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

Reference number
Numéro de référence
IEC/CEI 60671:2007

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

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

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:

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

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.

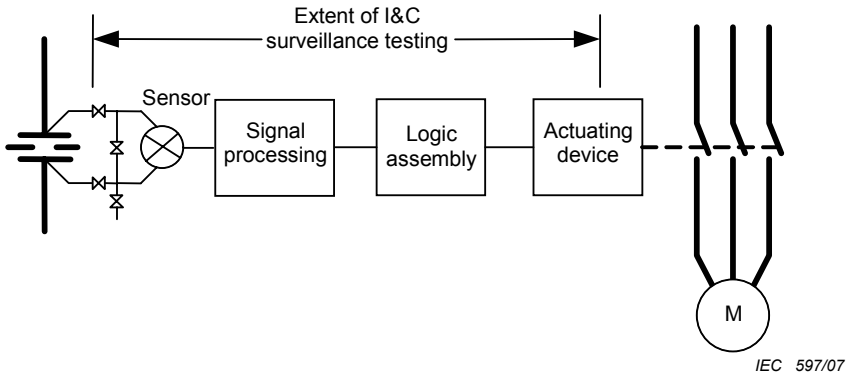

Figure 1 – Extent of I&C surveillance testing

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*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
automatic test
a test in which the operation of all or part of the instrumentation and control system is checked in a completely automatic sequence. The automatic test sequence can be started either manually by the operator, cyclically by a clock or automatically by the verification of a well-defined condition

3.2
availability
the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided

[IEV 191-02-05]

3.3
bypass
a device to inhibit, deliberately but temporarily, the functioning of a circuit or system by, for example, short circuiting the contacts of a relay.

- **maintenance bypass**: a bypass of safety system equipment during maintenance, testing or repair;
- **operational bypass**: a bypass of certain protective actions when they are not necessary in a particular mode of plant operation

[IAEA Safety Glossary, Ed. 2.0 2006]

NOTE 1 A maintenance bypass that is applied to a channel may still leave the safety function operable through redundancy and majority voting (e.g. two out of four coincidence logic becomes two out of three).

NOTE 2 A maintenance bypass is not the same as an operational bypass. A maintenance bypass may reduce the degree of redundancy of equipment, but it does not result in the loss of a safety function.

3.4
full functional test
test that includes perturbation of the process variable, detection by the sensor, processing of the signal(s), actuation of the appropriate sub-assemblies, logic assemblies and actuation devices

3.5
functional reliability
ability to comply with requirements on complete and correct functionality and performance in:

a) all defined plant operational modes and conditions,

b) in all defined plant I&C system operational modes, and

c) with all stipulated failures/failure modes of the plant I&C system under which correct function and performance is required

3.6
monitoring
means provided to indicate continuously the state or condition of a system, sub-system, equipment or assembly

[IEV 393-08-48]

3.7
periodic testing
performance of tests at predetermined time points to demonstrate that the functional capabilities of I&C systems and equipment important to safety are retained and that the characteristics relevant to the claims of the safety analysis are satisfied

3.8
self-supervision
automatic testing of system hardware performance and software consistency of a computer-based I&C system

3.9
surveillance testing
complete scope of activities to demonstrate that the functional capabilities of I&C systems and equipment important to safety are retained and confirmation that the design basis requirements are met

3.10
test duration
the elapsed time between the test initiation and the test termination

3.11
test initiation
the application of a test input

3.12
test input
a real or simulated, but deliberate, perturbation of a measured variable or signal which is imposed upon all or part of a signal processing device, a logic assembly, or a final actuation device for the purpose of testing

3.13
test interval
the elapsed time between the initiation of identical tests on the same sensor and signal processing device, logic assembly or final actuation device

3.14
test termination
the removal of a test input with the results of the test being known

4 Basic principles for surveillance testing

4.1 General

The goals of surveillance testing are to ensure the functional capability of I&C systems and the related control path to actuate the process components important to safety and to give periodic confirmation that design basis requirements such as those for reliability, accuracy, response time and set points are met (Clause 4.82 of IAEA NS-G-1.3).

4.1.1 Surveillance testing of I&C systems and equipment important to safety shall demonstrate and contribute to the achievement of the desired system reliability and availability, by means of the detection of faults, and shall call attention to performance that is not within prescribed limits. Prescribed limits are minimum performance requirements, such as response time and set-point accuracy and any other characteristics of the system which are essential to its satisfactory functioning. The surveillance testing has to confirm that the essential safety features are retained in comparison to a reference status which may originate from commissioning tests that verify the design basis requirements. While surveillance testing could permit the detection of some specific wear and ageing mechanisms, the detection scope is not sufficient to detect *a priori* all ageing mechanisms. The operability of equipment or a system under normal conditions is generally not sufficient to lead to judgements on the conservation of this property under design accident conditions. It is noted that many types of unrevealed faults that could be a cause of unsafe failures can only be detected by testing.

4.1.2 Surveillance testing shall verify the relevant systems and equipment characteristics given directly by the safety assessment report, or other relevant safety documents, for the functions performed by the I&C systems important to safety. It could also be combined with maintenance tests for performance measures that do not have a direct contribution to safety. Such tests are not defined as surveillance tests (see 3.1) and are outside the scope of this standard.

4.2 Gradation of requirements based on category

4.2.1 I&C functions important to safety are assigned a safety category according to the principles of IEC 61226. The surveillance requirements of the systems and equipment shall be commensurate with the category of the functions they perform.

4.2.2 I&C systems and equipment performing category A functions shall be periodically tested to demonstrate proper function.

4.2.3 I&C systems and equipment performing category B functions shall be periodically tested to the extent determined by an analysis taking into account the reliability goals of the functions.

4.2.4 I&C systems and equipment performing category C functions may rely on general periodic observation of acceptable performance for continuously operating functions and on checks during shutdown periods, for functions which are not continuously operating.

4.2.5 For I&C systems and equipment performing category B or C functions where redundancy is provided to meet established reliability goals, periodic individual testing of the functional capacity of all systems or sub-systems shall be included to the extent that faults of the redundant equipment are not revealed through other means, for example self-supervision.

4.2.6 In the general case, test equipment may be assigned to a lower category than the systems or equipment that is being tested. However, to the extent that the test features could interfere in an inappropriate manner with the proper operation of the system or equipment performing the function important to safety, it shall be assigned to the same category.

4.3 Extent of surveillance testing

4.3.1 The verification of correct operation during reactor operation shall include as much of the sensor and signal processing devices, of the logic assembly and the final actuation device under test as possible, without interfering unacceptably with normal plant operation.

4.3.2 Where overall functional testing is not practicable, a series of partially overlapping tests shall be used in such a way that the combination of partial tests will satisfy all testing requirements.

4.3.3 Functional tests may be supplemented with continuous monitoring to check for specific failure modes.

4.4 Self-supervision in lieu of periodic testing

I&C systems that have the capability to reveal faults, within a short time interval of their occurrence, by self-supervision performed by the equipment itself or by supervision of adjunct equipment, may be excluded from the requirement for periodic testing provided the following requirements are met.

4.4.1 An analysis shall be performed on such equipment to identify those postulated failure modes that are revealed by the self-supervision.

4.4.2 Any residual failure modes that are not revealed by self-supervision shall be shown not to affect the function important to safety of the equipment, or shall be covered by periodic testing designed to the requirements of this standard.

4.4.3 Equipment faults revealed by self-supervision shall be made known to the plant operating staff through appropriate alarms and indicating displays.

4.5 Continuous operation in lieu of periodic testing

Equipment that performs its function important to safety on a continuous basis, such as regulating controls, or that performs its function frequently during normal operation, as opposed to equipment that performs its function only in response to a plant upset condition or event, may be excluded from the requirement for periodic testing provided that the following requirements are met.

4.5.1 Equipment actions and behaviours that are required for a function important to safety and that are demonstrated on a continuing basis may be excluded from periodic testing. Deviations of such actions and behaviours from acceptable states shall be made known to the operating staff by appropriate indicators and alarms.

4.5.2 Equipment actions and behaviours that are required for a function important to safety and that are not demonstrated on a continuing basis shall be covered by periodic testing.

4.5.3 If the adequate performance of equipment excluded from periodic testing under 4.5.1 (for instance time response or accuracy) cannot be confirmed through observation then other means shall be provided to confirm its adequate performance.

5 General requirements for surveillance testing

5.1 Design requirements

5.1.1 The I&C system and equipment important to safety, including the final actuation devices, shall be designed for testing during operation of the nuclear power generating station, as well as during station shut-down (attention is drawn to 7.2). This design shall permit independent testing of redundant assemblies while maintaining the system capability to respond to bona-fide signals during operation.

5.1.2 The design shall provide for periodic testing to simulate accident signal trajectories, as closely as practicable, to verify the performance of the system required. The test shall be such as to demonstrate the full functional capability of the items under test.

5.1.3 Testing equipment shall not cause a loss of independence between redundant assemblies.

5.1.4 I&C systems and equipment shall be designed with due consideration of the impact of testing on plant availability and operation. Redundant equipment with coincidence logic should be provided, where necessary, to fulfil this provision.

NOTE This is not always possible for all parts of a system, for example for final actuation devices.

5.1.5 The I&C system and equipment important to safety and the testing equipment shall be designed so as to avoid functional degradation while under test. In all cases where the I&C system important to safety includes redundancy, it shall be designed so that while a signal processing channel and the associated logic assembly are under test, the function can be provided by the remaining part of the system not under test even if the system is degraded by a single random failure. An artificial actuation signal may be induced as part of the testing procedure to fulfil this requirement.

NOTE "One out of two" systems can be justified for exemption of the single-failure criterion during surveillance testing, provided that the reliability goals for the function are met.

5.1.6 Testability shall be considered in the selection of all components of I&C systems important to safety. Sensors should be accessible and, where practicable, installed so that their performance capability can be verified *in situ*. Selection of actuation devices shall consider their state indication capability.

5.1.7 A means of communication shall be provided between remote testing stations and the main control room to ensure that station operators are cognizant of the state of the systems under test.

5.1.8 Signal processing channels to be tested shall be capable of accepting simulated actuation signals in lieu of sensor output so that actuation of the signal processing channel can be verified from the point of test input, for example, during testing, to assist in verifying the overall response time of the I&C system important to safety.

5.1.9 The signal path for the test signal after the point of injection shall be the same as the signal path for the plant signal. No by-pass of the normal signal path is allowed.

5.1.10 All the circuits of an I&C system or equipment important to safety that carry out timing or filtering functions shall react to the testing signal, which may be of very short duration, so as to ensure that a positive result of the test is given only when:

– the circuit has switched over;
– the state after switching is stable and correct;
– the time delay or the time constant has the correct value.

5.2 Procedures

Periodic tests shall be made on the basis of carefully prepared test programmes in which identification of the tested parts, test conditions including initial plant state, test procedures and test periods are stated.

5.3 Data to be recorded upon detection of a fault

Upon detection of a fault at least the following data shall be recorded:

– identification of the tested part;
– test device description;
– detectable fault combinations;
– date and time of the test during which faults have been detected;
– period between this test and the previous test that would have permitted the detection of the faults;
– type of failure which could be caused by the fault in case of demand;
– operating mode of I&C system and plant for which the fault could be relevant (normal operation, start-up, shut-down, etc.);
– authorization signature(s);
– title of test programme;
– action taken when fault is detected.

5.4 Other data to be recorded

5.4.1 After each test where no fault was detected at least the following data shall be recorded:

– test frequency (for automatic tests only);
– test schedule used;
– date, time and duration of the test (for manually initiated tests);
– identification of tested equipment.

NOTE It is recommended that statistical data related to the test results be carefully recorded and analyzed to give realistic “failure rate” data. When such data become available with a reasonable confidence level, they should be compared with the frequency of testing to determine whether modification of the frequency in either direction is appropriate.

5.4.2 Any non-safety relevant values that can be measured during the surveillance tests should be analysed from the maintenance point of view and recorded. The only limitation of these measurements is that they shall not jeopardise the safety surveillance testing.

5.5 Test intervals

The test interval is the relevant design parameter for the demonstration that reliability and availability goals are met for the system under consideration. The test intervals shall be based on mathematical relations involving the reliability and availability goals, the type of system architecture, the expected fault-rate or experienced fault-rate, test duration and permissible system unavailability.

5.6 Verification of actuation set-points

5.6.1 Testing to verify actuation set-points that are continuously calculated or likewise testing to verify a calculated complex safety function with a fixed set-point level shall be performed by manipulating each variable that enters into the computation. While the signal for one or more variables is being varied to achieve actuation or change in computer output, the signals for the other variables should be adjusted to normal expected values for the actuation condition.

5.6.2 For computer-based I&C systems, where it can be shown by analysis that faults cannot alter set-point values or computations without causing other effects that are revealed by self-supervision, verification of actuation set-points may be excluded from periodic testing.

5.7 Bypass

5.7.1 Where parts of an I&C system important to safety require a maintenance bypass means to allow testing during a state of reactor operation (including shut-down) such bypasses shall be designed to standards applicable to the I&C system important to safety. In addition, the following shall be applied:

5.7.2 The state of the maintenance bypasses shall be clearly indicated to the operator in the control room. Indication of the state of the bypass shall be continuous.

5.7.3 Each maintenance bypass shall be interlocked with the remainder of the I&C system important to safety to ensure either that it can be applied only when predetermined plant conditions exist, or that incorrect application leads to automatic safety function being actuated. If this is not possible, an alarm shall be initiated when plant conditions demand that the bypass must be changed to the alternative state. This alarm shall be capable of being reset only when the bypass is moved to the correct position.

5.7.4 Bypasses are preferably applied and withdrawn automatically and in such cases redundancy and coincidence techniques shall be employed in their design to guard against incorrect application or withdrawal under conditions of equipment failure. Due consideration shall be given in the design of the automatic bypass to its performance under all plant transient conditions.

5.8 Response time

5.8.1 Response measurement of I&C systems and equipment important to safety shall verify the overall response time of the signal processing and logic assemblies from, and including where practicable, the sensor through to the operation of the actuation device (see Figure 1). Response time testing shall be performed on those systems or subsystems whose response time is critical to plant safety as described in the plant safety analysis report.

5.8.2 For I&C systems, where it can be shown by analysis that faults in some portions, for example computer based parts, cannot alter system time response without causing other effects that are revealed by self-supervision, response time verification of such portions may be excluded from periodic testing.

5.8.3 Where it is impracticable to perform response time tests during normal plant operation, response time testing should be performed during reactor shutdown. In some cases, when the periodic tests cannot be performed at the real conditions under which the system would be used for its safety function, it may be necessary to make corrections to the test results (for instance to compensate for temperature effects).

5.9 Restoration

The test procedure shall ensure that, after a test, the equipment is restored to its normal operational mode.

6 Requirements for testing of sensors and signal processing devices

6.1 General

6.1.1 The in-service verification of correct operation shall include as much of the signal processing and logic assembly as possible, without interfering unacceptably with normal plant operation.

6.1.2 When the characteristics of the sensor and of the remainder of the signal processing equipment are such as to require a different approach to their testing, overlap partial testing shall be undertaken to make sure that the equipment interfacing the sensor is fully functional.

6.2 Non-tested parts

For those parts that cannot be tested during reactor operation, the necessary availability shall be demonstrated by a combination of the following: the system design philosophy (for example fail safe design principles), continuous monitoring, and sufficient frequency of shutdowns to allow opportunity for testing (which may coincide with shutdowns scheduled for other reasons such as refuelling). The design of the I&C systems shall support, as completely as practical, full functional testing during shutdown conditions.

6.3 Testing devices

The testing devices may be part of each subassembly, or be the plug-in type. The first approach is preferable when test intervals must be very short (of the order of one or two months).

6.4 Signals

To introduce a test signal as close as practicable to the sensor, one of the following approaches may be adopted:

6.4.1 Perturbing the monitored variable. This refers to variations introduced into the variable, such as modified pressure, temperature or power.

6.4.2 Introducing and varying, as appropriate, a substitute input to the sensor, of the same nature as the monitored variable. This refers to such actions as opening an equalizing valve on differential-pressure cells, isolating and bleeding the input to pressure-measuring devices, or injecting hot or cold fluids into fluids whose temperature is monitored, or heating fluids by means of heating coils.

6.4.3 Introducing and varying, as appropriate, an analogue input for partial testing of a signal processing device when complete checks, including those of the sensors, are not practicable. This refers to the use of simulated signals such as voltage, current, or resistance, applied to portions of the circuit.

6.4.4 The test procedure shall explicitly include the steps required to return the system to the operating state and confirm that this has been done correctly.

6.5 Variation of signals

6.5.1 General

The capability to vary the test signal amplitude shall be sufficient to confirm that the safety function will result for expected extremes of variable values. The nature of the test signal variation shall be developed in recognition of the performance characteristics of the particular devices involved. The response to rise-time, amplitude, or other wave-shape characteristics may be affected by equipment degradation or malfunction.

Examples of the nature of the test signals that may be used are:

6.5.2 Slowly changing signal

This type of signal should be selected if protective action is required for this kind of signal and if the equipment condition indicates that a slow rate of change of the signal might not produce the protective action.

6.5.3 Rapidly changing signal

This type of signal should be selected if protective action is required for this kind of signal and if the equipment condition indicates that a high rate of change of the signal might not produce the protective action.

6.5.4 Large change in signal

This type of signal should be selected if protective action is required for this kind of signal and if the equipment condition indicates that large deviations of the signal from normal might not produce the protective action (for example, by saturation).

The test to be performed on given devices may be a single type or a combination of types as necessary to demonstrate the devices' performance under various expected conditions.

6.6 Operability

6.6.1 The operability of instruments equipped with an indicator shall be verified by one, or a combination of, the following means:

– Comparisons of readings on sensors and signal processing devices that monitor the same variable and are not spatially dependent.
– Comparison of readings on sensors and signal processing devices that monitor the same variable and bear a known relationship to one another (e.g., by comparing intermediate-range and source-range neutron monitoring assemblies during a start-up or shut-down when both devices indicate within range).
– Comparison of readings on sensors and signal processing devices that monitor different variables and bear a known relationship to one another (e.g., the primary coolant outlet temperature and the associated power level).

6.6.2 The basis of the verification shall be identified in the test documentation along with the permitted tolerance of the measured value.

6.7 Sensor response time

6.7.1 Sensors whose response time is shown to be critical to reactor safety in the safety analysis report shall be tested for response time accuracy. The test documentation shall give the accepted tolerance of the measured value. Where practical, this response time testing should be combined with that of the complete functional chain including sensor, signal processing, logic assembly and actuating device.

6.7.2 Sensors others than those covered by 6.7.1 whose response time is a significant part of the overall system response time should be tested for response time accuracy.

6.8 Testing equipment

6.8.1 Sensor response time testing equipment shall include whatever is necessary to stimulate sensor input and simultaneously record input and output conditions for the determination of the overall response time.

6.8.2 Sensor response time may be inferred from analysis of process signal noise spectrum in lieu of direct stimulation of the sensor input.

6.9 Calibration and transfer function

Sensor and signal processing device calibration tests shall be performed to prove that with an input of known accuracy the instrument or associated circuitry gives the required analogue or digital output. In addition, the signal processing device transfer function shall be checked. Portions of the signal processing that are downstream of an analogue to digital converter, and which handle the signal as a numeric value, do not require calibration tests.

6.10 Surveillance

To facilitate surveillance of sensors and signal processing devices, the following examples are acceptable design approaches:

6.10.1 Sensors with an electric output may be provided with elevated zero and a high-threshold circuit to allow a plausibility check of the signal (check that the signal neither drops to zero nor goes above the normal range).

6.10.2 Logic devices may be designed for fail-safe behaviour with respect to their supply failure.

6.10.3 Logic devices may be provided with a single-pole-double-throw contact output to allow for a consistency check (exclusive OR) on the contact and on the wiring connecting the signal monitor to the logic assembly.

7 Requirements for testing of electromechanical equipment

7.1 General

Although electromechanical devices are suited for automatic testing, consideration should be given to the dependence of their life on the number of operations.

7.2 Interface

7.2.1 To overcome the difficulty of testing final actuation devices without causing a safety action, provisions shall be made in the design of the interface between testing equipment and the I&C system important to safety, so that one of the following three requirements is met:

7.2.2 Actuation devices and actuated equipment shall be tested individually or in judiciously selected groups; for example, testing the actuation device for a system pump separately from the actuation device for the system valves.

7.2.3 The operation of certain actuated equipment shall be prevented during a test of the related actuation devices; for example, moving the circuit breaker for a pump to a test position that prevents power from being supplied to the pump during a test closure of its circuit breaker. Operation of the actuated equipment itself shall be tested when plant conditions permit in a way that overlaps this test.

7.2.4 Operation of the actuated equipment shall require the coincident operation of more than one actuator device; for example, individual testing of the two solenoid-operated valves that act in coincidence to control compressed air to an isolation valve.

7.2.5 Design in accordance with the requirements of 7.2.3 or 7.2.4 shall be justified on the basis that the probability of failure of any actuated equipment that is not tested during station operation is acceptably low.

7.3 Typical functional tests

7.3.1 To ascertain that an I&C system important to safety is capable of performing its design function, tests for the actuators shall be made. Typical tests consist of one or more of the following, as appropriate:

7.3.2 Manual start-up of equipment (e.g., motor, pump, compressor, turbine or engine) and verification of proper operation. Test duration shall be sufficient to achieve stable operating conditions. Where it is impractical to start a pump or other equipment, test operation of the breaker in "test" position may be acceptable, as described in 7.2.3.

7.3.3 Manual stroking of valve and timing of full stroke, if required. In cases where full stroking of the valve is not practicable, a partial stroke test (e.g., main steam stop valves, turbine stop or control valves) or a valve control system test (e.g., control system for electrically operated relief valves, or the control circuit for explosive poison injection valves) may be acceptable.

7.3.4 Operation of actuating devices and verification of safety functions.

7.3.5 Verification of manually initiated safety functions. When this is not possible during plant operation, the test may be performed during reactor shutdown (e.g. manual tripping of the reactor).

7.3.6 Test of the actuator response time.

7.4 Continuous monitoring

To improve monitoring of actuator availability, continuous monitoring of actuator-associated variables (speed, pressure, supply voltage, etc.) may be performed.

7.5 Relays and valves

For electromagnetic devices that act upon energization, such as relays and solenoid valves, the testing system shall be designed to check coil continuity, but should also check the integrity of the electromagnetic circuit, i.e. the capability of generating the required magnetic flux.

8 Requirements for testing of logic assemblies

8.1 Scope

The requirements listed in this section also apply to the testing of the final part of the signal processing for trip actuation which may be designed for automatic testing (e.g. solid-state threshold circuits or timers). Whereas the general principles apply to all solid-state systems, this Clause does not primarily concern itself with techniques other than short-pulse testing. The application of short-pulse testing may be necessary in cases where full functional testing would unacceptably actuate plant equipment.

8.2 General

In a solid-state logic assembly the intrinsic technological characteristics are such as to allow more sophisticated functions and a better interface with the testing equipment and supervisory equipment without significant loss of system availability. Testing by automatic equipment is, of course, easier and it is recommended, but manual periodic testing is also permitted.

8.3 Switching of signals

8.3.1 The possibility of rapid switching in solid-state logic assemblies allows testing with pulse signals of short enough duration to avoid change of state of the final actuation assembly. Where this type of testing is applied, it shall be done in such a manner as to allow a bona fide actuation of the safety function to propagate through the circuit being tested. In this case there is no need for either a bypass or to place the tested circuit in the actuation condition because the single-failure criterion is met (see 5.1).

8.3.2 Where pulse testing of the sort described in 8.3.1 is used, the number of operations should not adversely affect equipment life.

8.3.3 When solid-state I&C systems important to safety are designed for automatic testing, they should be associated with a supervisory system (as detailed in sub-clause 8.6).

8.3.4 Since the testing equipment carries on cyclic operation without continuous supervision by the operator, the testing system should itself be equipped with self-checking features (as detailed in 8.9).

8.4 Testing signals

8.4.1 By injecting testing signals in all inputs of all signal processing devices and by comparing all outputs of the I&C system important to safety considered in all possible logic configurations, the testing system should automatically check that:

– there are no outputs corresponding to a request for actuation when all the configurations of inputs not simulating a request for safety function actuation have been injected;

– there are outputs corresponding to a request for actuation when all the configurations of inputs simulating a request for safety function actuation have been injected;

– the time constant of the signal processing device is correct;

– the duration and timing of output signals are correct.

The above applies to all the inputs to the signal processing device that may lead to a partial or total actuation.

8.4.2 In the case that overlapping testing is applied at least one component shall be tested in the overlapping signal path (see 4.3.2 and 6.1.2).

8.5 Interface

Consideration shall be given in the design of the interface between the test equipment and the I&C system important to safety to minimize the effect of failures in the testing equipment on the I&C system important to safety.

8.6 Data to be displayed

In the case of fault detection, the supervisory equipment of the I&C system important to safety shall display at least the following information for the operator's guidance:

– identification of the tested circuit;
– detectable fault combinations;
– test interrupted;
– I&C system unavailable;
– test equipment failure (see 8.9);
– unsafe failure in the tested circuit;
– safe failure in the tested circuit;
– partial actuation;
– total actuation;
– position of operating mode switches, if any (normal operation, start-up, shutdown, etc.);
– incorrect signal processing device time constant;
– period between this test and previous test that would have detected the fault(s).

8.7 Data to be recorded

For the purpose of post-failure documentation, the following information should be recorded:

– all the information relating to a displayed failure;
– time of detection of a failure;
– time at which full availability of the I&C system is restored.

8.8 Detailed display

Following an actuation of a safety function, a detailed display shall be available to the operator to inform him that all of the required actuations have been correctly performed. Generally, any real activation of a safety function should be analyzed, even spurious ones. Depending on the results and the completeness of the data collected, it may be concluded that the objectives of periodic surveillance have been met and that the next scheduled periodic testing for a subset of the equipment may be skipped.

8.9 Testing equipment

With the aid of the self-checking features mentioned below, the automatic testing equipment shall be automatically isolated from the I&C system important to safety in case of mal-operation. A testing equipment failure alarm shall also be given to the operator. In a pulse signal testing system this could be achieved by monitoring the following:

– testing pulse duration and amplitude;
– operation of the circuit comparing the output from the I&C system important to safety with the related inputs (by a suitable check routine);
– operation of the testing system;
– characteristics of testing system internal supplies;
– stall of automatic sequencing.

8.10 Testing equipment using pulses

8.10.1 Automatic testing equipment using pulses, the duration of which may become longer because of a fault, shall be designed to withhold testing of any parts of the I&C system important to safety where a partial actuation has occurred and the test could cause full actuation of safety functions.

8.10.2 The equipment to implement test inhibition and information display shall not be allowed to reduce overall safety through the introduction of undue complexity.

9 Self-supervision in computer-based I&C systems

Modern computer-based I&C can perform supervision of its operation in addition to doing the functions important to safety for which it is designed. To the extent that the self-supervision detects faults in the equipment before a system failure occurs, it can reduce the scope of periodic surveillance testing, or at a minimum relax the required interval of that testing so that it will coincide with plant shutdowns.

Testing performed during plant shutdown may require fewer provisions to avoid actuation of plant equipment, such as maintenance bypasses or excess redundancy to accommodate single failures, if the equipment being tested is not required to be operational during that plant mode. This allows a simplification of the I&C system design and enhances overall safety of the plant.

IEC 60987 requires that in order to meet the reliability requirements, the computer system shall supervise itself by software means.

9.1 Coverage of self-supervision

The self-supervision performed should confirm the following attributes. In some cases, hardware features, such a memory parity checks, may provide adequate coverage, while in other cases specific software tests may be needed.

9.1.1 Self-supervision should confirm the integrity of the stored program, e.g. by checksum of the program memory.

9.1.2 Self-supervision should confirm the ability of temporary memory (RAM) to retain values.

9.1.3 Self-supervision should confirm the capability of the processor to correctly execute the subset of instructions used in the performance of the function important to safety, with particular attention paid to those instructions that are not used to control program flow, such as floating point arithmetic.

9.1.4 Self-supervision should confirm the integrity of the address and data busses that are used to access memory and peripheral devices.

9.1.5 Self-supervision should confirm the correctness of messages sent between processors via multiplexed communication links.

9.1.6 Self-supervision should confirm the freshness of message sent between asynchronous processes.

9.1.7 Self-supervision should confirm the correctness of memory access (data not accessed as program, non-overflow of stack, etc.).

9.1.8 Self-supervision should confirm the validity of process signals (range checks, rate of change, etc.).

9.1.9 Self-supervision should confirm the correctness of control flow of the program execution.

9.1.10 During periodic functional testing, the behaviour of self-supervision features should be assessed for expected results.

It is expected that the extent of application of self-supervision features will depend on the safety category of the functions being performed by the computer-based equipment. Computers performing category A or B functions should apply more of the above listed means than computers performing category C functions.

IEC 60880 and IEC 62138 provide guidelines on defensive programming techniques that support detection of abnormal conditions which may occur during the execution of software in computer-based I&C equipment.

9.2 Balance of diagnostic versus functional processing

9.2.1 The amount of resources (cycle time, processing capacity, etc.) devoted to self-supervision shall be appropriately balanced with the performance of the function important to safety of the computer-based equipment. Execution of self-supervision features shall not degrade the performance of the function important to safety to an unacceptable level.

9.2.2 It may be appropriate to design the self-supervision such that only a portion is done on each execution cycle, thereby requiring several cycles to complete the entire set of supervision tasks. Where such a technique is applied, a positive means shall be provided to monitor the execution of the self-supervision features to verify that they are being completed within the specified time interval.

9.3 Watchdog timers

Many failures of computer-based equipment will lead to the cessation of program execution. Also, software anomalies may cause the execution of non-terminated loops that prevent other program sequences from being executed.

9.3.1 To protect against such contingencies, the computer-based I&C equipment performing functions important to safety should be fitted with watchdog timers that detect when normal program execution does not occur.

9.3.2 When applied, such watchdog timers shall be independent, to the extent practical, of the failure modes that could cause the cessation of program execution.

9.3.3 Upon reaching the set point value of the timer, the watchdog timer shall initiate an appropriate default action as specified in 9.4.

9.3.4 The watchdog timer shall be subject to periodic surveillance testing.

9.4 Action taken on detected fault

When a fault in a system or equipment important to safety is detected by self-supervision, an appropriate action shall be taken. This action shall consist of one, or a combination of, the following:

– reset and re-initialization of the computer-based equipment;

– actuation of the function important to safety (either partial or total);

– transfer of function to an alternate or backup computer-based equipment;

– alteration of coincidence logic to make the function tolerant of the failure;

– change of operating mode to make the function tolerant of the failure;

– selection of alternate or default signal values or parameters to allow continued safe operation of the plant;

– actuation of an alarm and display in the main control room of the status of the equipment important to safety.

Selection of the action to be taken upon detected failure shall be identified in the functional specification of the equipment, and shall be subject to the design requirements and verification appropriate to the category of the function important to safety.

9.5 Categorization of self-supervision software

9.5.1 While equipment that is used solely for the surveillance of systems and equipment performing functions important to safety may be categorized to be lower than the equipment being tested, software performing self-supervision of computer-based I&C equipment generally executes in the same processor as the software performing the function important to safety. As such, failure of the self-supervision software could disrupt the proper functioning of the equipment.

9.5.2 Software performing self-supervision functions shall be assigned to the same category as the equipment it is testing, and shall be designed and verified according to the requirements for that category. These requirements are established in IEC 60880 and IEC 62138, as appropriate.

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.

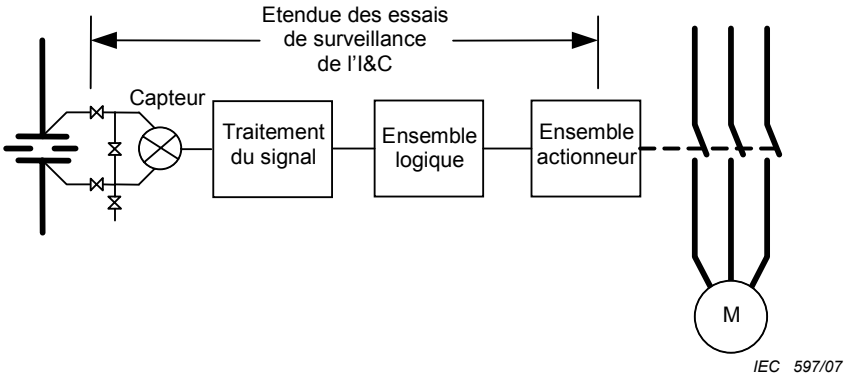

Figure 1 – Domaine des essais de surveillance de l'I&C

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*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1
essai automatisé
essai dans lequel le fonctionnement de tout ou partie du système d'I&C est vérifié par une séquence entièrement automatique. La séquence d'essai automatique peut être amorcée soit manuellement par un opérateur, soit cycliquement par une horloge ou automatiquement par la vérification d'une condition prédéfinie

3.2
disponibilité
aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné en supposant que la fourniture des moyens nécessaires est assurée

[VEI 191-02-05]

3.3
inhibition
dispositif permettant d'inhiber de façon délibérée mais temporaire, la fonction d'un circuit ou d'un système par, par exemple, le court-circuit des contacts d'un relai.

- **inhibition de maintenance**: inhibition du matériel d'un système de sûreté durant la maintenance, les essais ou la réparation ;
- **inhibition d'exploitation**: inhibition de certaines actions de protection lorsque celles-ci ne sont plus nécessaires dans des modes particuliers de fonctionnement de la tranche

[AIEA glossaire de sûreté, éd. 2.0 2006]

NOTE 1 Malgré l'application d'une inhibition de maintenance sur un canal, une fonction de sûreté peut quand-même être opérationnelle du fait de la présence de redondance et de voteurs majoritaires (par exemple une logique de vote en deux sur quatre passe en en deux sur trois).

NOTE 2 Une inhibition de maintenance n'est pas la même chose qu'une inhibition opérationnelle. Une inhibition en maintenance peut réduire le degré de redondance d'un matériel, mais elle n'entraîne pas la perte de la fonction de sûreté.

3.4
essai fonctionnel complet
essai comprenant une perturbation de la variable procédé, une détection par le capteur, un traitement du signal ou des signaux, une mise en service des sous-ensembles, des ensembles logiques et des actionneurs

3.5
fiabilité fonctionnelle
aptitude à être conforme à des exigences relatives aux fonctionnalités et aux performances globales et correctes :

a) dans tous les modes et conditions d'exploitation de la tranche définis,

b) dans tous les modes de fonctionnement définis des systèmes d'I&C de la tranche et

c) en présence de toutes défaillances ou modes de défaillance envisagés pour les systèmes d'I&C de la tranche dont le bon fonctionnement et les bonnes performances sont requis

3.6
surveillance
moyens prévus pour indiquer en permanence l'état ou les conditions dans lesquels se trouve un système ou un sous système, un équipement ou un ensemble

[VEI 393-08-48]

3.7
essais périodiques
réalisation d'essais à des instants prédéfinis permettant de démontrer que les capacités fonctionnelles des systèmes et des matériels d'I&C importants pour la sûreté sont assurées et de confirmer que les caractéristiques importantes pour satisfaire aux exigences de l'analyse de sûreté sont satisfaites

3.8
auto-surveillance
test automatique des performances matérielles et de la cohérence logicielle d'un système d'I&C informatisé

3.9
essais de surveillance
ensemble complet d'activités permettant de démontrer que les capacités fonctionnelles des systèmes et des matériels d'I&C importants pour la sûreté sont assurées et de confirmer que les exigences de dimensionnement sont satisfaites

3.10
durée d'essai
laps de temps écoulé entre le début et la fin d'essai

3.11
début d'essai
instant d'application du signal d'essai

3.12
signal d'essai
perturbation, réelle ou simulée, mais toujours délibérée, d'une variable mesurée ou d'un signal qui, en vue d'un essai, est imposé à tout ou à une partie d'un dispositif de traitement du signal, d'un ensemble logique ou d'un ensemble actionneur terminal

3.13
intervalle entre essai
laps de temps qui s'écoule entre les débuts d'essais identiques sur le même capteur, un même dispositif de traitement du signal, ou logique ou un même ensemble actionneur terminal

3.14
fin d'essai
suppression du signal d'essai dès la connaissance des résultats

4 Principes de base des essais de surveillance

4.1 Généralités

Les objectifs des essais de surveillance sont de garantir que les capacités fonctionnelles des systèmes d'I&C importants pour la sûreté et des canaux de commande pour mettre en service les composants du procédé associés importants pour la sûreté, sont assurées et de confirmer périodiquement que les exigences de dimensionnement telles que la fiabilité, la précision, le temps de réponse et le réglage des seuils, sont satisfaites (article 4.82 du document de l'AIEA NS-G-1.3).

4.1.1 Les essais de surveillance des systèmes d'I&C importants pour la sûreté doivent démontrer et contribuer, au travers de la détection des défauts, à l'atteinte du niveau de fiabilité et de disponibilité exigé pour le système et attirer l'attention sur les performances qui se situent hors des limites prescrites. Les limites prescrites sont des exigences de performances minimales, telles que le temps de réponse et la précision des points de consigne ou toute autre caractéristique du système essentielle à son bon fonctionnement. Les essais de surveillance doivent confirmer que les caractéristiques de sûreté essentielles sont assurées au regard des états de référence qui peuvent provenir des essais de mise en service vérifiant la satisfaction des exigences de dimensionnement. Bien que les essais de surveillance puissent permettre la détection de certains mécanismes d'usure et de vieillissement, ce domaine de détection n'est pas suffisant pour *a priori* détecter tous les mécanismes de vieillissement. Le bon fonctionnement opérationnel d'un matériel ou d'un système en conditions normales n'est généralement pas suffisant pour conclure sur le maintien de ces propriétés en présence des conditions d'un accident de dimensionnement. Il convient de noter que plusieurs types de défauts cachés qui pourraient être à l'origine de défaillances dangereuses, ne peuvent qu'être détectés par les essais.

4.1.2 Les essais de surveillance doivent permettre de vérifier les caractéristiques pertinentes des systèmes et matériels fournies directement par le rapport d'évaluation de sûreté, ou par d'autres documents de sûreté applicables, pour les fonctions réalisées par les systèmes d'I&C importants pour la sûreté. Ceci peut aussi être combiné aux essais de maintenance permettant la mesure des performances qui ne contribuent pas directement à la sûreté. De tels essais ne sont pas définis comme des essais de surveillance (voir 3.1) et sont en dehors du domaine de cette norme.

4.2 Gradation des exigences à partir des catégories

4.2.1 Les fonctions d'I&C importantes pour la sûreté sont affectées à des catégories de sûreté conformément aux principes de la CEI 61226. Les exigences concernant la surveillance des systèmes et des matériels doivent être fonction de la catégorie des fonctions réalisées.

4.2.2 Les systèmes et les matériels d'I&C réalisant des fonctions de catégorie A doivent être périodiquement testés pour démontrer leur bon fonctionnement.

4.2.3 Les systèmes et les matériels d'I&C réalisant des fonctions de catégorie B doivent être périodiquement testés d'une façon suffisante, déterminée par analyse en prenant en compte les objectifs de fiabilité fixés pour ces fonctions.

4.2.4 Pour les systèmes et les matériels d'I&C réalisant des fonctions de catégorie C on peut faire confiance à une observation périodique d'ensemble des performances acceptables pour les fonctions opérant de façon continue et à des vérifications en périodes d'arrêt pour les fonctions n'opérant pas en continu.

4.2.5 Pour les systèmes et les matériels d'I&C réalisant des fonctions de catégorie B ou C qui présentent des redondances pour satisfaire aux objectifs de fiabilité fixés, la couverture des essais périodiques individuels des capacités fonctionnelles de tous les systèmes ou sous-systèmes doit garantir que les défauts des matériels redondants ne puissent être révélés par aucun autre moyen, par exemple par auto-surveillance.

4.2.6 En général, les matériels d'essai peuvent être affectés à une catégorie plus basse que celle des systèmes ou des matériels testés. Cependant, dans la mesure où les caractéristiques d'essai pourraient interférer de façon inappropriée avec le bon fonctionnement du système ou du matériel réalisant la fonction importante de sûreté, ils doivent être affectés à la même catégorie.

4.3 Couverture des essais de surveillance

4.3.1 La vérification du fonctionnement correct pendant l'exploitation du réacteur doit concerner autant de capteurs, de dispositifs de traitement du signal, d'ensembles logiques et d'appareils actionneurs terminaux que possible, sans interférences inacceptables avec le fonctionnement normal de l'installation.

4.3.2 Lorsque des essais fonctionnels d'ensemble ne sont pas pratiquement réalisables, on doit réaliser une série d'essais se chevauchant partiellement pour que la combinaison de ces essais partiels satisfasse à toutes les exigences d'essai.

4.3.3 Les essais fonctionnels peuvent être complétés par une surveillance continue pour s'intéresser à des modes de défaillances particuliers.

4.4 Auto-surveillance en lieu et place d'essais périodiques

Les systèmes d'I&C ayant la capacité, du fait de l'auto-surveillance qu'ils assurent eux-mêmes ou qui est assurée par un matériel ajouté, de révéler les défauts, dans un laps de temps court après l'apparition de ceux-ci, peuvent ne pas être soumis aux exigences des essais périodiques si les exigences suivantes sont satisfaites.

4.4.1 Une analyse doit être faite de ces matériels pour identifier les modes de défaillance hypothétique qui seront révélés par les fonctions d'auto-surveillance.

4.4.2 Pour tous les modes de défaillance restants et qui ne sont pas révélés par les fonctions d'auto-surveillance on doit démontrer qu'ils ne portent pas atteinte aux matériels des fonctions importantes pour la sûreté, ou bien ceux-ci doivent faire l'objet d'essais périodiques conçus conformément aux exigences de cette norme.

4.4.3 Le personnel d'exploitation doit être averti, par des affichages d'alarmes et d'indicateurs adaptés, des défauts matériels révélés par les fonctions d'auto-surveillance.

4.5 Fonctionnement continu remplaçant les essais périodiques

Le matériel fonctionnant en continu pour réaliser sa fonction importante pour la sûreté, telle que le contrôle et la commande de régulation, ou qui réalise sa fonction fréquemment en exploitation normale, en opposition au matériel qui réalise sa fonction seulement sur demande et uniquement pour répondre à des conditions de la centrale perturbées ou à des événements, peut ne pas être considéré par les exigences relatives aux essais périodiques si les exigences suivantes sont satisfaites.

4.5.1 La mise en marche et le comportement des matériels tels que requis par les fonctions de sûreté et garanti par un fonctionnement continu peuvent être exclus des essais périodiques. Le personnel d'exploitation doit être averti, par des affichages d'alarmes et d'indicateurs adaptés, des écarts concernant de telles mises en marche et de tels comportements par rapport aux états admissibles.

4.5.2 La mise en marche et le comportement des matériels tels que requis par les fonctions de sûreté et non garantis par un fonctionnement continu doivent être couverts par des essais périodiques.

4.5.3 Si on ne peut vérifier par l'observation le bon fonctionnement du matériel non soumis aux essais périodiques au titre du paragraphe 4.5.1 (par exemple le temps de réponse ou la précision), alors d'autres moyens doivent être mis à disposition pour confirmer celui ci.

5 Prescriptions générales applicables aux essais de surveillance

5.1 Exigences de conception

5.1.1 Le système et le matériel importants pour la sûreté, y compris les appareils actionneurs terminaux, doivent être conçus pour pouvoir être essayés aussi bien lorsque la centrale nucléaire de puissance est en fonctionnement, que lorsque celle-ci est à l'arrêt (on attire l'attention sur 7.2). Cette conception doit permettre de tester indépendamment les ensembles redondants tout en maintenant la capacité du système à répondre aux signaux prévus en exploitation normale.

5.1.2 Des essais périodiques doivent être prévus lors de la conception pour simuler les trajectoires de signaux relatives aux accidents, aussi fidèlement que possible, pour vérifier les performances spécifiées pour le système. L'essai doit permettre de démontrer les pleines capacités fonctionnelles des éléments en essai.

5.1.3 L'essai de matériel ne doit pas entraîner de perte d'indépendance entre les ensembles redondants.

5.1.4 On doit concevoir les systèmes et le matériel d'I&C en considérant l'influence des essais sur la disponibilité et l'exploitation de la centrale. Il convient de prévoir, où ce sera nécessaire pour remplir ces conditions, les matériels redondants avec éléments de vote logiques.

NOTE Cela n'est pas toujours possible pour toutes les parties du système, comme par exemple pour les appareils actionneurs terminaux.

5.1.5 Le système et le matériel importants pour la sûreté ainsi que le matériel d'essai doivent être conçus de façon à éviter les dégradations fonctionnelles lors des essais. Dans tous les cas, lorsque le système d'I&C important pour la sûreté comporte des redondances, celles-ci doivent être conçues pour que lorsqu'on procède aux essais d'une chaîne de traitement du signal et de l'ensemble logique de sécurité associé, leurs fonctions puissent être assurées par les autres parties du système non soumises à l'essai, même si le système est affecté par une défaillance aléatoire unique. Pour satisfaire à cette exigence, un signal de déclenchement fictif peut être prévu dans la procédure d'essai.

NOTE Dans le cas d'un système en « un sur deux » on peut justifier de ne pas respecter le critère de défaillance unique durant les essais de surveillance, si les objectifs de fiabilité de la fonction sont satisfaits.

5.1.6 L'aptitude à subir des essais doit être prise en compte au moment du choix des composants des systèmes d'I&C importants pour la sûreté. Il convient que les capteurs soient accessibles et de préférence installés de sorte qu'il soit possible de contrôler leurs caractéristiques sur site. Le choix des actionneurs doit se faire en fonction du degré d'aptitude à indiquer leur état.

5.1.7 Un moyen de communication doit être prévu entre les points d'essai éloignés et la salle de commande principale, afin que les opérateurs placés aux points d'essais soient informés de l'état des systèmes soumis aux essais.

5.1.8 Les chaînes de traitement du signal à essayer doivent pouvoir accepter des signaux de mise en service simulés à la place des signaux issus des capteurs, de manière à pouvoir contrôler l'efficacité de la chaîne de traitement du signal à partir du point d'essai, par exemple pour contribuer à la vérification du temps global de réponse des systèmes importants pour la sûreté.

5.1.9 Le cheminement du signal d'essai à partir du point d'injection doit être identique au trajet suivi par le signal réel. Il n'est pas permis de faire emprunter au signal un contournement par rapport à son cheminement normal.

5.1.10 Tous les circuits d'un système et du matériel important pour la sûreté qui remplissent des fonctions de temporisation ou de filtrage doivent réagir au signal d'essai qui peut être de durée très réduite, de manière à s'assurer que l'essai ne donne des résultats positifs que dans les cas suivants:

– le circuit s'est commuté;
– l'état consécutif à la commutation est stable et correct;
– le retard ou la constante de temps a la bonne valeur.

5.2 Procédures

Les essais périodiques doivent être effectués suivant des programmes soigneusement préparés identifiant les parties à essayer, définissant les conditions d'essai, y compris l'état initial de la centrale, ainsi que les procédures d'essai et leur périodicité.

5.3 Informations à enregistrer lors de la détection d'un défaut

Lors de la détection d'un défaut on doit au moins enregistrer les informations suivantes:

– identité de la partie à essayer;
– description de l'appareillage d'essai;
– combinaison des défauts détectés;
– date et heure de l'essai durant lequel les défauts ont été détectés;
– intervalle de temps entre cet essai et le précédent qui aurait permis la détection du défaut;
– type de défaillance qui pourrait être la conséquence de ce défaut en cas de sollicitation;
– mode de fonctionnement du système d'I&C et de la centrale pour lequel ce défaut pourrait être important (fonctionnement normal, démarrage, arrêt, etc.);
– signature(s) d'autorisation;
– intitulé du programme d'essai;
– décision ou mesure prise après détection d'un défaut.

5.4 Autres informations à enregistrer

5.4.1 Après chaque essai où aucun défaut n'a été détecté, les informations suivantes doivent être enregistrées:

– fréquence des essais (pour les essais automatiques seulement);
– plan d'exécution utilisé pour l'essai;
– date, heure et durée de l'essai (pour les essais commandés manuellement);
– identité de l'équipement essayé.

NOTE Il est conseillé d'enregistrer, d'analyser soigneusement les informations statistiques obtenues aux essais pour avoir une estimation réaliste du « taux de défaillance ». Quand on peut obtenir ce taux de défaillance avec un taux de crédibilité raisonnable, il convient de réexaminer la fréquence des essais afin de déterminer s'il serait judicieux de la modifier dans un sens ou dans un autre.

5.4.2 Il convient d'analyser et d'enregistrer, du point de vue maintenance, toute information pertinente non liée à la sûreté qui peut être mesurée durant l'essai de surveillance. L'acquisition de ces mesures doit être seulement limitée lorsque celle-ci compromet le bon déroulement des essais de surveillance de sûreté.

5.5 Intervalles entre essais

L'intervalle entre essais est le paramètre de conception pertinent permettant de démontrer que les objectifs de fiabilité et de disponibilité du système considéré sont atteints. Le calcul des intervalles entre essais doit reposer sur les relations mathématiques prenant en compte les objectifs de fiabilité et de disponibilité, le type d'architecture système, le taux de défaillance prévu ou le taux de défaillance observé, les durées d'essais et les indisponibilités système admissibles.

5.6 Vérification des points de consigne

5.6.1 On doit effectuer, en utilisant chaque variable entrant dans le calcul, des essais pour vérifier les points de consignes de mise en service calculés en permanence ainsi que les fonctions de sûreté complexes calculées pour un pour un point de consigne. Pendant que l'on fait varier le signal correspondant à une ou plusieurs variables pour provoquer la mise en service ou modifier le résultat des calculs, il convient de régler les signaux relatifs aux autres variables sur les valeurs correspondant aux conditions ordinaires attendues pour la mise en service.

5.6.2 Lorsque, pour les systèmes d'I&C informatisés, on peut montrer par analyse que les défaillances ne peuvent avoir d'effet sur la valeur des points de consigne ou sur les calculs, sans produire d'autres effets qui sont détectés par les mécanismes d'auto-surveillance, alors la vérification des points de consigne de mise en service peut être exclue des essais périodiques.

5.7 Inhibitions

5.7.1 Lorsque certaines parties des systèmes d'I&C importants pour la sûreté nécessitent l'intervention d'une inhibition de maintenance pour les essais à un régime de fonctionnement donné du réacteur (y compris à l'arrêt), ces inhibitions doivent être conçues conformément aux normes applicables aux systèmes d'I&C importants pour la sûreté. En outre les exigences suivantes doivent être satisfaites:

5.7.2 L'état d'inhibition de maintenance doit être clairement indiqué à l'opérateur en salle de commande. L'indication de cet état d'inhibition doit être permanente.

5.7.3 Chacune de ces inhibitions de maintenance doit être assujettie au reste du système d'I&C important pour la sûreté de telle sorte qu'elles ne puissent être activées que lorsque certaines conditions liées à la centrale existent ou qu'en cas d'activation incorrecte d'une fonction automatique de sûreté mise en service. En cas d'impossibilité, une alarme de sécurité doit être émise dès qu'une condition liée à la centrale exige que l'inhibition soit supprimée. Cette alarme ne doit pouvoir être réarmée qu'après suppression de l'inhibition.

5.7.4 Les inhibitions sont de préférence activées et supprimées de manière automatique. Dans ce cas, on doit appliquer des techniques de redondance et de coïncidence dès la conception pour se prémunir contre tout établissement ou suppression incorrects en cas de défaillance du matériel. On doit concevoir les inhibitions automatiques en tenant compte de leur comportement dans toutes les conditions transitoires affectant la centrale.

5.8 Temps de réponse

5.8.1 Pour mesurer la réponse de systèmes et de leur matériel importants pour la sûreté, on doit vérifier la durée globale de réponse des ensembles logiques et de traitement du signal, y compris si possible le capteur et l'appareillage actionneur (voir la Figure 1). On doit procéder à ces essais sur ceux des systèmes ou des sous-systèmes dont le temps de réponse est critique pour la sûreté de la centrale et qui sont identifiés dans le rapport de sûreté établi pour la centrale.

5.8.2 Lorsque, pour les systèmes d'I&C informatisés, on peut montrer par analyse que les défaillances de certaines parties, par exemple les ensembles de calculateurs, ne peuvent avoir d'effet sur la valeur du temps de réponse sans produire d'autres effets qui sont détectés par les mécanismes d'auto-surveillance, alors la vérification du temps de réponse de ces parties peut être exclue des essais périodiques.

5.8.3 Quand des raisons pratiques empêchent l'exécution d'essais relatifs au temps de réponse pendant l'exploitation normale de la centrale, il convient de se placer en période d'arrêt du réacteur. Dans certains cas, lorsque les essais périodiques ne peuvent être réalisés dans les conditions réelles où le système serait utilisé pour assurer ses fonctions de sûreté, il peut être nécessaire d'ajuster les résultats d'essai (par exemple pour compenser l'effet de température).

5.9 Remise en fonction

La procédure d'essai doit être conçue de telle sorte que, l'essai terminé, le matériel soit replacé dans son état normal de fonctionnement.

6 Exigences relatives aux essais des capteurs et des appareils de traitement du signal

6.1 Généralités

6.1.1 La vérification du fonctionnement correct au cours de l'exploitation du réacteur doit inclure une part aussi importante que possible de l'ensemble logique et de traitement du signal, sans perturber de manière inacceptable l'exploitation normale de la centrale.

6.1.2 Quand les caractéristiques du capteur et du reste de l'équipement de traitement du signal obligent à adopter une méthode d'essai différente, on doit procéder à des essais partiels se recoupant de manière à s'assurer du bon fonctionnement de l'interface du capteur.

6.2 Parties non soumises aux essais

Pour les parties qui ne peuvent être essayées en fonctionnement, la fiabilité nécessaire doit être démontrée par une combinaison des éléments suivant: principes de conception du système (par exemple principes de conception intégrant des positions de repli sûr suite aux défaillances), surveillance permanente, et fréquence d'arrêt suffisante permettant des essais (qui peuvent coïncider avec des arrêts programmés pour d'autres raisons telles que des rechargements). La conception des systèmes d'I&C doit permettre autant que possible de réaliser des essais fonctionnels complets aux conditions d'arrêt.

6.3 Dispositifs d'essai

Les dispositifs d'essai peuvent être incorporés à chaque sous-ensemble ou être du type embrochable. La première solution est préférable quand les intervalles entre essais sont très courts (de l'ordre de un à deux mois).

6.4 Signaux

Pour introduire un signal d'essai aussi près que possible du capteur, on peut adopter une des solutions suivantes:

6.4.1 Perturbation de la variable à surveiller. Il s'agit d'introduire des variations correspondant par exemple à une modification de pression, de température ou de puissance.

6.4.2 Introduction ou variation, selon le cas, d'un signal fictif appliqué au capteur, de même nature que la variable à surveiller. Il s'agit par exemple de commander l'ouverture d'une vanne d'équilibrage de capteur de pression différentielle, ou d'isoler et de purger les canalisations des manomètres ou d'injecter des fluides froids ou chauds dans des fluides dont on contrôle la température ou encore d'échauffer ces fluides à l'aide de résistances.

6.4.3 Introduction ou variation selon le cas d'un signal analogique pour l'essai partiel d'un dispositif de traitement du signal qu'on ne peut vérifier complètement avec ses capteurs. Il s'agit de signaux fictifs, par exemple tensions, courants ou résistances appliqués ou introduits en des points du circuit.

6.4.4 Les procédures d'essais doivent explicitement comprendre les étapes nécessaires pour remettre le système en état d'exploitation et pour confirmer que cela a été correctement fait.

6.5 Variations du signal

6.5.1 Généralités

Les caractéristiques des variations du signal d'essai doivent être suffisantes pour assurer la mise en œuvre de la fonction de sûreté quand les variables dépassent les limites prévues. La nature de ces variations de signal doit être définie d'après les caractéristiques fonctionnelles de l'appareil en question. La réponse en fonction du temps de montée de l'amplitude ou d'autres caractéristiques de la forme d'onde peut être affectée par la détérioration du matériel ou son fonctionnement défectueux.

Quelques exemples de la nature des signaux d'essai que l'on peut employer sont:

6.5.2 Signal à variation lente

Il convient de choisir un signal de ce type si l'action de protection est prescrite pour de tels signaux et si l'état du matériel indique qu'une faible vitesse de modification du signal risque de ne pas déclencher l'action de protection.

6.5.3 Signal à variation rapide

Il convient de choisir un signal de ce type si l'action de protection est prescrite pour de tels signaux et si l'état du matériel indique qu'une vitesse élevée de modification du signal risque de ne pas déclencher l'action de protection.

6.5.4 Signal à variation de grande amplitude

Il convient de choisir un signal de ce type si l'action de protection est prescrite pour de tels signaux et si l'état du matériel indique que des variations de grande amplitude du signal risquent de ne pas déclencher l'action de protection (en cas de saturation, par exemple).

L'essai à effectuer sur des dispositifs donnés peut faire appel à des signaux de type unique ou à une combinaison de plusieurs types, suivant le cas, pour garantir le comportement du dispositif en fonction des diverses conditions attendues.

6.6 Aptitude opérationnelle

6.6.1 L'aptitude opérationnelle des appareils munis d'un indicateur doit être vérifiée par une, ou par une combinaison des méthodes suivantes:

– Comparaison de lectures faites sur des capteurs et des appareils de traitement du signal qui contrôlent la même variable et qui sont géographiquement séparés.

– Comparaison des lectures faites sur des capteurs et des appareils de traitement du signal qui contrôlent la même variable, des lectures étant liées par une relation (par exemple en comparant les ensembles de contrôle des flux de neutrons de niveau intermédiaire et de niveau source pendant un démarrage ou un arrêt, quand les deux ensembles travaillent dans les limites de leur étendue de mesure).
– Comparaison des lectures faites sur des capteurs et des appareils de traitement du signal qui contrôlent des variables différentes, mais liées par une relation connue (par exemple température de sortie du réfrigérant primaire et la puissance correspondante).

6.6.2 La méthode de la vérification, ainsi que les tolérances admises associées aux valeurs mesurées doivent être indiquées dans la documentation d'essai.

6.7 Temps de réponse des capteurs

6.7.1 La précision du temps de réponse des capteurs dont on sait que celle-ci présente un caractère critique pour la sûreté du réacteur, d'après le rapport de sûreté, doit être vérifiée. Les tolérances admises associées aux valeurs mesurées doivent être indiquées dans la documentation d'essai. Il convient de combiner autant que possible cet essai du temps de réponse avec un essai fonctionnel complet de la chaîne couvrant le capteur, le traitement du signal, l'ensemble logique et l'appareil actionneur.

6.7.2 Il convient de vérifier la précision du temps de réponse des capteurs, autres que ceux couverts par 6.7.1, dont le temps de réponse représente une part significative du temps de réponse global du système.

6.8 Matériel d'essai

6.8.1 Le matériel employé pour l'essai du temps de réponse des capteurs doit comprendre tous les éléments nécessaires pour stimuler la variation du signal d'entrée du capteur et, si nécessaire, pour enregistrer simultanément les signaux d'entrée et de sortie afin de déterminer le temps de réponse global.

6.8.2 Le temps de réponse des capteurs peut être déduit de l'analyse du spectre de bruit procédé remplaçant la stimulation directe des entrées capteur.

6.9 Etalonnage et fonction de transfert

Les essais d'étalonnage de capteur et de dispositif de traitement du signal doivent être réalisés pour montrer qu'avec un signal d'entrée connu et avec une précision donnée, l'appareil ou les circuits qui lui sont associés engendrent le signal de sortie numérique ou analogique prévu. En outre, on doit vérifier la fonction de transfert de l'appareil de traitement du signal. La partie du dispositif de traitement du signal en aval du convertisseur analogique-numérique, qui traite le signal comme une valeur numérique, ne nécessite pas d'essais d'étalonnage.

6.10 Surveillance

Pour faciliter la surveillance des capteurs et des dispositifs de traitement du signal, on peut s'inspirer, au stade de la conception, des exemples suivants:

6.10.1 Les capteurs à sortie électrique peuvent être munis d'un zéro décalé et d'un circuit à seuil élevé pour permettre un contrôle de vraisemblance du signal (on vérifie que le signal ne s'annule ni ne sort de la plage normale).

6.10.2 Le dispositif logique peut être doté d'un comportement de défaillance non dangereuse en cas d'interruption de l'alimentation.

6.10.3 Le dispositif logique peut être muni, à la sortie, d'un contact inverseur unipolaire permettant un contrôle de cohérence (OU exclusif) portant sur ce contact et sur le câble reliant le moniteur de signal à l'ensemble logique.

7 Exigences relatives aux essais périodiques des matériels électromécaniques

7.1 Généralités

Bien que les dispositifs électromécaniques soient adaptés à l'automatisation des essais, il convient de tenir compte du fait que leur durée de vie est fonction du nombre d'opérations.

7.2 Interface

7.2.1 Pour contourner la difficulté de soumettre aux essais les dispositifs actionneurs terminaux sans provoquer le déclenchement des mécanismes de sûreté, la conception de l'interface des matériels d'essai et du système d'I&C important pour la sûreté doit être telle qu'une des trois exigences suivantes est satisfaite:

7.2.2 Les dispositifs actionneurs et les matériels actionnés doivent être essayés individuellement ou par groupes judicieusement choisis, par exemple en séparant l'essai de l'actionneur associé à une pompe de celui de l'actionneur des vannes.

7.2.3 Le fonctionnement de certains matériels actionnés doit être interdit pendant l'essai de leur actionneur. Par exemple en plaçant le disjoncteur d'une pompe en position «essai», on interdit l'arrivée du courant à la pompe pendant un essai de fermeture du disjoncteur. Le fonctionnement des matériels actionnés eux-mêmes doit être essayé lorsque les conditions de l'installation le permettent et ceci de façon à assurer un chevauchement avec cet essai

7.2.4 Le fonctionnement des matériels actionnés doit impliquer l'intervention simultanée de plusieurs actionneurs comme par exemple, pour l'essai individuel de vannes commandées par deux électro-aimants agissant en coïncidence pour commander l'admission d'air comprimé sur une vanne d'isolement.

7.2.5 La justification de toute conception conforme aux exigences de 7.2.3 ou 7.2.4 doit se fonder sur une probabilité suffisamment faible de défaillance de chacun des matériels actionnés qui ne sont pas soumis aux essais pendant l'exploitation de la centrale.

7.3 Essais fonctionnels

7.3.1 Pour s'assurer qu'un système d'I&C important pour la sûreté est apte à remplir les fonctions prévues à la conception, des essais doivent être effectués sur les actionneurs. Les essais types consistent en une ou plusieurs des opérations suivantes suivant les cas:

7.3.2 Démarrage manuel du matériel (moteur, pompe, compresseur, turbine par exemple) avec vérification du fonctionnement. La durée de l'essai doit être suffisante pour atteindre la stabilité de régime. S'il n'est pas indiqué de faire démarrer le matériel (pompe, etc.), un essai de fonctionnement de la commande en position «essai», comme mentionné en 7.2.3 peut être admis.

7.3.3 Si besoin est, ouverture et fermeture manuelle de la vanne avec minutage de l'opération complète. S'il n'est pas indiqué de procéder à cette opération, on pourra se contenter d'un essai partiel d'ouverture et de fermeture (cas des vannes principales d'arrêt de vapeur, des vannes d'arrêt ou de commande des turbines) ou d'un essai du système de commande (cas des systèmes de commande des soupapes de détente fonctionnant électriquement ou des circuits de commande des vannes explosives d'empoisonnement).

7.3.4 Mise en service de l'actionneur et vérification de la fonction de protection.

7.3.5 Vérification des fonctions de sûreté lancées manuellement. S'il n'est pas possible de procéder à ces opérations en cours d'exploitation, l'essai peut être effectué pendant un arrêt du réacteur (déclenchement manuel du réacteur par exemple).

7.3.6 Essai de temps de réponse de l'actionneur.

7.4 Surveillance permanente

Pour améliorer la surveillance de la disponibilité des actionneurs, on peut procéder au contrôle permanent des variables qui leur sont associées (vitesse, pression, tension d'alimentation, etc.).

7.5 Relais et vannes

Pour les dispositifs électromagnétiques qui agissent par mise sous tension, comme les relais et les électrovannes on doit prévoir lors de la conception du système d'essai non seulement la continuité des enroulements, mais aussi l'intégrité du circuit électromagnétique, c'est-à-dire son aptitude à produire le flux magnétique voulu.

8 Exigences relatives aux essais d'ensembles logiques

8.1 Domaine d'application

Les exigences énumérées dans cet article s'appliquent aux parties terminales du dispositif de traitement du signal associé au déclenchement de l'arrêt d'urgence qui peut être soumis à des essais automatisés (comme les circuits à seuil ou les horloges à semi-conducteurs). Bien que les principes généraux s'appliquent à tous les systèmes à semi-conducteurs, cet article ne concerne pratiquement pas d'autres techniques que les essais par impulsions. L'exécution d'essais par impulsion peut être nécessaire lorsque les essais fonctionnels complets impliquent une mise en service d'actionneurs incompatible avec l'exploitation.

8.2 Généralités

Dans un ensemble logique à semi-conducteurs, les caractéristiques techniques permettent des fonctions plus élaborées ainsi que de meilleures interconnexions avec les matériels d'essai et de contrôle sans perte notable de disponibilité du système. Les essais effectués avec un matériel automatisé sont naturellement plus faciles et conseillés, mais il est aussi permis de procéder à des essais périodiques manuels.

8.3 Commutation des signaux

8.3.1 La possibilité de commutation rapide pour les ensembles logiques à semi-conducteurs permet de réaliser des essais avec des signaux d'impulsion d'une durée assez courte pour éviter le changement d'état de l'ensemble actionneur terminal. Lorsque ce type d'essai est réalisé, ceci doit être fait de façon à permettre à une fonction de sûreté justifiée qui serait lancée de se réaliser avec le circuit en essai. Dans ce cas, il n'y a besoin ni d'inhibition, ni de mettre le circuit en service, car le critère de défaillance unique est satisfait (voir 5.1).

8.3.2 Lorsque des essais par impulsion du type de ceux décrits en 8.3.1 sont réalisés, il convient que le nombre d'essais n'ait pas d'influence sur la durée de vie du matériel.

8.3.3 Lorsqu'on utilise des systèmes à semi-conducteurs importants pour la sûreté conçus pour être testés automatiquement, il convient de leur associer un système de supervision (comme indiqué en 8.6).

8.3.4 Les matériels d'essai réalisant des opérations périodiques sans surveillance permanente des opérateurs, il convient que le système d'essai soit lui-même équipé de fonctions d'auto-vérification (comme indiqué en 8.9).

8.4 Signaux d'essai

8.4.1 Par injection de signaux d'essai sur toutes les entrées de tous les dispositifs de traitement du signal et en comparant les états de sortie du système important pour la sûreté considéré, dans toutes les configurations logiques possibles, il convient que le système d'essai vérifie automatiquement:

– qu'aucun signal de sortie ne correspond à un ordre de mise en service à la suite de l'injection de toute configuration de signaux d'entrée ne simulant pas un ordre de déclencher l'action de protection;
– qu'il existe des signaux de sortie correspondant à un ordre de mise en service à la suite de l'injection de toute configuration de signaux d'entrée simulant un ordre de mise en service de fonction de sûreté;
– que la constante de temps du dispositif de traitement du signal est correcte;
– que la durée et l'ordre de succession de sortie sont corrects.

Ces remarques s'appliquent à toutes les entrées des dispositifs de traitement du signal qui peuvent donner lieu à une mise en service partielle ou totale.

8.4.2 Dans le cas d'essais se chevauchant au moins un composant doit être testé sur le chemin des signaux chevauchants (voir 4.3.2 et 6.1.2).

8.5 Interface

L'interface entre le matériel d'essai et le système d'I&C important pour la sûreté doit être étudiée pour minimiser l'influence sur le système important pour la sûreté des défaillances du matériel d'essai.

8.6 Informations à afficher

Lors de la détection d'un défaut, le matériel de surveillance du système important pour la sûreté doit, pour guider l'opérateur, afficher au moins les informations suivantes:

– identité du circuit essayé;
– combinaison de défauts détectés;
– essai interrompu;
– système d'I&C indisponible;
– défaillance du matériel d'essai (voir 8.9);
– défaillance dangereuse dans le circuit essayé;
– défaillance non dangereuse dans le circuit essayé;
– mise en service partielle;
– déclenchement total;
– position des commandes d'exploitation, le cas échéant (fonctionnement normal, démarrage, arrêt, etc.);
– constante de temps incorrecte du dispositif de traitement du signal;
– fréquence des essais qui aurait permis de détecter le ou les défauts.

8.7 Informations à enregistrer

Il est recommandé, pour constituer une documentation expérimentale sur les défauts, d'enregistrer les renseignements suivants:

– toutes les informations affichées à l'occasion du défaut;
– le moment de détection du défaut;
– le moment où le système d'I&C important pour la sûreté a recouvré sa pleine disponibilité.

8.8 Affichage détaillé

Suite à une mise en service d'une fonction de sûreté, un affichage détaillé doit informer l'opérateur que toutes les opérations prescrites ont bien été réalisées correctement. En général, il convient d'analyser toutes activations effectives de fonctions de sûreté, même les intempestives. Suivant les résultats et la complétude des données rassemblées, on peut en conclure que les objectifs de la surveillance périodique sont atteints et que les essais périodiques de sûreté prévus pour la fois suivante sur un sous-ensemble de matériel ne soient pas réalisés.

8.9 Matériel d'essai

En cas de mauvais fonctionnement, le matériel d'essai automatisé doit pouvoir être isolé automatiquement du système d'I&C important pour la sûreté, au moyen de fonctions d'auto contrôle présentées ci-dessous. Une alarme relative à la défaillance du matériel d'essai doit être fournie à l'opérateur. Pour un système d'essai par impulsions on peut y parvenir en surveillant les points suivants:

– durée et amplitude des impulsions d'essai;
– fonctionnement du circuit comparant le signal de sortie du système d'I&C important pour la sûreté avec les signaux d'entrée correspondants (à base d'une procédure de contrôle);
– fonctionnement du système d'essai;
– caractéristiques du système d'essai des alimentations internes;
– interruption des séquences automatiques.

8.10 Matériel d'essai à impulsions

8.10.1 Le matériel d'essai automatisé travaillant en impulsions dont la durée peut augmenter à la suite d'un défaut doit être conçu de manière à interdire l'essai de toute partie du système d'I&C important pour la sûreté pour lequel s'est produite une mise en service partielle que l'essai risque de transformer en mise en service totale des fonctions de sûreté.

8.10.2 Le matériel servant à interdire la poursuite de l'essai et à afficher l'information correspondante ne doit pas, en introduisant une complexité inutile, porter atteinte à la sûreté d'ensemble.

9 Auto-surveillance des systèmes d'I&C informatisés

Les systèmes d'I&C informatisés peuvent assurer la surveillance de leur propre fonctionnement, en plus de la réalisation des fonctions importantes pour la sûreté pour lesquelles ils ont été conçus. Considérant qu'une telle auto-surveillance détecte les défauts de l'équipement avant qu'une défaillance système ne survienne, ceci peut réduire le domaine d'essais de surveillance périodiques, ou au minimum relaxer les contraintes relatives à l'intervalle de temps entre essais pour que ces essais coïncident avec les arrêts de tranche.

Les essais réalisés pendant les arrêts de tranche peuvent nécessiter moins de précautions pour éviter les démarrages de matériels de tranche, tels que des inhibitions de maintenance ou des niveaux de redondance supplémentaires pour faire face au critère de défaillance unique, si la disponibilité opérationnelle du matériel en essai n'est pas requise pour le mode de fonctionnement de la tranche considéré. Ceci autorise des simplifications de conception du système d'instrumentation et contrôle commande et augmente le niveau de sûreté d'ensemble de la tranche.

D'après la CEI 60987, le système informatisé doit s'auto-surveiller au moyen de logiciels afin de satisfaire aux exigences de fiabilité.

9.1 Couverture des fonctions d'auto-surveillance

Il convient que les fonctions d'auto-surveillance vérifient les propriétés suivantes. Dans certains cas des fonctionnalités matérielles, comme la vérification de la parité mémoire, peuvent assurer une couverture satisfaisante, alors que dans d'autre cas des essais particuliers de type logiciel sont nécessaires.

9.1.1 Il convient que les fonctions d'auto-surveillance assurent l'intégrité des programmes enregistrés, par exemple par des sommes de contrôle de la mémoire de rangement du programme.

9.1.2 Il convient que les fonctions d'auto-surveillance vérifient l'aptitude de la mémoire temporaire (RAM) à mémoriser des valeurs.

9.1.3 Il convient que les fonctions d'auto-surveillance vérifient l'aptitude du processeur à exécuter correctement des sous-ensembles d'instructions utilisés pour réaliser des fonctions importantes pour la sûreté, en faisant particulièrement attention aux instructions qui ne sont pas utilisées pour gérer le flux de commandes, telles que les fonctions arithmétiques en virgule flottante.

9.1.4 Il convient que les fonctions d'auto-surveillance assurent l'intégrité des bus d'adresses et de données utilisés pour accéder à la mémoire et aux appareils périphériques.

9.1.5 Il convient que les fonctions d'auto-surveillance vérifient que les messages envoyés entre processeurs par les liaisons multiplexées soient corrects.

9.1.6 Il convient que les fonctions d'auto-surveillance s'assurent du rafraîchissement des messages échangés entre les processus asynchrones.

9.1.7 Il convient que les fonctions d'auto-surveillance garantissent la validité des accès mémoire (données non accessibles comme un programme, non-débordement de pile, etc.).

9.1.8 Il convient que les fonctions d'auto surveillance garantissent la validité des signaux des processus (vérification des bornes, taux de changement, etc.).

9.1.9 Il convient que les fonctions d'auto-surveillance vérifient que le flux de commandes de l'exécution du programme soit correct.

9.1.10 Il convient d'évaluer durant les essais périodiques fonctionnels le comportement des fonctions d'auto-surveillance en fonction des résultats attendus.

Il est entendu que le domaine d'application des fonctions d'auto-surveillance dépend de la catégorie de sûreté des fonctions réalisées par les équipements informatiques. Il convient que les calculateurs réalisant des fonctions de catégories A ou B utilisent plus les moyens dont la liste est fournie ci-dessus que des calculateurs réalisant des fonctions de catégories C.

La CEI 60880 et la CEI 62138 fournissent des recommandations concernant les techniques de programmation défensive qui permettent une détection des conditions anormales pouvant survenir lors de l'exécution des logiciels par les matériels numériques d'I&C.

9.2 Equilibre entre diagnostique et traitement fonctionnel

9.2.1 Le montant de ressources (temps de cycle, capacité de traitement, etc.) dédié à l'auto-surveillance doit être équilibré avec celui réservé à la réalisation des fonctions de sûreté importantes pour la sûreté. L'exécution des fonctions d'auto-surveillance ne doit pas dégrader de façon inacceptable la réalisation de fonctions importantes pour la sûreté.

9.2.2 Il peut être judicieux de concevoir les fonctions d'auto-surveillance pour que seulement une partie d'entre elles soit exécutée à chaque cycle, ainsi plusieurs cycles sont nécessaires pour que la totalité des tâches de surveillance soit exécutée. Lorsque de telles techniques sont utilisées, on doit avoir à disposition le moyen de vérifier que celle-ci a été exécutée dans l'intervalle de temps spécifié.

9.3 Chiens de garde

De nombreuses défaillances de matériels numériques entraînent un arrêt de l'exécution des programmes. De plus, des anomalies logicielles peuvent avoir pour conséquence l'exécution de boucles sans fin qui empêche les autres séquences de programme d'être exécutées.

9.3.1 Pour se protéger contre de telles contingences, il convient de munir les matériels numériques d'I&C réalisant des fonctions importantes pour la sûreté de chiens de garde qui détectent les exécutions de programme anormales.

9.3.2 Lorsqu'on utilise de tels chiens de garde, ceux-ci doivent autant que possible être indépendants des modes de défaillance qui pourrait entraîner l'interruption des exécutions de programmes.

9.3.3 Lorsque les temporisations de surveillance sont dépassées, le chien de garde doit lancer les actions prévues pour la défaillance comme spécifié en 9.4.

9.3.4 Le chien de garde doit faire l'objet d'essais de surveillance périodique.

9.4 Action à réaliser lors de la détection d'un défaut

Lorsqu'un défaut est détecté dans un système ou dans un matériel important pour la sûreté par les fonctions d'auto surveillance, une action adaptée doit être lancée. Cette action correspond à un élément, ou à une combinaison des éléments suivants:

– remise à zéro et reinitialisation du matériel informatique;
– démarrage des fonctions importantes pour la sûreté (ou partiel ou total);
– transfert des fonctions vers un autre matériel informatique ou vers le matériel de secours;
– modification de la logique de coïncidence pour que la fonction tolère la défaillance;
– changement du mode de fonctionnement pour que la fonction soit tolérante au défaut;
– sélection de paramètres ou de valeurs de signal par défaut ou redondants pour assurer une exploitation sûre de la tranche dans la durée;
– activation d'alarmes et d'affichages concernant l'état des matériels importants pour la sûreté en salle de commande principale.

L'ensemble des actions à lancer lors de la détection des défaillances doit être déterminé par les spécifications fonctionnelles du matériel, et doit être conforme aux exigences de conception et faire l'objet de vérifications appropriées par rapport à la catégorie des fonctions importantes pour la sûreté réalisées.

9.5 Catégorisation des logiciels d'auto-surveillance

9.5.1 Alors que le matériel utilisé uniquement pour assurer la surveillance des systèmes et matériels réalisant des fonctions importantes pour la sûreté peut être classé dans une catégorie inférieure à celle du matériel surveillé, les logiciels réalisant les fonctions d'auto-surveillance des matériels numériques d'I&C s'exécutent généralement sur les mêmes processeurs que les logiciels réalisant les fonctions importantes pour la sûreté. Ainsi les défaillances des logiciels d'auto-surveillance peuvent porter atteinte au fonctionnement correct du matériel.

9.5.2 Les logiciels réalisant les fonctions d'auto-surveillance doivent être affectés à la même catégorie que le matériel surveillé et ils doivent être conçus et vérifiés conformément aux exigences applicables à cette catégorie. Ces exigences sont établies par les CEI 60880 et CEI 62138, suivant les cas.

_____

ISBN 2-8318-9124-8

ICS 27.120.20

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND