NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60231A

Première édition
First edition
1969-01

Premier complément à la Publication 60231 (1967)

Principes généraux de l'instrumentation des réacteurs nucléaires

First supplement to Publication 60231 (1967)

General principles of nuclear reactor instrumentation

Numéro de référence
Reference number
CEI/IEC 60231A: 1969

Numéros des publications

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

Publications consolidées

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

Validité de la présente publication

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

Des renseignements relatifs à la date de reconfirmation de la publication sont disponibles dans le Catalogue de la CEI.

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

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

Terminologie, symboles graphiques et littéraux

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

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

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

Numbering

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

Consolidated publications

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

Validity of this publication

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

Information relating to the date of the reconfirmation of the publication is available in the IEC catalogue.

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

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

Terminology, graphical and letter symbols

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

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

* See web site address on title page.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60231A

Première édition
First edition
1969-01

Premier complément à la Publication 60231 (1967)

Principes généraux de l'instrumentation des réacteurs nucléaires

First supplement to Publication 60231 (1967)

General principles of nuclear reactor instrumentation

International Electrotechnical Commission 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 e-mail: inmail@iec.ch IEC web site http: //www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE Q

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

COMPLÉMENT A LA PUBLICATION 231 (1967)

PRINCIPES GÉNÉRAUX DE L'INSTRUMENTATION DES RÉACTEURS NUCLÉAIRES

PRÉAMBULE

1) Les décisions ou accords officiels de la C E I en ce qui concerne les questions techniques, préparés par des Comités d'Etudes où sont représentés tous les Comités nationaux s'intéressant à ces questions, expriment dans la plus grande mesure possible un accord international sur les sujets examinés.

2) Ces décisions constituent des recommandations internationales et sont agréées comme telles par les Comités nationaux.

3) Dans le but d'encourager cette unification internationale, la C E I exprime le vœu que tous les Comités nationaux ne possédant pas encore de règles nationales, lorsqu'ils préparent ces règles, prennent comme base fondamentale de ces règles les recommandations de la C E I dans la mesure où les conditions nationales le permettent.

4) On reconnaît qu'il est désirable que l'accord international sur ces questions soit suivi d'un effort pour harmoniser les règles nationales de normalisation avec ces recommandations dans la mesure où les conditions nationales le permettent. Les Comités nationaux s'engagent à user de leur influence dans ce but.

PRÉFACE

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

Elle constitue le premier complément à la Publication 231 de la CEI: Principes généraux de l'instrumentation des réacteurs nucléaires.

Elle contient les textes des articles 5 et 8 restés à l'étude. Des projets de ces articles furent discutés lors de la réunion tenue à Tel-Aviv en 1966, à la suite de laquelle un projet définitif fut soumis à l'approbation des Comités nationaux suivant la Règle des Six Mois en février 1967.

Les pays suivants se sont prononcés explicitement en faveur de la publication:

Allemagne	Japon
Australie	Pays-Bas
Belgique	Pologne
Danemark	Roumanie
Etats-Unis d'Amérique	Royaume-Uni
Finlande	Suède
France	Suisse
Israël	Turquie
Italie	Union des Républiques Socialistes Soviétiques

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SUPPLEMENT TO PUBLICATION 231 (1967)

GENERAL PRINCIPLES OF NUCLEAR REACTOR INSTRUMENTATION

FOREWORD

1) The formal decisions or agreements of the I E C on technical matters, prepared by Technical Committees on which all the National Committees having a special interest therein are represented, express, as nearly as possible, an international consensus of opinion on the subjects dealt with.

2) They have the form of recommendations for international use and they are accepted by the National Committees in that sense.

3) In order to promote this international unification, the I E C expresses the wish that all National Committees having as yet no national rules, when preparing such rules, should use the I E C recommendations as the fundamental basis for these rules in so far as national conditions will permit.

4) The desirability is recognized of extending international agreement on these matters through an endeavour to harmonize national standardization rules with these recommendations in so far as national conditions will permit. The National Committees pledge their influence towards that end.

PREFACE

This Publication has been prepared by Sub-Committee 45A, Reactor Instrumentation, of IEC Technical Committee No. 45, Nuclear Instrumentation.

It constitutes the first supplement to IEC Publication 231, General Principles of Nuclear Reactor Instrumentation.

It contains the texts of Clauses 5 and 8 which were still under consideration. Drafts of these clauses were discussed at the meeting held in Tel-Aviv in 1966, as a result of which a final draft was submitted to the National Committees for approval under the Six Months' Rule in February 1967.

The following countries voted explicitly in favour of publication:

Australia	Netherlands
Belgium	Poland
Denmark	Romania
Finland	Sweden
France	Switzerland
Germany	Turkey
Israel	Union of Soviet Socialist Republics
Italy	United Kingdom
Japan	United States of America

COMPLÉMENT A LA PUBLICATION 231 (1967)

PRINCIPES GÉNÉRAUX DE L'INSTRUMENTATION DES RÉACTEURS NUCLÉAIRES

---

5. Système de protection

5.1 *Définitions*

5.1.1 *Remarques préliminaires*

a) Dans le texte français de la Publication 231, le mot « équipement » a été parfois employé dans le sens du terme « système » tel qu'il est défini ci-dessous.

b) Les définitions suivantes sont établies pour les besoins du présent article.

5.1.2 *Système*

Association d'équipements, d'ensembles, de sous-ensembles ou d'éléments fonctionnels étudiés, interconnectés et utilisés suivant une doctrine définie pour atteindre un but déterminé.

Exemple: le système de commande et de contrôle d'une installation industrielle.

Note. — Le concept de « système » comprend l'organisation et les procédés aussi bien que le matériel.

5.1.3 *Système de protection*

Système dont le rôle est uniquement d'empêcher le fonctionnement d'un réacteur hors des limites sûres spécifiées ou de réduire les conséquences du franchissement de ces limites. Le système de protection comprend le système d'arrêt d'urgence de sécurité et, le cas échéant, le système de confinement, le système de refroidissement de secours, etc.

5.1.4 *Système d'arrêt d'urgence de sécurité*

Partie du système de protection commandant l'arrêt rapide du réacteur.

5.1.5 *Système de verrouillage de sécurité*

Partie du système de protection permettant l'exécution de certaines manœuvres intéressant la sécurité du réacteur seulement dans le cas où les conditions prescrites sont remplies.

5.1.6 *Système de délestage de puissance de sécurité (système de sécurité d'action programmée)*

Partie du système de protection qui commande et contrôle suivant un programme une réduction limitée de puissance.

5.1.7 *Système de signalisation d'ordre de sécurité*

Partie du système de protection qui comprend la totalité des signalisations d'ordre de sécurité (voir les limitations au paragraphe 5.4.5).

5.1.8 *Signalisation d'ordre de sécurité*

Signalisation qui exige, de la part de l'opérateur, une action protectrice nécessaire.

SUPPLEMENT TO PUBLICATION 231 (1967)

GENERAL PRINCIPLES OF NUCLEAR REACTOR INSTRUMENTATION

---

5. Protection system

5.1 *Definitions*

5.1.1 *Preliminary comments*

a) In the French text of Publication 231, the word "équipement" has been used sometimes with the sense of "system" as defined below.

b) For the purpose of this clause, the following definitions are established.

5.1.2 *System*

An association of equipments, assemblies, sub-assemblies or units, designed, interconnected and used to perform a determined objective.

For example: the control system of an industrial plant.

Note. — The concept of " system " includes organization and procedures as well as hardware.

5.1.3 *Protection system*

The system which acts only to prevent the reactor conditions from exceeding specified safe limits or reduce the consequences of their being exceeded. The protection system includes the safety shutdown system and, where provided, the containment isolation system, the system which initiates emergency cooling, etc.

5.1.4 *Safety shutdown system*

That part of a protection system which initiates a rapid shutdown of the reactor.

5.1.5 *Safety interlock system*

That part of a protection system which permits certain operations affecting reactor safety only when prescribed conditions exist.

5.1.6 *Safety power cutback system (programmed action safety system)*

That part of a protection system which controls a limited decrease of power according to a programme.

5.1.7 *Safety alarm system*

That part of a protection system which comprises the totality of all safety alarms (see the limitations in Sub-clause 5.4.5).

5.1.8 *Safety alarm*

An alarm function which calls for necessary protective action by the operator.

5.1.9 *Ensemble de mesure et surveillance de sécurité*

Ensemble de mesure et surveillance utilisé pour la sécurité du réacteur. Un ensemble de mesure et surveillance de sécurité comprend le transducteur, les sous-ensembles de traitement du signal et de discrimination (qui convertissent un signal analogique en un signal logique « tout ou rien »), les liaisons par câbles et le circuit de sortie.

Exemple: un thermocouple alimentant un amplificateur à seuil de température et comportant un relais à la sortie.

Note. — Plusieurs ensembles de mesure et surveillance de sécurité peuvent être utilisés pour chaque grandeur physique de manière à obtenir la redondance nécessaire.

5.1.10 *Ensemble logique de sécurité*

Ensemble relié à un ou plusieurs ensembles de mesure et surveillance de sécurité, et destiné à élaborer une fonction logique et à fournir un signal de commande à un ou plusieurs ensembles terminaux.

5.1.11 *Ensemble terminal*

Ensemble qui reçoit des signaux de commande d'un ou plusieurs ensembles logiques de sécurité et qui commande et contrôle directement une action de sécurité.

Exemples: ensemble terminal d'arrêt;
ensemble terminal de délestage;
ensemble terminal de refroidissement de secours.

5.1.12 *Défaillance non dangereuse*

Avarie du système de protection qui augmente la probabilité d'une action de sécurité adéquate, si une anomalie de fonctionnement du réacteur vient à se produire.

5.1.13 *Défaillance dangereuse*

Avarie qui réduit la probabilité d'une action de sécurité adéquate par le système de protection, si une anomalie de fonctionnement du réacteur vient à se produire.

5.1.14 *Arrêt d'urgence intempestif*

Arrêt d'urgence en l'absence d'anomalie du réacteur. L'arrêt intempestif peut survenir lorsque se produisent une ou plusieurs défaillances non dangereuses dans le système de protection.

5.1.15 *Déclenchement*

Basculement du signal de sortie d'un élément bistable de son état normal à son état complémentaire.

Dans la présente recommandation, l'état « normal » correspond à l'exploitation du réacteur à l'intérieur de limites sûres spécifiées, et l'état « complémentaire » correspond à une situation qui nécessite une action de sécurité. D'où:

a) Déclenchement d'un ensemble de mesure et surveillance de sécurité

Basculement vers son état complémentaire d'un ou plusieurs signaux de sortie d'éléments bistables (par exemple signalisation, délestage, arrêt d'urgence) d'un ensemble de mesure et surveillance de sécurité.

b) Déclenchement d'un ensemble logique de sécurité

Basculement vers son état complémentaire du signal ou des signaux de sortie d'un ensemble logique de sécurité.

5.1.9 *Safety monitoring assembly*

A monitoring assembly used for reactor safety. A safety monitoring assembly typically comprises the sensor, signal processing and discriminating sub-assemblies (which convert an analogue signal into an on-off signal), intermediate cabling and output circuit.

For example: a thermocouple feeding into a temperature trip amplifier with a relay output stage

Note. — Several safety monitoring assemblies may be used for each variable to provide the necessary redundancy

5.1.10 *Safety logic assembly*

An assembly connected to one or more safety monitoring assemblies and designed to perform a logical function and give a command signal to one or more final assemblies.

5.1.11 *Final assembly*

An assembly which accepts command signals from one or more safety logic assemblies and directly controls safety action.

For example: shutdown final assembly;
cutback final assembly;
emergency cooling final assembly.

5.1.12 *Safe failure*

A failure in the protection system which increases the probability of appropriate safety action should an abnormal condition arise on the reactor.

5.1.13 *Unsafe failure*

A failure which reduces the probability of appropriate safety action by the protection system should an abnormal condition arise on the reactor.

5.1.14 *Spurious shutdown*

A shutdown initiated when there is no abnormal condition in the reactor. It may arise as a result of one or more safe failures in the protection system.

5.1.15 *Trip*

Switching of a device with two stable states from its normal state to its non-normal state.

In this Recommendation, the "normal" state corresponds to an operational reactor condition within specified safe limits and the "non-normal" state corresponds to a condition which calls for safety action. Hence:

a) Safety monitoring assembly trip

Switching to its non-normal state of one or more bistable output signals (e.g. alarm, cut-back, safety shutdown) of a safety monitoring assembly.

b) Safety logic assembly trip

Switching to its non-normal state of the output signal or signals of a safety logic assembly.

5.1.16 *Niveau de déclenchement*

Valeur mesurée d'une grandeur physique à laquelle est déclenchée l'action de protection.

5.1.17 *Marge de déclenchement*

Différence entre la valeur mesurée d'une grandeur physique et celle du niveau de déclenchement associé à cette grandeur physique.

5.1.18 *Réarmement*

Basculement du signal de sortie d'un élément bistable de son état complémentaire à son état normal.

5.1.19 *Inhibition d'exploitation*

Suppression voulue, pour des raisons liées à l'exploitation du réacteur, de l'action d'une partie du système de protection qui remplit une fonction déterminée.

Exemple : un court-circuit peut être réalisé entre les contacts d'un relais à la sortie d'un ensemble de mesure et surveillance de sécurité.

5.1.20 *Redondance*

Accumulation de moyens identiques pour remplir une fonction donnée, de telle sorte que la défaillance d'un seul moyen (ou d'un nombre maximal spécifié de moyens) n'entraîne pas la défaillance de la fonction.

5.2 *Echelle des valeurs de cette recommandation*

Le choix des formes verbales utilisées dans la présente recommandation implique l'échelle suivante de valeurs:

5.2.1 *Obligation*

— en anglais: « shall » ou « must »;
— en français: verbe au temps futur ou bien à l'infinitif présent complété exclusivement par le verbe « devoir » au futur.

5.2.2 *Recommandation*

— en anglais: « should »;
— en français: « devrait ».

5.2.3 *Méthode acceptable, exemple de pratique courante*

— en anglais: « may »;
— en français: « peut » ou le mode conditionnel d'un autre verbe que « devoir ».

Ou bien encore, on peut noter que telle recommandation est une « méthode acceptable » ou un « exemple de pratique courante ».

5.1.16 *Trip level*

That measured value of a variable at which protective action is initiated.

5.1.17 *Trip margin*

The difference between the measured value of a variable and a trip level associated with this variable.

5.1.18 *Reset*

Switching of a device with two stable states from its non-normal state to its normal state.

5.1.19 *Operational bypass*

A deliberate inhibition for operational reasons of the action of a part of the protection system performing a specific function.

For example : a short-circuit may be applied across the contacts of a relay at the output of a safety monitoring assembly.

5.1.20 *Redundancy*

The existence of more than one means of performing a given function such that failure of one (or a stated maximum number) of the means does not induce failure of the function.

5.2 *Interpretation of this Recommendation*

The moods of verbs used in this Recommendation have the following implications:

5.2.1 *Mandatory*

— in English: "shall" or "must";
— in French: verb in the future tense or else in the present infinitive completed exclusively by the verb "devoir" in the future.

5.2.2 *Recommendation*

— in English: "should";
— in French: "devrait".

5.2.3 *Acceptable method, example of good practice*

— in English: "may";
— in French: "peut" or the conditional mood of a verb other than "devoir".

Alternatively, the item may be titled "acceptable method" or "example of good practice".

5.3 *Introduction*

5.3.1 Le rôle du système de protection d'un réacteur est d'empêcher le fonctionnement de celui-ci hors des limites sûres spécifiées ou de réduire les conséquences du franchissement de ces limites dans le cas où se produit une avarie de matériel, une erreur de conduite ou d'autres anomalies. L'élaboration de la définition des limites sûres pour un réacteur donné sort du cadre de cette recommandation.

5.3.2 Le système de protection du réacteur déclenche les actions de sécurité appropriées à l'endroit et au moment où elles sont nécessaires et garantit la disponibilité des fonctions indispensables à la sécurité de ce réacteur. L'étendue des possibilités offertes par le système de protection est déterminée par la prise en considération des facteurs « sûreté » et « économie ». Par exemple, les réacteurs de faible puissance peuvent ne pas nécessiter tous les systèmes décrits dans cette recommandation.

5.3.3 La sécurité et l'efficacité d'un système de protection correctement conçu peuvent être compromises à la suite de méthodes défectueuses d'entretien ou de vérification. Il est essentiel à la sécurité de l'installation que de telles procédures soient étudiées, fixées et exécutées de manière adéquate. Il est essentiel aussi d'obtenir un haut niveau de qualité dans la fabrication et l'installation du matériel.

5.3.4 Des possibilités de protection supplémentaires peuvent devoir être prévues pour des circonstances particulières, par exemple lors du chargement initial du combustible, des essais de recette, du rechargement du combustible et de l'entretien. Même si ces dispositifs ont un caractère temporaire, ils devront remplir les conditions édictées pour le système de protection.

5.3.5 Pour les besoins de la présente recommandation, on considère que le système de protection comprend tout l'équipement depuis le capteur jusqu'aux ensembles terminaux, mais ne comprend pas les barres de commande et de contrôle et leurs mécanismes ni les autres mécanismes de sécurité.

5.4 *Fonctions du système de protection*

5.4.1 *Généralités*

Pendant son exploitation normale, un réacteur est commandé et contrôlé manuellement et/ou par un certain nombre de systèmes de commande et de contrôle automatiques. Cependant, en cas d'anomalies de fonctionnement, des régimes transitoires pourraient survenir, conduisant à endommager le réacteur et créant une situation potentiellement dangereuse. L'opérateur et/ou le système de commande et de contrôle automatique peuvent être capables de maîtriser des régimes transitoires à évolution lente; mais, pour garantir l'installation contre des régimes transitoires à évolution rapide et contre des manœuvres incorrectes ou des défauts du système de commande et de contrôle, l'ultime action de protection devra être automatique et, dans toute la mesure du possible, avoir priorité sur toute manœuvre d'opérateur. Pour protéger le réacteur dans ces conditions, un certain nombre de grandeurs physiques essentielles à sa protection sont mesurées et surveillées continuellement et les signaux de sortie des appareils correspondants sont envoyés dans le système de sécurité approprié du réacteur.

En cas d'anomalies de fonctionnement, le système de sécurité engendre automatiquement l'action adéquate telle qu'un arrêt d'urgence du réacteur. De plus, pour quelques cas d'incidents, ces signaux peuvent être utilisés pour engendrer d'autres actions de sécurité, par exemple la mise en œuvre du refroidissement de secours.

5.3 *Introduction*

5.3.1 The purpose of a reactor protection system is to prevent reactor conditions exceeding safe specified limits or reduce the consequences of their being exceeded, in the event of equipment failure or operational error or other abnormal conditions. The establishment of what constitutes safe limits for a particular reactor is outside the scope of this Recommendation.

5.3.2 The reactor protection system takes appropriate safety action where and when needed and ensures the availability of services essential to reactor safety. The extent of the facilities afforded by the protection system are determined by appropriate consideration of safety and economics. For example, low power reactors may not require all the systems described in this Recommendation.

5.3.3 The safety and availability of a properly designed protection system can be compromised as a result of poor maintenance and test procedures. Adequate design, documentation and administration of such procedures are essential to the safety of the plant. A high standard of workmanship in manufacture and installation is essential.

5.3.4 Additional protection facilities may have to be provided in special circumstances, for example initial fuel loading, commissioning, refuelling, maintenance. Even if these facilities are of a temporary nature, they shall comply with the protection system requirements.

5.3.5 For the purpose of this Recommendation, the protection system is considered to include all equipment from the sensor to the final assemblies but not including the control rods and their actuators or other safety mechanisms.

5.4 *Functions within protection system*

5.4.1 *General*

During normal operation, a reactor is controlled by manual operation and/or a number of automatic control systems. However, under abnormal conditions, transients could occur which would lead to damage to the reactor and potentially hazardous conditions. The operator and/or the automatic control system may be able to deal with slow transients, but to guard against fast transients and incorrect operation or failures in the control system the ultimate protection shall be automatic and, as far as possible, override any operator action. To protect the reactor under these conditions, a number of variables essential to reactor protection are monitored continuously, and the output signals of these initiating devices are fed into the appropriate specific reactor safety system.

Under abnormal conditions, the safety system initiates automatically the appropriate safety action such as rapidly shutting down the reactor. In addition, for some incidents, these signals may be required to initiate other safety actions, for example the introduction of emergency cooling.

Le système de protection peut comprendre plusieurs systèmes de sécurité tels que:

— le système d'arrêt d'urgence de sécurité;
— le système de délestage de sécurité;
— le système de verrouillage de sécurité;
— le système de signalisation d'ordre de sécurité.

Les différents systèmes de sécurité sont considérés comme comprenant la totalité des organes depuis les capteurs jusqu'aux boîtes de raccordement des appareils de commande mécanique. On devra s'assurer, en étudiant de tels systèmes, que leurs fonctions n'ont pas d'interactions contraires et ne sont pas influencées par d'autres systèmes.

Certains accidents, pour quelques types de réacteurs (particulièrement des accidents dans lesquels se produit une rupture de l'enceinte de pression primaire), ont des conséquences éventuelles qui ne peuvent être convenablement réduites par l'arrêt d'urgence seul du réacteur. En pareil cas, l'ultime protection doit être assurée par d'autres moyens tels que le confinement.

Le système de protection peut, par conséquent, comprendre l'instrumentation et l'équipement associé au confinement. Le système de confinement de sécurité devrait comporter des ensembles de mesure et surveillance de sécurité et/ou des ensembles logiques de sécurité pour le mettre en action, par exemple pour fermer les valves d'isolement. La conception du système de confinement de sécurité devrait respecter les recommandations générales pour le système de protection, paragraphe 5.6, et celles du paragraphe 5.7.1 qui lui sont applicables.

Des inhibitions d'exploitation peuvent être prévues pour empêcher l'action d'une partie du système de protection, ce qui peut être nécessaire à l'exploitation du réacteur (voir paragraphe 5.11).

Des signalisations de défauts, examinées à l'article 8, sont nécessaires pour donner des indications sur l'origine de l'anomalie qui a occasionné l'action de sécurité; une analyse de ces signalisations peut être utile à l'opérateur pour guider ses réactions.

5.4.2 *Système d'arrêt d'urgence de sécurité*

Le système d'arrêt d'urgence de sécurité assure la protection du réacteur en déclenchant l'insertion automatique d'antiréactivité. Cette insertion devra être d'une amplitude et d'une rapidité telles qu'elle entraîne l'arrêt d'urgence du réacteur, cette action étant d'une fiabilité convenable dans toutes les conditions possibles d'accidents. On doit cependant reconnaître que certains accidents très improbables, par exemple ceux qui sont dus à des défauts catastrophiques, pourraient provoquer des régimes transitoires que le système d'arrêt d'urgence de sécurité ne pourrait juguler pour protéger le réacteur. Savoir si de tels accidents sont plausibles et si leurs conséquences sont acceptables sort du cadre de la présente recommandation.

L'insertion d'antiréactivité pour provoquer un arrêt d'urgence du réacteur peut être effectuée de différentes manières. Dans cette publication, les recommandations s'appliquent seulement à un système normal d'arrêt d'urgence de sécurité déclenchant automatiquement l'arrêt du réacteur au moyen des signaux issus des ensembles de mesure et surveillance de sécurité et des ensembles logiques de sécurité. Les systèmes de secours pour commander l'arrêt, qui utilisent des dispositifs annexes, fusibles et empoisonnement du réacteur, sortent du cadre de cette recommandation.

Un moyen manuel de déclencher l'arrêt du réacteur devra être prévu à titre de sécurité complétant l'action automatique du système d'arrêt d'urgence de sécurité.

5.4.3 *Système de délestage de puissance de sécurité*

Pour réduire le nombre des arrêts d'urgence de sécurité du réacteur et les inconvénients qui en découlent (par exemple indisponibilité, empoisonnement passager, choc thermique sur l'installation), on adopte quelquefois un dispositif de délestage qui réduit la puissance du réacteur en le contrôlant suivant un programme donné. Lorsque le système de délestage de puissance est consi-

The protection system may comprise specific safety systems such as:

— the safety shutdown system;
— the safety power cut-back system;
— the safety interlock system;
— the safety alarm system.

The various safety systems are deemed to comprise the whole of the equipment from the sensors to the input terminals of the actuating devices. Provision shall be made in the design of these systems to ensure that their functions do not interact adversely and are not influenced by other systems.

Certain accidents in some reactors (particularly those accidents associated with failure of the primary pressure enclosure) involve possible consequences which cannot be adequately reduced by reactor shutdown alone. In such cases, ultimate protection must be provided by other means such as containment.

The protection system may therefore include instrumentation and equipment associated with containment. The containment safety system should include safety monitoring assemblies and/or safety logic assemblies to initiate its operation, for example the closure of isolating valves. The design of the containment safety system should be in accordance with the general recommendations for the protection system in Sub-clause 5.6 and where appropriate Sub-clause 5.7.1.

Operational bypasses may be provided to inhibit the action of a part of a protection system as a necessary function of the reactor operation (see Sub-clause 5.11).

Alarms, considered in Clause 8, are required to give indication of the abnormal condition which precipitated the safety action and an analysis of these alarms may be used to determine subsequent operator action.

5.4.2 *Safety shutdown system*

The safety shutdown system ensures protection of the reactor by the automatic insertion of negative reactivity. This shall be of such a magnitude and speed as to shut down the reactor with an adequate reliability of action under all accident conditions. It is nevertheless recognized that certain very unlikely accidents, for example those due to catastrophic failures, could induce transients beyond the capability of the safety shutdown system to protect the reactor. Judgments regarding the credibility of such accidents, and the tolerability of their consequences, are beyond the scope of this Recommendation.

The insertion of negative reactivity to bring about a reactor shutdown may be performed in a number of ways. In this Publication, recommendations are given only for a normal safety shutdown system in which the reactor is shutdown automatically as a result of signals from the safety monitoring and logic assemblies. Back-up shutdown systems using secondary shutdown devices, fuses and poisoning, are outside the scope of this Recommendation.

As an additional safeguard to the automatic shutdown action of the safety shutdown system, a manually operated reactor safety shutdown device shall be provided.

5.4.3 *Safety power cut-back system*

To minimize the number of reactor safety shutdowns and their attendant inconveniences (for example — loss of availability, transitory poisoning, thermal shock on plant), a cut-back feature is sometimes adopted which reduces reactor power in a controlled and programmed

déré comme faisant partie du système de protection, il devra être dénommé « système de délestage de puissance de sécurité » et être conçu conformément aux normes du système de protection.

Les systèmes de délestage de puissance installés pour répondre à des avantages d'exploitation et non aux exigences de la sécurité du réacteur ne sont pas considérés dans cette recommandation.

5.4.4 *Système de verrouillage de sécurité*

Certaines manœuvres sur un réacteur peuvent devoir être effectuées dans un ordre déterminé et/ou seulement autorisées lorsqu'existent des conditions prescrites; des conditions de fonctionnement éventuellement dangereuses peuvent être évitées ou leurs conséquences réduites grâce à l'emploi d'un système de verrouillage de sécurité. Lorsque des verrouillages sont considérés comme faisant partie du système de protection, ils devront être dénommés « verrouillages de sécurité » et conçus conformément aux normes du système de protection.

5.4.5 *Système de signalisation d'ordre de sécurité*

Dans un nombre limité de circonstances, on peut admettre de considérer l'opérateur lui-même et les signalisations convenables comme faisant partie du système de protection du réacteur. Cette possibilité n'est admise que si le délai permis pour exécuter l'action appropriée est suffisamment long et si l'on peut raisonnablement compter sur l'opérateur pour exécuter cette action. Les signalisations nécessaires pour indiquer le défaut dans ces conditions seront dénommées « signalisations d'ordre de sécurité ». Les signalisations d'ordre de sécurité devront être conçues conformément aux normes du système de protection.

5.4.6 *Inhibitions d'exploitation*

Pour quelques types de réacteurs, notamment les réacteurs de puissance, il est nécessaire, en exploitation, d'inhiber une partie du système de protection, par exemple supprimer certaines causes de déclenchement de l'arrêt du réacteur à des niveaux de puissance prescrits. Dans ces circonstances, une inhibition d'exploitation peut être effectuée, mais, comme cette opération peut réduire le degré de protection, les inhibitions d'exploitation relatives au système de protection devront être conçues conformément aux normes de ce système de protection.

5.5 *Mesure des grandeurs physiques nécessaires à la protection*

5.5.1 La mesure des grandeurs physiques utilisées pour la sécurité d'un réacteur devrait être séparée des autres mesures et n'être employée pour aucune autre fonction. Au cas où elle ne serait pas séparée, on devra prendre soin, dans la conception, d'éviter que tout défaut dans l'équipement associé avec la fonction secondaire puisse affecter l'action de sécurité. On devrait aussi prendre soin, dans la conception, d'éviter que l'action de sécurité puisse être affectée de toute autre manière.

5.5.2 Le système devrait être conçu de telle sorte que les grandeurs physiques utilisées pour la sécurité du réacteur soient mesurées aussi directement qu'il est possible de le faire.

5.5.3 Les performances des ensembles de mesure et surveillance de sécurité devront être appropriées aux nécessités de la sécurité du réacteur.

5.5.4 Bien qu'il ne soit pas toujours nécessaire d'indiquer la valeur des grandeurs mesurées, une telle information fournit un renseignement d'exploitation supplémentaire et est utile aussi lors de la vérification du fonctionnement de l'ensemble de mesure et surveillance de sécurité. Comme autre possibilité, l'indication de la marge de déclenchement peut constituer un renseignement plus valable pour l'exploitation.

manner. Where this is claimed as a part of the protection system it shall be designated as a "safety power cut-back system" and engineered to protection system standards.

Power cut-back systems provided for reasons of operational convenience and not reactor safety, are not considered in this Recommendation.

5.4.4 *Safety interlock system*

Some reactor operations may be required to be carried out in a predetermined sequence and/or only permitted when prescribed conditions exist and potentially hazardous reactor conditions may be designed out, or their consequences reduced, by the use of a safety interlock system. Where interlocks are claimed as part of the protection system, they shall be designated "safety interlocks" and engineered to protection system standards.

5.4.5 *Safety alarm system*

Under limited circumstances, it may be permissible for the operator together with suitable alarms to be considered as part of the reactor protection system. This situation is permissible only where the time available for appropriate action is acceptably long and the operator can be reasonably expected to take that action. The alarms required to indicate this fault condition shall be designated " safety alarms ". Safety alarms shall be designed according to protection system standards.

5.4.6 *Operational bypasses*

In some reactor systems, particularly power reactors, there is an operational necessity to inhibit a part of the protection system, such as the inhibition of certain reactor shutdowns at prescribed power levels. In these circumstances, an operational bypass may be applied, but as this may reduce the degree of protection, operational bypasses in the protection system shall be designed to protection system standards.

5.5 *Measurement of protection variables*

5.5.1 The measurement of variables used for reactor safety should be separate from other measurements and not used for any other function. If they are not separate, provision shall be made in the design to prevent the safety action from being affected by any failure in the equipment associated with the secondary function. Provision should also be made in the design to prevent the safety action from being affected in any other way.

5.5.2 The system should be designed so that reactor safety variables are measured as nearly directly as practicable.

5.5.3 The performance of the safety monitoring assemblies shall be appropriate to the reactor safety requirements.

5.5.4 Even though it is not always necessary to display the magnitude of the variables measured, such information provides additional operational information and also serves a useful purpose when checking the operation of the safety monitoring assembly. Alternatively, a display of the trip margin may be a more valuable operational indication.

5.5.5 Il est quelquefois utile, en cas d'anomalies de fonctionnement, d'enregistrer à cadence rapide plusieurs des grandeurs physiques placées sous surveillance, dont la valeur serait autrement perdue au moment où se produit l'action de sécurité. Tout système de traitement des informations employé pour la surveillance des grandeurs physiques de l'installation pourrait remplir cette fonction. L'enregistrement des grandeurs physiques serait fait au choix sur commandes automatique ou manuelle. Une amélioration possible du système consiste à stocker les valeurs des grandeurs choisies dans une mémoire à court terme. Le déclenchement du système de protection provoquerait alors l'enregistrement des valeurs actuelles de ces grandeurs.

5.6 *Conception du système de protection*

5.6.1 *Généralités*

La conception et le fonctionnement des systèmes de sécurité particuliers compris dans le système de protection sont suffisamment semblables pour que des principes généraux puissent être énoncés pour couvrir toutes ces fonctions.

5.6.2 *Principes de conception*

5.6.2.1 L'un des problèmes majeurs dans la conception de chaque système particulier de sécurité est de réduire les conséquences des défaillances de composants. La conception devra être telle que n'importe quelle défaillance prise isolément ou les défaillances multiples qui peuvent résulter d'un seul événement ne puissent entraîner de défaut de protection. La conception des circuits et des équipements devra être telle que les probabilités de défaillances dangereuses et d'actions de sécurité intempestives soient assez faibles.

5.6.2.2 Toutes les parties de chaque système de sécurité devront être examinées sous l'angle des fonctions qu'elles accomplissent et du défaut vraisemblable qui peut troubler leur fonctionnement correct. Autant que faire se peut, les appareils utilisés pour constituer chaque système de sécurité devraient être étudiés pour que le défaut d'un composant quelconque ou le manque d'alimentation se traduise dans le système par une défaillance non dangereuse.
La fréquence des défaillances non dangereuses dans le système de protection d'un réacteur de puissance est d'importance, car un arrêt d'urgence intempestif du réacteur peut en résulter, avec des conséquences économiques. De plus, un taux excessif de défaillances non dangereuses peut être l'indication d'une conception erronée. La fréquence des défaillances, même non dangereuses, devrait être la plus réduite possible.

5.6.2.3 Malgré les précautions résultant des dispositions ci-dessus (paragraphe 5.6.2.2), des appareils et des circuits de commutation peuvent cependant avoir des défaillances dangereuses. Pour assurer un niveau convenable de sécurité du réacteur et de sa disponibilité, les techniques de redondance, de coïncidence et de vérifications en service devront être employées.

5.6.2.4 La conception du système de protection devrait assurer l'indépendance physique et électrique de ses sous-ensembles pour empêcher tout défaut isolé d'endommager d'autres sous-ensembles ou de provoquer une défaillance non dangereuse ou dangereuse du système.

5.6.2.5 Autant que possible, le système de protection devrait être de conception simple et d'un comportement en service approprié aux fonctions à remplir.

5.6.2.6 Pour maintenir une fiabilité convenable, l'équipement nécessitera une maintenance périodique et des vérifications. On devra prévoir lors de sa conception les moyens pour rendre possible la vérification de l'équipement en service de manière à s'assurer que ses performances demeurent dans les limites prescrites.

5.5.5 It is sometimes useful, under abnormal reactor conditions, to record on a fast time scale many of the variables monitored, a record of which would otherwise be lost at the initiation of safety action. Any data processing system used for monitoring plant variables could be used for this function. Recording of the variables would be initiated automatically or manually as desired. A possible refinement of this system is storing the values of selected plant variables on a short-term memory. The operation of the protection system would then initiate recording recent values of these variables.

5.6 *Design of protection system*

5.6.1 *General*

The design and operation of the specific safety systems within an over-all protection system are sufficiently alike for general principles to be formulated covering all these functions.

5.6.2 *Design principles*

5.6.2.1 One of the main problems in the design of each specific safety system is to reduce the consequences of component failures. The design shall be such that no single failure, or multiple failures that can arise from a single event, can result in loss of the protection function. The circuit arrangement and equipment design shall be such that the probabilities of unsafe failures and spurious safety actions are acceptably small.

5.6.2.2 Every part of each safety system shall be considered in relation to the function it performs and the probable fault which may interfere with its correct operation. As far as practicable, the apparatus used for each safety system should be designed so that failure of any component or loss of power results in the system going to the safe condition i.e. produces a safe failure.

The frequency of occurrence of safe failures in the power reactor system is of significance since a spurious shutdown may result, having economic penalties. Moreover, an excessive rate of safe failures may be evidence of faulty design. The frequency of failures, even of a safe nature, should be kept to the lowest possible level.

5.6.2.3 Notwithstanding the precautions in Sub-clause 5.6.2.2, apparatus and switching networks may still fail in an unsafe manner. To ensure an adequate degree of reactor safety and availability, redundancy, coincidence and in-service testing techniques will need to be employed.

5.6.2.4 The design of the protection system should provide physical and electrical independence of its sub-assemblies to prevent any single fault from damaging other sub-assemblies or causing a safe or unsafe system failure.

5.6.2.5 As far as is practicable, the protection system should be of simple design and operation commensurate with its required functions.

5.6.2.6 To maintain an adequate standard of reliability, the equipment will require periodic maintenance and testing. Facilities shall be provided to enable the equipment to be tested in service to determine whether its performance is within prescribed limits.

5.6.2.7 Après une commande de déclenchement, le système ne devra pas pouvoir être réarmé tant que les grandeurs mesurées en vue de la protection du réacteur ne seront pas revenues à une valeur sûre. Le réarmement du système devrait être effectué manuellement dans le cas d'arrêt d'urgence du réacteur; d'autres actions de sécurité, telle que le délestage du réacteur, peuvent être à réarmement automatique si la conception de l'installation permet de le faire en sécurité.

5.6.2.8 L'ensemble de mesure et surveillance de sécurité devra fournir un signal de déclenchement pour toutes les valeurs de la grandeur situées hors des limites de sécurité.
Dans cet esprit, on devrait considérer les valeurs de signaux en dehors de la plage normale de variation, valeurs qui peuvent résulter de défaillances typiques de l'équipement.
Les signaux de déclenchement ne devront pas être inhibés par le taux de variation du paramètre mesuré, quelle que soit sa valeur.

5.6.2.9 Autant que possible, un seul défaut, quel qu'il soit, sur un appareil, ne devrait pas déclencher l'arrêt d'urgence du réacteur.

5.6.2.10 Pour se garantir contre une erreur fondamentale ou des incorrections dans la conception ou dans le comportement en service de l'équipement, chacune des situations de défaut spécifiées du réacteur devrait être surveillée en utilisant, autant que possible, deux phénomènes physiques différents et indépendants.
Dans certaines circonstances, des équipements de types différents mesurant le même phénomène physique peuvent être utilisés pourvu que la probabilité de non-protection du réacteur soit assez faible et que l'on ait pris soin de minimiser la possibilité de défauts systématiques.

5.6.2.11 La fréquence des opérations d'entretien et de vérification en service devrait être appropriée à la fiabilité prédite et à la disponibilité souhaitée de l'équipement.

5.6.2.12 La dérive de tous les appareils du système de protection devra être suffisamment faible pour qu'aucun calibrage ne soit nécessaire entre les vérifications de routine. Des changements dans la correspondance entre la quantité mesurée et la grandeur physique peuvent, dans certains cas, exiger des calibrages plus fréquents.

5.6.2.13 L'équipement devrait avoir un nombre minimal de réglages nécessaires pour simplifier sa procédure de mise en œuvre. Lorsque des seuils de déclenchement sont réglables, la plage de réglage devrait être matériellement limitée eu égard aux considérations de sécurité.

5.6.2.14 Lorsque, pour répondre à des situations d'exploitation différentes, le réglage d'un niveau de déclenchement est essentiel à la protection du réacteur, ceci devrait être assuré par l'emploi d'une marge de déclenchement par excès, en plus de la marge de déclenchement de valeur zéro. Le déclenchement par excès garantit que, si la marge de déclenchement dépasse une valeur spécifiée, l'ensemble se met automatiquement dans les conditions de sécurité. Par raison de commodité, afin d'éviter une erreur systématique d'opérateur, et également lorsque la vitesse de réglage tend à être trop élevée pour que l'opérateur puisse suivre facilement, le niveau de déclenchement peut être ajusté automatiquement de façon à conserver une marge correcte dans tout le domaine de puissance du réacteur. Dans ce cas, la vitesse à laquelle le niveau de déclenchement peut varier devra être limitée à une valeur de sécurité prédéterminée et des limites hautes et basses de déclenchement devront être prévues afin de se protéger contre les variations exagérées résultant de défauts des composants de l'équipement. D'une autre manière, le niveau de déclenchement peut être fixé automatiquement par des verrouillages de sécurité convenables ou à partir des mesures relatives à d'autres grandeurs physiques du réacteur (par exemple, le débit de fluide de refroidissement), afin de maintenir une marge correcte dans le domaine de puissance du réacteur.

5.6.2.15 Une variation rapide des grandeurs physiques entraîne un retard inévitable de l'apparition du signal de déclenchement; mais le déclenchement ne devra pas être inhibé par cette variation rapide à moins qu'on ne puisse démontrer que la grandeur reprendra une valeur de sécurité sans qu'il en résulte une situation inacceptable pour le réacteur.

5.6.2.7 After a trip initiation, the system shall not be capable of being reset until the variables being measured for protection purposes return to a safe value. The reset of the system should be manual in the case of reactor shutdown; other safety actions such as reactor cut-back may be automatically reset, if the design permits this to be done safely.

5.6.2.8 The safety monitoring assembly shall give a trip signal for all values of the variable outside the safe limits.
In this context, consideration should be given to signals outside the normal range which may arise as a result of equipment failure modes.
The trip signals shall not be inhibited by any rate of change of the variable measured.

5.6.2.9 As far as possible, no single apparatus fault should produce a reactor shutdown.

5.6.2.10 To guard against any fundamental error or inadequacies in the design or operation of the equipment, each specified reactor fault condition should be monitored by using two different and independent physical effects as far as practicable.

In some circumstances, different kinds of equipment measuring the same physical effect may be used provided that the probability of the reactor not being protected is acceptably small and care is taken to minimize the possibility of systematic faults.

5.6.2.11 The frequency of routine maintenance and in-service functional testing should be commensurate with the predicted reliability and the desired availability of the equipment.

5.6.2.12 The drift of all protection system apparatus shall be sufficiently small that no adjustment to the calibration is necessary during the intervals between routine tests. Variations in the correlation of the measured quantity to the physical variable may in some cases require more frequent adjustments to the calibration.

5.6.2.13 The equipment should have a minimum of required adjustments to simplify setting up procedures. Where trip settings are variable, the range of variation should be physically limited as required by safety considerations.

5.6.2.14 Where adjustment of a trip level to meet differing operational situations is essential for reactor protection, it should be assured by the provision of an excess margin trip, in addition to the zero margin trip. The excess margin trip ensures that as the trip margin exceeds a specified value, the assembly goes automatically to the safe condition. For convenience and to avoid systematic operator error, and also where rates of change tend to be too high for the operator to follow easily, the trip level may be adjusted automatically to maintain a correct margin over the reactor power range. In this case, the rate at which the trip level can be varied shall be limited to a predetermined safe value, and upper and lower limit trips provided to guard against equipment runaway due to component failures. Alternatively, the trip level may be reset by suitable safety interlocks or from measurements of other reactor variables (e.g. coolant flow), to maintain a correct margin over the reactor power range.

5.6.2.15 For rapidly changing variables the trip signal experiences an unavoidable delay, but the trip shall not be inhibited by the rapid variation unless it can be shown that the variable will return to a safe value without resulting in an unacceptable reactor condition.

5.6.2.16 Les performances du système de protection devront être appropriées aux exigences de la sécurité du réacteur.

5.6.2.17 Les composants devraient être de qualité éprouvée et avoir été essayés dans des conditions d'emploi représentatives.

5.6.2.18 L'appareillage de sécurité, dépendant de sources d'alimentation incorporées ou d'une source auxiliaire, devra comporter un dispositif de surveillance de l'état normal de l'alimentation. L'alimentation incorrecte d'un appareil quelconque utilisé au sein du système d'arrêt d'urgence de sécurité devra entraîner une action dans le sens de la sécurité dans l'élément considéré; une signalisation devrait être prévue en ce cas.

5.6.2.19 Lorsque des ensembles logiques de sécurité sont groupés pour obtenir une redondance, ces groupes et les ensembles de mesure et surveillance de sécurité qui leur sont associés devraient être électriquement indépendants les uns des autres et posséder des alimentations individuelles.

5.6.2.20 Il devrait être possible d'accéder à l'un des ensembles logiques de sécurité et aux ensembles de mesure et surveillance qui lui sont associés sans qu'il soit nécessaire d'accéder aux autres ensembles logiques de sécurité et à l'équipement qui leur est associé.

5.6.2.21 Les circuits logiques de sécurité devraient être aussi compacts que possible. Des dispositifs de coupure galvanique, des relais par exemple, devraient être prévus à l'entrée des ensembles logiques de sécurité pour les signaux provenant de l'extérieur comme, par exemple, les signaux fournis par le système de verrouillage de sécurité aux circuits logiques de sécurité faisant partie du système d'arrêt d'urgence de sécurité (voir paragraphe 5.9.1).

5.6.2.22 Les conducteurs et câbles d'interconnexion qui font partie du système de protection devraient être séparés autant que possible de tous les autres; ils devraient être, ainsi que leurs extrémités, protégés convenablement contre tout dommage qui pourrait aller à l'encontre de la sécurité. De tels câbles d'interconnexion devront être blindés ou protégés autant qu'il le faudra pour réduire à des valeurs convenables le bruit induit électriquement et mécaniquement (effet microphonique). Les extrémités de ces conducteurs et câbles devront être repérés distinctement et disposés de manière à éviter toute erreur de connexion. Les grandes longueurs de tels conducteurs et câbles devraient être séparées en plusieurs groupes pour réduire les conséquences d'une avarie mécanique à un seul groupe. Lorsque des ensembles logiques de sécurité sont organisés en groupes, la séparation des câblages aide à conserver l'indépendance de ces ensembles et des ensembles de mesure et surveillance de sécurité associés.

5.7 *Conception du système d'arrêt d'urgence de sécurité*

5.7.1 *Equipement*

5.7.1.1 Les dispositions du paragraphe 5.6 seront appliquées au système d'arrêt d'urgence de sécurité. De plus, on respectera les principes suivants:

a) Un unique défaut, quel qu'il soit, sur un appareil ne devra pas empêcher l'arrêt d'urgence du réacteur dans les conditions normales de sécurité, si cet arrêt est nécessité par un défaut du réacteur.

b) Pour être acceptables, les combinaisons plausibles de défaillances d'appareils, susceptibles d'empêcher l'arrêt d'urgence du réacteur en cas de besoin de façon sûre, devraient avoir une probabilité de survenir suffisamment faible.

c) L'ensemble terminal d'arrêt d'urgence et les mécanismes de commande et de contrôle devraient comporter un degré convenable de redondance et l'emploi de coïncidences, eu égard à la conception et à la fonction de l'équipement.

5.6.2.16 The performance of the protection system shall be appropriate to the reactor safety requirements.

5.6.2.17 Components should be to approved quality and have been tested under suitable environmental conditions.

5.6.2.18 Safety apparatus relying on built-in power supplies or auxiliary power unit shall include a monitor of correct supply conditions. Incorrect supply to any instrument used within the safety shutdown system shall result in the affected unit going into the safe condition, and an alarm should be raised.

5.6.2.19 Where safety logic assemblies are arranged into redundant groups, the groups and their associated safety monitoring assemblies should be electrically independent from each other, including the provision of individual power supplies.

5.6.2.20 It should be possible to gain access to one safety logic assembly and its associated safety monitoring assemblies without the need for access to other safety logic assemblies and their associated equipment.

5.6.2.21 Safety logic circuits should be as compact as practicable. Interposing devices, for example relays, should be provided for outside information fed into safety logic assemblies, as for example, information from the safety interlock system to safety logic within the safety shutdown system (see Sub-clause 5.9.1).

5.6.2.22 Interconnecting wires and cables which are part of the protection system should, as far as possible, be separated from all others and, together with their appropriate terminations, adequately protected against such damage as could impair safety. Such interconnecting cables shall be shielded and otherwise protected as necessary to reduce electrically and mechanically (microphonic) induced noise pick-up to tolerable values.

The terminations of such wires and cables shall be distinctly marked and physically arranged to avoid wrong connections. Long runs of such wires and cables should be separated into more than one group to reduce the consequences of physical damage to one such group. When safety logic assemblies are arranged in groups, the segregation of cabling assists in maintaining the independence of those assemblies and their associated safety monitoring assemblies.

5.7 *Design of safety shutdown system*

5.7.1 *Equipment*

5.7.1.1 For the safety shutdown system, the provisions of Sub-clause 5.6 shall be applied together with the following design principles:

a) No single apparatus fault shall prevent the reactor being safely shutdown if this is necessitated by a reactor fault condition.

b) Credible combinations of apparatus failures, that would prevent the reactor from being safely shutdown when needed, should have acceptably low probability.

c) An adequate level of redundancy and coincidence should be incorporated in the shutdown final assembly and control mechanisms commensurate with the design and operation of the equipment.

5.7.1.2 Le système d'arrêt d'urgence de sécurité devrait être considéré dans le cadre des objectifs suivants:

a) Un moyen d'évaluer la qualité du système consiste à connaître l'intervalle de temps moyen entre défaillances non dangereuses et l'intervalle de temps moyen entre défaillances dangereuses. Une méthode pour prédire ces intervalles de temps est de calculer une valeur statistique, en supposant que les défauts dans les constituants sont des événements fortuits indépendants et en utilisant des données sur les performances des composants et/ou des sous-ensembles. Cette méthode de prédiction permet des comparaisons entre systèmes de conceptions différentes. Un autre moyen d'estimer la fiabilité est d'utiliser l'expérience acquise sur des équipements semblables déjà en service auprès des réacteurs.
Cependant, l'on doit noter que la fiabilité recherchée — qu'il s'agisse de se garantir de défauts réduisant ou non la sécurité — peut être très différente pour des systèmes eux-mêmes différents. La qualité d'un système d'arrêt d'urgence de sécurité est déterminée par la fiabilité de ses ensembles et la manière dont ils sont combinés pour remplir une fonction de sécurité.

b) Pour chaque ensemble de mesure et surveillance de sécurité du système d'arrêt d'urgence de sécurité d'un réacteur de puissance, un temps réel moyen d'au moins une année devrait s'écouler entre deux défaillances de toute nature dans les conditions normales de fonctionnement.

c) Le rapport entre l'intervalle moyen de temps entre défaillances dangereuses d'une part et l'intervalle moyen de temps entre défaillances non dangereuses d'autre part devrait être supérieur à l'unité pour les ensembles de mesure et de surveillance de sécurité pris individuellement. Un rapport beaucoup plus grand que l'unité permettra de réduire la fréquence nécessaire des vérifications.

d) En ce qui concerne la partie du système d'arrêt d'urgence de sécurité — c'est-à-dire les ensembles de mesure et de surveillance de sécurité, les ensembles logiques de sécurité et les ensembles terminaux d'arrêt d'urgence — partie nécessaire et suffisante pour provoquer l'arrêt du réacteur à partir d'une seule grandeur physique, l'intervalle moyen de temps entre défaillances dangereuses devrait être prévu pour chaque défaut envisagé du réacteur, en utilisant la méthode exposée au paragraphe 5.7.1.2*a)*. Le calcul devrait tenir compte de la fréquence et de l'ampleur des vérifications en service et de la maintenance. L'intervalle ainsi calculé devrait être assez grand pour que, dans la pratique, le taux de défaillances dangereuses soit déterminé par des événements non considérés dans le calcul, tels que des événements non fortuits ou non indépendants. Une valeur numérique, quelquefois employée, de la probabilité pour que la partie du système, ayant pour fonction d'arrêter d'urgence le réacteur à partir d'une grandeur unique soit en défaillance dangereuse au moment où son action serait nécessaire, est au plus d'une chance sur 10^5.

5.7.2 *Possibilités de vérification en service*

Si le fonctionnement du réacteur doit être continu, le système d'arrêt d'urgence de sécurité devrait comporter des dispositifs redondants de telle façon que les ensembles de mesure et de surveillance de sécurité, ainsi que les ensembles logiques de sécurité, puissent être vérifiés sans déclencher l'arrêt du réacteur et sans diminuer de manière appréciable sa sécurité. La vérification en service devrait s'appliquer à l'ensemble de mesure et de surveillance de sécurité ainsi qu'aux parties correspondantes de l'ensemble logique de sécurité et aller aussi loin que possible dans l'ensemble terminal d'arrêt.

5.7.3 *Possibilités manuelles de déclencher l'arrêt d'urgence du réacteur*

5.7.3.1 Des possibilités manuelles de déclencher l'arrêt d'urgence du réacteur au moyen d'un bouton-poussoir ou d'un interrupteur de secours devront être prévues sur son pupitre de commande et de contrôle et agir aussi directement que possible sur l'ensemble terminal d'arrêt d'urgence. Le bouton-poussoir ou l'interrupteur devraient être protégés contre des manœuvres involontaires pour éviter l'arrêt d'urgence intempestif du réacteur.

5.7.1.2 The safety shutdown system should be considered in relation to the following design objectives :

a) One measure of the quality of the system is its mean time between safe failures and mean time between unsafe failures. A method of predicting these is to calculate a statistical quantity by assuming that failures in constituents are independent random events, and using data on the performance of components and/or sub-assemblies. This method of prediction permits comparison between systems of different design. Another approach to the assessment of reliability is to make use of actual operating experience of similar systems under reactor conditions. However it must be recognized that the required reliability — both safe and unsafe — may be very different for different systems. The quality of a safety shutdown system is determined by the reliability of its assemblies and the manner in which they are combined to perform a safety function.

b) Each safety monitoring assembly in the safety shutdown system of a power reactor should have a true mean time between failures of all kinds of at least one year under operating conditions.

c) The ratio of mean time between unsafe failures to mean time between safe failures should be greater than unity, for safety monitoring assemblies considered individually. A ratio much larger than unity will permit increasing the required interval between tests.

d) For that part of the safety shutdown system which is necessary and sufficient to shut the reactor down from a single variable — that is the safety monitoring assemblies, safety logic and shutdown final assemblies — the mean time between unsafe failures should be predicted for each specified reactor fault condition, as described in Sub-clause 5.7.1.2*a)*. The calculation should take into account the frequency and completeness of in-service testing and maintenance. The predicted value should be so large that in practice the unsafe failure rate will be controlled by events not considered in the calculation, such as non-random or non-independent events. A value sometimes used is that the probability of that part of the system concerned with shutting the reactor down from a single variable, being in an unsafe condition when it may be called upon to protect the reactor, should not be greater than one chance in 10^5.

5.7.2 *In-service test facilities*

If continuous reactor operation is required, the safety shutdown system should contain adequate redundancy so that individual safety monitoring and safety logic assemblies can be proof tested without shutting down the reactor and without significant reduction in reactor safety. The proof test should embrace the safety monitoring assembly and relevant sections of the safety logic assembly and as far as possible the shutdown final assembly.

5.7.3 *Manual reactor shutdown facility*

5.7.3.1 Manual shutdown facilities in the form of a push-button or switch shall be provided at the reactor control and instrument desk, to operate as directly as possible into the shutdown final assembly. The push-button or switch should be protected against inadvertent operation to guard against spurious reactor shutdown.

5.7.3.2 Des possibilités supplémentaires de déclencher manuellement l'arrêt d'urgence du réacteur peuvent être prévues en différents points de l'installation, notamment s'il s'agit de réacteurs expérimentaux.

5.7.3.3 L'utilisation de la commande manuelle permettant de déclencher l'arrêt d'urgence du réacteur devrait être enregistrée de la même manière que les autres arrêts d'urgence. Ceci peut s'obtenir au moyen d'un verrouillage mécanique libérable seulement avec une clé.

5.7.3.4 La réalisation de l'interrupteur et du câblage associé doit tenir compte de ce que ce dispositif peut constituer un point commun dans le système et la plus grande attention devrait être apportée à la recherche du meilleur degré de séparation possible entre les circuits.

5.8 *Conception du système de délestage de puissance de sécurité*

5.8.1 *Généralités*

Le système de délestage de puissance de sécurité ne devra pas être considéré comme assurant l'unique protection du réacteur. En cas de défaillance dangereuse dans le système de délestage de puissance de sécurité, le système d'arrêt d'urgence de sécurité (ou un système équivalent) devra être capable en toutes circonstances de provoquer l'arrêt du réacteur, si nécessaire. L'action du système d'arrêt d'urgence de sécurité ou de son équivalent devra alors être automatique en cas de besoin.

5.8.2 *Principes de conception*

Pour déterminer le système de délestage de puissance de sécurité on appliquera les dispositions du paragraphe 5.6 et, le cas échéant, celles des paragraphes 5.7.1 et 5.7.2, en outre:

— le fonctionnement du système de délestage de puissance de sécurité devra être clairement indiqué à l'opérateur dans la salle de commande et de contrôle.

5.9 *Conception du système de verrouillage de sécurité*

5.9.1 *Généralités*

On considère les systèmes de verrouillage de sécurité comme ayant seulement un rôle de prévention et d'interdiction. Il est possible que les conditions détectées par le système de verrouillage aient à engendrer le déclenchement d'un arrêt du réacteur; si tel est le cas, cette action devrait être effectuée au moyen du système d'arrêt d'urgence de sécurité (voir paragraphe 5.6.2.21).

5.9.2 *Principes de conception*

5.9.2.1 Pour déterminer le système de verrouillage de sécurité, on appliquera les dispositions du paragraphe 5.6 et, le cas échéant, celles des paragraphes 5.7.1 et 5.7.2, en outre:

a) Les verrouillages de sécurité devraient être conçus de manière à continuer à remplir leur fonction en cas de défaut d'un seul des composants ou d'une coupure des alimentations. Dans ces circonstances, les verrouillages de sécurité commandant une séquence devraient provoquer l'arrêt de la séquence et, lorsque cela est nécessaire, le retour au stade requis par la protection du réacteur. De plus, l'opérateur devrait être informé par un signal.
Lors du rétablissement des alimentations après une coupure, les verrouillages de sécurité devraient revenir en leur état de fonctionnement normal, correspondant à la situation du réacteur au moment considéré, mais la séquence ne devrait pas pouvoir se poursuivre sans l'intervention de l'opérateur.

b) Des techniques de redondance et de coïncidence devraient être utilisées lors de la conception des verrouillages de sécurité pour garantir qu'un défaut unique de l'équipement ne provoque pas un verrouillage ou un déverrouillage incorrects.

5.7.3.2 Additional manual reactor shutdown facilities may be provided at local positions around the plant, especially for experimental reactors.

5.7.3.3. The action of the manual reactor shutdown should be recorded in the same way as other reactor shutdowns. This may be in the form of a mechanical latch-in facility which can be released only with a key.

5.7.3.4 The engineering of the switch and associated wiring should recognize that this facility may be a common point in the system and due attention should be paid to providing as high a degree of segregation as possible.

5.8 *Design of safety power cut-back system*

5.8.1 *General*

The safety power cut-back system shall not be regarded as the sole reactor protection. In the event of unsafe failure in the safety power cut-back system, the safety shutdown system (or an equivalent system) shall have the capability under all circumstances of shutting down the reactor if needed. Initiation of action of the safety shutdown system or its equivalent, when needed in this case, shall be automatic.

5.8.2 *Design principles*

For the safety power cut-back system, the provisions of Sub-clause 5.6, and, where appropriate, Sub-clauses 5.7.1 and 5.7.2 shall be applied, and in addition:

— the operation of the safety power cut-back system shall be clearly indicated to the operator in the control room.

5.9 *Design of safety interlock system*

5.9.1 *General*

Safety interlock systems are regarded as having a preventative or inhibiting feature only. It is possible that conditions sensed by the interlock system should initiate a reactor shutdown; if this is the case, the shutdown should take place via the safety shutdown system (see Sub-clause 5.6.2.21).

5.9.2 *Design principles*

5.9.2.1 For safety interlocks, the provisions of Sub-clause 5.6 and, where appropriate, Sub-clauses 5.7.1 and 5.7.2 shall be applied and in addition:

a) Safety interlocks should be so designed that they continue to provide their design function in the event of any single component failure or interruption of power supplies. Under these circumstances, safety interlocks controlling a sequence should cause the sequence to halt and where necessary revert to an earlier stage as required for reactor protection, and an indication should be given to the operator.

On restoration of power supplies following an interruption, safety interlocks should return to their normal operating position as determined by reactor conditions at the time, but sequences should not be allowed to continue without the intervention of the operator.

b) Redundancy and coincidence techniques should be incorporated in the design of the safety interlocks to ensure that a single equipment failure does not permit the interlocks to be released or withheld incorrectly.

c) Lorsque cela est possible, tous les signaux de position et de cote devraient être obtenus, à partir de la fonction contrôlée, par un dispositif servant uniquement au système de protection et non être déduits de la mesure d'une fonction différente.

5.9.2.2 Dans le cas de verrouillages de sécurité employés pour assurer la mise en position correcte de dispositifs commandés à distance, les dispositions du paragraphe 5.9.2.1 devraient être appliquées, en outre:

a) Si une commande manuelle est prévue comme secours aux dispositifs mécaniques utilisés pour la manœuvre à distance, l'emploi de la commande manuelle d'urgence ne devrait entraîner ni rupture de connexion avec le système de verrouillage de sécurité, ni aucune modification de celui-ci.

b) On devrait utiliser des techniques de redondance et de coïncidence dans la conception des verrouillages de mise en position à distance pour permettre le retrait, pour entretien, d'un dispositif, sans affecter la sécurité du réacteur.

5.10 *Conception des signalisations d'ordre de sécurité*

Les conditions fixées aux paragraphes 5.6 et 8.3 et, le cas échéant, aux paragraphes 5.7.1 et 5.7.2 devraient être appliquées aux signalisations d'ordre de sécurité, en outre:

5.10.1 Les signalisations d'ordre de sécurité devraient être conçues et réalisées autant que possible avec les normes des systèmes de sécurité, c'est-à-dire en employant les techniques des circuits à redondance et à défaillance non dangereuse, de telle sorte qu'un défaut d'un composant quelconque ou un manque d'alimentation soient indiqués à l'opérateur.

5.10.2 Les signalisations d'ordre de sécurité devraient être particularisées dans leur présentation à l'opérateur.

5.10.3 La présentation des signalisations d'ordre de sécurité devrait être aussi directe que possible et ne pas être affectée par une défaillance dans un quelconque système de traitement des informations ou dans les autres signalisations.

5.10.4 Les signalisations d'ordre de sécurité devront rester visibles et il ne devra pas être possible de les effacer tant que la grandeur mesurée est en dehors des valeurs admises de fonctionnement sûr.

5.11 *Conception des inhibitions d'exploitation*

Les dispositions du paragraphe 5.6 et, lorsqu'elles conviennent, celles du paragraphe 5.7.1 devront être appliquées à la conception d'une inhibition d'exploitation, en outre:

5.11.1 Il devrait exister une combinaison adéquate des ensembles de mesure et surveillance de sécurité en exploitation avec des recouvrements convenables de leurs étendues de mesure et une corrélation appropriée de leurs fonctions pour garantir la protection du réacteur lorsqu'une inhibition d'exploitation est correctement effectuée.

5.11.2 La situation des inhibitions d'exploitation sera clairement indiquée à l'opérateur dans la salle de commande et de contrôle.

5.11.3 Chaque inhibition d'exploitation devrait comporter les verrouillages nécessaires avec le reste du système de protection pour être certain qu'elle ne peut être effectuée que lorsque les conditions fixées pour le réacteur sont réalisées, ou qu'une manœuvre incorrecte entraîne une action de protection automatique.
Si cette disposition ne peut être satisfaite, une signalisation de sécurité, pour laquelle les dispositions des paragraphes 5.4.5 et 5.10 seraient appliquées, devrait être déclenchée lorsque l'état du réacteur exige que l'inhibition d'exploitation passe en position inverse. Cette signalisation ne devrait pouvoir être effacée que lorsque l'inhibition d'exploitation est mise dans la position convenable. L'indication de la situation de l'inhibition devrait être permanente.

c) Where practicable, all position and level signals should be obtained, from the function being monitored, by a system unique to the protection system and not by inference from measurement of a different function.

5.9.2.2 For safety interlocks used to enforce the correct positioning of remote devices, the provisions in Sub-clause 5.9.2.1 should be applied and in addition:

a) If a manual scheme is provided as a back-up to the mechanical devices used for the movement of remote devices, the use of the emergency manual scheme should not involve breaking any connections to or amending in any way the safety interlock system.

b) Redundancy and coincidence techniques should be used in the design of the remote device positioning interlocks, permitting the withdrawal of any device for maintenance purpose without violating reactor safety.

5.10 *Design of safety alarms*

For safety alarms, the provisions of Sub-clauses 5.6 and 8.3 and, where appropriate, Sub-clauses 5.7.1 and 5.7.2 should be applied and in addition:

5.10.1 Safety alarms should be designed and engineered as far as possible to safety system standards, that is employing redundancy and failsafe techniques such that the failure of any component or loss of supplies is brought to the attention of the reactor operator.

5.10.2 Safety alarms should be distinctive in their presentation to the operator.

5.10.3 The annunciation of safety alarms should be as direct as practicable, and not affected by faults in any data processing system or other alarms.

5.10.4 Safety alarm indications shall remain visible and not be capable of being reset whilst the variable measured is outside the normal safe operating levels.

5.11 *Design of operational bypasses*

In the design of an operational bypass, the provisions of Sub-clause 5.6 and where appropriate Sub-clause 5.7.1 shall be applied and in addition:

5.11.1 There should be an adequate combination of operational safety monitoring assemblies, with suitable overlap in their ranges of operation, and suitable correlation in their functions, to ensure that the reactor is protected when an operational bypass is correctly applied.

5.11.2 The state of the operational bypasses shall be clearly indicated to the operator in the control room.

5.11.3 Each operational bypass should be interlocked with the remainder of the protection system to ensure either that it can be applied only when predetermined reactor conditions exist, or that incorrect application leads to automatic protective action being taken.

