

**NORME  
INTERNATIONALE  
INTERNATIONAL  
STANDARD**

**CEI  
IEC**

**61497**

Première édition  
First edition  
1998-10

---

---

**Centrales nucléaires –  
Verrouillages électriques relatifs aux fonctions  
importantes pour la sûreté –  
Recommandations pour la conception  
et la mise en oeuvre**

**Nuclear power plants –  
Electrical interlocks for functions important  
to safety – Recommendations for design  
and implementation**



Numéro de référence  
Reference number  
CEI/IEC 61497:1998

## 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**

**61497**

Première édition  
First edition  
1998-10

---

---

**Centrales nucléaires –  
Verrouillages électriques relatifs aux fonctions  
importantes pour la sûreté –  
Recommandations pour la conception  
et la mise en oeuvre**

**Nuclear power plants –  
Electrical interlocks for functions important  
to safety – Recommendations for design  
and implementation**

© IEC 1998 Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Electrotechnical Commission  
Telefax: +41 22 919 0300

3, rue de Varembe Geneva, Switzerland  
e-mail: [inmail@iec.ch](mailto:inmail@iec.ch) IEC web site <http://www.iec.ch>



Commission Electrotechnique Internationale  
International Electrotechnical Commission  
Международная Электротехническая Комиссия

CODE PRIX  
PRICE CODE

**R**

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

## SOMMAIRE

|                                                                                                                 | Pages |
|-----------------------------------------------------------------------------------------------------------------|-------|
| AVANT-PROPOS .....                                                                                              | 4     |
| INTRODUCTION .....                                                                                              | 6     |
| Articles                                                                                                        |       |
| 1 Domaine d'application .....                                                                                   | 8     |
| 2 Références normatives.....                                                                                    | 8     |
| 3 Définitions et abréviations .....                                                                             | 10    |
| 3.1 Définitions.....                                                                                            | 10    |
| 3.2 Abréviations .....                                                                                          | 14    |
| 4 Prescriptions .....                                                                                           | 14    |
| 4.1 Prescriptions du système .....                                                                              | 14    |
| 4.2 Conception du système .....                                                                                 | 16    |
| 4.3 Intégrité des verrouillages de sûreté .....                                                                 | 18    |
| 4.4 Matériel de verrouillage de sûreté.....                                                                     | 22    |
| 4.5 Documentation.....                                                                                          | 26    |
| 4.6 Matériel programmé .....                                                                                    | 26    |
| 4.7 Actions de l'opérateur.....                                                                                 | 28    |
| 4.8 Alimentation électrique.....                                                                                | 28    |
| 5 Méthodes d'essai .....                                                                                        | 30    |
| 5.1 Installations d'essai et de surveillance .....                                                              | 30    |
| 5.2 Outils d'essai automatiques.....                                                                            | 30    |
| 5.3 Auto-test et surveillance.....                                                                              | 30    |
| Annexe A (informative) Verrouillages de sûreté types .....                                                      | 32    |
| Annexe B (informative) Guide d'application des verrouillages de sûreté monocanaux, bicanaux et multicanaux..... | 36    |

## CONTENTS

|                                                                                                                      | Page |
|----------------------------------------------------------------------------------------------------------------------|------|
| FOREWORD .....                                                                                                       | 5    |
| INTRODUCTION .....                                                                                                   | 7    |
| Clause                                                                                                               |      |
| 1 Scope .....                                                                                                        | 9    |
| 2 Normative references .....                                                                                         | 9    |
| 3 Definitions and abbreviations.....                                                                                 | 11   |
| 3.1 Definitions.....                                                                                                 | 11   |
| 3.2 Abbreviations .....                                                                                              | 15   |
| 4 Requirements.....                                                                                                  | 15   |
| 4.1 System requirements .....                                                                                        | 15   |
| 4.2 System design .....                                                                                              | 17   |
| 4.3 Interlock integrity.....                                                                                         | 19   |
| 4.4 Interlock equipment.....                                                                                         | 23   |
| 4.5 Documentation.....                                                                                               | 27   |
| 4.6 Computer-based equipment .....                                                                                   | 27   |
| 4.7 Operator actions .....                                                                                           | 29   |
| 4.8 Power supplies.....                                                                                              | 29   |
| 5 Test methods .....                                                                                                 | 31   |
| 5.1 Test and monitoring facilities.....                                                                              | 31   |
| 5.2 Automatic test aids.....                                                                                         | 31   |
| 5.3 Self-testing and monitoring.....                                                                                 | 31   |
| Annex A (informative) Typical interlocks .....                                                                       | 33   |
| Annex B (informative) Guidance on application of single-channel, double-channel or<br>multi-channel interlocks ..... | 37   |

# COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

## **Centrales nucléaires – Verrouillages électriques relatifs aux fonctions importantes pour la sûreté – Recommandations pour la conception et la mise en oeuvre**

### AVANT-PROPOS

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

La Norme internationale CEI 61497 a été établie par le sous-comité 45A: Instrumentation des réacteurs, 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/335/FDIS | 45A/343/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.

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

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

**Nuclear power plants – Electrical interlocks  
for functions important to safety –  
Recommendations for design and implementation**

## FOREWORD

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

This International Standard IEC 61497 has been prepared by subcommittee 45A: Reactor instrumentation, of IEC technical committee 45: Nuclear instrumentation.

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

| FDIS         | Report on voting |
|--------------|------------------|
| 45A/335/FDIS | 45A/343/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.

Annexes A and B are for information only.

## INTRODUCTION

Les fonctions de verrouillage de sûreté des centrales nucléaires évitent les conditions ou opérations présentant un risque pour la sûreté, assurent une protection du personnel et préviennent les dangers. Les fonctions de verrouillage de sûreté empêchent toute action susceptible de provoquer ou d'accroître un risque ou un endommagement de la centrale et ne prennent généralement aucune mesure de correction des conditions. Les fonctions de verrouillage de sûreté peuvent limiter un fonctionnement continu afin d'empêcher le développement d'une situation critique ou peuvent empêcher une action éventuelle, et par conséquent une telle situation. Les fonctions de verrouillage de sûreté peuvent générer un signal d'autorisation permettant de sélectionner la sortie d'un instrument uniquement dans sa gamme de fonctionnement, en vue d'une utilisation par le système de protection du réacteur ou par un système de commande d'alimentation, de gamme de température ou de condition.

Les fonctions de verrouillage de sûreté peuvent être fournies par des moyens mécaniques ou grâce à des dispositions administratives, par une action de l'opérateur ou par des moyens électriques. Les dispositions administratives relèvent des responsables de la centrale et impliquent l'apposition de signatures sur les documents ainsi que sur les registres d'autorisation permettant de réaliser des opérations; ces dispositions ne seront pas détaillées ici. Elles peuvent être utilisées pour contrôler l'accès du personnel à une zone contrôlée, permettre à l'opérateur d'utiliser une commande, autoriser l'utilisation d'une clef permettant de libérer une commande bloquée ou autoriser une opération pour certaines raisons spécifiques ou non permanentes.

Les moyens électriques comprennent l'utilisation du système de protection du réacteur, de logique dans les systèmes de commande, de logique dans les équipements informatisés, d'interconnexion dans les interrupteurs et d'équipements spécifiques à relais ou en logique câblée. Des fonctions de verrouillage de sûreté typiques ainsi que des méthodes permettant d'obtenir un verrouillage de sûreté électrique sont présentées dans l'annexe A.

Les prescriptions de sûreté nucléaire concernant les verrouillages de sûreté peuvent s'ajouter aux prescriptions relatives à la protection contre l'incendie, à la protection du personnel ou de la centrale, ou peuvent s'en écarter. Ces prescriptions sont susceptibles d'entrer en conflit et des lignes directrices sont indiquées pour résoudre ces conflits.

Les prescriptions relatives à la classification et à la fiabilité des systèmes de contrôle-commande importants pour la sûreté sont données dans la CEI 61226. Les verrouillages de sûreté électriques nécessitent une classification selon cette norme pour identifier les prescriptions de base. Certaines prescriptions concernant les verrouillages de sûreté peuvent être dérivées du document AIEA 50-SG-D3, mais ce n'est pas le cas pour tous les verrouillages importants pour la sûreté. Les prescriptions relatives au système, à la conception, à la fiabilité et au matériel, appropriées aux catégories A, B et C sont développées dans la présente norme.

Des fonctions de verrouillage de sûreté sont présentes dans de nombreux systèmes dans une centrale nucléaire, ce qui peut donner lieu à différentes approches au niveau de la mise en oeuvre de différents systèmes. Il convient donc de les appliquer de façon cohérente dans l'ensemble de la centrale. La présente norme traite des implications pratiques de la conception et de la mise en oeuvre des verrouillages de sûreté électrique permettant d'atteindre les niveaux de performances, de fiabilité et de cohérence requis au niveau des centrales nucléaires.

## INTRODUCTION

Interlock functions on nuclear power plants prevent unsafe conditions or operations, protect personnel and prevent hazards. Interlock functions prevent actions which could lead to or increase danger or damage to the plant, and do not normally take steps to correct conditions. Interlock functions may limit a continuing action in order to prevent a condition developing, or may prevent a possible action and thereby prevent a condition. Interlock functions may generate a permissive signal to allow selection of the output of an instrument only when in its operating range, for use by the reactor protection system or a control system for the current power, temperature range or condition.

