du réacteur, telles que celles liées aux commandes de systèmes automatiques pour le contrôle des conditions de puissance normale ou pour le contrôle de l'alimentation en eau de secours ou pour l'arrêt.

e) Il peut y avoir des alarmes qui alertent le personnel d'un risque procédé, ou d'un rejet d'activité, telles que celles liées au chauffage ou à la ventilation de la salle de commande ou celles du système de surveillance de l'environnement.

f) Il convient de prendre en compte le besoin d'enregistrement des alarmes pour pouvoir analyser après chaque arrêt d'urgence ou défaut.

g) La majorité des alarmes du réacteur de la centrale et des sources électriques supports n'ont pas de lien direct avec la sûreté du réacteur, mais elles peuvent être liées à la réduction de la fréquence des incidents réacteur.

h) Les alarmes liées à la partie conventionnelle de la centrale et à ses sources électriques supports, ainsi que celles du système électrique associé à la génération d'énergie ne sont normalement pas liées à la sûreté du réacteur, par contre il convient de les prendre en compte lors de la conception.

Annex G
(informative)

Examples of points to consider in the categorisation of alarms

Alarms are normally either category C or unclassified in IEC 61226. However, some alarms can be associated with higher categories.

The following factors may be considered in the categorisation of alarms:

a) There can be some alarms for infrequent conditions which are needed for safety. These should be considered in association with the timescale of action needed by the operator.

b) There can be some alarms which require some manual actions after a trip to ensure successful shutdown. These should be considered in association with the timescale of action needed by the operator.

c) There are usually alarms which warn that the safety system, engineered safety features (ESF) or their support systems are partially unavailable or faulty, or have failed to operate as required.

d) There can be alarms which support safety or reduce the frequency of reactor fault conditions, such as those of the automatic control systems for control of normal power conditions or control of emergency or shutdown feedwater.

e) There can be alarms which warn personnel of process hazard, or activity release, such as those from a control room heating and ventilation system or from the environmental monitoring system.

f) The need to record alarms for analysis after any reactor trip or fault should be considered.

g) The majority of the alarms from the reactor plant and its supporting electrical supplies do not have any direct association with reactor safety, but they may have some association with reducing the frequency of reactor faults.

h) The alarms from the conventional plant and its supporting electrical supplies, and from the electrical systems associated with outgoing power generation do not normally have any reactor safety association, but this should be considered in the design.

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

- purchasing agent ❑
- librarian ❑
- researcher ❑
- design engineer ❑
- safety engineer ❑
- testing engineer ❑
- marketing specialist ❑

other.....

Q3 I work for/in/as a: *(tick all that apply)*

- manufacturing ❑
- consultant ❑
- government ❑
- test/certification facility ❑
- public utility ❑
- education ❑
- military ❑

other.....

Q4 This standard will be used for: *(tick all that apply)*

- general reference ❑
- product research ❑
- product design/development ❑
- specifications ❑
- tenders ❑
- quality assessment ❑
- certification ❑
- technical documentation ❑
- thesis ❑
- manufacturing ❑

other.....

Q5 This standard meets my needs: *(tick one)*

- not at all ❑
- nearly ❑
- fairly well ❑
- exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

- standard is out of date ❑
- standard is incomplete ❑
- standard is too academic ❑
- standard is too superficial ❑
- title is misleading ❑
- I made the wrong choice ❑

other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

- French text only ❑
- English text only ❑
- both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Enquête sur les normes

La CEI ambitionne de vous offrir les meilleures normes possibles. Pour nous assurer que nous continuons à répondre à votre attente, nous avons besoin de quelques renseignements de votre part. Nous vous demandons simplement de consacrer un instant pour répondre au questionnaire ci-après et de nous le retourner par fax au +41 22 919 03 00 ou par courrier à l'adresse ci-dessous. Merci !

Centre du Service Clientèle (CSC)

Commission Electrotechnique Internationale
3, rue de Varembé
1211 Genève 20
Suisse

ou

Télécopie: **CEI**/CSC +41 22 919 03 00

Nous vous remercions de la contribution que vous voudrez bien apporter ainsi à la Normalisation Internationale.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Centre du Service Clientèle (CSC)
Commission Electrotechnique Internationale
3, rue de Varembé
1211 GENÈVE 20
Suisse

Q1 Veuillez ne mentionner qu'**UNE SEULE NORME** et indiquer son numéro exact: (*ex. 60601-1-1)*

.....

Q2 En tant qu'acheteur de cette norme, quelle est votre fonction?
(cochez tout ce qui convient)
Je suis le/un:

agent d'un service d'achat ❑
bibliothécaire ❑
chercheur ❑
ingénieur concepteur ❑
ingénieur sécurité ❑
ingénieur d'essais ❑
spécialiste en marketing ❑
autre(s).....

Q3 Je travaille:
(cochez tout ce qui convient)

dans l'industrie ❑
comme consultant ❑
pour un gouvernement ❑
pour un organisme d'essais/ certification ❑
dans un service public ❑
dans l'enseignement ❑
comme militaire ❑
autre(s).....

Q4 Cette norme sera utilisée pour/comme
(cochez tout ce qui convient)

ouvrage de référence ❑
une recherche de produit ❑
une étude/développement de produit ❑
des spécifications ❑
des soumissions ❑
une évaluation de la qualité ❑
une certification ❑
une documentation technique ❑
une thèse ❑
la fabrication ❑
autre(s).....

Q5 Cette norme répond-elle à vos besoins:
(une seule réponse)

pas du tout ❑
à peu près ❑
assez bien ❑
parfaitement ❑

Q6 Si vous avez répondu PAS DU TOUT à Q5, c'est pour la/les raison(s) suivantes:
(cochez tout ce qui convient)

la norme a besoin d'être révisée ❑
la norme est incomplète ❑
la norme est trop théorique ❑
la norme est trop superficielle ❑
le titre est équivoque ❑
je n'ai pas fait le bon choix ❑
autre(s) .....

Q7 Veuillez évaluer chacun des critères ci-dessous en utilisant les chiffres
(1) inacceptable,
(2) au-dessous de la moyenne,
(3) moyen,
(4) au-dessus de la moyenne,
(5) exceptionnel,
(6) sans objet

publication en temps opportun .....
qualité de la rédaction.....
contenu technique .....
disposition logique du contenu .....
tableaux, diagrammes, graphiques, figures.....
autre(s) .....

Q8 Je lis/utilise: *(une seule réponse)*

uniquement le texte français ❑
uniquement le texte anglais ❑
les textes anglais et français ❑

Q9 Veuillez nous faire part de vos observations éventuelles sur la CEI:

.....
.....
.....
.....
.....
.....

ISBN 2-8318-7711-3

ICS 27.120.20

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND