# NORME INTERNATIONALE

# INTERNATIONAL STANDARD

**CEI**
**IEC**
**60744**

Première édition
First edition
1983-01



## Ensembles logiques de sûreté des centrales nucléaires – Caractéristiques et méthodes d'essai

## Safety logic assemblies of nuclear power plants – Characteristics and test methods

Numéro de référence
Reference number
CEI/IEC 60744: 1983

## 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**
**60744**

Première édition
First edition
1983-01

## Ensembles logiques de sûreté des centrales nucléaires – Caractéristiques et méthodes d'essai

## Safety logic assemblies of nuclear power plants – Characteristics and test methods





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

IEC Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE M

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

# SOMMAIRE

# CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

# ENSEMBLES LOGIQUES DE SÛRETÉ DES CENTRALES NUCLÉAIRES CARACTÉRISTIQUES ET MÉTHODES D'ESSAI

## PRÉAMBULE

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

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

3) Dans le but d'encourager l'unification internationale, la CEI exprime le vœu que tous les Comités nationaux adoptent dans leurs règles nationales le texte de la recommandation de la CEI, dans la mesure où les conditions nationales le permettent. Toute divergence entre la recommandation de la CEI et la règle nationale correspondante doit, dans la mesure du possible, être indiquée en termes clairs dans cette dernière.

## PRÉFACE

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

Un premier projet fut discuté lors de la réunion tenue à Stockholm en 1980. A la suite de cette réunion, un projet, document 45A(Bureau Central)67, fut soumis à l'approbation des Comités nationaux suivant la Règle des Six Mois en avril 1981.

Les Comités nationaux des pays ci-après se sont prononcés explicitement en faveur de la publication:

| | |
|---|---|
| Afrique du Sud (République d') | France |
| Allemagne | Italie |
| Autriche | Pays-Bas |
| Belgique | Pologne |
| Canada | République Démocratique Allemande |
| Espagne | Union des Républiques Socialistes Soviétiques |
| Etats-Unis d'Amérique | |
| Finlande | |

*Autres publications de la CEI citées dans la présente norme:*

Publications n$^{os}$ 231A: Premier complément à la Publication 231 (1967): Principes généraux de l'instrumentation des réacteurs nucléaires.

255-1-00: Relais électriques de tout-ou-rien.

255-3: Relais électriques, Troisième partie: Relais de mesure à une seule grandeur d'alimentation d'entrée à temps non spécifié ou à temps indépendant spécifié.

410: Plans et règles d'échantillonnage pour les contrôles par attributs.

671: Essais périodiques et surveillance du système de protection des réacteurs nucléaires.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

# SAFETY LOGIC ASSEMBLIES OF NUCLEAR POWER PLANTS CHARACTERISTICS AND TEST METHODS

## FOREWORD

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

## PREFACE

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

A first draft was discussed at the meeting held in Stockholm in 1980. As a result of this meeting, a draft, Document 45A(Central Office)67, was submitted to the National Committees for approval under the Six Months' Rule in April 1981.

The National Committees of the following countries voted explicitly in favour of publication:

Austria
Belgium
Canada
Finland
France
German Democratic Republic
Germany
Italy
Netherlands
Poland
South Africa (Republic of)
Spain
Union of Soviet Socialist Republics
United States of America

*Other IEC publications quoted in this standard:*

Publications Nos. 231A: First supplement to Publication 231 (1967): General Principles of Nuclear Reactor Instrumentation.
255-1-00: All-or-nothing Electrical Relays.
255-3: Electrical relays, Part 3: Single Input Energizing Quantity Measuring Relays with Non-specified Time or with Independent Specified Time.
410: Sampling Plans and Procedures for Inspection by Attributes.
671: Periodic Tests and Monitoring of the Protection System of Nuclear Reactors.

# ENSEMBLES LOGIQUES DE SÛRETÉ DES CENTRALES NUCLÉAIRES CARACTÉRISTIQUES ET MÉTHODES D'ESSAI

## 1. Domaine d'application et objet

La présente norme comprend les principes de conception, de construction et d'essai des ensembles logiques de sûreté utilisés dans les systèmes de protection.

Elle présume que les principes énoncés dans la Publication 231A de la CEI: Premier complément à la Publication 231: Principes généraux de l'instrumentation des réacteurs nucléaires, sont appliqués et elle donne des recommandations pour leur mise en œuvre.

Cette norme comprend des dispositions sur les essais de réception, les vérifications en service, les critères de fiabilité et la protection contre les influences extérieures.

Les fonctions logiques de sûreté réalisées à l'intérieur des ensembles logiques de sûreté ne sont pas concernées par cette norme.

## 2. Terminologie

Les définitions ci-après, conformes à la Publication 231A de la CEI, sont applicables pour les besoins de la présente norme:

2.1 Déclenchement (Publication 231A de la CEI, paragraphe 5.1.15).

2.2 Arrêt d'urgence intempestif (Publication 231A de la CEI, paragraphe 5.1.14).

2.3 Ensemble terminal (Publication 231A de la CEI, paragraphe 5.1.11).

2.4 Ensemble logique de sûreté (Publication 231A de la CEI, paragraphe 5.1.10).

2.5 Défaillance dangereuse (Publication 231A de la CEI, paragraphe 5.1.13).

2.6 Défaillance non dangereuse (Publication 231A de la CEI, paragraphe 5.1.12).

2.7 Réarmement (Publication 231A de la CEI, paragraphe 5.1.18).

2.8 Système (Publication 231A de la CEI, paragraphe 5.1.2).

2.9 Système de protection (Publication 231A de la CEI, paragraphe 5.1.3).

2.12 *Niveau de confiance*

Probabilité, exprimée généralement sous forme de pourcentage, que la valeur vraie d'une quantité estimée se trouve à l'intérieur d'un intervalle déterminé au voisinage de la valeur estimée.

2.13 *Equipement de logique dynamique*

Système, ensemble ou sous-ensemble utilisant des signaux de logique dynamique.

# SAFETY LOGIC ASSEMBLIES OF NUCLEAR POWER PLANTS
# CHARACTERISTICS AND TEST METHODS

## 1. Scope and object

This standard includes principles of design, construction and testing of safety logic assemblies used in protection systems.

It assumes that the principles set out in IEC Publication 231A: First supplement to IEC Publication 231: General Principles of Nuclear Reactor Instrumentation, are to be applied and gives recommendations for their implementation.

It includes provisions for acceptance and in operating testing, reliability criteria and protection from external influences.

Safety logic functions performed within the safety logic assemblies are not included.

## 2. Terminology

For the purpose of this standard, the following definitions, in agreement with IEC Publication 231A, apply:

2.1 Trip (IEC Publication 231A, Sub-clause 5.1.15).

2.2 Spurious shutdown (IEC Publication 231A, Sub-clause 5.1.14).

2.3 Final assembly (IEC Publication 231A, Sub-clause 5.1.11).

2.4 Safety logic assembly (IEC Publication 231A, Sub-clause 5.1.10).

2.5 Unsafe failure (IEC Publication 231A, Sub-clause 5.1.13).

2.6 Safe failure (IEC Publication 231A, Sub-clause 5.1.12).

2.7 Reset (IEC Publication 231A, Sub-clause 5.1.18).

2.8 System (IEC Publication 231A, Sub-clause 5.1.2).

2.9 Protection system (IEC Publication 231A, Sub-clause 5.1.3).

2.12 *Confidence level*

The probability, generally expressed as a percentage, that the true values of an estimated quantity falls within a pre-established interval at the estimated value.

2.13 *Dynamic logic equipment*

System assembly or subassembly employing dynamic logic signals.

2.14 *Signal de logique dynamique*

Tension ou courant variant périodiquement – la fréquence étant compatible avec le temps de réponse exigé du système. Les différents états logiques sont associés aux différentes valeurs que prennent, au cours de la variation périodique, un ou plusieurs paramètres, par exemple l'amplitude, la pente, la périodicité d'impulsions ou d'alternances, ou le codage d'impulsions.

Un seul état logique peut être associé à l'absence de variation périodique d'un tel signal.

2.15 *Evénements initiateurs hypothétiques*

Evénements (ou combinaisons possibles d'événements) tels que des défaillances de matériel, des erreurs d'opérateur, des tremblements de terre et leurs conséquences, pris en compte à la conception, qui pourraient conduire à des incidents de fonctionnement prévus ou à des situations accidentelles.

2.16 *Vie prévue à la conception*

Durée pendant laquelle il peut être démontré que, dans des conditions d'utilisation spécifiées, des caractéristiques fonctionnelles satisfaisantes sont obtenues.

2.17 *Vie qualifiée*

Période pendant laquelle il peut être vérifié que l'ensemble logique de sûreté satisfait à toutes les exigences prévues à la conception pour les conditions d'utilisation spécifiées.

2.18 *Conditions d'utilisation*

Conditions concernant l'environnement, l'alimentation et les signaux, auxquelles on peut s'attendre pour le fonctionnement normal et les événements initiateurs hypothétiques.

2.19 *Vie en service*

Intervalle de temps compris entre l'installation et la mise hors service définitive, pendant lequel l'ensemble logique de sûreté satisfait à toutes les exigences prévues à la conception pour les conditions d'utilisation spécifiées.

2.20 *Durée de mission*

Intervalle de temps pendant lequel, à la suite d'événements initiateurs hypothétiques, les ensembles logiques de sûreté doivent être opérationnels pour commander les actions de sûreté prévues.

2.21 *Marge de fonctionnement*

Différence entre les conditions de service spécifiées les plus sévères, et les conditions mises en œuvre lors de l'essai de type pour tenir compte des dispersions normales de fabrication du matériel et des erreurs que l'on peut raisonnablement faire en fixant la performance satisfaisante.

Lorsqu'on définit l'essai de type, l'accroissement des sévérités des essais, l'augmentation du nombre des cycles d'essais et de la durée des essais, sont considérés comme des méthodes permettant de s'assurer qu'une marge convenable existe effectivement.

2.22 *Défaillance de cause commune*

Défaillance de plusieurs dispositifs ou composants qui sont dans l'incapacité de remplir leurs fonctions du fait d'un événement ou d'une cause spécifique unique.

2.14 *Dynamic logic signal*

A periodically changing voltage or current, the frequency being consistent with the required system response time. The different logic states are associated with different values of one or more parameters of the periodic change, for example, amplitude, slope, repetition rate of pulses or alternations, or pulse coding.

One logic state may be associated with the absence of periodic change of such a signal.

2.15 *Postulated initiating events*

Events (or their credible combinations) such as equipment failures, operator errors, earthquakes and their consequences which are postulated as part of the design basis and which could lead to Anticipated Operational Occurrences or Accident Conditions.

2.16 *Design life*

The time for which satisfactory performance can be demonstrated for a specific set of operating conditions.

2.17 *Qualified life*

The period of time that can be verified for which the safety logic assembly will meet all design requirements for the specified operational conditions.

2.18 *Operating conditions*

Environmental, power and signal conditions expected as a result of normal operation and postulated initiating events conditions.

2.19 *Installed life*

The interval of time from installation to permanent removal from operation, during which the safety logic assembly shall meet all design requirements for the specified operational conditions.

2.20 *Mission time*

The interval of time for which the safety logic assemblies shall survive the postulated initiating events conditions in order to operate engineered safeguards.

2.21 *Margin*

The difference between the most severe specified operational conditions and the conditions used in type testing to account for normal variations in production of equipment and reasonable error in defining satisfactory performance.

In defining the type test, increasing levels of testing, number of test cycles and test duration shall be considered as methods of ensuring that adequate margin does exist.

2.22 *Common cause failure*

The failure of a number of devices or components to perform their functions as a result of a single specific event or cause.

## 3. Conception des ensembles logiques de sûreté

3.1 Les spécifications et les bases de conception du système de protection (en dehors du domaine d'application de la présente norme) déterminent les exigences de fiabilité de l'ensemble logique de sûreté.

3.2 Les moyens d'obtenir la fiabilité requise pour un ensemble logique de sûreté sont:
- la fiabilité intrinsèque des composants;
- la configuration, les redondances et les dispositifs d'essai.

3.3 La conception de l'ensemble logique de sûreté doit être telle qu'elle permette de se conformer aux critères d'indépendance énoncés au paragraphe 5.6.2.4 de la Publication 231A de la CEI, s'appliquant au système de protection considéré comme un tout.

3.4 Prévoir les moyens d'essais pour détecter la perte d'aptitude au fonctionnement.

3.5 Le temps de réponse d'un ensemble logique de sûreté, tel qu'il est défini, doit avoir une valeur adaptée aux exigences du système de protection et ne doit pas être altéré par les nécessités de l'immunisation aux parasites électriques.

3.6 L'état du signal de sortie (normal ou déclenché) de chaque ensemble logique de sûreté doit être indiqué (ou des dispositifs avertisseurs doivent être prévus). L'état des signaux d'entrée importants peut aussi être indiqué.

3.7 Les modifications de configuration logique (par exemple passage de 2/4 en 2/3) dans l'ensemble logique de sûreté doivent être indiquées (ou des dispositifs avertisseurs doivent être prévus).

3.8 L'ensemble logique de sûreté doit être capable de fonctionner correctement en présence de perturbations d'un niveau spécifié. De même, on devrait prévoir une protection pour éviter les perturbations électriques entre ensembles logiques de sûreté.

3.9 Les circuits d'entrée et de sortie doivent être protégés contre les tensions existant dans l'environnement et ne doivent pas risquer, à la suite d'un défaut, d'être mis en contact avec ces sources de tension.

3.10 Si des moyens particuliers sont nécessaires pour supprimer les effets d'arc, ces moyens ne doivent pas affecter fâcheusement la vitesse de commutation ni la fiabilité de l'ensemble logique de sûreté au-delà de valeurs acceptables.

3.11 La fiabilité des composants doit être prise en considération pour la conception de l'ensemble logique de sûreté. Le choix des données de fiabilité doit tenir compte de la possibilité d'employer les données statistiques existantes et les incertitudes sur ces données (par exemple emploi du niveau de confiance).

3.12 La spécification des ensembles logiques de sûreté doit définir la vie en service et la durée de mission en fonction des conditions de fonctionnement requises.

## 4. Caractéristiques générales

L'ensemble logique de sûreté doit être conçu et qualifié comme un équipement lié à la sûreté pour supporter les conditions d'environnement découlant du fonctionnement normal et des événements initiateurs hypothétiques. Les effets des paramètres suivants doivent être inclus:

1) température;

2) pression;

## 3. Safety logic assembly design

3.1 The specifications and design basis of the protection system (outside the scope of the present standard) establish the requirements for the reliability of the safety logic assembly.

3.2 Means to achieve the required reliability of a safety logic assembly are:
- the intrinsic reliability of the components;
- the configuration, the redundancies and provisions for testing.

3.3 The design of the safety logic assembly shall be such as to allow conformity with independence criteria stated in Sub-clause 5.6.2.4 of IEC Publication 231A, as it applies to the protection system as a whole.

3.4 Means shall be provided for testing for loss of capability to function.

3.5 The response time of a safety logic assembly shall be so defined and shall have a value adequate for the requirements of the protection system and shall not be impaired by the requirements of electrical interference insensitivity.

3.6 The state of the output signal (normal or trip) from each safety logic assembly shall be indicated (or warning means shall be provided). The status of important input signals may also be indicated.

3.7 Changes of logic configuration (for example going from 2/4 to 2/3) in the safety logic assembly shall be indicated (or warning means shall be provided).

3.8 The safety logic assembly shall be able to operate properly in the presence of a specified interference level. Similarly, protection should be provided to avoid electrical interference between one safety logic assembly and another.

3.9 Input and output circuits shall be protected from voltages existing in the environment and from possible electrical contact with them as a consequence of a fault.

3.10 If means are required to suppress arcing, such means shall not affect adversely the switching speed nor the reliability of the safety logic assembly beyond acceptable values.

3.11 The reliability of the components shall be considered in the design of the safety logic assembly. The selection of reliability data shall take account of the applicability of existing statistical data and uncertainties on the data (e.g. use of confidence level).

3.12 The specification for safety logic assemblies shall define with respect to the required operating conditions the equipment installed life and mission time.

## 4. General characteristics

The safety logic assemblies shall be designed and qualified as an equipment important to safety to withstand environmental conditions arising from normal and postulated initiating events. The effects of the following parameters shall be included:

1) temperature;

2) pressure;

3) humidité;

4) vibrations mécaniques;

5) séismes;

6) radiation.

Cette liste n'est pas limitative.

4.1 Les ensembles logiques de sûreté redondants devraient être conçus de façon à présenter une indépendance électrique et une séparation physique suffisantes.

Cela est nécessaire mais non suffisant pour réduire la probabilité de défaillance multiple à un niveau acceptable en fonction des exigences de fiabilité prises en compte dans les spécifications de conception du système de protection.

4.2 Des moyens doivent être prévus, en local ou à distance, pour identifier rapidement l'état logique de l'ensemble logique de sûreté, ainsi que celui des modules déconnectables, afin de faciliter la maintenabilité.

4.3 Lorsqu'un module déconnectable est retiré, la probabilité de réalisation d'une action de sûreté doit être maintenue à un niveau acceptable.

Le retrait du module doit être signalé.

4.4 Les ensembles logiques de sûreté doivent être capables de satisfaire aux essais décrits aux articles 7 et 8.

4.5 Les ensembles logiques de sûreté doivent être conçus de manière à faciliter leur identification, leur localisation, le remplacement, la réparation et le réglage des modules ou composants en panne.

4.6 Une alimentation électrique de secours doit être prévue avec une autonomie et une indépendance suffisantes si elle est nécessaire pour mettre et maintenir l'installation en état sûr en cas d'arrêt.

## 5. Caractéristiques des relais utilisés dans les ensembles logiques de sûreté

5.1 La Publication 255-1-00 de la CEI: Relais électriques de tout-ou-rien, et la Publication 255-3 de la CEI: Relais électriques, Troisième partie: Relais de mesure à une seule grandeur d'alimentation d'entrée à temps non spécifié ou à temps indépendant spécifié, sont à appliquer.

5.2 Les relais à utiliser dans les ensembles logiques de sûreté doivent être de la classe «service continu» et être choisis dans la classe d'action *b)* conformément à la Publication 255-1-00 de la CEI.

5.3 La tension d'essai de l'isolement des bobines de relais utilisées dans les ensembles logiques de sûreté doit être spécifiée.

5.4 La tension assignée d'isolement des contacts doit être spécifiée.

5.5 Les contacts des relais doivent être calculés avec une marge de sécurité.

5.6 On peut prévoir la surveillance ou la vérification de la continuité de bobine dans les cas exceptionnels où le déclenchement est à émission. Dans ces cas, le courant d'essai devrait être de l'ordre du dixième du courant minimal susceptible d'actionner le relais.

Cette dernière recommandation ne s'applique pas nécessairement à la vérification ou à la surveillance de la continuité effectuée par impulsions.

3) humidity;

4) mechanical vibration;

5) earthquake;

6) radiation.

This list is not exclusive.

4.1 Redundant safety logic assemblies should be designed with sufficient electrical independence and physical separation.

This is a necessary but not a sufficient condition to reduce multiple failure probability to an acceptable degree consistent with the reliability requirements specified in the design basis of the protection system.

4.2 Internal or external means shall be provided to identify quickly the logical state of the safety logic assembly and of the replaceable modules to facilitate maintainability.

4.3 When a replaceable module is removed the probability of the safe action of the associated system shall be maintained at an acceptable level.

Removal of the module shall be indicated.

4.4 Safety logic assemblies shall be able to withstand the tests described in Clauses 7 and 8.

4.5 Safety logic assemblies shall be designed to facilitate recognition, location, replacement, repair and adjustment of malfunction components or modules.

4.6 An emergency electric power supply shall be provided with suitable independence and capacity when power is necessary to keep the safety logic assembly in a safe shutdown condition.

## 5. Characteristics of relays used in safety logic assemblies

5.1 IEC Publications 255-1-00: All-or-nothing Electrical Relays, and IEC Publication 255-3: Electrical Relays, Part 3: Single Input Energizing Quantity Measuring Relays with Non-specified Time or with Independent Specified Time, apply here.

5.2 Relays to be used in the safety logic assembly shall be of the continuous duty class, pick-up class *b)* according to IEC Publication 255-1-00.

5.3 The insulation test voltage of the relay coils to be used in the safety logic assemblies shall be specified.

5.4 The contact rated insulation voltage shall be specified.

5.5 The relay contacts shall be sized with a safety margin.

5.6 Provision may be made for coil continuity monitoring or testing in those exceptional cases where energization causes a trip. In such cases, the test current should be of the order of one-tenth of the minimum current which can energize the relay.

This last recommendation does not necessarily apply to pulse continuity testing or monitoring.

## 6. Caractéristiques des circuits statiques utilisés dans les ensembles logiques de sûreté

Cet article concerne les dispositifs logiques magnétiques et à semi-conducteurs fonctionnant en mode statique ou dynamique.

L'ensemble logique de sûreté peut être réalisé de différentes façons pour obtenir le niveau de protection spécifié. Le choix du système logique (statique, dynamique) doit être en rapport avec les exigences de fiabilité du système de protection considéré comme un tout.

De très hauts niveaux de protection sont généralement obtenus par des systèmes conçus pour présenter un mode de défaillance préférentiel (défaillance non dangereuse). Lorsqu'on utilise le fonctionnement dynamique des éléments logiques magnétiques ou à semi-conducteurs dans ce but, les modes de défaillance des éléments logiques choisis doivent être étudiés pour vérifier qu'ils correspondent tous à des défaillances non dangereuses (habituellement l'absence de signaux de logique dynamique).

La redondance peut être employée pour accroître la sûreté et (ou) la disponibilité et peut être appliquée aux systèmes logiques statiques ou dynamiques.

Les essais du système logique statique augmentent la fiabilité en réduisant le temps moyen entre réparations et, par conséquent, le temps pendant lequel une défaillance non sûre demeure non révélée dans le système.

Les dispositifs logiques statiques nécessitent généralement, pour leur fonctionnement, des signaux de puissance moindre que les relais. Par conséquent, on doit prendre un soin particulier pour éviter la création de signaux indésirables (bruit) provenant de rayonnements électromagnétiques, de décharges statiques, de courants de terre ou de surtensions d'alimentation.

Les méthodes de mesure appropriées de la marge de fonctionnement en cas de défaut en présence des niveaux les plus défavorables des sources de perturbations doivent être spécifiées.

Les exigences ci-dessus ayant été respectées, il est peu probable que des perturbations électriques puissent causer des dommages aux composants des ensembles logiques de sûreté. Cependant, les composants utilisés pour les interfaces d'entrée et de sortie des ensembles logiques de sûreté (par exemple les photocoupleurs) doivent être capables de tenir, sans subir de dommage, les niveaux de perturbations électriques induits sur les câbles d'interconnexion et correspondant au cas considéré comme le plus défavorable.

## 7. Essais de type

L'essai de type doit être conçu pour démontrer que les performances observées sur les ensembles logiques de sûreté atteignent ou dépassent les caractéristiques spécifiées.

L'essai de type doit consister en une séquence préétablie de conditions d'essai conformément aux spécifications de la Publication YYY de la CEI: Qualification des équipements électriques liés à la sûreté, destinés aux centrales électronucléaires (en préparation).

Il peut être admis que des parties de l'essai de type soient remplacées par des analyses théoriques. De telles analyses seront jointes en justification à la documentation de qualification.

### 7.1 *Essais de l'ensemble logique de sûreté*

#### 7.1.1 *Essais des caractéristiques fonctionnelles*

Les ensembles logiques de sûreté sont essayés pour vérifier les caractéristiques de fonctionnement suivantes:

## 6. Characteristics of solid-state circuits used in safety logic assemblies

This clause includes both semiconductor and magnetic logic devices and both static and dynamic modes of operation.

The safety logic assemblies may be implemented in a variety of ways to achieve the specified level of protection. The choice of logic systems (static, dynamic) shall be consistent with the reliability requirements for the protection system as a whole.

Highest levels of protection will generally be achieved from systems designed to have a preferred mode-of-failure (safe-failure). When the dynamic operation of semiconductor or magnetic logic devices is used for this purpose, the failure modes of the chosen logic devices shall be studied to ensure that they all correspond to safe-failures (usually the absence of dynamic logic signals).

Redundancy may be used to enhance safety and/or availability and may be applied to either static or dynamic logic systems.

Testing of the static logic systems enhances reliability by reducing the mean time between repairs and hence the length of time for which an unrevealed unsafe failure remains in the system.

Solid state logic devices generally require lower-power signals than relays for their operation. Therefore special care shall be taken to avoid the generation of extraneous (noise) signals from electromagnetic radiations, electrostatic discharges, earth currents or power supply surges.

Appropriate methods of measuring the margin against malfunction in the presence of postulated worst case interference levels sources shall be specified.

Provided that the above requirements have been met, it is unlikely that damage to components of the safety logic assembly will result from electrical interference. However, the components used at the input and output interfaces of the safety logic assembly (e.g. optical isolators) shall be capable of withstanding without damage the postulated worst case electrical interference levels induced in the interconnecting cables.



## 7. Type tests

The type test shall be designed to demonstrate that the observed performance characteristics of the safety logic assembly meet or exceed its specified performance characteristics.

The type test shall consist of a predetermined sequence of test conditions in accordance with that specified in IEC Publication YYY: Qualification of Safety-related Electrical Equipment for Nuclear Power Generating Stations (in preparation).

It is acceptable for parts of the type test to be replaced by theoretical analysis. Such analysis shall be justified in the qualification documentation.

### 7.1 *Safety logic assembly test*

#### 7.1.1 *Functional characteristics tests*

The safety logic assemblies shall be tested to verify the following performance characteristics:

- plage du signal d'entrée (tolérance sur le 0 et le 1 logiques);
- plage du signal de sortie (tolérance sur le 0 et le 1 logiques);
- fonction logique;
- temps de réponse (l'ensemble logique de sûreté doit produire son signal de sortie en temps spécifié à partir de l'apparition de la configuration de déclenchement à l'entrée);
- contraintes de dépassement de gamme à l'entrée;
- impédances d'entrée et de sortie;
- capacité de charge;
- caractéristiques autorisées du signal d'entrée;
- caractéristiques autorisées du signal de sortie lorsque cela est applicable;
- caractéristiques d'isolement et de découplage (pour chaque entrée et sortie vis-à-vis de chaque entrée et sortie);
- pouvoir de coupure des contacts (en continu, en alternatif, surcharges résistive et inductive);
- rapport signal/bruit (mesuré en décibels rapportés à la valeur la plus faible du niveau logique 1).

7.1.2 *Essai de l'alimentation*

Le matériel est essayé en vue de vérifier ses caractéristiques lors de variations spécifiées de la tension et de la fréquence de l'alimentation.

7.1.3 *Vérification de l'influence des paramètres d'environnement pour le fonctionnement normal et les événements initiateurs hypothétiques*

Les paramètres à prendre en considération, lorsqu'ils sont justifiés, sont les suivants:

- températures (de fonctionnement, de stockage et leurs variations);
- pression;
- humidité relative (fonctionnement et stockage);
- vibrations (mécaniques et sismiques);
- rayonnements.

7.1.4 *Durée de vie prévue à la conception et durée de mission*

Le matériel doit être qualifié pour une durée qui soit en rapport avec les conditions de fonctionnement requises et la durée de mission.

7.1.5 *Essais aux séismes*

Le prototype, y compris son support, doit être soumis à des essais de séismes qui soient représentatifs de l'installation de la centrale.

La surveillance des caractéristiques fonctionnelles et des paramètres d'environnement doit être continue ou effectuée à une fréquence permettant l'évaluation des caractéristiques de l'ensemble logique de sûreté.

7.2 *Procédure d'essai écrite*

Avant d'effectuer l'essai de type, une procédure écrite est préparée, revue et approuvée. La procédure doit comprendre au minimum ce qui suit:

- input signal range (tolerance for logic 0 and logic 1);
- output signal range (tolerance for logic 0 and logic 1);
- logic function;
- time to respond (the safety logic assembly shall produce its output signal within a specified time after the initiation of the input configuration);
- input overrange constraints;
- input and output impedance;
- load capability;
- permitted characteristics of the input signal;
- permitted characteristics of the output signal where applicable;
- insulation and decoupling characteristics (for any input and output from any input and output);
- contact rating (a.c., d.c. inductive and resistive);
- signal to noise ratio (measured in decibels as referred to the lower value of logic level 1).

7.1.2 *Power supply test*

Equipment shall be tested to check its performance against the specified variations in the voltage and frequency of the power supply.

7.1.3 *Test for the influence of normal and postulated initiating event environmental conditions*

The following parameters shall, when relevant, be taken into account:

- temperature (operating, storage and transients);
- pressure;
- relative humidity (operating and storage);
- vibration (mechanical and seismic);
- radiation.

7.1.4 *Design life and mission time*

The equipment shall be qualified for a design life that shall be adequate with respect to the required operating conditions and mission time.

7.1.5 *Seismic testing*

The prototype including its supporting structure shall be subjected to seismic testing which shall be representative of the plant installation.

The monitoring of performance characteristics and environmental parameters shall be continuous or of such a frequency as to allow evaluation of the performance characteristics of the safety logic assembly.

7.2 *Written test procedure*

Prior to performing the type test, a written procedure shall be prepared, reviewed and approved. The procedure shall, as a minimum, include the following:

7.2.1 Des instructions détaillées relatives aux différentes opérations à effectuer pour l'essai de type de l'ensemble logique de sûreté ainsi que les étapes de ces opérations, incluant:

*a)* mode de découpage de l'ensemble logique de sûreté en unités pour les essais;

*b)* description des unités y compris les caractéristiques fonctionnelles;

*c)* nombre (quantité) d'unités à essayer;

*d)* caractéristiques de montage et de raccordement à respecter (incluant les diagrammes appropriés, décrivant les interfaces entre les unités et l'équipement d'essai);

*e)* procédure de simulation de vieillissement;

*f)* conditions de service à simuler;

*g)* caractéristiques et conditions d'environnement à mesurer;

*h)* séquence détaillée, étape par étape, des opérations relatives aux conditions d'environnement, de fonctionnement et de mesure;

*i)* procédures d'étalonnage et de réglage;

*j)* durée de l'essai.

7.2.2 La liste des appareils et de l'instrumentation utilisés doit indiquer, pour chacun d'eux, le fabricant, le numéro de série du modèle, la durée de validité de l'étalonnage et comprendre aussi:

*a)* une rubrique indiquant les critères d'acceptation pour chacun des essais de type. Les critères d'acceptation doivent normalement être fondés sur les spécifications de l'unité;

*b)* les spécifications pour la documentation et l'analyse du résultat des essais;

*c)* un emplacement pour indiquer les dates de l'essai et la signature des personnes qui l'ont effectué;

*d)* un emplacement pour indiquer les dates et les signatures des personnes qui ont revu et analysé les résultats des essais;

*e)* une description de toutes les particularités du matériel qui n'ont pas été mentionnées ci-dessus, mais qui pourraient probablement affecter ce matériel pendant l'essai.

7.3 *Prescriptions pour la mise en œuvre du matériel d'essai*

7.3.1 Le matériel doit être monté de façon et dans une position telles que son installation prévue soit simulée, chaque fois que cela est possible. D'autres montages peuvent être utilisés, mais doivent être justifiés en montrant que la configuration d'essai n'avantage en rien les caractéristiques examinées par rapport à l'installation prévue pour le service.

7.3.2 Les moyens d'essais doivent permettre d'effectuer, pour les caractéristiques fonctionnelles, les essais combinés qui pourraient être requis (voir paragraphe 7.1.1).

7.3.3 L'essai doit être conduit avec un matériel offrant une résolution suffisante pour détecter les variations significatives des variables mesurées. Le matériel d'essai doit être étalonné selon les normes d'étalonnage officielles et accompagné des documents attestant ces étalonnages.

L'enregistrement des caractéristiques fonctionnelles et des paramètres d'environnement doit être continu ou affecté d'une fréquence permettant l'évaluation des caractéristiques de l'ensemble logique de sûreté.

7.4 *Conditions d'utilisation*

7.4.1 Les caractéristiques fonctionnelles de l'unité doivent être déterminées aux conditions nominales contrôlées d'environnement et d'alimentation de référence pour le service.

7.2.1 Detailed instructions pertaining to the test required to type test safety logic assembly and steps to accomplish the tests, including the following:

*a)* way in which safety logic assembly is to be separated into units for testing;

*b)* description of units including functional performance;

*c)* number (quantity) of units to be tested;

*d)* mounting and connection requirements (including appropriate diagrams depicting interface between units and test equipment);

*e)* ageing procedure;

*f)* operational conditions to be simulated;

*g)* performance and environmental variable to be measured;

*h)* environmental, operating and measurement sequence in step-by-step detail;

*i)* calibration and adjustment procedures;

*j)* test duration.

7.2.2 A listing shall be made of equipment and instrumentation used during the test. This shall include manufacturer, model serial number and calibration due state and containing also:

*a)* a section giving the acceptance criteria for each type test. The acceptance criteria should be based upon the unit specifications;

*b)* requirements for documentation and analysis of the test results;

*c)* space for the date of the test and the signature of the party who performed the test;

*d)* place for dates and signature of persons who reviewed and analyzed the results of the tests;

*e)* a description of any conditions peculiar to the equipment which are not covered above, but which would probably affect said equipment during testing.

7.3 *Requirements for test equipment layout*

7.3.1 Equipment should be mounted in a manner and position which simulates its expected installation wherever possible. Other mounting means may be used but shall be justified on the basis that the configuration does not provide any advantage to the characteristics under investigation when compared to the intended operational installation.

7.3.2 The test facilities shall allow performance of combined tests for function characteristics that may be required (see Sub-clause 7.1.1).

7.3.3 The test shall be monitored using equipment that provides sufficient resolution for detecting meaningful changes in the measured variables. The test equipment shall be calibrated against auditable calibration standards and shall have documentation to support such calibrations.

The monitoring of performance characteristics and environmental parameters shall be continuous or of such a frequency as to allow evaluation of the performance characteristics of the safety logic assembly.

7.4 *Operational conditions*

7.4.1 The performance characteristics of the unit shall be determined at nominal controlled environmental and power supply reference operating conditions.

7.4.2 Les caractéristiques fonctionnelles de l'unité doivent être déterminées pour la gamme prévue à la conception de chaque paramètre significatif d'environnement et d'alimentation et/ou pour chaque combinaison significative de ces paramètres.

7.5 *Vieillissement*

L'objectif de l'exigence de vieillissement au cours de la qualification du matériel est de mettre les unités dans des conditions telles que les essais de type puissent contribuer à révéler les effets du temps sur les caractéristiques de fonctionnement significatives. En outre, des méthodes d'acquisition de données en centrale pourront révéler des renseignements supplémentaires sur les caractéristiques d'endurance. Ce travail peut être accompli en utilisant une approche statistique.

En variante, des unités vieillies naturellement peuvent être essayées aux événements initiateurs hypothétiques.

7.5.1 Les méthodes de vieillissement suivantes sont suggérées. Des techniques d'extrapolation décrites dans la bibliographie courante peuvent être combinées avec ces méthodes:

1) les ensembles logiques de sûreté ayant un fonctionnement cyclique peuvent être essayés à une fréquence accélérée pourvu que cette accélération ne soit pas assez élevée pour produire des effets inexistants à vitesse normale;

2) utilisation de procédés de vieillissement accéléré (comme l'élévation de la température) lorsque les lois physico-chimiques de leur influence sur le mécanisme de la défaillance sont bien connues.

7.6 *Séquence d'essais*

L'essai de type de l'ensemble logique de sûreté doit se dérouler suivant une séquence spécifiée, qui fera partie de la procédure écrite d'essai. Il doit vérifier que le matériel fonctionne conformément aux spécifications, avant, pendant et après un événement initiateur hypothétique.

La séquence suivante est recommandée:

1) prélèvement des échantillons au hasard;

2) examen visuel;

3) montage suivant la configuration d'essai;

4) vérification de l'étalonnage;

5) fonctionnement dans les conditions normales (y compris le déverminage);

6) fonctionnement aux valeurs extrêmes de toutes les gammes prévues à la conception en excluant les événements initiateurs hypothétiques et ceux qui en découlent;

7) vieillissement;

8) fonctionnement dans l'environnement le plus sévère (événement initiateur hypothétique);

9) vérification du fonctionnement correct pour des événements qui découlent des événements initiateurs hypothétiques (E.I.H.);

10) préparation du compte rendu d'essai.

## 8. Essais individuels de série

Afin de vérifier que les ensembles logiques de sûreté produits en usine demeurent tout à fait conformes à ceux qui ont été utilisés pour l'essai de type, il est recommandé d'effectuer les essais suivants sur un nombre convenable d'échantillons.