Interlock functions may be provided by mechanical means or by administration, by operator action or by electrical methods. Administration is under control of the plant management, and involves signatures on permits and records of authority to perform operations, which are not discussed. Such methods may be used to control personnel access to an active area, to permit operator use of a control, to authorize issue of a key which can release a locked control or which allows access to perform some operation for special or non-routine reasons.

Electrical methods include use of the reactor protection system, logic within control systems, logic in computer-based equipment, interconnections in switchgear and dedicated units of relay or solid-state logic. Typical interlock functions and methods of providing electrical interlocks are given in annex A.

The nuclear safety requirements for interlocks may be in addition to or different from the interlock requirements for fire protection, personnel safety or plant protection. These requirements may conflict and guidance is given on resolution of conflicts.

The requirements for classification and for reliability of instrumentation and control systems important to safety are discussed in IEC 61226. Electrical interlocks require classification according to that standard to identify basic requirements. Some requirements for safety system interlocks can be derived from IAEA 50-SG-D3, but not for all interlocks important to safety. The system, design, reliability and equipment requirements appropriate to categories A, B and C are developed in this standard.

Interlock functions exist in many systems on a nuclear plant, which can result in different approaches to their implementation in different systems. They should therefore be implemented in a consistent manner throughout a plant. This standard is concerned with the practical implications of electrical interlock design and implementation to meet the levels of performance, reliability and consistency required on nuclear plants.

## **Centrales nucléaires – Verrouillages électriques relatifs aux fonctions importantes pour la sûreté – Recommandations pour la conception et la mise en oeuvre**

### **1 Domaine d'application**

La présente Norme internationale fournit des recommandations relatives à la conception et la mise en oeuvre des verrouillages électriques de sûreté utilisés de façon active ou passive pour empêcher l'apparition de conditions présentant un risque pour la sûreté ou pour assurer des conditions et des états de sûreté spécifiques durant l'exploitation des centrales nucléaires. Les verrouillages du système de sûreté sont couverts par les normes relatives aux systèmes de sûreté.

La présente norme fournit des critères de conception, de fiabilité et d'essai à partir de l'étude des verrouillages de sûreté importants pour la sûreté conformément à la CEI 61226. Elle utilise les catégories A, B et C selon les définitions fournies dans ce document. Elle tient compte des fonctions ainsi que de l'importance sur la sûreté, ainsi que du rôle de l'opérateur au niveau de certains verrouillages.

Un guide est fourni concernant la redondance et la diversité du matériel dans le cadre de la mise en oeuvre des verrouillages de sûreté, en cas de grande disponibilité ou intégrité, ou lorsqu'une défaillance de mode commun est susceptible de limiter la fiabilité.

L'utilisation de technologie programmée pour les fonctions de verrouillage de sûreté est examinée ici, et des recommandations sont données concernant la diversité. Des prescriptions relatives aux logiciels ainsi qu'à la vérification et la validation sont indiquées en référence à la CEI 60880.

Les installations d'essai sont étudiées ainsi que les méthodes d'essai et de surveillance automatiques.

Le système de verrouillage de sûreté pour une fonction spécifique comprend les capteurs d'état de la centrale (par exemple les dispositifs de mesure et les interrupteurs de fin de course), l'alimentation des verrouillages et de leur commande, le matériel de contrôle-commande fournissant la fonction logique particulière pour la prévention ou la limitation des opérations, ainsi que les câbles, les dispositifs électromécaniques, la commande par clef et la procédure administrative associés à la fonction.

### **2 Références normatives**

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Tout document normatif est sujet à révision, et les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 60231A:1969, Premier complément à la CEI 60231:1967, *Principes généraux de l'instrumentation des réacteurs nucléaires* <sup>1)</sup>

CEI 60617-12:1997, *Symboles graphiques pour schémas – Partie 12: Opérateurs logiques binaires*

---

<sup>1)</sup> Cette norme comporte des conseils techniques utiles, mais n'est pas mise à jour par la CEI et n'est donc pas complètement normative.

## **Nuclear power plants – Electrical interlocks for functions important to safety – Recommendations for design and implementation**

### **1 Scope**

This International Standard provides recommendations for the design and implementation of electrical interlocks used actively or passively to prevent unsafe conditions or to ensure specific safe conditions and states during the operation of nuclear power plants. Safety system interlocks are covered by standards for safety systems.

This standard gives design, reliability and test criteria arising from the consideration of interlocks important to safety in accordance with IEC 61226. It uses categories A, B and C as defined by that document. It takes into account the interlock safety significance and functions, and the role of the operator in some interlocks.

Guidance is given on redundancy and on diversity of equipment for implementing interlocks, where high availability or integrity is involved, or where common mode failure may limit reliability.

The use of computer-based equipment for interlock functions is discussed, and recommendations for diversity are given. Requirements for software and for verification and validation are given by reference to IEC 60880.

The provision of test facilities is discussed together with self-testing and self-monitoring methods.

The system of interlocks for a specific function includes the sensors of plant state (e.g., measuring devices and limit switches), the interlock and control power supplies, the control and instrumentation equipment providing the particular logic function for prevention or limitation of operation, and the cables, electromechanical features, key control and administrative control associated with the function.

### **2 Normative references**

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60231A:1969, First supplement to IEC 60231:1967, *General principles of nuclear reactor instrumentation* <sup>1)</sup>

IEC 60617-12:1997, *Graphical symbols for diagrams – Part 12: Binary logic elements*

---

<sup>1)</sup> This standard contains valuable technical advice, but is not maintained by IEC and is not therefore fully normative.

CEI 60812:1985, *Techniques d'analyse de la fiabilité des systèmes – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

CEI 60880:1986, *Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires*

CEI 60987:1989, *Calculateurs programmés importants pour la sûreté des centrales nucléaires*

CEI 61225:1993, *Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande pour la sûreté – Prescriptions pour les alimentations électriques*

CEI 61226:1993, *Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Classification*

CEI 61500:1996, *Centrales nucléaires – Systèmes de contrôle-commande importants pour la sûreté – Prescriptions fonctionnelles pour transmission de données multiplexées*

AIEA 50-C-D (Rev. 1):1989, *Conception pour la sûreté des centrales nucléaires*

AIEA 50-SG-D3:1981, *Système de protection et dispositifs connexes dans les centrales nucléaires*

AIEA 50-SG-D8:1985, *Systèmes d'instrumentation et de commande liés à la sûreté dans les centrales nucléaires*

### **3 Définitions et abréviations**

#### **3.1 Définitions**

Pour les besoins de la présente Norme internationale, les définitions suivantes s'appliquent.

##### **3.1.1**

##### **disponibilité**

caractéristique d'une fraction de temps pendant laquelle un système est effectivement en état d'accomplir sa mission (AIEA 50-SG-D8)

##### **3.1.2**

##### **catégorie**

catégorie de sûreté A, B, C ou non classée, définie pour la fonction, le système ou le matériel selon la classification de la CEI 61226

##### **3.1.3**

##### **canal**

trajet distinct le long duquel le flux d'informations est acheminé au travers d'un système redondant ou distribué. Ce trajet peut également nécessiter une redondance (adapté à partir de la CEI 61500).

##### **3.1.4**

##### **diversité**

existence de deux ou plusieurs façons ou moyens différents d'atteindre un objectif spécifié. La diversité est spécifiquement prévue comme une défense contre les défaillances de mode commun. Elle peut être réalisée en prévoyant des systèmes physiquement différents les uns des autres, ou par une diversité fonctionnelle, où des systèmes similaires assurent les objectifs spécifiés de façon différente (voir article 3 de la CEI 61226).

IEC 60812:1985, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 60880:1986, *Software for computers in the safety systems of nuclear power stations*

IEC 60987:1989, *Programmed digital computers important to safety for nuclear power stations*

IEC 61225:1993, *Nuclear power plants – Instrumentation and control systems important for safety – Requirements for electrical supplies*

IEC 61226:1993, *Nuclear power plants – Instrumentation and control systems important for safety – Classification*

IEC 61500:1996, *Nuclear power plants – Instrumentation and control systems important to safety – Functional requirements for multiplexed data transmission*

IAEA 50-C-D(Rev. 1):1988, *Code on the safety of nuclear power plants – Design*

IAEA 50-SG-D3:1980, *Protection system and related features in nuclear power plants*

IAEA 50-SG-D8:1985, *Safety-related instrumentation and control systems for nuclear power plants*

### **3 Definitions and abbreviations**

#### **3.1 Definitions**

For the purpose of this International Standard, the following definitions apply.

##### **3.1.1**

##### **availability**

fraction of time that a system is actually capable of performing its mission (IAEA 50-SG-D8)

##### **3.1.2**

##### **category**

safety category as A, B, C or unclassified, defined for the function, system or equipment by classification to IEC 61226

##### **3.1.3**

##### **channel**

separate path along which information flows through a redundant or distributed system. That path may also require redundancy (adapted from IEC 61500).