If this is not possible, a safety alarm, to meet the provision of Sub-clauses 5.4.5 and 5.10, should be raised when reactor conditions demand that the operational bypass is changed to the alternative state. This alarm should be capable of being reset only when the operational bypass is moved to the correct position. Indication of the state of the bypass should be continuous.

5.11.4 Les inhibitions d'exploitation sont de préférence effectuées et supprimées automatiquement; dans ce cas, on devrait les concevoir avec redondance et coïncidence pour se protéger contre leur mise en service et leur suppression incorrectes lors de défaillances de l'équipement. Dans la conception d'une inhibition d'exploitation, on devrait considérer attentivement ses performances dans toutes les conditions de défaut du réacteur en régime transitoire.

8. Signalisations de défaut

8.1 *Définitions*

Les définitions suivantes s'appliquent au présent article.

8.1.1 *Signaleur de défaut*

Sous-ensemble qui fournit une signalisation visible et/ou audible attirant l'attention de l'opérateur du réacteur.

8.1.2 *Système de signalisation de défaut*

Système comprenant la totalité des signaleurs de défaut.

8.2 *Introduction*

Un système de signalisation de défaut est prévu pour surveiller l'état du réacteur et tous les services auxiliaires essentiels à son exploitation. Le rôle du système de signalisation de défaut est d'indiquer à l'opérateur les anomalies de fonctionnement pour lui permettre d'entreprendre une action correctrice. Les signalisations sont réalisées au moyen de circuits qui interprètent les signaux issus des ensembles de mesure et surveillance du réacteur ainsi que des services associés et fournissent les indications visuelles et audibles convenables pour attirer l'attention de l'opérateur. Le nombre de signalisations de défaut présentées dans la salle de commande et de contrôle peut être réduit en groupant judicieusement les informations, les signalisations particulières étant faites localement, à proximité de l'équipement ou de l'installation en cause. Un système de traitement d'information donne une possibilité de groupement. Les signalisations de défaut peuvent être divisées en « urgentes » et « non urgentes » et leur mode de présentation devrait indiquer leur degré de priorité, par exemple par les couleurs des signaux visuels ou les tonalités des signaux sonores.

Lorsqu'un système de traitement d'information est prévu, il devrait être capable d'enregistrer des signalisations de défaut de très courte durée ou survenant à de faibles intervalles de temps et de distinguer leur chronologie.

Dans une grande installation comportant un système de traitement d'information, la possibilité d'analyser les signalisations de défaut peut être justifiée. Avec cette disposition les signalisations de défaut sont scrutées automatiquement au fur et à mesure de leur apparition; la cause première du défaut est indiquée à l'opérateur en même temps que ses conséquences sur l'installation et la conduite à tenir.

8.3 *Conception des systèmes de signalisation de défaut*

Dans la conception des systèmes de signalisation de défaut, il est recommandé d'appliquer les critères suivants:

8.3.1 Les défaillances du système de signalisation de défaut ne devraient avoir aucune influence sur un autre équipement.

8.3.2 Le système de signalisation de défaut ne devrait pas introduire de complication ni diminuer l'intégrité des ensembles de mesure et surveillance élaborant les informations correspondantes.

5.11.4 Operational bypasses are preferably applied and withdrawn automatically and in such cases redundancy and coincidence techniques should be employed in their design to guard against incorrect application or withdrawal under conditions of equipment failure. Due consideration should be given in the design of the automatic bypass to its performance under all reactor fault transient conditions.

8. General alarms

8.1 *Definitions*

The following definitions apply for this clause.

8.1.1 *Alarm*

A sub-assembly which gives a visible and/or audible warning to the reactor operator that his attention is required.

8.1.2 *Alarm system*

System comprising the totality of all alarms.

8.2 *Introduction*

An alarm system is provided to monitor the reactor state and all auxiliary services essential to the operation of the reactor. The function of the alarm system is to indicate abnormal conditions to the reactor operator so that corrective action can be taken. Alarms are provided by circuits which interpret signals from assemblies monitoring reactor variables and services and give suitable visual and audible warning to the operator. The number of alarms displayed in the control room may be reduced by judicious grouping of alarms, individual alarms being displayed locally to the equipment or plant. One form of grouping is by a data processing system. Alarms may be divided into "urgent" and "non-urgent", and the presentation should indicate the degree of priority of alarm, e.g. by colour of facia, different tone of audible alarm.

Where a data processing system is provided, this should have the capability of being able to record alarms of extremely short duration or alarms occurring at short intervals of time, and distinguish the order in which alarms occur.
In a large plant having a data processing system, an alarm analysis facility may be justified. In this arrangement, the alarms are scanned automatically as they occur, and the prime cause of the failure is indicated to the operator, together with an indication of the effect on the plant and the required action by the operator.

8.3 *Design of alarm systems*

In designing alarm systems, the following requirements are recommended:

8.3.1 Failures within the alarm system should not influence any other equipment.

8.3.2 The alarm system should not complicate or reduce the integrity of the monitoring assemblies supplying the alarm signals.

8.3.3 Le signal sonore peut être arrêté par l'opérateur en reconnaissant le défaut, mais la signalisation visible devrait demeurer jusqu'au réarmement après disparition de ce défaut; en outre, le système sonore devrait rester en état de fonctionner pour tout autre défaut pouvant survenir. Le dispositif d'arrêt de signalisation sonore ne devrait pas pouvoir inhiber la signalisation des défauts subséquents. Une signalisation visuelle, lorsque les défauts disparaissent, est souvent utile.
Toute indication particulière sur le modèle usuel de panneau annonciateur, clignotement par exemple, peut être annulé par l'opérateur en reconnaissant le défaut, mais la signalisation visible devrait demeurer jusqu'à réarmement après disparition du défaut. Si la signalisation concerne un groupe de défauts, l'indication devrait reprendre l'état décrit ci-dessus (clignotement ou autre indication spéciale) pour tout défaut subséquent affectant le groupe en question.

8.3.4 La puissance de la signalisation sonore ne devrait pas empêcher les opérateurs, dans la salle de commande et de contrôle ou ailleurs dans l'installation, d'entendre les communications essentielles. Un réglage du volume sonore peut être nécessaire dans ce cas.

8.3.5 Les signalisations de défaut produites par des informations de courte durée (signalisations fugitives) ne devraient pas s'acquitter lorsque le contact qui les déclenche se rétablit. L'opérateur devrait avoir à manœuvrer le bouton-poussoir de réarmement pour effacer ces signalisations. Le bouton-poussoir de réarmement ne devait pas avoir d'effet avant que le défaut n'ait été reconnu.

8.3.6 Les performances des circuits engendrant les signalisations de défaut devraient être appropriées à la situation à signaler.

8.3.7 Toute disposition devrait être prise pour permettre la vérification du fonctionnement des signalisations de défaut.

8.3.8 Toute disposition devrait être prise pour permettre l'identification de la condition particulière et/ou de l'équipement engendrant la signalisation de défaut.

8.3.9 Il est quelquefois souhaitable que la signalisation de défaut apparaissant la première soit repérable par l'opérateur. Cette signalisation apparaissant la première ne devrait pas empêcher l'apparition d'une quelconque signalisation subséquente.

8.3.10 Tout système de traitement d'information utilisé pour l'analyse et l'affichage des signalisations de défaut devrait comporter un enregistrement de longue durée des informations de signalisation reçues et de leur ordre d'arrivée. Ces enregistrements, sur machine imprimante ou bande perforée, par exemple, pourraient servir aux recherches entreprises après tout incident survenu à l'installation. Un enregistrement codé suffirait.

8.3.11 Si les signalisations de défaut sont importantes pour une exploitation correcte dans les périodes où le réacteur ne produit pas d'énergie, on devrait pouvoir alimenter tout ou partie convenable du système de signalisation de défaut à partir d'une source de secours.

8.3.3 The audible warning may be cancelled by the operator acknowledging the fault but the visual signal should persist until reset on clearing the fault condition, and the audible system should remain available for any subsequent fault which may occur. The audible alarm cancellation facility should not inhibit the annunciation of subsequent alarms. A visual indication when faults are cleared is often useful.

Any distinctive indication, e.g. a flashing lamp, in the conventional type of facia may be cancelled by the operator acknowledging the fault, but the alarm should stay visible until reset on clearing the fault condition. If the alarm is for a group, the alarm indication should revert to flashing or other distinctive indication for any subsequent fault which may occur within that group.

8.3.4 The audible warning should not be so loud that operators in the control room or around the plant cannot hear essential communications. Volume control may be needed for this purpose.

8.3.5 Alarms which arise from signals of short duration (fleeting alarms) should continue when the initiating contact clears. It should be necessary to operate the reset push-button to reset these. The reset push-button should not be effective until after the fault condition has been acknowledged.

8.3.6 The performance of the alarm initiation circuits should be appropriate to the characteristics of the situation to be alarmed.

8.3.7 Provision should be made for checking the proper functioning of the alarm indications.

8.3.8 Provision should be made for identifying the particular condition and/or equipment initiating the alarm.

8.3.9 It is sometimes desirable that the alarm occurring first is identified to the operator. The first-up indication should not lock out any subsequent alarms.

8.3.10 Any data processing system used for alarm analysis and presentation should provide a long-term record of alarm annunciations received, including the order in which they occurred. These records — which may be on a teleprinter or paper tape for example — could be used for analysis purposes after any plant incident and a coded record would suffice for this purpose.

8.3.11 If alarms are important to correct operation during power outages, then all, or an appropriate portion, of the alarm system should be capable of operating from an emergency power source.

ICS 27.120.10

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND