INTERNATIONAL STANDARD

NORME INTERNATIONALE

IEC
CEI
60671

Second edition
Deuxième édition
2007-05

Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE
CODE PRIX T

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

CONTENTS

FOREWORD 4
INTRODUCTION 6

1 Scope 8
2 Normative References 9
3 Terms and definitions 9
4 Basic Principles for Surveillance Testing 11
4.1 General 11
4.2 Gradation of Requirements Based on Category 12
4.3 Extent of Surveillance Testing 12
4.4 Self-supervision in Lieu of Periodic Testing 12
4.5 Continuous Operation in Lieu of Periodic Testing 13
5 General Requirements for Surveillance Testing 13
5.1 Design Requirements 13
5.2 Procedures 14
5.3 Data to be recorded upon detection of a fault 14
5.4 Other data to be recorded 14
5.5 Test intervals 15
5.6 Verification of actuation set-points 15
5.7 Bypass 15
5.8 Response time 15
5.9 Restoration 16
6 Requirements for Testing of Sensors and Signal Processing Devices 16
6.1 General 16
6.2 Non-tested parts 16
6.3 Testing devices 16
6.4 Signals 16
6.5 Variation of signals 17
6.5.1 General 17
6.5.2 Slowly changing signal 17
6.5.3 Rapidly changing signal 17
6.5.4 Large change in signal 17
6.6 Operability 17
6.7 Sensor response time 18
6.8 Testing equipment 18
6.9 Calibration and transfer function 18
6.10 Surveillance 18
7 Requirements for Testing of Electromechanical Equipment 18
7.1 General 18
7.2 Interface 18
7.3 Typical functional tests 19
7.4 Continuous monitoring 19
7.5 Relays and valves 19
8 Requirements for Testing of Logic Assemblies 20
8.1 Scope 20
8.2 General 20

8.3 Switching of signals 20
8.4 Testing signals 20
8.5 Interface 21
8.6 Data to be displayed 21
8.7 Data to be recorded 21
8.8 Detailed display 21
8.9 Testing equipment 21
8.10 Testing equipment using pulses 22
9 Self-supervision in computer-based I&C systems 22
9.1 Coverage of self supervision 22
9.2 Balance of diagnostic versus functional processing 23
9.3 Watchdog timers 23
9.4 Action taken on detected fault 23
9.5 Categorization of self-supervision software 24

Figure 1 – Extent of I&C Surveillance Testing 9

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SURVEILLANCE TESTING

FOREWORD

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

International Standard IEC 60671 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1980 and constitutes a technical revision.

The main technical changes with respect to the previous edition are as follows:

– Expand scope to cover all systems important to safety, and clarify requirement gradation for systems and equipment performing category A, B and C functions.
– Align with the new revisions of IAEA documents NS-R-1 and NS-G-1.3 (replacing D3 and D8).

– Provide references to relevant normative standards.
– Harmonize terminology with the existing standard hierarchy.
– Strengthen the role of computer self-supervision as an alternative to periodic surveillance testing.
– Introduce features of digital I&C that present special opportunities or problems to on-line testing.
– Present design requirements on testing features themselves (categorization, verification, etc.) that derive from the standards adopted since the first issue of IEC 60671, which will thus be updated to become consistent with the newer standards.

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

FDIS	Report on voting
45A/648/FDIS	45A/655/RVD

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

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

In the United Kingdom some differences exist:

Introduction, Clauses 1, 2 and 4.2: The classification scheme captured in standard IEC 61226 edition 2 (2005-02) is contrary to the custom, practice, and regulatory expectations as set down by the United Kingdom Health and Safety Executive's Nuclear Installations Inspectorate and the understanding in the United Kingdom of IAEA safety guides. Users of this standard are advised that, in the United Kingdom, this standard should be read in conjunction with the edition of IEC 61226 published by the BSI, and the Health and Safety Executive's Nuclear Installations Inspectorate's Safety Assessment Principles to determine the classification of a function or system.

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

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

INTRODUCTION

a) Background, main issues and organization of the standard

A fundamental requirement for I&C (instrumentation and control) systems important to safety in nuclear power plants is that they be capable of being demonstrated to be ready to perform their safety functions if needed. Surveillance testing may be performed by the execution of functional tests or by self-supervision within the I&C systems important to safety, and is augmented by diagnostic functions and by visual inspections of the I&C systems and their status indicators by the plant operation staff. Depending on the reliability targets and the testing conditions the demonstration of functional readiness may be performed either while the plant is on-line or during plant shutdown. This Standard provides technical requirements and recommendations for the implementation of surveillance testing for I&C systems important to safety.

The object of this standard is:

– in Clause 4:

  to establish the principles for surveillance testing of I&C equipment important to safety.

– in Clauses 5 through 9:

  to give requirements to be fulfilled in the design and operation of I&C equipment important to safety in regards to the surveillance testing.

b) Situation of the current standard in the structure of the SC 45A standard series

IEC 61513 establishes the top level requirements for I&C systems and equipment important to safety. Among these requirements is the need to demonstrate, on a continuing basis, the operability of the equipment and its readiness to perform its safety or safety related functions.

IEC 61226 establishes the principles of categorization of I&C functions according to their level of importance to safety. The reliability required from any function in categories A, B or C should be determined by either a quantitative probabilistic assessment of the NPP, or by qualitative engineering judgment, and included in the specification.

IEC 60671 provides the bases and requirements for surveillance testing to demonstrate the operability, under normal conditions, of these systems and equipment during their operative life.

IEC 60671 supports the achievement of the target reliability by detecting faults within the equipment allowing appropriate measures to be initiated (timely repair or any alternative solutions).

IEC 60671 is the third level SC 45A document tackling the issue of surveillance testing for I&C systems important to safety

For more details on the structure of the SC 45A standard series see item d) of this introduction.

c) Recommendations and limitations regarding the application of the Standard

IEC 60671 applies to I&C systems and equipment important to safety. It establishes requirements for surveillance testing as a means of demonstrating on a continuing basis the readiness of the systems and equipment to perform their functions important to safety.

Additional requirements relating to reliability and detailed requirements for redundancy and diversity are not given in this standard but can be found in other documents of SC 45A.

The attention of the reader is drawn to the fact that in some countries the scope and the content of periodic testing are defined by regulatory requirements and that these definitions could differ from the ones used in this standard.

In the case of existing plants it may not be possible to apply all of the requirements of this standard. Therefore, at the beginning of a modernization project of an I&C system important to safety the subset of requirements to be applied shall be identified in regards to the overall scope and consequences of modification of the I&C systems.

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

The top-level document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

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

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

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

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

IEC 61513 refers to ISO as well as to IAEA 50-C-QA (now replaced by IAEA 50-C/SG-Q) for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the Requirements NS-R-1, establishing safety requirements related to the design of Nuclear Power Plants, and the Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in Nuclear Power Plants. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SURVEILLANCE TESTING

1 Scope

Where functional reliability is required by general safety standards, one aspect of demonstrating this reliability is testing performed on-line during plant operation or during plant shutdown in preparation for return to power operation.

This standard lays down principles for testing I&C systems performing category A, B and C functions, per IEC 61226, during normal power operation and shutdown, so as to check the functional availability especially with regard to the detection of faults that could prevent the proper operation of the functions important to safety. It covers the possibility of testing at short intervals or continuous surveillance, as well as periodic testing at longer intervals. It also establishes basic rules for the design and application of the test equipment and its interface with the systems important to safety. Further, the effect of any test equipment failure on the reliability of the I&C systems is considered.

Types of surveillance tests may include:

– self-tests for I&C equipment;
– test of a group of equipment or components to confirm properties that support the safety function (continuity, power availability, etc.);
– test based on information redundancy or comparison of control signatures (consistency checking for redundant sensors, CRC-checking, Checksum, etc.);
– periodic testing which is related to the correctness of functional behaviour of an I&C system.

The dependability targets of any I&C system is reached using an appropriate combination of tests of the form indicated above.

The extent of the I&C system to be tested is from the interface of the sensors with the process through to the actuation devices (see Figure 1). It is applicable to the installed I&C systems as well as to temporary installations which are part of those I&C systems important to safety (for example, auxiliary equipment for commissioning tests and experiments). This standard also applies to individual electromechanical equipment, such as relays and solenoid actuators.

Additional testing and inspections may be performed on I&C equipment for purposes other than the demonstration of functional capability, such as to optimise preventive maintenance, etc. Such tests are beyond the scope of this standard; however, they may be combined with the surveillance testing discussed herein.

For any on-line tests the potential interaction and fault dependencies between the part of the system under test and the testing part, have to be carefully studied and their influences have to be fully integrated into the reliability assessment of the functions important to safety (in accordance with IEC 61513).

This standard applies to the I&C of new nuclear power plants as well as to I&C upgrading or back-fitting of existing plants. For I&C upgrades, only a subset of the requirements may be applicable; this subset is to be identified at the beginning of any project.

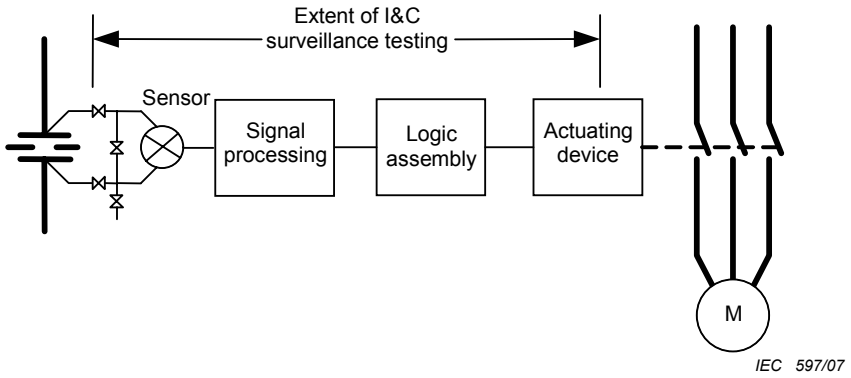


Figure 1 – Extent of I&C surveillance testing

2 Normative references

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

IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 60987, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*

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

IEC 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

IEC 62138, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B and C functions*

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

SOMMAIRE

AVANT-PROPOS 28
INTRODUCTION 30

1 Domaine 32
2 Références normatives 33
3 Termes et définitions 33
4 Principes de base des essais de surveillance 35
4.1 Généralités 35
4.2 Gradation des exigences à partir des catégories 36
4.3 Couverture des essais de surveillance 37
4.4 Auto surveillance en lieu et place d'essais périodiques 37
4.5 Fonctionnement continu remplaçant les essais périodiques 37
5 Prescriptions générales applicables aux essais de surveillance 38
5.1 Exigences de conception 38
5.2 Procédures 39
5.3 Informations à enregistrer lors de la détection d'un défaut 39
5.4 Autres informations à enregistrer 39
5.5 Intervalles entre essais 40
5.6 Vérification des points de consigne 40
5.7 Inhibitions 40
5.8 Temps de réponse 40
5.9 Remise en fonction 41
6 Exigences relatives aux essais des capteurs et des appareils de traitement du signal 41
6.1 Généralités 41
6.2 Parties non soumises aux essais 41
6.3 Dispositifs d'essai 41
6.4 Signaux 41
6.5 Variations du signal 42
6.5.1 Généralités 42
6.5.2 Signal à variation lente 42
6.5.3 Signal à variation rapide 42
6.5.4 Signal à variation de grande amplitude 42
6.6 Aptitude opérationnelle 42
6.7 Temps de réponse des capteurs 43
6.8 Matériel d'essai 43
6.9 Etalonnage et fonction de transfert 43
6.10 Surveillance 43
7 Exigences relatives aux essais périodiques des matériels électromécaniques 44
7.1 Généralités 44
7.2 Interface 44
7.3 Essais fonctionnels 44
7.4 Surveillance permanente 45
7.5 Relais et vannes 45
8 Exigences relatives aux essais d'ensembles logiques 45
8.1 Domaine d'application 45

8.2 Généralités....45
8.3 Commutation des signaux....45
8.4 Signaux d'essai....46
8.5 Interface....46
8.6 Informations à afficher....46
8.7 Informations à enregistrer....46
8.8 Affichage détaillé....47
8.9 Matériel d'essai....47
8.10 Matériel d'essai à impulsions....47
9 Auto surveillance des systèmes d'I&C informatisés....47
9.1 Couverture des fonctions d'auto-surveillance....48
9.2 Equilibre entre diagnostique et traitement fonctionnel....48
9.3 Chiens de garde....49
9.4 Action à réaliser lors de la détection d'un défaut....49
9.5 Catégorisation des logiciels d'auto surveillance....49

Figure 1 – Domaine des essais de surveillance de l'I&C....33

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ESSAIS DE SURVEILLANCE

AVANT-PROPOS

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

La Norme internationale CEI 60671 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Cette seconde édition annule et remplace la première édition publiée en 1980, dont elle constitue une révision technique.

Les changements techniques principaux par rapport à l'édition précédente sont les suivants :

- Etendre le domaine de la norme pour couvrir tous les systèmes importants pour la sûreté, et clarifier la gradation des exigences pour les systèmes et matériels réalisant des fonctions de catégorie A, B ou C.
- Mettre la norme en cohérence avec les nouvelles révisions des documents de l'AIEA NS-R-1 et NS-G-1-3 qui remplacent les documents D3 et D8.

- Fournir des références normatives pertinentes.
- Harmoniser la terminologie avec la hiérarchie normative existante.
- Mettre en avant le rôle de l'auto-surveillance comme solution alternative aux essais de surveillance périodique.
- Présenter les caractéristiques propres aux systèmes informatisés qui correspondent à des possibilités ou à des problèmes particuliers en ce qui concerne les essais en ligne.
- Présenter les exigences de conception qui portent sur les fonctionnalités d'essai en particulier (catégorisation, vérification, etc.) et qui proviennent des normes adoptées depuis la première édition de la CEI 60671, qui ainsi mise à jour sera cohérente avec ces normes plus récentes.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/648/FDIS	45A/655/RVD

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

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

Au Royaume Uni des différences existent:

Introduction, Articles 1, 2 et 4.2: Le schéma de classement établi par la norme CEI 61226 édition 2 (2005) est contraire aux habitudes, aux pratiques et aux attentes réglementaires telles que définies par le «United Kingdom Health and Safety Executive's Nuclear Installations Inspectorate» et à l'interprétation britannique des guides de sûreté de l'AIEA. Les utilisateurs de cette norme sont prévenus que celle-ci doit être lue conjointement avec l'édition de la CEI 61226 publiée par le BSI et le «Health and Safety Executive's Nuclear Installations Inspectorate's Safety Assessment Principles» pour déterminer le classement d'une fonction ou d'un système.

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

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

INTRODUCTION

a) Contexte technique, questions importantes et structure de cette norme

La capacité des systèmes d'I&C (instrumentation et contrôle-commande) à démontrer qu'ils sont prêts si nécessaire à réaliser leurs fonctions de sûreté est une exigence fondamentale. Les essais de surveillance peuvent être réalisés en exécutant des essais fonctionnels ou par auto-surveillance, ceci étant renforcé par les fonctions de diagnostique et par les inspections visuelles des systèmes d'I&C et de leurs indicateurs d'état, par les personnels d'exploitation. La démonstration de l'aptitude fonctionnelle peut être réalisée tranche en service ou à l'arrêt, suivant les objectifs de fiabilité visés et les conditions d'essai. Cette norme fournit les exigences et les recommandations techniques applicables à la mise en œuvre des essais de surveillance pour les systèmes d'I&C importants pour la sûreté.

Les objectifs de cette norme sont:

- à l'Article 4:

  d'établir les principes des essais de surveillance pour les matériels d'I&C importants pour la sûreté;

- de l'Article 5 à l'Article 9:

  de donner des exigences devant être satisfaites au niveau de la conception et de l'exploitation des matériels d'I&C importants pour la sûreté dans le domaine des essais de surveillance.

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

La CEI 61513 établit les exigences de haut niveau applicables aux systèmes et aux matériels d'I&C importants pour la sûreté. Parmi ces exigences on trouve le besoin de démontrer de façon permanente la disponibilité des matériels et leur aptitude à être prêts à réaliser leurs fonctions de sûreté ou liées à la sûreté.

La CEI 61226 établit les principes de catégorisation des fonctions d'I&C suivant leurs niveaux d'importance pour la sûreté. Il convient de déterminer les objectifs de fiabilité de toute fonction de catégorie A, B ou C, ou sur la base de l'évaluation probabiliste quantitative de la centrale, ou sur la base d'un jugement qualitatif de l'ingénieur, et d'intégrer ceux-ci aux spécifications.

La CEI 60671 fournit les éléments de base et les exigences relatives aux essais de surveillance pour démontrer la satisfaction aux exigences de principe données par les deux normes citées précédemment. Les essais de surveillance décrits dans la CEI 60671 permettent d'atteindre les objectifs de fiabilité fixés en détectant les défauts survenant dans les matériels et en permettant de les réparer à temps ou en permettant de lancer une autre action.

La CEI 60671 est le document de troisième niveau du SC 45A qui traite du problème des essais de surveillance des systèmes d'I&C importants pour la sûreté.

Pour plus de détails sur la collection de normes du SC 45A, voir le point d) de cette introduction.

c) Recommandations et limites relatives à l'application de cette norme

La CEI 60671 s'applique aux systèmes et aux matériels d'I&C importants pour la sûreté. Elle établit les exigences applicables aux essais de surveillance qui permettent de démontrer de façon permanente l'aptitude des systèmes et des matériels à être prêts à réaliser leurs fonctions importantes pour la sûreté.

Cette norme ne fournit pas d'exigence supplémentaire dans le domaine de la fiabilité, ni d'exigences détaillées pour ce qui concerne la redondance et la diversité, par contre on peut trouver celles-ci dans d'autres normes du sous-comité 45A.

L'attention du lecteur est attirée sur le fait que dans certains pays le domaine et le contenu des essais périodiques sont définis par des exigences réglementaires et que ces définitions peuvent être différentes de celles utilisées dans cette norme.

Dans le cas d'installations existantes, il peut ne pas être possible d'appliquer toutes les exigences de cette norme. Ainsi, au début du projet de modernisation d'un système de contrôle-commande important pour la sûreté, le sous-ensemble des exigences à appliquer doit être identifié en prenant en compte le domaine général et les conséquences de la modification des systèmes de contrôle-commande.

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

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

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

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

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

La CEI 61513 a adopté une présentation similaire à celle de la CEI 61508, avec un cycle de vie et de sûreté global, un cycle de vie et de sûreté des systèmes, et une interprétation des exigences générales des parties 1, 2 et 4 de la CEI 61508 pour le secteur nucléaire. La conformité à la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire. Dans ce cadre, la CEI 60880 et la CEI 62138 correspondent à la CEI 61508-3 pour le secteur nucléaire.

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA 50-C-QA (remplacé depuis par le document AIEA 50-C/SG-Q) pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de la CEI sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle-commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ESSAIS DE SURVEILLANCE

1 Domaine d'application

La fiabilité fonctionnelle étant requise par les normes de sûreté de haut niveau, un des aspects de la démonstration de cette fiabilité relève des essais réalisés en ligne lorsque la centrale fonctionne ou lorsque celle-ci est à l'arrêt et s'apprête à fonctionner à nouveau en puissance.

Cette norme établit les principes applicables aux systèmes d'I&C réalisant des fonctions de catégories A, B ou C, telles que définies par la CEI 61226, durant le fonctionnement normal en puissance ou les arrêts de l'installation, de façon à en vérifier la disponibilité fonctionnelle en particulier en ce qui concerne la détection des défauts qui pourraient empêcher le bon fonctionnement des fonctions importantes pour la sûreté. Elle traite des capacités d'essais réalisés à intervalles courts ou de surveillance continue, aussi bien que d'essais périodiques réalisés à intervalles plus longs. Elle établit aussi les règles de base de conception et de réalisation des essais matériels et de leur interface avec les systèmes importants pour la sûreté. De plus, les effets de toute défaillance des matériels d'essai sur la fiabilité des systèmes d'I&C sont pris en compte.

Les types d'essais de surveillance peuvent comprendre:

– les auto-tests des matériels d'I&C;
– les essais d'ensemble de matériels ou de composants pour en vérifier les propriétés sur lesquelles reposent les fonctions de sûreté (continuité, disponibilité des sources électriques, etc.);
– les essais basés sur l'information redondante ou sur la comparaison de signatures de contrôle (vérification de la cohérence pour les capteurs redondants, vérification du caractère de contrôle de parité, vérification de la somme de contrôle, etc.);
– les essais périodiques liés à la vérification de la correction du comportement fonctionnel des systèmes d'I&C.

L'atteinte des objectifs de sûreté de fonctionnement de tout système d'I&C est assurée par une combinaison appropriée des essais dont la forme est indiquée ci-dessus.

Le domaine des systèmes d'I&C à tester, va de l'interface des capteurs avec le procédé jusqu'aux appareils actionneurs (voire la Figure 1). La norme est applicable aussi bien aux systèmes d'I&C permanents qu'à ceux installés provisoirement pourvu qu'ils fassent partie des systèmes importants pour la sûreté (par exemple, matériel auxiliaire d'essai de mise en service et d'expérimentation). Cette norme est aussi applicable aux matériels individuels électromécaniques tels que les relais et les électrovannes d'actionneurs.

Des inspections et des essais complémentaires peuvent être réalisés sur les matériels d'I&C à des fins autres que celles de la démonstration de l'aptitude fonctionnelle, telles que pour optimiser la maintenance préventive, etc. De tels essais se situent hors du domaine de la présente norme, même s'ils peuvent être combinés avec les essais de surveillance dont il est question ici.

Pour les essais en ligne, quels qu'ils soient, il faut étudier soigneusement les interactions possibles et les défauts de dépendance entre les parties du système en essai et le testeur; leurs influences doivent être pleinement prises en compte dans l'évaluation de la fiabilité des fonctions de sûreté et ceci conformément à la CEI 61513.

Cette norme est applicable à l'I&C des nouvelles centrales nucléaires de puissance comme à l'I&C mis à niveau ou rénové des centrales existantes. Pour les mises à niveau d'I&C, seul un sous-ensemble des exigences peut être applicable; ce sous-ensemble doit être identifié au début de tout projet.

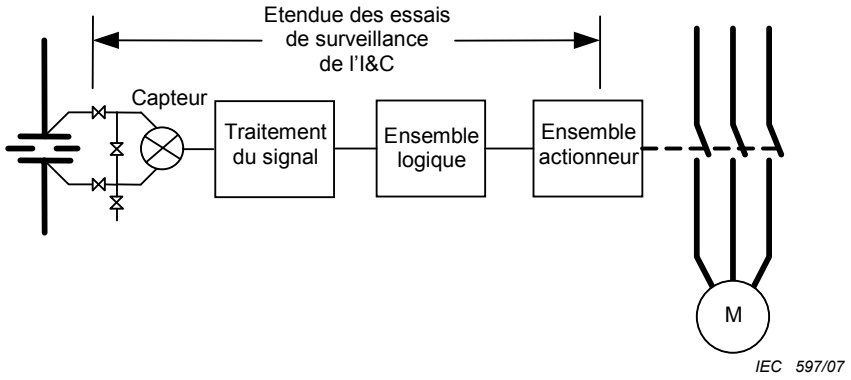


Figure 1 – Domaine des essais de surveillance de l'I&C

2 Références normatives

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

CEI 60880, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

CEI 60987, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés*

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

CEI 61513, *Centrales nucléaires – Instrumentation et contrôle-commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*

CEI 62138, *Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

AIEA Guide de sûreté NS-G-1.3, *Systèmes d'I&C importants pour la sûreté des centrales nucléaires*