##### **3.1.4**

##### **diversity**

existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defense against common mode failure. It may be achieved by providing systems that are physically different from each other, or by functional diversity, where similar systems achieve the specified objective in different ways (see clause 3 of IEC 61226).

### 3.1.5

#### **verrouillages électriques**

contacts auxiliaires ou matériel électriquement associé à l'appareil commandé et réagissant sur le circuit ou le matériel, afin que ceux-ci fonctionnent correctement, de la façon et dans l'ordre prévu

### 3.1.6

#### **intégrité**

qualité de complétude, fiabilité et absence de défaut

### 3.1.7

#### **verrouillages**

verrouillages monocanaux, bicanaux et multicanaux

- Les verrouillages monocanaux utilisent un seul canal de capteurs, d'unités logiques ainsi qu'un élément de manoeuvre tel qu'un contacteur ou un relais.
- Les verrouillages bicanaux utilisent deux canaux des matériels ou capteurs, disposés de façon que chaque canal puisse, indépendamment, éviter la condition ou l'état présentant un risque pour la sûreté. Les canaux peuvent comprendre deux ensembles de matériels globalement identiques. Une autre solution est que deux canaux différents remplissent les fonctions de verrouillage de façon différente, ou que deux canaux similaires fonctionnent l'un en mode normal et l'autre en mode de secours afin d'éviter l'apparition d'une condition ou d'un état présentant un risque pour la sûreté si le premier canal échoue.
- Les verrouillages multicanaux utilisent plusieurs canaux comprenant des matériels et capteurs. Ils sont disposés de façon que chaque canal puisse, indépendamment, éviter la condition ou l'état provoquant un risque pour la sûreté. Un canal défaillant ne peut pas bloquer les actions permettant d'éviter les conditions ou les états provoquant un risque pour la sûreté. L'utilisation de systèmes multicanaux peut offrir l'avantage de permettre la maintenance en ligne et d'éviter d'avoir besoin d'un contournement de canal.

### 3.1.8

#### **fonctions de verrouillage de sûreté**

fonctions faisant partie du système de contrôle-commande de la centrale, permettant d'éviter les conditions ou opérations présentant un risque pour la sûreté, de protéger le personnel et de prévenir les dangers

### 3.1.9

#### **redondance**

existence d'un nombre d'éléments ou de systèmes (identiques ou divers) supérieur au nombre minimal, de manière que la perte de l'un d'entre eux n'entraîne pas la perte de la fonction requise pour l'ensemble (AIEA 50-C-D)

### 3.1.10

#### **système de verrouillage de sûreté**

partie du système de protection empêchant certaines opérations susceptibles de porter atteinte à la sûreté du réacteur à moins que toutes les conditions prescrites ne soient remplies

### 3.1.11

#### **système de verrouillage de sûreté important pour la sûreté**

partie des systèmes électriques et des systèmes de contrôle-commande importants pour la sûreté empêchant ou limitant certaines opérations susceptibles de porter atteinte à la sûreté du réacteur à moins que toutes les conditions prescrites ne soient remplies

### 3.1.12

#### **logiciel**

programmes, procédures, règles et documentation associée se rapportant à l'exploitation d'un système informatique (voir 2.16 de la CEI 60880)

**3.1.5****electrical interlocks**

auxiliary contacts or equipment electrically associated with the controlled apparatus and reacting upon the control circuit or equipment to ensure the equipment operates safely and in the required manner or sequence

**3.1.6****integrity**

a quality of completeness, dependability and freedom from defects

**3.1.7****interlocks**

single-channel, double-channel and multi-channel interlocks

- Single-channel interlocks use a single channel of sensors, logic units and an actuation item such as a contactor or relay.
- Double-channel interlocks use two channels of equipment and sensors, arranged so that each channel is capable, on its own, of preventing the unsafe condition or state. The channels may consist of two sets of essentially identical equipment. An alternative is two different channels which perform the interlock functions differently, or two similar channels, one in normal operation and the other in backup operation to prevent an unsafe condition or state if the first channel fails.
- Multi-channel interlocks use several channels of equipment and sensors. They are arranged so that each channel is capable, on its own, of preventing the unsafe condition or state. One failed channel cannot block actions which prevent unsafe conditions or states. Use of multi-channel systems can provide benefits due to allowing on-line maintenance and avoiding the need for a channel bypass.

**3.1.8****interlock functions**

functions implemented as part of the instrumentation and control system of the plant, which prevent unsafe conditions or operations, protect personnel and prevent hazards

**3.1.9****redundancy**

provision of more than the minimum number of (identical or diverse) elements or systems, so that the loss of any one does not result in the loss of the required function of the whole (IAEA 50-C-D)

**3.1.10****safety interlock system**

that part of the protection system which prevents certain operations which may affect the safety of the reactor unless all prescribed conditions are met

**3.1.11****interlock system important to safety**

that part of the electrical and instrumentation and control systems important to safety which prevents or limits certain operations which may affect the safety of the reactor, unless all prescribed conditions are met

**3.1.12****software**

programs, procedures, rules and any associated documentation pertaining to the operation of a computer system (see 2.16 of IEC 60880)

### 3.2 Abréviations

EIH Événement initiateur hypothétique  
API Automate programmable industriel

## 4 Prescriptions

### 4.1 Prescriptions du système

#### 4.1.1 Prescriptions fonctionnelles des verrouillages de sûreté

Les fonctions de verrouillage de sûreté doivent être définies et documentées, et leur rôle de sûreté déterminé. Les fonctions, systèmes et matériels se rapportant aux verrouillages de sûreté doivent être classifiés à l'aide des critères de la CEI 61226 permettant l'attribution d'une catégorie (A, B, C ou non classée) et la détermination des prescriptions d'assurance de la fonctionnalité, de la fiabilité, des performances, de la résistance à l'environnement ainsi que d'assurance et de contrôle de la qualité.

Il est permis d'utiliser des fonctions de verrouillage de sûreté pour:

- a) empêcher qu'un opérateur ou qu'un système automatique n'effectue une opération incorrecte ou présentant un risque pour la sûreté;
- b) éviter l'apparition de conditions incorrectes ou présentant un risque pour la sûreté en limitant une action de commande;
- c) bloquer la progression d'une suite d'opérations jusqu'au rétablissement de conditions sûres ou correctes;
- d) générer un signal d'autorisation permettant de sélectionner la sortie d'un instrument uniquement dans sa gamme de fonctionnement;
- e) empêcher l'exploitation d'un matériel dans un certain mode de fonctionnement lorsque son exploitation, pour garantir la sûreté, nécessite un autre mode de fonctionnement;
- f) permettre le fonctionnement du matériel au-delà de sa fonction ou de sa base de conception prévue, si ce fonctionnement favorise la sûreté nucléaire dans des conditions dépassant les conditions de la base de conception;
- g) éviter que des dangers tels que l'incendie et la chute de charges n'engendrent une condition ou un état présentant un risque pour la sûreté.

Les fonctions de verrouillage de sûreté opérationnelles permettent typiquement l'arrêt et la mise en marche d'une pompe, l'arrêt des dispositifs de commande de vannes au niveau des limites, le blocage du démarrage d'une pompe lorsque les vannes sont fermées ainsi que des fonctions de commande et de conditionnement similaires. Les fonctions de verrouillage de sécurité de la centrale évitent la surcharge de moteurs ou d'actionneurs, empêchent l'exploitation de la centrale en dehors de son enveloppe normale et évitent son endommagement. Ces fonctions doivent être comprises dans le processus de classification des verrouillages. Des fonctions typiques de verrouillage, importantes pour la sûreté et significatives pour l'exploitation, sont indiquées à titre d'information dans l'annexe A, avec une référence croisée aux types de fonctions ci-dessus.

Il convient de vérifier la formulation des prescriptions en se référant à l'analyse de sûreté de la centrale. La simulation et la modélisation de la logique constituent des outils de réalisation du processus de vérification.

#### 4.1.2 Prescriptions de fiabilité des verrouillages

Les prescriptions de fiabilité et d'intégrité pour chaque fonction de verrouillage doivent être déterminées en se référant à l'analyse de sûreté de la centrale. Il convient d'utiliser les prescriptions de fiabilité et d'intégrité pour identifier les prescriptions de conception relatives à la redondance et de les utiliser conformément à la CEI 61226 pour identifier les moyens d'assurance de la fiabilité pour la catégorie.

## 3.2 Abbreviations

PIE Postulated initiating event  
PLC Programmable logic controller

## 4 Requirements

### 4.1 System requirements

#### 4.1.1 Interlock functional requirements

The interlock functions shall be defined and documented, and their safety role determined. The functions, systems and equipment for interlocks shall be classified using the criteria of IEC 61226 to assign them to a category (A, B, C or unclassified) and to determine the requirements for assurance of functionality, reliability, performance, environmental durability, and quality assurance and control.

Interlocks functions may be used:

- a) to prevent an unsafe or incorrect operation being taken by an operator or by an automatic system;
- b) to prevent conditions developing which are unsafe or incorrect by restricting a control action;
- c) to inhibit the progress of a sequence of operations until conditions are safe or correct;
- d) to generate a permissive signal to allow selection of the output of the instrument when it is in its operating range;
- e) to prevent operation of equipment in one operating mode when it is only safe to operate it in another operating mode;
- f) to permit the operation of the equipment beyond its intended function or design basis, if the operation would enhance nuclear safety in beyond design basis conditions;
- g) to prevent hazards such as fire and dropped load from causing an unsafe condition or state.

Operational interlock functions typically provide stopping and starting a pump, stopping of valve actuators at valve limits, prevention of pump start against closed valves and similar control or conditioning functions. Plant protection interlock functions prevent motor or actuator overload, plant operation outside its normal envelope and prevent plant damage. These functions shall be included in the interlock classification process. Typical interlock functions important to safety and significant to operation are given, for information, in annex A, with a cross reference to the above types of function.

The expression of requirements should be verified by reference to the safety analysis of the plant. Animation or modelling of the logic are tools for the verification process.

#### 4.1.2 Interlock reliability requirements

The reliability and integrity requirements for each interlock function shall be determined with reference to the safety analysis of the plant. The reliability and integrity requirements should be used to identify design requirements on redundancy and used as required by IEC 61226 in identifying the means of assurance of reliability for the category.

Il convient de déterminer les prescriptions de fiabilité et d'intégrité des verrouillages concernant la sûreté et la disponibilité au début du processus de conception. Des verrouillages fiables sont spécifiés pour assurer la sûreté, mais également pour des raisons de disponibilité et d'économie. Des restrictions d'accès en cas de réparation peuvent nécessiter une grande fiabilité.

Il convient, lors de la détermination des prescriptions de fiabilité des verrouillages, de tenir compte des conséquences que pourrait avoir la défaillance d'un verrouillage lorsque le blocage d'une action est requis et lorsque se produit un blocage intempestif.

## **4.2 Conception du système**

### **4.2.1 Configuration des verrouillages**

Des fonctions de verrouillage sont présentes dans de nombreux systèmes d'une centrale nucléaire. On utilise trois conceptions principales pour les verrouillages électriques: les verrouillages monocanaux, bicaux et multicanaux, comme indiqué dans les définitions.

Lorsqu'un verrouillage est nécessaire pour remplir une fonction de sûreté, il s'intègre dans le système de sûreté et doit être mis en oeuvre selon les mêmes prescriptions de conception que le système de protection. Il convient que les verrouillages de catégorie A qui ne font pas partie du système de sûreté soient aussi pris en compte dans ces prescriptions.

Il est admis de mettre en oeuvre des verrouillages multicanaux de catégorie A dans le système de protection, qui comprend normalement des canaux distincts de capteurs, de matériel de traitement et de fonctions de vote au sein de sa structure. Il est admis d'utiliser des ensembles multicanaux avec fonction de vote pour commander des actions, ou des ensembles bicaux, pour les verrouillages de catégorie B, de catégorie C ou non classés (verrouillages non importants pour la sûreté).

Lorsque l'on utilise des verrouillages bicaux ou multicanaux, il convient que les canaux redondants soient indépendants. Il convient d'éviter de dépendre d'éléments communs tels qu'un interrupteur unique ou le relais de commande associé. Il convient de considérer la possibilité d'utiliser des moyens fonctionnellement diversifiés pour obtenir la fonction de verrouillage. Par exemple, un verrouillage pour éviter l'écoulement de fluide sous certaines conditions pourrait être réalisé par un verrouillage monocanal pour éviter le démarrage d'une pompe, associé à un verrouillage monocanal pour éviter l'ouverture des vannes qui permettraient l'écoulement du fluide.

Lorsque l'on utilise des verrouillages bicaux ou multicanaux, il convient de démontrer que l'importance de la séparation des canaux, la dépendance vis-à-vis de types communs de composants ou de signaux, ainsi que la séparation physique et la protection contre des effets communs correspondent aux prescriptions de la catégorie.

Lorsque des verrouillages sont mis en oeuvre dans un calculateur ou dans un API, les prescriptions de la CEI 60987 et de la CEI 60880 sont applicables, selon l'importance pour la sûreté et la catégorie du verrouillage. Si l'on utilise un matériel de multiplexage, les prescriptions de la CEI 61500 sont applicables.

### **4.2.2 Priorité des verrouillages**

La priorité d'une action effectuée par un interrupteur ou un actionneur en réponse aux commandes et aux verrouillages doit être définie au niveau de la conception. La priorité doit tenir compte des verrouillages concernant la sûreté nucléaire, la protection contre l'incendie, la protection du personnel, la protection et l'exploitation de la centrale. La priorité de commande dépend des pratiques nationales et il convient de l'identifier pour toute centrale spécifique, afin de fournir une approche uniforme.

The interlock reliability and integrity requirements for safety and availability should be determined early in the design process. Reliable interlocks are specified for safety and also for availability and economic reasons. Restrictions on access for repair may require high reliability.

The determination of interlock reliability requirements should take into account the consequences of failure of an interlock to prevent action when required and of interlock operation when not required.

## **4.2 System design**

### **4.2.1 Interlock configuration**

Interlock functions exist in many different systems on a nuclear plant. Three main system designs are used for electrical interlocks, referred to as single-channel, double-channel and multi-channel interlocks, as given in the definitions.

When an interlock is required as a safety system function, it forms part of the safety system and shall be implemented to the same design requirements as the protection system. Interlocks in category A which do not form part of the safety system should also be implemented to those requirements.

Multi-channel category A interlocks may be implemented in the protection system, which normally includes separated channels of sensors and logic equipment and voting functions within its structure. Multi-channel arrangements with voting for actuation, or double-channel interlocks, may be used for category B, and may be used for category C or for unclassified interlocks (interlocks not important to safety).

Where double or multi-channel interlocks are used, then the redundant channels should be independent. Reliance on common elements, such as a single switchgear element or associated trip relay, should be avoided. The possibilities for use of functionally diverse means of providing the interlock function should be considered. For example, an interlock to prevent fluid flow under certain conditions could be implemented as a single-channel interlock to prevent energisation of a pump together with a single-channel interlock to prevent opening of valves which would allow flow.

When double or multi-channel interlocks are used, the importance of separation of channels, dependency on common types of components or signals and the physical segregation and protection from common effects should be shown to correspond to the requirements of the category.

When interlocks are implemented in computer-based or PLC equipment, the requirements of IEC 60987 and IEC 60880 are applicable, in accordance with the significance to safety and category of interlock. If multiplexing equipment is used, the requirements of IEC 61500 are applicable.

### **4.2.2 Interlock priority**

The priority of action taken by electrical switchgear or actuators in response to control commands and interlocks shall be defined in design. The priority shall take account of interlocks for nuclear safety, fire safety, personnel protection, plant protection and plant operation. Priority of command will depend on national practice and should be identified for any specific plant, in order to provide a uniform approach.

Il convient que la conception place les verrouillages de protection de la centrale à un niveau de priorité garantissant la protection de la centrale même pour des commandes de priorité élevée, sans provoquer de risque pour la sûreté nucléaire, de risque d'incendie ou de danger pour le personnel à la suite d'un endommagement de la centrale. Il convient de prendre en compte, au niveau de la priorité et de la conception des verrouillages de protection de la centrale, la nécessité (dans certaines centrales nucléaires) de neutraliser la protection de la centrale pour effectuer une manoeuvre de sûreté dans certaines circonstances particulières. Sur cette base, il convient d'attribuer aux verrouillages de protection de la centrale le niveau de priorité le plus élevé dans la plupart des cas, de manière qu'aucune commande ne puisse provoquer d'endommagement de la centrale. Dans certains cas, lorsque la centrale peut dépasser sa fonction et sa base de conception prévues à l'origine pour améliorer la sûreté nucléaire, il est admis de fixer la priorité de protection de la centrale à un niveau inférieur à celui de la commande des actionneurs du système de sûreté.

La priorité de verrouillage de sûreté et de commande dépend de chaque cas et des pratiques nationales. A titre de référence, la priorité de commande d'autres fonctions peut suivre l'ordre suivant, le chiffre 1 représentant la priorité la plus élevée:

- 1) verrouillage pour système de catégorie A ou commande des actionneurs de sûreté;
- 2) commande des actionneurs de lutte contre l'incendie ou verrouillage du système de protection contre l'incendie;
- 3) verrouillages de protection du personnel ou verrouillages de catégorie B;
- 4) verrouillages de catégorie C;
- 5) commande des actionneurs depuis la salle de commande ou verrouillages de sûreté opérationnels.

Dans cette liste, si un conflit apparaît entre des fonctions de même niveau, la première possède la priorité la plus élevée.

NOTE – La priorité peut être différente dans le cadre de l'application à une centrale spécifique. La priorité de référence indiquée attribue à la sûreté nucléaire l'importance la plus grande, et place ensuite la protection contre l'incendie car elle possède souvent des implications nucléaires et des implications pour la sûreté du personnel. La sûreté du personnel, la catégorie B et la catégorie C possèdent un niveau de priorité dérivé de la CEI 61226. Enfin, la salle de commande et l'exploitation de la centrale possèdent un niveau de priorité inférieur à la sûreté nucléaire ou à celle du personnel.

### **4.3 Intégrité des verrouillages de sûreté**

#### **4.3.1 Méthodes de verrouillage de sûreté**

Il convient, pour identifier une méthode appropriée de mise en oeuvre d'une fonction de verrouillage de sûreté, de commencer par définir les prescriptions de fiabilité relatives à cette fonction.

Il est permis d'utiliser des méthodes électriques, mécaniques et administratives pour réaliser une fonction de verrouillage de sûreté. Des méthodes administratives peuvent être nécessaires si aucune méthode physique ne permet d'empêcher une opération. Des mesures administratives peuvent être utilisées pour améliorer la fiabilité d'un verrouillage électrique de sûreté.

Pour la fiabilité de niveau le plus élevé, il se peut que deux méthodes différentes ou plus soient nécessaires pour fournir une fonction de verrouillage de sûreté. Il peut s'agir de verrouillages sur des éléments interactifs de la centrale, tels qu'une pompe et une vanne, ou à la fois une procédure administrative et un verrouillage électrique de sûreté. Les paragraphes suivants fournissent des recommandations relatives aux méthodes électriques.

#### **4.3.2 Prescriptions de redondance**

La catégorie de la fonction de verrouillage de sûreté et la fiabilité requise doivent être utilisées pour déterminer si un verrouillage monocal, bicanal ou multicanal est nécessaire, et pour définir la nécessité de capteurs ou de verrouillages différents. Le paragraphe 8.2.2 de la CEI 61226 fournit des prescriptions relatives aux fonctions de catégorie A. Pour obtenir une fiabilité supérieure à celle d'un verrouillage de sûreté multicanal, il convient de fournir un verrouillage supplémentaire de sûreté différent.

The design should place plant protection interlocks at a priority such that the plant is protected even for high-priority commands and does not cause a nuclear safety challenge, fire or personnel hazard due to plant damage. Plant protection interlock priority and design should take account of the need (on some nuclear plants) to override plant protection to achieve a safety actuation in special circumstances. On this basis, plant protection interlocks should be at the highest priority for most cases, such that no command can cause damage to plant. For some cases, where the plant can be operated beyond its originally intended function and design basis if it enhances nuclear safety, the priority of plant protection may be lower than that of the safety actuation system command.

Interlock and command priority depends on each case and on national practice. To provide a reference, the priority of command of other functions may be in the following order, with 1 as highest priority:

- 1) interlock at category A or safety actuation system command;
- 2) fire safety actuation command or fire safety interlock;
- 3) personnel protection interlock or interlock at category B;
- 4) interlock at category C;
- 5) control room actuation command or operational interlock.

In this list, if conflict is found between functions at the same level, the first is of higher priority.

NOTE – The priority may be different for application to a specific plant. The reference priority given shows nuclear safety with highest importance, and fire safety next, since it often has nuclear implications as well as personnel safety implications. Personnel safety, category B and category C are in a priority order derived from IEC 61226. Finally, control room and plant operation has lower priority than nuclear or personnel safety.

### **4.3 Interlock integrity**

#### **4.3.1 Interlock methods**

The identification of a suitable method for implementing an interlock function should start from the definition of reliability requirements for the function.

Electrical, mechanical and administrative methods may be used to achieve an interlock function. Administrative methods may be needed where no physical method of preventing an operation is practicable. Administrative measures may be used to enhance an electrical interlock reliability.

For the highest reliability, two or more different methods of providing an interlock function may be needed. This may involve interlocks on interacting plant items, such as a pump and a valve, or both an administrative control and electrical interlocking. The following subclauses give recommendations for electrical methods.

#### **4.3.2 Redundancy requirements**

The category of the interlock function and the reliability required shall be used to determine if a single-channel, double-channel or multi-channel interlock is necessary, and to determine any need for diverse sensors or interlocks. For category A functions, 8.2.2 of IEC 61226 gives requirements. For greater reliability than that achievable for a multi-channel interlock, an additional diverse interlock should be provided.

Les fonctions de verrouillage de sûreté imposent que la redondance du système respecte le critère de défaillance unique. Par conséquent, il convient d'évaluer la mise en oeuvre de la fonction de verrouillage sur la base d'une défaillance potentielle. Si la défaillance d'un verrouillage de sûreté de catégorie A affecte un seul élément redondant de la centrale et n'empêche pas la réduction des effets d'un incident par un élément redondant de la centrale, un canal de verrouillage de sûreté unique peut être suffisant sur une base déterminée. Si une défaillance d'un verrouillage de sûreté est susceptible de provoquer un EIH, d'affecter plus d'un canal redondant ou de provoquer le relâchement de produits radioactifs, il convient de fournir une redondance au niveau de la mise en oeuvre du verrouillage de sûreté d'une manière telle qu'une défaillance unique ne puisse pas faire obstacle à l'action de sûreté. Certaines fonctions de verrouillage de catégorie A peuvent éventuellement permettre l'essai de vannes ou des opérations de maintenance prioritaires par rapport à des commandes d'actionneurs de sûreté potentielles, et il est admis d'utiliser des verrouillages monocanaux si la durée du fonctionnement est restreinte selon une procédure administrative adaptée.

Il se peut qu'une stratégie de conception spécifique impose un verrouillage bicanal sur une base déterministe, afin d'atteindre des niveaux de fiabilité spécifiques, ou pour certaines catégories de sûreté spécifiques. Les verrouillages de catégorie A sont donc susceptibles de nécessiter des verrouillages bicanaux ou multicanaux dans certains pays. La CEI 61226 (paragraphe 8.2.2) privilégie la redondance pour les fonctions de catégorie B. L'annexe B fournit à titre d'information des lignes directrices concernant la fiabilité type pouvant être obtenue à partir de verrouillages monocanaux, bicanaux et multicanaux, avec des applications types, n'utilisant pas de calculateur.

#### 4.3.3 Evaluation de la fiabilité

La conception du système de verrouillage doit être évaluée afin d'estimer la fiabilité des verrouillages importants pour la sûreté. Il convient d'estimer la fiabilité pour d'autres verrouillages afin de montrer que les prescriptions de disponibilité sont respectées. Il convient de tenir compte, pour l'estimation, de la probabilité de défaillance de mode commun. Lorsqu'on utilise un matériel de verrouillage de sûreté programmé, la fiabilité du matériel informatique doit être évaluée. La méthodologie utilisée pour développer le logiciel doit être adaptée à partir de la CEI 60880 en fonction de la catégorie de verrouillage de sûreté déterminée en utilisant la CEI 61226.

Il convient que les estimations de fiabilité prennent en compte les éléments suivants:

- type de matériel (technologie, conception nouvelle ou éprouvée, fonctionnement à pannes sûres);
- complexité de la conception;
- nombre de dispositifs utilisés au niveau des verrouillages de sûreté;
- taux de défaillance du matériel;
- environnement;
- ségrégation des canaux;
- test, auto-test et indications de défaillance;
- couverture des défaillances par les tests et auto-tests;
- intervalles entre les tests et entre les auto-tests;
- fréquence d'utilisation opérationnelle des verrouillages de sûreté;
- contrôle d'accès;
- temps de début et durée de réparation des défaillances.

Il convient également de tenir compte, dans le cadre de l'évaluation de la fiabilité, de la façon dont les défaillances apparaissent, en considérant les défauts apparaissant immédiatement, par des enregistrements périodiques, des essais fonctionnels ou des essais de performances complets. Les opérations d'étalonnage de l'opérateur et les essais fonctionnels peuvent imposer une limite de défaillance d'origine commune, qu'il convient de prendre en compte pour l'évaluation de la fiabilité.

Il convient d'utiliser une analyse de fiabilité du matériel pour déterminer un intervalle approprié entre les essais. Il convient de confirmer par les essais le bon fonctionnement des verrouillages de sûreté. Si une opération a lieu à un moment défini, la réalisation d'un essai sur un verrouillage associé peut être possible immédiatement avant l'opération pour montrer qu'il fonctionne correctement.

Safety interlock functions require system redundancy to meet the single failure criterion. Therefore, the implementation of the interlock function should be assessed on the basis of potential failure. If failure of the interlock at category A affects one redundant plant item only, and does not prevent a mitigating action by a redundant plant item, then a single interlock channel may be sufficient on deterministic grounds. If a failure of the interlock could cause a PIE or affect more than one redundant channel, or cause an activity release, then redundancy should be provided in the interlock implementation so that a single failure cannot prevent the safety action. Some interlock functions at category A may permit valve testing or maintenance operations to override potential safety actuations, and single-channel interlocks may be used if the operation is of restricted duration under suitable administration.

A specific plant design strategy may require a double-channel interlock on a deterministic basis, to meet specific reliability levels, or for specific safety categories. Category A interlocks may therefore require double-channel or multi-channel interlocks in some countries. Sub-clause 8.2.2 of IEC 61226 prefers redundancy for category B functions. Annex B gives guidance on the typical reliability which can be achieved from single-channel, double-channel and multi-channel interlocks, with typical applications, not using computers.

#### 4.3.3 Reliability assessment

The interlock system design shall be assessed to estimate the reliability for interlocks important to safety. The reliability should be estimated for other interlocks to show that availability requirements are met. The estimation should include consideration of common mode failure probability. Where computer-based interlock equipment is used, the reliability of the computer hardware shall be assessed. The methodology used to develop the software shall be adapted from IEC 60880 suitably for the category of interlock, determined using IEC 61226.

The estimates of reliability should take into account:

- type of equipment (technology, new or proven design, inherently fail-safe operation);
- complexity of the design;
- number of devices used in the interlock;
- equipment failure rates;
- environment;
- channel segregation;
- test, self-test and failure indications;
- coverage of failures by the test and self-test features;
- intervals between tests and between self-tests;
- frequency of operational use of the interlock;
- access control;
- time to start and complete repair of failures.

The reliability assessment should also take into account how faults are revealed, allowing, as appropriate, for faults revealed immediately, by routine logging, by functional testing or by full performance testing. The operator actions of calibration and functional testing can impose a common cause failure limit and should be taken into account in assessing reliability.

A hardware reliability analysis should be used to determine an appropriate interval between tests. The tests should confirm that the interlock operates correctly. If an operation takes place at a known time, a test of an associated interlock may be possible immediately before the operation to show that it is functioning correctly.

L'analyse des modes de défaillance et de leurs effets (AMDE) doit être effectuée pour les systèmes de catégorie A et B et est recommandée pour les systèmes de verrouillage de catégorie C, suivant les méthodes de la CEI 60812.

#### **4.4 Matériel de verrouillage de sûreté**

##### **4.4.1 Signaux d'entrée**

Les verrouillages bicanaux et multicanaux doivent utiliser des signaux d'entrée distincts, provenant de capteurs, de contacts et d'interrupteurs de fin de course séparés. Lorsque des signaux redondants surveillent une condition pour des canaux redondants, chaque signal doit être traité indépendamment. Des signaux d'initialisation unique peuvent éventuellement être acceptables pour deux canaux ou plus si des mémoires intermédiaires sont utilisées selon des conceptions à sûreté intégrée.

Lorsqu'un capteur peut présenter une défaillance et provoquer la défaillance d'un verrouillage de sûreté sans que le danger soit détecté, il convient d'effectuer des mesures ou une détection d'état redondantes et d'utiliser un verrouillage bicanal ou multicanal.

Il convient que le concepteur note que des commutateurs multiples sur le même dispositif, tels que des interrupteurs de fin de course actionnés par le mouvement d'une tige de vanne, peuvent fonctionner à différents moments et engendrer une synchronisation différente pour la fonction de vote requise.

##### **4.4.2 Matériel pour le traitement des verrouillages de sûreté**

Il est permis d'intégrer les fonctions de verrouillage de sûreté dans la fonctionnalité d'autres matériels de la même catégorie, tels qu'un organe de manœuvre, un matériel de commande, le système de protection ou le système de commande des actionneurs de sûreté.

Il convient de placer le matériel de verrouillage de sûreté dans des unités ou des structures séparées au sein d'un système s'il est nécessaire que le verrouillage de sûreté soit indépendant des autres fonctions du système. L'indépendance d'un verrouillage vis-à-vis des autres matériels associés peut éventuellement être nécessaire afin de limiter la possibilité d'inhibition inappropriée de son fonctionnement au cours de la maintenance. Il convient de garantir une indépendance entre les verrouillages opérationnels et les verrouillages de protection d'un système. Il convient que les matériels de verrouillage de protection soient, dans la mesure du possible, séparés physiquement de tous les circuits de commande normale. Il convient que les capteurs, les circuits et les dispositifs d'actionnement qui sont utilisés par les verrouillages de protection ne soient pas partagés. Quand on utilise des verrouillages bicanaux ou multicanaux, il n'est pas exclu qu'une séparation entre les canaux soit nécessaire pour limiter les effets d'une défaillance d'origine commune, ou soit prescrite par l'AIEA 50-SG-D3 (voir 3(7), 7.5, 9.1), AIEA 50-SG-D8 (voir 2.2(1), (7), (8), (9), (10), 4.3.1) ou l'AIEA 50-C-D section 7.

Le matériel de verrouillage de sûreté peut fournir des informations à un opérateur de façon directe ou par l'intermédiaire de signaux envoyés aux systèmes d'affichage de la salle de commande, concernant les conditions préalables nécessaires au lancement sûr ou correct de certaines opérations, quand plusieurs vérifications sont requises.

Des verrouillages électriques utilisant un matériel à base de relais ayant fait ses preuves peuvent être utilisés pour des systèmes simples; on privilégie cependant les solutions utilisant des composants électroniques. Certaines exceptions peuvent être nécessaires concernant les interrupteurs de fin de course, les voyants, les contacteurs de moteur, les relais pour les circuits de sortie et les commutateurs manuels. Les normes nationales applicables au matériel de relais doivent être suivies.

Il convient que les verrouillages de catégorie A ou B utilisent un matériel de traitement à sûreté intégrée fonctionnant sur un principe dynamique. Pour les verrouillages de catégorie A, particulièrement dans le cas de fonctions simples, il convient d'utiliser une logique câblée pour réduire les prescriptions de validation par rapport aux systèmes programmés. Il est permis d'utiliser une logique à relais lorsque l'isolation électrique est importante. Les systèmes informatiques sont adaptés dans le cas de verrouillages étendus et d'opérations séquencées.

Failure mode and effect analysis (FMEA) shall be carried out for category A and B systems and should be carried out for category C systems of interlocks, following the methods of IEC 60812.

## **4.4 Interlock equipment**

### **4.4.1 Input signals**

Double and multi-channel interlocks shall use separate input signals for each channel, from separate sensors, contacts and limit switches. Where redundant signals monitor one condition for redundant channels, each signal shall be processed independently. Single initiation signals may be acceptable for two or more channels if buffering is used with fail safe designs.

Where a sensor can fail and cause an interlock to fail, without the danger being detected, the measurements or state detection should be redundant, and the interlock should be double or multi-channel.

The designer should note that multiple switches on the same device, such as limit switches actuated by the movement of a valve stem, can operate at different times and result in different timing of voted interlock requirements.

### **4.4.2 Interlock logic equipment**

The interlock functions may be included in the functionality of other equipment at the same category such as switchgear, control equipment, the protection system, or the safety actuation system.

Interlock equipment should be in separate units or cabinets of a system if interlock independence is needed from other system functions. Independence of an interlock from the other associated equipment may be needed to limit the possibility of incorrect override of its action during maintenance. Independence should be provided between the operational interlocks and the protection interlocks of a system. Where possible, protection interlock equipment should be physically separate from any normal control circuits. Sensors, circuits and actuating devices which are used by the protection interlocks should not be shared. Where double- or multi-channel interlocks are used, separation between the channels to limit common cause failure effects may be necessary, or can be required by IAEA 50-SG-D3 (see 3(7), 7.5, 9.1), IAEA 50-SG-D8 (see 2.2(1), (7), (8), (9), (10), 4.3.1) or IAEA 50-C-D section 7.

Interlock equipment may provide information to an operator directly or by signals to control room display systems on the pre-conditions necessary before some operation may be initiated safely or correctly, when many checks are needed.

Electrical interlocks using relay equipment with a proven record may be used for simple systems, however solid-state components are preferred. Exceptions may be necessary for limit switches, lamps, motor contactors, relays for output circuits and manually operated switches. Applicable national standards for relay equipment shall be followed.

Interlocks of category A or B should use failsafe logic equipment operating on a dynamic principle. For Category A interlocks, particularly for simple functions, hardwired logic should be used to reduce requirements for validation compared to systems using computer software. Relay logic may be used where electrical isolation is important. Computer-based systems are suitable where extensive interlocks and sequenced operations are involved.

Les verrouillages monocanaux peuvent utiliser un matériel normalisé de haute qualité et une pratique correspondant à celle utilisée pour les verrouillages d'interrupteurs. Il est permis de mettre en oeuvre des verrouillages de protection monocanaux ou des verrouillages opérationnels par le biais de connexions entre interrupteurs de fin de course et relais de commande. Cela peut être effectué au niveau de l'organe de commande, ou par montage dans des armoires, coffrets ou tableaux proches de l'organe de commande.

Lorsque des verrouillages bicaux ou multicanaux sont nécessaires, chaque canal doit effectuer la logique de verrouillage de sûreté de façon indépendante. Les verrouillages bicaux peuvent comprendre deux canaux similaires, un en fonctionnement normal et l'autre en secours afin d'éviter l'apparition d'une condition ou d'un état présentant un risque pour la sûreté en cas de défaillance du premier canal. Un verrouillage de sûreté bicanal peut inclure un canal remplissant une fonction de verrouillage de sûreté et un autre canal remplissant une fonction de verrouillage de sûreté indépendante et fonctionnellement différente. Dans certains cas, un verrouillage de sûreté opérationnel au sein d'un système peut nécessiter un verrouillage de protection séparé situé dans des unités indépendantes, ou dans un système indépendant.

Si tous les canaux de verrouillage de sûreté sont identiques, il convient que des comparaisons séparées soient effectuées entre les états détectés ou traités par chaque canal, afin de détecter les défaillances et déclencher des alarmes. Ces caractéristiques ne doivent pas compromettre l'indépendance entre les canaux redondants. Il convient, en cas de détection d'une différence entre deux canaux, que le verrouillage de sûreté agisse afin de favoriser la sûreté ou de manière à conserver l'état de sûreté précédent.

Une fonction de verrouillage de sûreté bicanal peut être mise en oeuvre sous la forme de verrouillages de sûreté monocanaux séparés situés sur deux éléments de la centrale; une défaillance simultanée des verrouillages de sûreté sur les deux éléments est ainsi nécessaire pour qu'il apparaisse un danger potentiel. Une défaillance sur l'un ou l'autre canal doit déclencher des alarmes, et il est recommandé d'utiliser des contacts ou signaux auxiliaires pour surveiller l'état de la centrale.

Lorsque l'indépendance est nécessaire, il convient de s'assurer que la défaillance d'un canal ne peut pas se propager à d'autres canaux et conduire ainsi à une situation dangereuse.

#### **4.4.3 Connexions de verrouillages de sûreté**

Les verrouillages peuvent requérir des câbles de liaison souples ou des connexions enfichables avec une installation mobile. Ce point est important dans le cas du matériel utilisé pour le transport du combustible du réacteur ou pour la manipulation ou le soulèvement des principaux composants du réacteur. La fiabilité de ces connexions et câbles doit faire l'objet d'une attention particulière. Le matériel de verrouillage de sûreté peut être monté sur l'installation déplacée afin de réduire le nombre de connecteurs. Le montage physique doit garantir le blocage des opérations à moins que l'ensemble des verrouillages de sûreté reliés ne soit en opération.

Les signaux d'autorisation détectés dans une partie du système peuvent être nécessaires à d'autres parties du système de verrouillage de sûreté, ou à d'autres matériels. Les signaux doivent être disposés de manière que le verrouillage instaure une situation sûre ou conserve l'état de sûreté précédent si le signal d'autorisation est déconnecté ou s'il est invalide. Les prescriptions de la CEI 61500 concernant la transmission de signaux dans les systèmes multiplexés sont applicables.

Les signaux de verrouillage de sûreté et les signaux d'autorisation présentant des connexions sur borniers, connecteurs montés sur cartes, ou par fiches et prises doivent être conçus pour aller dans le sens de la sûreté ou conserver l'état de sûreté précédent en cas de circuit ouvert ou de déconnexion. Il convient de disposer de connexions avec des témoins permettant de déclencher des alarmes si les connecteurs, châssis, modules ou cartes sont déconnectés.

Single-channel interlocks may use standard high quality power station equipment and practice as followed for switchgear interlocks. Single-channel protection or operational interlocks may be implemented by connections from plant limit switches to switchgear relays. These may be within the switchgear, or mounted in cabinets, boxes or panels near the switchgear.

When double or multi-channel interlocks are required, each channel shall perform the interlock logic independently. Double-channel interlocks may include two similar channels, one in normal operation and the other in backup operation to prevent an unsafe condition or state if the first channel fails. A double-channel interlock may involve one channel performing one interlock function, and the other an independent and functionally diverse safety interlock function. In some cases, an operational interlock within a system may require a separate protection interlock in independent units, or in an independent system.

When all interlock channels are the same, separate comparisons should be made between the states detected or processed by each channel to detect failures and provide alarms. These features shall not compromise independence between redundant channels. Detection of a difference between two channels should actuate the interlock in a direction which is chosen to enhance safety or retain the previous safe state.

A double-channel interlock function may be implemented as separate single-channel interlocks on two plant items, such that the interlocks must fail to operate on both items before potential danger results. Failure of either channel shall provide alarms, and auxiliary contacts or signals should be used to monitor plant state.

Where independence is required, it should ensure that the failure of one channel cannot propagate into other channels in a manner able to result in danger.

#### **4.4.3 Interlock connections**

Interlocks may require flexible cables and plug-in connections for a movable plant. This is important for reactor fuel handling equipment and equipment for handling or lifting major reactor plant components. Special attention shall be given to the reliability of these connections and cables. The interlock equipment may be mounted on the plant which is moved to reduce the number of connectors. The physical arrangements shall ensure that plant operations are inhibited unless all related interlocks are functional.

Permissive signals detected in one part may be needed by other parts of the interlock system, or by other equipment. The signals shall be arranged to actuate the interlock towards a safe condition or to retain the previous safe state if the permissive signal is disconnected or is invalid. The requirements of IEC 61500 for signal transmission in multiplexed systems are applicable.

Interlock signals and permissives which have connections by screw terminals, logic card edge connectors or plugs and sockets shall be arranged to actuate the interlock in a direction which is chosen to enhance safety or to retain the previous safe state for open circuit or disconnection. Trace connections should be provided to operate alarms if connectors, logic chassis, modules or cards are disconnected.

#### 4.4.4 Commande de verrouillage de sûreté

Des signaux de commande provenant d'un matériel logique sont nécessaires pour que les verrouillages empêchent ou autorisent le fonctionnement d'un organe de manoeuvre, d'un matériel de commande de vannes, d'électrovannes, de contrôleurs ou de moteurs. Lorsqu'un verrouillage de sûreté bicanal ou multicanal est nécessaire, on doit effectuer au moins deux coupures distinctes d'alimentation finale au niveau de l'installation ou de son équivalent afin d'empêcher toute opération. Des méthodes possibles sont décrites ci-dessous.

Parmi les dispositions qui peuvent être utilisées pour les verrouillages de sûreté bicaux et multicaux, on distingue (mais la liste n'est pas exhaustive):

- deux coupures de circuits réalisées électriquement sur chaque côté de la commande finale;
- coupure de circuit sur chaque borne positive et négative d'une alimentation en courant continu;
- contacteurs triphasés, avec deux coupures de circuit séparées, au niveau d'une alimentation;
- arrêt du fonctionnement par une première méthode consistant à couper l'alimentation d'un actionneur final, et par une seconde méthode consistant à appliquer séparément une force de freinage;
- méthodes permettant d'annuler le fonctionnement d'un canal dans un état dangereux, grâce à la mise en oeuvre d'une chaîne de secours.

Il est recommandé que le matériel combinant les canaux de verrouillage de sûreté nécessite une harmonisation de tous les canaux avant d'autoriser le fonctionnement. Certaines fonctions peuvent exiger un blocage du fonctionnement par n'importe quel canal. D'autres fonctions peuvent exiger que la moitié de tous les canaux ou qu'une majorité de canaux en état de blocage de fonctionnement arrêtent le fonctionnement. Une défaillance de l'actionneur de verrouillage de sûreté doit se dérouler de manière à instaurer une condition de sûreté ou conserver l'état de sûreté précédent.

#### 4.5 Documentation

Il convient que la documentation fasse apparaître clairement la fonction de chaque verrouillage de sûreté, et son rapport avec les opérations de protection, de commande, les fonctionnements séquentiels ou les actions de l'opérateur.

La logique de verrouillage de sûreté de chaque fonction de verrouillage de sûreté doit être représentée par des schémas logiques selon la forme normalisée utilisée par le reste du système intégrant le verrouillage de sûreté. Les conventions de la CEI 60617-12 se rapportant à la représentation logique sont applicables. Il convient de présenter les fonctions de verrouillage de sûreté répétées ou similaires sous un format normalisé de façon à pouvoir reconnaître facilement les similarités de circuit ou les similarités logiques.

Il est recommandé de joindre une liste détaillée de tous les verrouillages importants pour la sûreté dans la documentation relative à la centrale.

#### 4.6 Matériel programmé

On souligne l'importance des prescriptions de la CEI 60880 et de la CEI 60987, relatives à la documentation, la vérification, la validation et les auto-tests.

Les prescriptions de la CEI 60880 sont applicables aux logiciels des verrouillages de sûreté programmés importants pour la sûreté, selon la répartition des catégories définie par la CEI 61226. Les produits logiciels (de qualité industrielle) courants, propres à un constructeur, peuvent être acceptables pour des verrouillages sans importance pour la sûreté (verrouillages «non classés», selon la CEI 61226).

#### 4.4.4 Interlock actuation

Interlocks require actuation signals from logic equipment to prevent or permit operation of switchgear, valve control equipment, solenoid valves, controllers or motors. When a double or multi-channel interlock is needed, two or more separate interruptions of the final power to plant or its equivalent, to prevent action, shall be provided. Possible methods are described below.

Arrangements which may be used for double or multi-channel interlocks include but are not restricted to:

- two circuit interruptions performed electrically on either side of the final actuation;
- circuit interruption on both positive and negative sides of a d.c. power supply;
- three-phase contactors, with two separate circuit interruptions, in one supply;
- final actuator power interruption as one method of preventing action, and the separate application of a braking force as the other method of preventing action;
- methods to override the action of a channel in a dangerous state, by the safe action of a standby channel.

The equipment which combines the interlock channels should require all channels to agree before operation is allowed. Some functions may require that any channel shall be capable of preventing operation. Other functions may require that half of all channels, or a majority, in the state for preventing operation, should prevent operation. Failure of the interlock actuator shall be arranged in a direction which is chosen to enhance safety or to retain the previous safe state.

#### 4.5 Documentation

The documentation should make clear the function of each interlock, and its relation to protection, control or sequential operations, or to operator actions.

The interlock logic of each interlock function shall be represented by logic diagrams in the standard form used by the remainder of the system which includes the interlock. The conventions of IEC 60617-12 on logic representation are applicable. Interlock functions which are repeated or are similar should be shown in a standard format so that circuit or logic similarities can be easily recognized.

A comprehensive list of all interlocks important to safety is recommended for inclusion in the documentation of the plant.

#### 4.6 Computer-based equipment

Specific attention is drawn to the requirements of IEC 60880 and IEC 60987 for documentation, verification and validation and self-testing.

The requirements of IEC 60880 are applicable to the software in computer-based interlocks important to safety, according to the categorization defined in IEC 61226. Normal proprietary (industrial quality) software products may be acceptable for interlocks not important to safety (interlocks “not classified”, under IEC 61226).

Il est admis d'utiliser un matériel programmé de qualité reconnue pour les verrouillages de sûreté monocanaux. Les prescriptions nécessitant des verrouillages de sûretés bicaux ou multicanaux, mis en oeuvre par deux canaux programmés ou plus, peuvent présenter une sensibilité à la défaillance de mode commun (CMF) du fait de défauts de logiciel précédemment inconnus. Il convient d'analyser la sensibilité à la CMF selon la méthode indiquée dans la CEI 60880.

Si l'on utilise un matériel programmé, normalisé, de qualité industrielle et propre à un constructeur, la fiabilité et l'intégrité peuvent être limitées par les performances du logiciel. Pour des prescriptions de fiabilité supérieures à la valeur pouvant être atteinte dans le cas d'un verrouillage de sûreté monocanal, il convient de fournir un canal de verrouillage de sûreté supplémentaire indépendant et différent.

Il est recommandé que le système programmé utilisé pour les verrouillages fournisse des programmes d'application permettant une définition simple de la logique. Il convient que le système puisse afficher et enregistrer leurs actions et états logiques.

Il est recommandé que les logiciels d'application de verrouillage de sûreté fournissent des moyens de surveillance en ligne permettant de suivre directement la logique de verrouillage de sûreté des chemins logiques activés. Il convient que les verrouillages et états de l'installation puissent être affichés pour les essais et la mise en service.

#### 4.7 Actions de l'opérateur

Les actions de l'opérateur peuvent être intégrées dans une fonction de verrouillage de sûreté. Cela s'avère nécessaire lorsque la fonction intègre une intention humaine (par exemple, déroulement de la mise en service du réacteur avec sélection et verrouillage de sûreté des mesures de flux correctes en vue d'une utilisation par le système de sûreté). Une procédure administrative peut être nécessaire afin d'autoriser l'action de l'opérateur. L'intervention de l'opérateur au niveau de la vérification, du déblocage de touches et de commandes bloquées peut constituer le seul moyen possible de réaliser certaines fonctions de verrouillage de sûreté. Dans ce cas, il convient de prendre en compte les éléments suivants:

- enregistrement automatique des commandes utilisées par l'opérateur;
- utilisation de deux méthodes différentes de vérification de signaux visuels tels que le numéro d'identification de l'élément, l'identité du canal, les valeurs de mesure;
- enregistrement automatique des autorisations de fonctionnement;
- communication par le personnel des opérations effectuées.

Pour ce type d'action réalisée par une seule personne, il est toujours recommandé de faire une vérification par une autre personne. Il est recommandé qu'aucune fausse manoeuvre de l'opérateur ne puisse en elle-même provoquer un danger sans défaillance coïncidente du verrouillage de sûreté. Si un opérateur n'utilise pas de commutateur ou de commande d'autorisation sur un verrouillage de sûreté, le verrouillage doit être orienté vers un état sûr. Deux actions d'opérateur distinctes, différentes par nature, peuvent constituer une méthode acceptable pour remplir une prescription de verrouillage de sûreté dans certains cas particuliers où aucune méthode mécanique ou électrique n'est possible.

#### 4.8 Alimentation électrique

Il convient de concevoir l'alimentation électrique du matériel d'acquisition et de traitement des verrouillages de sûreté à partir de l'alimentation du système de contrôle-commande (I&C) conformément à la CEI 61225. Il convient que les verrouillages de sûreté bicaux et multicanaux comprennent des alimentations séparées pour chaque canal de verrouillage. Les verrouillages doivent toujours être capables de réaliser l'action de sûreté en cas de défaillance d'une seule source d'alimentation. Lorsque les manoeuvres de verrouillage de sûreté font intervenir un actionneur électrique de l'installation, il est recommandé d'utiliser l'alimentation des relais de commande de l'actionneur directement pour les manoeuvres de faible puissance, et il est permis de l'utiliser pour le matériel d'acquisition et de traitement.

Computer-based equipment of proven quality may be used for single-channel interlocks. Requirements which need double or multi-channel interlocks, implemented by two or more computer-based channels, can be sensitive to common mode failure (CMF) due to previously unknown software faults. The sensitivity to CMF should be analysed in accordance with the method given in IEC 60880.

If standard, industrial quality, proprietary computer-based equipment is used, the reliability and integrity can be limited by the performance of the software. For reliability requirements greater than the achievable figure for a single-channel interlock, an additional independent and diverse interlock channel should be provided.

The computer-based system used for interlocks should provide application program facilities to allow simple definition of logic. The system should be able to display and record their actions and logic states.

Interlock application software should provide on-line monitoring facilities which allow the interlock logic to be followed with direct monitoring of the activated logic paths. The interlocks and plant states should be able to be displayed for test and commissioning.

#### 4.7 Operator actions

Operator actions may be part of an interlock function. These are necessary where human intention is part of the function (e.g., the progress of reactor start-up with selection and interlocking of the correct flux measurements for use by the safety system). Administration can be needed to authorize operator action. Operator actions for checks, release of keys and locked controls may be the only practicable means of achieving some interlock functions. In such cases, consideration should be given to the following:

- automatic records of operator use of controls;
- use of two different methods of checking visual signals such as item identification number, channel identity, measurement values;
- automatic records of authorization for operations;
- staff communication of operations made.

Such action by one person should always be checked by a second person. Wrong operator action should not by itself cause danger without coincident interlock failure. Failure of an operator to use a permissive switch or control on an interlock shall result in the interlock retaining or producing a safe state. Two separate operator actions, different in nature, may be an acceptable method of achieving an interlock requirement in special cases where no mechanical or electrical method is possible.

#### 4.8 Power supplies

The power supplies for the interlock logic equipment and input signals should be taken from instrumentation and control (I&C) supplies designed in accordance with IEC 61225. Double and multi-channel interlocks should include separate power supplies for each interlock channel. The interlocks shall still be able to provide the safe action if a single supply source fails. Where interlock actuations involve the electrical switchgear of the plant, the power supplies for the switchgear control relays should be used directly for low power actuations, and may be used for the logic equipment and input signals.

## **5 Méthodes d'essai**

### **5.1 Installations d'essai et de surveillance**

Il est recommandé que l'équipement de verrouillage de sûreté comprenne des fonctions de surveillance étendues permettant une localisation rapide des défauts et une indication de l'état pour chaque condition logique et chaque commande de verrouillage. Il convient de fournir des installations d'essai automatiques. Lorsque les installations d'essai ne sont pas incorporées, on doit intégrer, au niveau de la conception, certaines méthodes garantissant que le matériel d'essai ne puisse rester connecté à la fin des essais. Il convient de fournir des installations de contrôle de continuité des circuits de sortie. Des méthodes utilisant des signaux d'essai impulsionnels ou à haute fréquence peuvent être utilisées pour permettre les essais en service.

Le matériel de verrouillage de sûreté doit être conçu et construit afin de permettre de réaliser des essais démontrant le bon fonctionnement des verrouillages en cas de besoin.

Il doit être possible de pratiquer des essais démontrant que chaque verrouillage de sûreté dans chaque canal effectue l'action correcte. Il convient que le matériel d'essai ne soit pas en mesure de compromettre les verrouillages. Tout matériel d'essai intégré doit être pris en compte dans l'analyse des performances, de l'intégrité et de la fiabilité d'un verrouillage de sûreté.

### **5.2 Outils d'essai automatiques**

Il est recommandé d'envisager des installations d'essai automatiques lors de la conception, afin de donner la possibilité de procéder à des essais réguliers et précis au niveau des fonctions de verrouillage. Il est recommandé que les installations d'essai automatiques puissent fournir systématiquement un enregistrement des essais et de leurs résultats.

L'essai automatique d'un canal redondant ne doit pas empêcher l'action de verrouillage de sûreté correcte par d'autres canaux.

Il est permis d'utiliser des installations d'essai automatiques pour faire apparaître des défaillances latentes en présence d'un danger. Dans ce cas, il faut considérer l'intégrité du matériel d'essai et le risque d'inhibition des verrouillages de sûreté.

### **5.3 Auto-test et surveillance**

Il convient d'intégrer, au niveau de la conception, des fonctions de surveillance permettant de détecter et de signaler les divergences entre des canaux similaires redondants. Il convient que des conceptions de systèmes dynamiques fournissent des alarmes signalant les défaillances de leur cycle, une source de signal dynamique ou une défaillance de transmission du signal dynamique. Un matériel de verrouillage de sûreté programmé doit intégrer des fonctions d'essai automatique conformément à la CEI 60987.