IEC 60744

Edition 2.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Instrumentation and control systems important to safety – Safety logic assemblies used in systems performing category A functions: Characteristics and test methods

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Ensembles logiques de sûreté utilisés dans les systèmes réalisant des fonctions de catégorie A: Caractéristiques et méthodes d'essai

IEC 60744:2018-05(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
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.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) 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 IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 21 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC 60744

Edition 2.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Instrumentation and control systems important to safety – Safety logic assemblies used in systems performing category A functions: Characteristics and test methods

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Ensembles logiques de sûreté utilisés dans les systèmes réalisant des fonctions de catégorie A: Caractéristiques et méthodes d'essai

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 21.120.20

ISBN 978-2-8322-5681-7

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SAFETY LOGIC ASSEMBLIES USED IN SYSTEMS PERFORMING CATEGORY A FUNCTIONS: CHARACTERISTICS AND TEST METHODS

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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 60744 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1983. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) update of the references to standards published or revised since the issue of the first edition of the current standard, including IEC 61513 and IEC 61226;
b) additional requirements for operational and maintenance bypass use; requirements of voting logic; requirements for interfacing with the MCR and SCR.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
45A/1188/FDIS	45A/1200/RVD

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

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

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

a) Technical background, main issues and organisation of the Standard

This standard IEC 60744 specifically focuses on safety logic assemblies used in NPPs (Nuclear Power Plants). Safety logic assemblies were originally hardwired parts of protection systems mainly used to control actuators. IEC 60744 specifically focuses on the design, including technology, interfaces with MCR and SCR, tests and qualification. It gives requirements for display of the safety system inputs and state.

IEC 60744 is the document concerning safety logic assembly functions and performance.

The use of a computer based equipment or software is covered comprehensively by other standards. The technology used to design SLAs therefore involves mainly hard-wired technologies and submicronic highly integrated components (HPDs), the implementation of which is limited due to the very high safety requirements.

The document addresses the design and test characteristics of safety logic assemblies, especially regarding functional requirements, reliability issues, and associated control means including alarm, indication and control. Also it suggests the requirements for performance, testing and qualification for safety logic assemblies, and the interface requirements for communication between assemblies.

It is intended that the document be used by operators of NPPs (utilities), systems evaluators and licensors.

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

IEC 60744 is the third level IEC SC 45A document tackling the specific issue of testing and design characteristics of safety logic assemblies.

IEC 60744 is to be read in association with IEC 61513 which is the appropriate IEC SC 45A document which provides guidance on I&C safety system, and IEC 60964 which is the appropriate document for guidance on the Control Rooms, since the safety system has extensive interfaces with the MCR and SCR.

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

c) Recommendations and limitations regarding the application of the Standard

It is important to note that this document establishes no additional functional requirements at safety system level.

Aspects for which special recommendations have been provided in this document are:

- The voting of partial trips to identify each safety actuation
- The output assemblies that provide the trips and actuations
- The design and test characteristics of functional requirements
- The reliability issue of safety logic assemblies
- The performance characteristics of logic assemblies
- Testing, qualification and interface requirements of safety logic assemblies

To ensure that the document will continue to be relevant in future years, the emphasis has been placed on issues of principle, rather than specific technologies.

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

The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defense against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 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 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, regarding control rooms, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the IEC SC 45A ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC SC 45A to decide how and where general requirement for the design of electrical systems were to be considered. IEC SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 is published this NOTE 2 of the introduction of IEC SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SAFETY LOGIC ASSEMBLIES USED IN SYSTEMS PERFORMING CATEGORY A FUNCTIONS: CHARACTERISTICS AND TEST METHODS

1 Scope

This document provides requirements and recommendations for the design, construction and test of safety logic assemblies used in safety systems to perform category A safety functions (in accordance with IEC 61226). Safety logic assemblies include logic such as the hardwired logic assembly interfacing computer-based systems to switchgear, actuators or contactors to provide trip or engineered safety feature actuations. Safety logic assemblies are significant parts of a safety system and may include voting logic between redundant channels.

This document provides a general description of safety logic assemblies for safety actuators control. The principles to meet dependability objectives are presented. The main features relating to the design requirements are described and explained.

Various tests and their requirements are given in order to validate the design (including the qualification tests), the manufacturing and the correct installation on site.

Annex A (informative) gives a list of possible applications of safety logic assemblies.

Annex B (normative) suggests a list of possible hardwired technologies with their respective requirements to design safety logic assemblies.

Annex C (informative) gives explanations on dependability and its attributes to improve reliability and to reduce the final risk which compromises the safety and the availability of the NPP.

The scope of this document does not address the design of a protection system, it covers only the technological and architectural solutions required to design a safety logic assembly. The design of safety systems using safety logic assemblies is covered by IEC 61513.

The detailed and specific functions implemented in a safety logic assembly strongly depend on the design of each reactor and are not addressed in this document.

As this document is focused on I&C part of the system, the final voting logic made with power breakers is excluded from the scope of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60255 (all parts), *Measuring relays and protection equipment*

IEC 60671, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 60709, *Nuclear power plants – instrumentation and control systems important to safety – Separation*

IEC/IEEE 60780-323, *Nuclear facilities – Electrical equipment important to safety – Qualification*

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

IEC 60964, *Nuclear power plants – Control rooms – Design*

IEC 60965, *Nuclear power plants – Control rooms – Supplementary control room for reactor shutdown without access to the main control room*

IEC 60980, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

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

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

IEC 61227, *Nuclear power plants – Control rooms – Operator controls*

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

IEC 62003, *Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*

IEC 62241, *Nuclear power plants – Main control room – alarm functions and presentation*

IEC 62566:2012, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

IAEA-GSR Part 2, *Leadership and Management for Safety*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
availability
ability of an item or a system 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, given that the necessary external resources are provided

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.2
channel
arrangement of interconnected components within a system that initiates a single output. A channel loses its identity where the single-output signals are combined with signals from another channels (eg; from a monitoring channel or a safety actuation channel)

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.3
dependability
general term describing the overall trustworthiness of a system; i.e. the extent to which reliance can justifiably be placed on this system. Reliability, availability and safety are attributes of dependability

Note 1 to entry: Annex C gives clarifications on this definition.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.4
dynamic logic equipment
system assembly or subassembly employing dynamic logic signals

3.5
dynamic logic signal
periodically changing voltage or current, the frequency being consistent with the required system response time. The different logic states are associated with different values of one or more parameters of the periodic change, for example, amplitude, slope, repetition rate of pulses or alternations, or pulse coding

Note 1 to entry: One logic state may be associated with the absence of periodic change of such a signal.

3.6
engineered safety feature
actuating part of a safety actuation system (actuator associated with its electrical and driving part)

Note 1 to entry: Engineered safety features need energy to operate (valves, motors, etc.). Generally, they are compared with reactor trip breakers which do not need energy to operate.

3.7
failure
loss of the ability of a structure, system or component to function within acceptance criteria

Note 1 to entry: The structure, system or component is considered to fail when it becomes incapable of functioning, whether or not this is needed at that time. A failure in, for example, a backup system may not be manifest until the system is called upon to function, either during testing or on failure of the system it is backing up.

Note 2 to entry: A failure of a structure, system or component is an event that results in a fault of that structure, system or component.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.8
Field Programmable Gate Array
FPGA
integrated circuit that can be programmed in the field by the I&C manufacturer. It includes programmable logic blocks (combinatorial and sequential), programmable interconnections between them and programmable blocks for input and/or outputs. The function is then defined by the I&C designer, not by the integrated circuit supplier

Note 1 to entry: While FPGAs are essentially digital devices, some of them may integrate analogue input/outputs and analogue to digital converters. FPGAs may include advanced digital functions such as hardware multipliers, dedicated memory and embedded processor cores.

[SOURCE: IEC 62566:2012, 3.5]

3.9
hardware description language
HDL
language used to formally describe the functions and/or the structure of an electronic component for documentation, simulation or synthesis

[SOURCE: IEC 62566:2012, 3.6]

3.10
HDL-Programmed Device
HPD
integrated circuit configured (for NPP I&C systems) with hardware description languages and related software tools

[SOURCE: IEC 62566:2012, 3.7]

3.11
operational states
states defined under normal operation and anticipated operational occurrences

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.12
partial trip signal
binary signal provided by a channel of a safety system after processing the signals received from the sensors of this channel, before it has been processed by the final voting logic to give a scram requirement or ESF actuation requirement

3.13
programmable logic device
PLD
integrated circuit that consists of logic elements with an interconnection pattern, parts of which are user programmable

Note 1 to entry: Different kinds of PLDs exist, e.g. Erasable PLD or Complex PLD (CPLD).

Note 2 to entry: The differences between “FPGA” and “PLD” are not well defined, but “PLD” usually refers to a simpler device than “FPGA”.

[SOURCE: IEC 62566:2012, 3.13]

3.14
qualified life
period for which a structure, system or component has been demonstrated, through testing, analysis or experience, to be capable of functioning within acceptance criteria during specific operating conditions while retaining the ability to perform its safety functions in accident conditions for a design basis accident or a design basis earthquake

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.15
redundancy
provision of alternative (identical or diverse) structures, systems and components, so that any single structure, system or component can perform the required function regardless of the state of operation or failure of any other

Note 1 to entry: This definition has to be clarified for the needs of this document:

- Non-diverse redundancy – to address the risk of single (random) failure.
- Diverse redundancy – to address the risk of random failure or common mode failure.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.16
reliability
probability that a device, system, component or facility will meet its minimum performance requirements when called upon to do so

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.17
safety (nuclear)
protection of people and the environment against radiation risks, and the safety of facilities and activities that give rise to radiation risks

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.18
safety function
specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions

Note 1 to entry: IAEA SSR2/1 establishes requirements on safety functions to be fulfilled by the design of a nuclear power plant in order to meet three general safety requirements:

a) the capability to safely shut down the reactor and maintain it in a safe shutdown condition during and after appropriate operational states and accident conditions;

b) the capability to remove residual heat from the reactor core, the reactor and nuclear fuel in storage after shutdown, and during and after appropriate operational states and accident conditions;

c) the capability to reduce the potential for the release of radioactive material and to ensure that any releases are within prescribed limits during and after operational states and within acceptable limits during and after design basis accidents.

Note 2 to entry: IEC 61226 gives recommendations related to categories of safety functions.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.19
safety logic assembly
equipment, part of a protection system performing simple category A logic functions with a very high level of dependability and generally used to send commands to safety actuators or signals to another safety logic assembly

Note 1 to entry: A simple logic function is combinatory and/or sequential. Consequently, such a function is fully testable.

3.20
safety system
system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the reactor core, or to limit the consequences of anticipated operational occurrences and design basis accidents

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.21
scram
rapid shutdown of a nuclear reactor in an emergency

Note 1 to entry: The term scram is associated with the trip unit which is the part of a circuit breaker that opens the circuit. Then a scram is often called a reactor trip.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.22
single failure
failure which results in the loss of capability of a single system or component to perform its intended safety function(s), and any consequential failure(s) which result from it

Note 1 to entry: A single failure is generally caused by effects such as corrosion, thermal stressing and wear-out which applies to hardware components within a system.

Note 2 to entry: Single failure is also called: ”random failure”.

Note 3 to entry: Due to their random nature, statistical information can be produced from testing and historical data. Thus, the average probability, and hence the risk, associated with the occurrence of a random failure can be calculated.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.23
trip
rapid reduction in the power of a nuclear reactor

Note 1 to entry: A reactor trip is also called “scram”.

[SOURCE: IEC 60050-395:2014, 395-07-91]

4 Abbreviated terms and acronyms

CCF	Common Cause Failure
CPLD	Complex Programmable Logic Device
EMC	Electro Magnetic Compatibility
EMR	Electro Magnetic Relay
EMI/RFI	Electromagnetic Interference / Radiofrequency Interference
ESF	Engineered Safety Feature (and post-trip actions and sequences)
ESFAS	Engineered Safety Feature Actuating System
FMEA	Failure Mode and Effect Analysis
FPGA	Field Programmable Gate Array
HDL	Hardware Description Language
HPD	HDL-Programmed Device
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
MCR	Main Control Room
NPP	Nuclear Power Plant
PIE	Postulated Initiating Event
PLD	Programmable Logic Device

PWR	Pressurised Water Reactor
QA	Quality Assurance
SCP	Supplementary Control Points
SCR	Safety Control Room / Emergency Control Room
SLA	Safety Logic Assembly
SSR	Solid State Relay
V&V	Verification and Validation
2oo3	Voting logic: 2 out of 3
2oo4	Voting logic: 2 out of 4

5 Safety logic assembly – Principles and description

5.1 Safety logic assembly

The protection system is generally designed with software based technology to perform safety functions with digital means.

Usually, it has multiple redundant and sometimes diverse divisions to, among other things, meet the single failure criteria, achieve the target reliability and allow on line testing and maintenance.

The outputs from the multiple divisions are subject to some additional processing, made by a safety logic assembly, before sending the final command signal to an actuator. This is dependent on the design but usually includes some form of voting to deal with divisions that may have failed or may be in bypass for periodic testing.

Annex A gives more examples of possible functions performed by a safety logic assembly.

As the final processing is simple (sequential and / or combinatorial) and important to safety (direct command of safety actuators), the technology to design a safety logic assembly shall be highly dependable: reliable and safe. Annex C gives clarifications on concepts related to dependability.

Safety logic assemblies using a software based technology are not addressed in this document since computer based systems and software development are adequately covered in other standards.

Therefore, in this document a safety logic assembly performs Category A logic functions to send the direct command signal to safety actuators without using a software based technology.

The safety logic assembly, as part of the protection system, shall be designed in accordance with IEC 61513.

5.2 Technology for safety logic assembly

A safety logic assembly can be designed with any type of technology if the dependability performance complies with requirements. In this document, two types of technology are considered: hardwired technology and HPD technology.

a) Hardwired technology:

   the function is defined by the characteristics of the components and connections between them. Hardwired technology has been used on the first electronic systems to ensure safety functions.

Several types of technological components are considered, such as: relays, solid state components, dynamic logic. The term “hardwired technology” is sometimes replaced by “analogue technology” to underline the fact that signals are analogue (voltages, current, frequency, etc.). But signals are not necessarily analogue, as early digital components were non programmable. The hardwired technology is simple, robust and fast. The function is fixed and stable.

After validation and tests, the remaining risk of failure is only associated with random failures due to ageing, wearing-down, environment conditions which may induce drifts.

As the probability of failure is assessable, the behaviour of a system is more or less predictable.

With hardwired technology, safety is built by addressing random failures and this is achieved with a specific design using an adequate non-diverse redundancy.

b) HPD based technology:

The significant recent miniaturization of electronic components has created a new kind of technology based on high density logic gates, capable of complex functions that are implemented using hardware description language (HDL). This technology is referred to as "HDL programmed devices" (HPD) and includes FPGAs, PLDs, CPLDs or ASICs. Its design is based on principles of hardwired technology because the functions are “hardwired” by connections between logic gates. Nevertheless, the realization of applications has many similarities with software based technology, in particular, the design can be affected by errors. The risk of error due to the complexity shall be specifically addressed by following the recommendations of IEC 62566.

Due to the very demanding reliability and safety performances to design SLA, HPD components shall be specifically selected to meet the requirements.

Subclause B.4.3 gives recommendations and specifies restrictions related to HPD components.

5.3 Interfaces of a safety logic assembly

Figure 1 shows a typical arrangement of an I&C channel in a protection system using a safety logic assembly to control safety actuators.

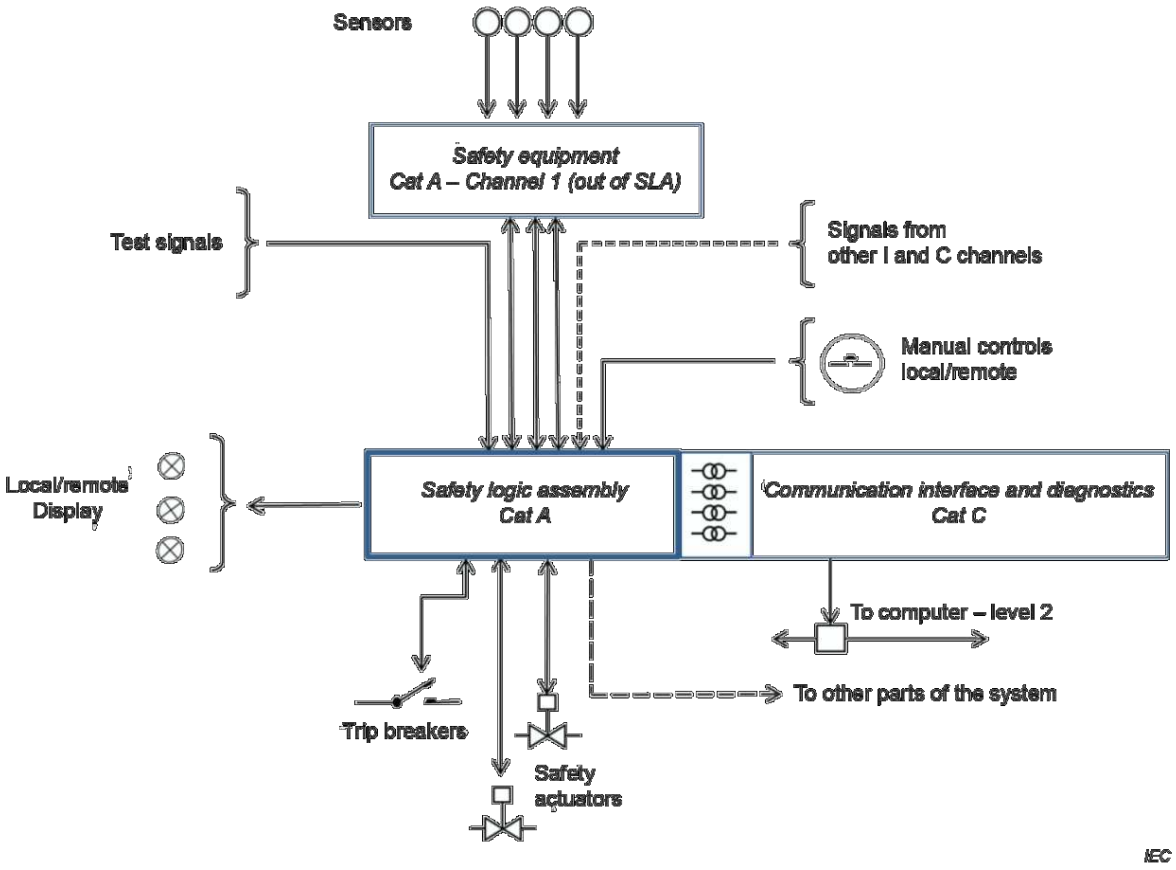

Figure 1 – Safety logic assembly:
typical interface arrangement in a protection system

A protection system using a safety logic assembly is typically divided in three main parts:

a) A safety equipment

For example a redundant I&C channel of the protection system. I&C channel 1 in Figure 1, performing Category A functions including analogue signals processing and setpoint comparisons with the signals from the sensors. This equipment generates binary signals which are input signals for the safety logic assembly.

b) The safety logic assembly (hardwired or HPD)

It performs category A functions using binary signals received from the digital safety equipment and other signals including manual controls, test signals and possibly signals from other I&C channels if a voting logic is required. In many projects, safety logic assemblies are used to send the final and direct controls to trip breakers or safety actuators.

Safety display indicators are available (remotely or locally). Some signals are connected to the interface, communication and diagnostic equipment (out of safety logic assembly) in order to improve the monitoring of the system with the support of the plant computer system.

Signals can also be connected to other parts of the safety system (e.g. to another safety logic assembly) depending on the functions and the architecture of the safety system.

The functions performed by a safety logic assembly depend on each specific project and may be very different. In some cases, the safety logic assembly can receive signals from the actuators like the status or the position.

c) The interface, communication and diagnostic equipment

It is associated with the safety logic assembly and performs category C functions with the signals received from the safety logic assembly. Signals and results of diagnostics can be

transferred to computers and control rooms, provided that this equipment is appropriately isolated from the safety logic assembly.

5.4 Dependability objectives

When considering the importance of a safety logic assembly as it sends the direct control signal to safety actuators, furthermore reliability, the behavior in case of failure shall be addressed. Then the probability of failure shall be divided into probability to fail in a safe state (spurious trip) or in an unsafe state (blocked actuation).

Dependability (refer to Annex C) is more pertinent to address both safety and availability objectives of the NPP. Dependability includes two main objectives related to the operation to the NPP: safety and availability of the plant.

The role of the safety logic assembly for the safety of the NPP is to guarantee the sending of a safety actuation command when a trip order is demanded.

A better safety and availability can be achieved by increasing reliability (probability to operate properly without failure).

But in case of failure of a SLA, two cases are considered:

- Failure with the output signal in an actuating state (spurious safety actuation). The plant will be shut-down and therefore less available but safe. To increase availability, it is needed to decrease the probability to fail in a safe state.
- Failure with the output signal blocked in an unsafe state. The plant is still operating but the safety is jeopardized. To increase safety it is needed to decrease the probability to fail in a non-actuating state.

Safety and availability are objectives which shall be expressed by two probabilities:

- Probability to fail to send an actuation command when required (probability to fail per demand)
- Probability to fail by sending a spurious actuation (probability to fail per year)

These probabilities shall be allocated to the safety logic assembly during the design of the protection system as prescribed by IEC 61513.

The effective probabilities are computed during the reliability analysis which shall be performed according to the procedure given in IEC 60812.

The probabilities can be adjusted by design: internal architecture, technology, failure detection.

5.5 Modes of operation

The following different modes of operation of a safety logic assembly shall be analysed to show the operation of the assembly is not compromised.

- Normal conditions:
  - No failure, normal environmental conditions
  - Failure mode
  - Test mode
  - Start-up mode for HDL technology
- Abnormal conditions:
  - Abnormal environment conditions as specified

- Human error: the risk of human error when implementing some preventive features is taken into account.

5.6 Principles to reach the safety objectives

5.6.1 Safe operation in normal operation mode

The proper operation of a safety logic assembly in normal conditions is addressed by the following recommendations:

a) Correctness of the functions implemented in the safety logic assembly. This is achieved from the quality of the specifications and their validation and the quality of the design.

b) Performing periodic tests to reveal any failure which cannot be detected by a permanent detection circuit. If the periodic test takes the tested part of the equipment out of operation, and operation of the equipment is required during the test, the design shall include adequate redundancy.

c) Reliability of the components in order to limit the failure rate when they are operated under the specified conditions. This is achieved by selecting the appropriate components in the design.

d) Forecasting the behavior in case of failure. Even if all the components have a low failure rate, the behavior in case of failure of a safety logic assembly shall be understood. Several features should be implemented to address this point:

   - A fail safe design: in case of failure, the control signals are automatically put in tripped state or safety state.
   - A design for limiting the time of operation with a failed component or a failed part of the equipment. This implies that the equipment is designed with a permanent failure detection circuitry, an alarm to inform the maintenance operators and a plan to quickly and easily repair the failed modules.
   - Internal redundancy of the safety logic assembly to address the risk of not tripping in case of failure.

5.6.2 Safe operation in abnormal operation mode

A safety logic assembly shall be able to operate in the specified environmental conditions. The design shall include all features to make the equipment robust by selecting appropriate components. The safe operation in abnormal conditions is achieved by a qualification process which is conducted as specified in 6.5.

5.6.3 Protection against human error

A safety logic assembly receives manual controls according to the functional specifications, for example to put the equipment in test mode or to start manually a safety actuation.

The design should address the risk of postulated non-appropriate control by the operator. For example, it is forbidden to put two redundant parts of the equipment in test mode at the same time. An interlock circuit should be implemented to change the logic depending on the number of units set in test mode. These features are important and should be carefully analyzed during the design of the equipment.

5.7 Principles to reach the availability objectives

5.7.1 NPP availability objectives

Availability objectives are understood for the NPP and are not limited to SLAs. As SLAs send commands directly to actuators, in case of failure, the consequences affect the plant operation and this aspect is fundamental.

5.7.2 NPP availability in normal operation conditions

The design should minimise the risk of a spurious actuation due to either a hardware failure, a design error or an inappropriate command of the operator. The principles are the same as those used to reach the safety objectives but some solutions (especially internal architecture with voting logic) shall be designed with care in order to not jeopardize the safety performance.

The probability that a single random failure induces an automatic actuation shall meet the allocated value for the safety logic assembly.

The voting logic after the redundant parts of the safety logic assembly shall be simple and highly reliable.

5.7.3 NPP availability in abnormal operation conditions

The principles to achieve the safety objectives in abnormal operation conditions apply also to achieve the availability of the NPP in abnormal operation mode.

5.7.4 Protection against human error

Solutions should be implemented to avoid spurious actuations due to operator error, for example:

- Display of the state of other redundant channels to clearly inform the operator about the risk of tripping in case of manual control, for example when a channel is already in test mode.
- Implementation of an interlock circuit to avoid a spurious actuation. If the designer decides to implement such a circuit, the design shall be carefully analyzed to not jeopardize the safety function.

6 Safety logic assembly – Design requirements

6.1 General

The design of a safety logic assembly shall be conducted to ensure that:

- it will operate properly in all the specified conditions,
- the dependability objectives are achieved,
- it complies with all requirements applicable to safety systems.

6.2 Functions

6.2.1 Specification of the functions

The safety functions of a safety logic assembly are specific to each project and shall be specified and validated as required in IEC 61513.

The functions with binary signals are mainly combinatory or sequential. The output signals are sent to actuators or to other units of the safety system.

As the functions of a safety logic assembly are category A according to IEC 61226, they shall be periodically tested according to the recommendations given by IEC 60671.

When possible, a permanent hardwired diagnostic circuit should be implemented in the safety logic assembly to detect a postulated failure or a wrong position for manual controls.

An alarm signal should be indicated and an automatic safety actuation control signal shall be generated if the position corresponds to an unsafe state (fail safe design).

When implemented, the principles of permanent hardwired diagnostic shall be carefully prepared during the design of a safety logic assembly. Reliability and safety analysis are conducted to help specifying permanent hardwired diagnostics functions. The coverage of the failures by this monitoring circuit shall be determined.

Permanent hardwired diagnostics shall not jeopardize the safety operation of the system.

Some examples of permanent hardwired diagnostic functions are a correct connection of a board, surveillance of power supplies or correct position of switches.

In case of failure detection, the result of a hardwired diagnostic function is transmitted:

- to the safety system if it is necessary to make invalid any safety signals transmitted by the faulty channel. This requirement shall be justified by analysis.
- to the operator, locally or remotely – direct connection for safety display or through the interface and communication equipment.

6.2.2 Manual controls

The manual controls are binary signals transmitted locally from the equipment itself or remotely from the control stations. For example, these controls are used:

- To start a manual actuation either for a given actuator or for a complete safety actuation with several actuators.
- To put a part of the equipment in test position.

IEC 60965 gives requirements for manual controls when the main control room is not available.

The operator's manual controls shall be designed according to IEC 61227.

6.2.3 Response time

The response time of a safety logic assembly shall be specified and so defined that it shall have an adequate value to comply with the requirements of the safety system.

The time behavior includes two aspects:

- the time sequence between each actuation (all the controls may be not activated at the same time);
- the response time between input and output signals of each module.

The time sequence and the response time of a safety logic assembly shall be validated and used to compute the response time of the safety system as a whole.

6.2.4 Display – Indicators-alarms

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

IEC 62241 gives recommendations and requirements related to alarm functions in main control room.

IEC 60964 gives requirements to implement signaling functions in control rooms.

Removal of a module for replacement shall be indicated.

A change in a voting logic function (e.g. voting change from 2oo4 to 2oo3) in the safety logic assembly shall be indicated (or warning means shall be provided), so that the time required to detect this situation and repair defective components is limited.

6.2.5 Interface

A safety logic assembly may be connected to an interface, diagnostic and communication equipment in order to provide the plant computer system and operators in control room with all important signals available from the safety logic assembly. These signals shall be isolated as specified in 6.7.

6.3 Architecture and redundancy

The architecture of a safety logic assembly dedicated to a set of actuators in a channel of the protection system shall be designed according to the dependability objectives as described in 5.4.

To reach the dependability and safety objectives, a safety logic assembly should have an internal redundant architecture and the redundant parts should be followed by a highly reliable voting logic.

The main requirements for the design of the architecture of a safety logic assembly are given by IEC 61513.

6.4 Technology

Various technological solutions are possible to design a safety logic assembly.

Annex B suggests several possible types of hardwired technology and the conditions for their use to design a safety logic assembly.

The main criteria for selection of technology include ability to perform the function, achieve the target reliability (see 5.4) and meet the qualification conditions (see 6.5).

6.5 Qualification

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

- temperature,
- pressure,
- humidity,
- mechanical vibration,
- earthquake,
- radiation,
- electromagnetic compatibility (EMC)
- electrical insulation.

The qualification tests and corresponding applicable standards are given in 7.2.4.

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

The qualified life that shall be adequate with respect to the required operating conditions and mission time of the safety system.

6.6 Maintenance

A safety logic assembly shall be easily and quickly repaired after failure detection and during preventive maintenance. This may include two features:

- detection of failures with a specific detection circuit to indicate to the operator which component or board is failed.
- fast replacement and limited needs for tuning or adjustment. The replacement of a failed component should be fast and easy. It is possible only after detection and signalling a failed component. This is brought for example by the use of printed circuit boards implemented in standard electronic racks.

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

A spare part (module, board) replacing a failed one, shall be verified and tested before installation on site. Subclause 7.3.3 gives requirements for the test of all fitted parts

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

As maintainability is specific to each kind of technological solution described in Annex B, it shall be carefully prepared during the design.

6.7 Separation

The design of a safety logic assembly shall be such that the independence criteria applicable to the safety system as a whole are met. Requirements for separation between redundant parts and other parts of the system shall comply with recommendations given in IEC 60709.

Safety logic assemblies in a redundant channel shall be designed with sufficient electrical independence and physical separation. This is a necessary but not a sufficient condition to reduce multiple failure probability to an acceptable degree consistent with the reliability requirements specified in the design basis of the protection system.

A safety logic assembly shall operate properly in the presence of a specified interference level. Similarly, protection should be provided to comply with EMC requirements between a safety logic assembly and another one. Principles of qualification are given in 6.5 and qualification tests in 7.2.4.

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

If means are required to suppress arcing, such means shall neither affect adversely the switching speed nor the reliability of the safety logic assembly beyond acceptable values.

The manual control signals received by a safety logic assembly (locally or from the MCR) shall be hardwired, protected against EMC interference and separated with an isolation module to avoid perturbations by unexpected voltage collected by cables.

A safety logic assembly may be connected to other assemblies belonging to other channels. All the signals shall be connected through isolation modules from the other channels.

The functional and communication separation requirements of the plant I&C architecture shall be fulfilled within the internal and external connections of the safety logic assemblies.

6.8 Power supply

Safety logic assemblies of a redundant channel shall be energized by the power supply of the redundant channel.

The power supply shall be provided with suitable independence and capacity when power is necessary to keep the required safety functions of the safety logic assembly.

The power supply shall be designed according to IEC 61225.

7 Tests of safety logic assemblies

7.1 General

Four kinds of tests are considered for a safety logic assembly:

- type tests to validate the design
- production tests to validate the manufacturing
- on site tests to validate the installation
- periodic test to detect failures when safety logic assemblies are operated

7.2 Type tests

7.2.1 General

Type tests shall be performed to validate the design of a safety logic assembly, and to demonstrate that the observed performance characteristics of the safety logic assembly meet or exceed its specified performance characteristics for the generic and/or specific design condition.

It is acceptable to replace some of the type tests by theoretical analysis. However, such analysis shall be justified and documented in the qualification programme.

7.2.2 Test sequences

Type tests shall be run on a safety logic assembly in a specified sequence which shall be part of the written test procedure.

It is recommended to perform two test sequences:

a) Functional and performance validation tests: To validate the functions and their performance in normal operating conditions
b) Qualification tests: To validate the operation of the equipment in abnormal and extreme environmental conditions.

7.2.3 Functional and performance validation tests

Safety logic assemblies are parts of a safety system and the functional validation tests should be included in the validation tests of this safety system.

The validation tests shall be performed by following a QA programme and documented.

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

- input signal range (tolerance for logic 0 and logic 1);
- output signal range (tolerance for logic 0 and logic 1);
- logic function;

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

7.2.4 Qualification tests

It shall be verified that the equipment performs its specified functions before, during and after a postulated initiating event. The type test shall consist of a predetermined sequence of test conditions:

- environmental conditions qualification tests according to IEC/IEEE 60780-323,
- seismic qualification tests according to IEC 60980,
- EMC qualification tests according to IEC 61000 series and IEC 62003, and
- Irradiation qualification, if applicable, according to IEC/IEEE 60780-323.

7.3 Production tests

7.3.1 General

To verify that the safety logic assemblies produced at the factory remain in full conformity with those used for type testing, the following tests may be carried out on a suitable number of samples.

Production tests conditions and procedures are defined in a quality assurance programme of the manufacturer.

7.3.2 Tests of spare parts

Spare parts are provided in the form of electronic modules or printed circuit boards. They may be manufactured at any time during the life of the equipment and they shall be tested according to the manufacturing procedures.

It is recommended to use a specific test bench representing all the interfaces in real conditions to check the function.

During the life time of the plant, obsolescence issues shall be considered and the new design of a spare part would be necessary. Therefore, the qualification of the new spare part shall be done according to the requirements given in 7.2.4.

The functional qualification and the qualification to environmental conditions shall be analysed to decide the sequence of the test to be performed in order to keep the qualification valid.

7.3.3 Production tests on manufactured safety logic assemblies

Such tests on safety logic assemblies shall include:

- visual inspection;
- check of welding, soldering, wire-wrapping or other methods of connection;
- check of mechanical tolerances;
- electrical tests (dielectric test, resistance insulation check);
- power supply tests;
- functional testing. A preliminary burn-in of the equipment may be specified.

The above-mentioned tests shall be carried out on the entire production of safety logic assemblies.

7.3.4 Tests on substitute components / modules

All purchased parts should be of the type used in the equipment that was qualified. However, when substitute components are required, they shall be adequately supported by qualification documentation. This shall consider manufacturing process, quality assurance procedures and difference in expected performance as related to equipment operation.

When the quality assurance programme includes tests by sampling, the number of parts or modules may be chosen according to the specified quality assurance level, sampling and inspection level.

7.3.5 Tests on assembled cabinets

The following tests shall be carried out on each assembled cabinet:

- functional tests possibly with automatic equipment, of at least all the input and output configurations necessary to identify fail-to-danger faults;
- check of correct operation of ventilation and other cooling means;
- checks on a statistical sample to verify the insulation between input and output terminals and between terminals and chassis. Number may be chosen in compliance with specification.

7.4 Tests on site

7.4.1 Equipment health checks before installation

Before installation on site, a safety logic assembly shall be checked to prove that it has not been damaged during transport.

The check shall be performed according to a written procedure and a report shall be issued to certify that all parts of the safety logic assembly are in correct conditions before installation.

7.4.2 Installation validation tests

After installation, tests shall be performed to prove that the safety logic assembly is properly installed and in correct operation.

Tests are performed according to a written procedure which specifically takes into account all possible influence of site conditions on the performance of the safety logic assembly, for example:

- cable addressing and connection
- cabinet anchoring
- earthing connection

After installation tests, commissioning tests are performed within the commissioning tests of the protection system.

Dielectric tests or EMI/RFI tests on site shall be considered with particular care and restrictions in order to avoid disturbance on other systems.

7.4.3 Periodic tests

Periodic tests shall be performed during normal operation in order to detect any failure which cannot be detected by permanent diagnostic circuits.

Safety logic assemblies perform Category A functions according to IEC 61226, they are part of the protection system and are operated for many years. They shall be tested and shall comply with the single failure criterion during the test.

The time intervals between periodic tests are defined during the dependability analysis to comply with the probabilistic safety requirements.

The use of an automatic tester with a report is recommended.

Methods and procedures for surveillance testing shall comply with IEC 60671 requirements.

8 Quality assurance

For the safety logic assembly, a quality assurance plan specific to the nuclear industry shall exist and shall comply with requirements of IAEA-GSR Part 2.

IEC 61513 gives a large set of recommendations regarding the design and implementation of systems including quality assurance.

Annex A
(informative)

Examples of safety logic assembly applications

Possible applications of safety logic assemblies are varied and may cover more or less important parts of the safety systems. Whenever the requirements of safety and availability are important, the choice of the hardwired technology is essential to reach the required safety and availability performance.

The following list provides examples of applications achievable with safety logic assemblies:

a) a specific parameter reactor trip in a channel;

b) logic within a channel, such as the logical operations of the many trip parameters normally present; Subgroup logic processing the inputs to a channel to ensure that a parameter is within a correct range. Examples include operational bypasses for flux and core outlet temperature. On some reactors, bypass logic is needed to ensure the main coolant pumps are operating within their envelope and not in a stalled or cavitation mode;

c) priority logic: The logic interface between the channel output and the trip switchgear or contactors, and between the channel output and the ESF actuators. This needs to include prioritization between controls of systems of different safety categories;

d) the logic for post-trip sequences and ESF operation;

e) the manual trip and the interconnections between that control and the switchgear, actuators or contactors;

f) the manual controls of the safety system for post-trip sequences and ESF operation;

g) the manual trip actuation from the SCP, and the methods of interconnection with other actuations;

h) where permitted or required, the interconnections between two diverse safety systems to ensure both trip if either does so;

i) the output actions for energize to actuate or de-energize to actuate for initiating a reactor trip or for actuating an engineered safety feature or post-trip sequence;

j) the facilities for the application and removal of operational bypasses, permissive and vetoes;

k) the use of a maintenance bypass;

l) the use of a trip bypass for sensors or for trip parameters;

m) the indications and alarms needed for a safety system;

n) the voting logic between redundant channels.

Annex B
(normative)

Safety logic assembly – Hardwired technological solutions

B.1 Overview

B.1.1 General

No electronic technology is 100 % reliable. Any solution has a failure rate. To achieve the very demanding safety objectives of a protection system, the choice of the technology and the final logic applied to the redundant control signals shall be made with a particular care.

Safety logic assemblies may be implemented with various technological solutions to achieve the specified level of safety. The choice of logic systems (static or dynamic) shall be consistent with the reliability requirements for the protection system as a whole.

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

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

Tests of the static logic systems enhance reliability by reducing mean time to failures and hence the time for which an unrevealed unsafe failure remains in the system. Recommendations are given in IEC 60671.

The electronic technology is limited to low power components to perform I&C functions.

A safety logic assembly may be designed with components of various technologies. The next paragraphs present possible hardwired technological solutions with their main features and requirements to design the safety logic assembly.

B.1.2 Relays

A safety logic assembly generating the final trip or ESF actuation may be implemented by means of relays.

Relays are simple and robust components which are used to perform logic functions by arranging adequately the connections between contacts and coils. Two main technologies exist for relays:

- electromechanical relays (EMR)
- solid state relays (SSR)

For safety logic assembly applications, we consider only relays operated with low voltages and low currents are considered.

B.1.3 Electromechanical relays

An electromechanical relay (EMR) is an electrically operated switch with contacts moved by a magnetic force controlled by a current.

Relays for use in the safety system shall be rated for continuous duty according to IEC 60255 series. The following shall apply:

- the insulation test voltage of the relay coils shall be specified,
- the contact rated insulation voltage shall be specified,
- the relay contacts shall be sized with a margin.

Specific features of EMRs in the safety logic assembly design are of particular interest:

- Isolation between the control signal and the controlled circuits, and isolation between contacts. It is important to keep the electrical isolation between signals coming from several redundant channels, even in case of failure. For that reason, electromechanical relays are preferably used to perform simple logic functions with isolated binary signals.
- The impedance of the coil permits continuity monitoring to be implemented in the design. Low current less than the operating current or pulse currents of duration less than the operation time may be appropriate for this. In those exceptional cases where energization causes a trip, the test current should be of the order of one-tenth of the minimum current which can energize the relay. This last recommendation does not necessarily apply to pulse continuity testing or monitoring.
- The switching time of EMRs may be significant and shall be specified and shall take into account the response time of the safety logic assembly.
- Due to the mechanical structure of EMRs, their design shall be robust to withstand shocks and accelerations during a seismic event.
- EMRs with multiple poles and isolated contacts are suitable to design logic functions between several signals.

Over a long period of time the moving parts wear out and may fail. Due to arcing, the resistance is changed and the contacts are eroded making the relay unusable with a shortened life time. The reliability of EMRs depends on several parameters including the number of manoeuvres, the voltage and the current at the contacts.

Relays shall be qualified for their response time and operation in the specified conditions of the safety system. Though the requirement of relay response time may vary depending on the type and/or mechanism, it shall be justified to show that relay response is appropriate for reactor trip and ESF system operation. The justification shall cover environmental suitability based on the IEC 60255 series.

B.1.4 Solid state relays

A solid state relay (SSR) is an electronic component that provides a similar function to an electromechanical relay but does not have any moving components, increasing long-term reliability.

A solid-state relay uses a thyristor or other solid-state switching device, activated by the control signal, to switch the controlled load, instead of a solenoid.

An opto-isolator (a light-emitting diode (LED) coupled with a photo transistor) can be used to isolate control and controlled circuits. But this feature implies implementation of a separate power supply.

The switching time of a SSR is very short and the self-inductance is negligible making more difficult the implementation of continuity monitoring circuit.

B.2 Magnetic amplifiers

Magnetic amplifier is an electromagnetic device based on few very simple components like coils, ferromagnetic core and diodes. It has no moving parts and no wear-out mechanism and

it has a good tolerance to mechanical shocks and vibrations. Multiple isolated signals may be summed by additional control windings on the magnetic cores. The windings of a magnetic amplifier have a higher tolerance to momentary overloads than comparable solid-state devices. The cores of magnetic amplifiers withstand radiation. For this reason, they have been used in nuclear power applications.

With its simple structure, a magnetic amplifier has a very low failure rate and can be used for a very long time without failure.

The use of magnetic amplifiers is limited to simple functions, compatible with the size and the mass of such components. The seismic qualification shall be considered at the very beginning of the design in order to make robust the fixing of heavy components.

B.3 Fail-safe – dynamic logic

Dynamic logic is an electronic technology based on discrete components and transformers using an alternating clock signal with several cells to perform a logic function. As long as the clock signal exists, the output signal is correct. In case of any failure, the clock signal stops and the output signal is zero. This feature is an interesting fail-safe characteristic because the output signal is predictable, and appropriate to improve the safety performance of a safety logic assembly.

Formal analysis of the design shall be undertaken and documented to confirm that the design meets the functional dependability requirements and does not have unknown failure modes.

B.4 Solid state circuits

B.4.1 General

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

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

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

B.4.2 Discrete components

Solid state circuits use discrete electronic components like transistors, capacitors, diodes, etc., to generate electric output signals from electric input signals and perform required functions.

The most important point is that, in case of failure, the output signal of a solid state circuit is not predictable. It may be energized or not.

Moreover, in some particular cases, a failure may lead to unstable control signals.

The design of a safety logic assembly with solid state circuits shall include redundant concepts to limit the consequences of failures. The redundant output control signals shall be combined with a very simple and reliable logic function.

B.4.3 Integrated components – HPD

Electronic components naturally evolve toward greater miniaturisation and make available components with a high level of integration: HDL-Programmed Device (HPD) such as Field-Programmable Gate Array (FPGA), PLD, CPLD.

They are basically wired components (assembly of a large number of logic gates), but their complexity is such that they require computing means for their design, for example the FPGA configuration is generally specified with a software program based on a hardware description language (HDL). In addition, they can reproduce the behavior of some microprocessors.

The recent and fast miniaturization of submicronic CMOS technology for HPD components shows three fundamental issues, related to the use of these components for safety functions, and these issues increase with the degree of miniaturization:

- They are susceptible to Single Event Upset (SEU) due to particle interference.
- They may be affected by electro-migration which may reduce life time.
- The complexity of highly integrated components is not favorable to safety justification.

Therefore, the use of HPD integrated components to design SLA shall be limited to simple logic functions, and they shall be selected among those having a proven performance for a long-term operation compatible with the life time target, and the need for safety justification. For that reason, highly-miniaturized HPD components are not recommended.

High density HPD components are designed to perform complex functions and that is not the case of functions performed by SLAs. HPD components shall be selected with low complexity.

The reliability and safety performance of SLAs shall be carefully evaluated and consistent with the reliability and safety objectives of the protection system in which they are implemented. These components can be used to achieve Category A functions, by complying with IEC 62566 requirements.

Annex C
(informative)

Dependability and its attributes

C.1 General

The main characteristic of a safety logic assembly is to operate properly when required by sending a command to actuators. Dependability includes methods and features to minimize the risk to fail when a command is required. The concept of dependability is not limited to reliability. Two main objectives are associated to the consequences of failures:

- Non-actuation per demand (non-safe failure): the consequence is that the safety of the NPP is compromised.
- Spurious actuation (safe failure): the consequence is that the NPP is stopped, safe, but not available.

Each of these events have their own probability.

C.2 Qualitative and quantitative attributes associated with dependability

Based on IAEA and IEC definitions, the following diagram shows the relationship between the different quantitative and qualitative attributes of dependability regarding the final risks related to actuators: to not operate when demanded (safety) or to operate when not demanded (availability), see Figure C.1.

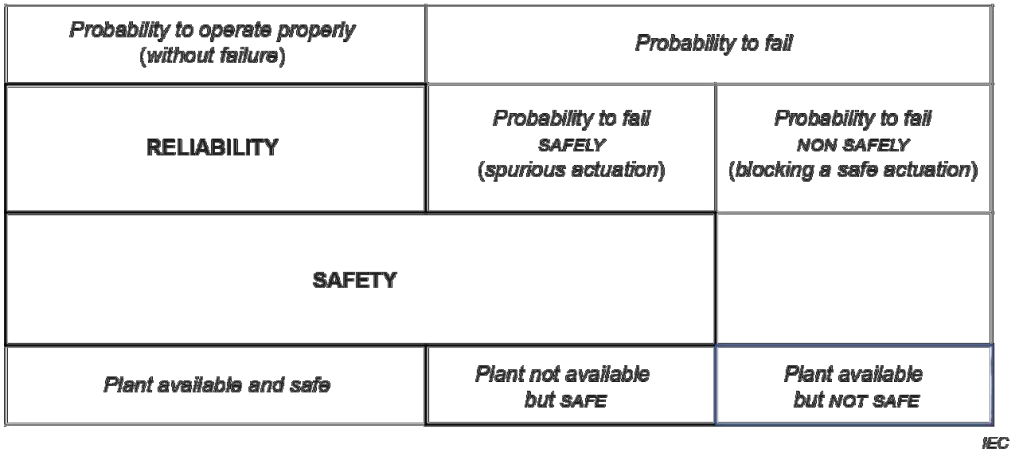

**Figure C.1 – Attributes of dependability –
Relationship between reliability and the final risk regarding safety**

The main and fundamental attribute is reliability. The safety logic assembly is reliable when the probability of failure is small (reliability). Without failure, the safety logic assembly is available (availability).

The probability of random failure is a quantitative attribute which can be computed from various data bases taking into account a description of the components and their environment conditions (temperature, vibrations, etc.). From this probability, it is simple to obtain the probability of non-failure which is directly associated to reliability.

Reliability is improved with methods to detect failures and to easily and quickly repair in order to minimize the time of operation with a failure. The corresponding attributes are testability and maintainability. These attributes are essentially qualitative.

In case of failure of a safety logic assembly, the output signal does not correspond to a real command. The signal is:

- Either in an actuating state (spurious actuation), in this case the NPP is tripped (trip breakers) or will be stopped, automatically or by manual control of operators. The NPP is safe, but is no more available.
- Or in a blocking state (blocked actuation), in this case the NPP is not safe, but is still available. Generally, it corresponds to a non-detected failure.

As safety logic assemblies are used to ensure safety, the design is generally fail-safe oriented.

Thus, both risks (spurious actuation and blocked safety actuation) can be mitigated by specific design features such as redundancy with adequate voting logic.

Bibliography

IEC 60050-395, *International Electrotechnical Vocabulary – Part 395: Nuclear instrumentation: Physical phenomena, basic concepts, instruments, systems, equipment and detectors*

IEC 60300 (all parts), *Dependability management*

IEC 60706 (all parts), *Maintainability of equipment*

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

IEC 62340, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

IAEA Safety fundamentals – SF-1, *Fundamental safety principles*

IAEA Safety Glossary – edition 2016

IAEA Specific Safety Guide – SSG-30, *Safety classification of structures, systems and components in nuclear power plants*

IAEA – SSG-39, *Design of Instrumentation and Control Systems for NPP (Specific Safety Guide)*

IAEA – SSR-2/1 Rev1, *Safety of Nuclear Power Plants Design (Specific Safety requirements)*

———————

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ENSEMBLES LOGIQUES DE SÛRETÉ UTILISÉS DANS LES SYSTÈMES RÉALISANT DES FONCTIONS DE CATÉGORIE A: CARACTÉRISTIQUES ET MÉTHODES D'ESSAI

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 60744 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Cette deuxième édition annule et remplace la première édition parue en 1983. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) actualisation des références aux normes publiées ou révisées depuis la publication de la première édition de la norme actuelle, y compris l'IEC 61513 et l'IEC 61226;

b) exigences supplémentaires concernant l'utilisation du bipasse de fonctionnement et du bipasse de maintenance; exigences concernant la logique de vote et exigences concernant l'interface avec les MCR et SCR.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
45A/1188/FDIS	45A/1200/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.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

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

L'IEC 60744 traite spécifiquement des ensembles logiques de sûreté utilisés dans les centrales nucléaires de puissance (CNP). Les ensembles logiques de sûreté étaient à l'origine des éléments câblés des systèmes de protection utilisés principalement pour commander les actionneurs. L'IEC 60744 traite spécifiquement de la conception, y compris la technologie, les interfaces avec les MCR et SCR, les essais et la qualification. Elle spécifie des exigences concernant l'affichage des entrées et de l'état des systèmes de sûreté.

L'IEC 60744 est le document qui traite des fonctions et des performances des ensembles logiques de sûreté.

L'utilisation des matériels informatiques ou de logiciel est couverte de façon exhaustive par d'autres normes. La technologie utilisée pour la conception des SLA intègre principalement des technologies câblée et des composants à haute intégration submicronique (HPD), dont la mise en œuvre est contrainte par le très haut niveau d'exigence de sûreté.

Le document traite des caractéristiques de conception et d'essai des ensembles logiques de sûreté, notamment en ce qui concerne les exigences fonctionnelles, les questions de fiabilité et les moyens de contrôle-commande associés, y compris l'alarme, l'indication et le contrôle-commande. Le document propose également les exigences concernant les performances, les essais et la qualification relatifs aux ensembles logiques de sûreté et les exigences d'interface concernant la communication entre les ensembles.

L'objectif du document est d'être utilisé par les exploitants de centrales nucléaires de puissance (réseaux), les évaluateurs de systèmes et les régulateurs.

b) Position de la présente norme dans la structure de la série de normes du SC 45A de l'IEC

L'IEC 60744 est le document du SC 45A de l'IEC de troisième niveau qui traite de la question spécifique des caractéristiques d'essai et de conception des ensembles logiques de sûreté.

L'IEC 60744 doit être utilisée en association avec l'IEC 61513 qui constitue le document approprié du SC 45A de l'IEC fournissant un guide sur le système de sûreté I&C et l'IEC 60964 qui constitue le document approprié servant de guide sur les salles de commande, étant donné que le système de sûreté comprend des interfaces extensives avec les MCR et SCR.

Voir le point d) de la présente introduction pour de plus amples informations détaillées sur la structure de la série de normes du SC 45A de l'IEC.

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

Il est important de noter que le présent document n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté.

Le présent document spécifie des recommandations particulières pour les aspects suivants:

- Le vote sur les déclenchements partiels afin d'identifier chaque actionnement de sûreté
- Les ensembles de sortie qui assurent les arrêts rapides et les actionnements
- Les caractéristiques de conception et d'essai des exigences fonctionnelles
- La question de fiabilité des ensembles logiques de sûreté
- Les caractéristiques de performances des ensembles logiques

- Les exigences d'essai, de qualification et d'interface des ensembles logiques de sûreté

Afin d'assurer la pertinence du présent document pour les années à venir, l'accent est mis sur les questions de principe plutôt que sur les technologies particulières.

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

Les documents de niveau supérieur de la collection de normes produites par le SC 45A de l'IEC sont les normes IEC 61513 et IEC 63046. La norme IEC 61513 traite des exigences générales 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. La norme IEC 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique; elle couvre les systèmes d'alimentation électrique jusqu'à et y compris les alimentations des systèmes d'I&C. Les normes IEC 61513 et IEC 63046 doivent être considérées ensemble et au même niveau. Les normes IEC 61513 et IEC 63046 structurent la collection de normes du SC 45A de l'IEC et forment un cadre complet, cohérent et consistant établissant les exigences générales relatives aux systèmes d'I&C et électriques des centrales nucléaires de puissance.

Les normes IEC 61513 et IEC 63046 font directement référence aux autres normes du SC 45A de l'IEC traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, la défense contre les défaillances de cause commune, la conception des salles de commande, compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes programmés numériques, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes, de second niveau, forment, avec les normes IEC 61513 et IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont généralement pas référencées directement par les normes IEC 61513 ou IEC 63046, 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 l'IEC correspond aux rapports techniques qui ne sont pas des documents normatifs.

Les normes de la collection produite par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté et de sécurité de haut niveau établis par les normes de sûreté de l'AIEA pertinentes pour les centrales nucléaires, ainsi qu'avec les documents pertinents de la collection de l'AIEA pour la sécurité nucléaire (NSS), en particulier avec le document d'exigences SSR-2/1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires, avec le guide de sûreté SSG-39 qui traite de la conception de l'instrumentation et du contrôle commande des centrales nucléaires, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires, et avec le guide de mise en œuvre NSS17 traitant de la sécurité informatique pour les installations nucléaires. La terminologie et les définitions utilisées pour la sûreté et la sécurité dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

Les normes IEC 61513 et IEC 63046 ont adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau sûreté nucléaire, les normes IEC 61513 et IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, de l'IEC 61508-2 et de l'IEC 61508-4 pour le secteur nucléaire. Dans ce domaine, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à l'IEC 61508-3 pour le secteur nucléaire. Les normes IEC 61513 et IEC 63046 font référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au second niveau, la norme IEC 62645 est le document

chapeau des normes du SC 45A de l'IEC portant sur la sécurité nucléaire. Elle est élaborée sur les principes pertinents de haut niveau des normes ISO/IEC 27001 et ISO/IEC 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le secteur nucléaire; elle est coordonnée étroitement avec la norme IEC 62443. Au second niveau, la norme IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et la norme IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

NOTE 1 Il est fait l'hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales.

NOTE 2 Le domaine de l'IEC SC 45A a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015 des discussions ont eu lieu au sein de l'IEC SC 45A pour décider des modalités et du cadre d'établissement des exigences générales portant sur la conception des systèmes électriques. Les experts de l'IEC SC 45A ont recommandé que pour établir des exigences générales pour les systèmes électriques une norme indépendante soit développée au même niveau que l'IEC 61513. Le projet IEC 63046 est lancé pour atteindre cet objectif. Lorsque la norme IEC 63046 sera publiée la présente NOTE 2 de l'introduction sera supprimée.

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ENSEMBLES LOGIQUES DE SÛRETÉ UTILISÉS DANS LES SYSTÈMES RÉALISANT DES FONCTIONS DE CATÉGORIE A: CARACTÉRISTIQUES ET MÉTHODES D'ESSAI

1 Domaine d'application

Le présent document spécifie les exigences et les recommandations pour la conception, la fabrication et les essais des ensembles logiques de sûreté utilisés dans les systèmes de sûreté pour réaliser des fonctions de sûreté de catégorie A (conformément à l'IEC 61226). Les ensembles logiques de sûreté réalisent des fonctions logiques comme, par exemple, la logique câblée faisant l'interface entre la partie programmée et les interrupteurs d'arrêt du réacteur, les actionneurs ou les contacteurs pour déclencher l'arrêt du réacteur ou les actions de sauvegarde. Les ensembles logiques de sûreté sont des éléments importants d'un système de sûreté et peuvent comporter une logique de vote entre des voies redondantes.

Le présent document décrit de manière générale les ensembles logiques de sûreté pour la commande des actionneurs de sûreté. Il donne les principes permettant d'atteindre les objectifs de sûreté de fonctionnement. Il décrit et explicite également les principales caractéristiques relatives aux exigences de conception.

Divers essais sont spécifiés, ainsi que leurs exigences, pour valider la conception (y compris les essais de qualification), la fabrication et l'installation correcte sur site.

L'Annexe A (informative) donne une liste des applications possibles des ensembles logiques de sûreté.

L'Annexe B (normative) propose une liste des technologies câblées possibles avec leurs exigences respectives portant sur la conception des ensembles logiques de sûreté.

L'Annexe C (informative) explicite la sûreté de fonctionnement et ses attributs afin d'améliorer la fiabilité et de réduire le risque final qui compromet la sûreté et la disponibilité des centrales nucléaires de puissance.

Le domaine d'application du présent document ne traite pas de la conception d'un système de protection, mais couvre uniquement les solutions technologiques et architecturales que nécessite la conception d'un ensemble logique de sûreté. L'IEC 61513 traite de la conception des systèmes de sûreté qui utilisent des ensembles logiques de sûreté.

Les fonctions spécifiques détaillées mises en œuvre dans un ensemble logique de sûreté dépendent dans une large mesure de la conception de chaque réacteur et ne sont pas traitées dans le présent document.

L'objectif principal de ce document étant la partie instrumentation et contrôle-commande du système, la logique de vote finale réalisée à partir de disjoncteurs de puissance est exclue du domaine de ce document.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences 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).

IEC 60255 (toutes les parties), *Relais de mesure et dispositifs de protection*

IEC 60671, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

IEC 60709, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Séparation*

IEC/IEEE 60780-323, *Installations nucléaires – Équipements électriques importants pour la sûreté – Qualification*

IEC 60812, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

IEC 60964, *Centrales nucléaires de puissance – Salles de commande – Conception*

IEC 60965, *Centrales nucléaires de puissance – Salles de commande – Salle de commande supplémentaire pour l'arrêt des réacteurs sans accès à la salle de commande principale*

IEC 60980, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

IEC 61000 (toutes les parties), *Compatibilité électromagnétique (CEM)*

IEC 61225, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences pour les alimentations électriques*

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

IEC 61227*, Centrales nucléaires de puissance – Salles de commande – Commandes opérateurs*

IEC 61513, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

IEC 62003, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences relatives aux essais de compatibilité électromagnétique*

IEC 62241, *Centrales nucléaires de puissance – Salle de commande principale – Fonctions et présentation des alarmes*

IEC 62566:2012*, Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie A*

IAEA-GSR Part 2, *Leadership and Management for Safety*

3 Termes et définitions

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

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
disponibilité
aptitude d'un élément ou d'un système à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou au cours d'un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires soit assurée

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.2
voie
ensemble de composants interconnectés dans un système qui produit un signal de sortie unique. Une voie perd ses propriétés lorsque les signaux de sortie uniques sont combinés avec ceux d'autres voies (par exemple une voie de surveillance ou une voie d'actionnement de sûreté)

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.3
sûreté de fonctionnement
terme général décrivant la fiabilité globale d'un système, c'est-à-dire le degré de confiance que l'on peut raisonnablement accorder à ce système. La fiabilité, la disponibilité et la sûreté sont des attributs de la sûreté de fonctionnement

Note 1 à l'article: L'Annexe C donne des explications qui concernent cette définition.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.4
équipement logique dynamique
ensemble de systèmes ou de sous-systèmes utilisant des signaux logiques dynamiques

3.5
signal logique dynamique
courant ou tension changeant périodiquement suivant une fréquence cohérente avec le temps de réponse. Les différents états logiques sont associés à différentes valeurs d'un ou de plusieurs paramètres de la variation périodique, par exemple l'amplitude, la pente, le taux de répétition des impulsions ou des alternances, ou des impulsions codées

Note 1 à l'article: Un état logique peut être associé à l'absence de variation périodique d'un tel signal.

3.6
dispositif motorisé de sauvegarde
partie active d'un système actionneur de sûreté (actionneur couplé à son alimentation électrique et son moteur d'entraînement)

Note 1 à l'article: Les dispositifs motorisés de sauvegarde ont besoin d'énergie pour fonctionner (vannes, moteurs, etc.). Généralement, ils sont comparés aux interrupteurs d'arrêt rapide qui n'ont pas besoin d'énergie pour fonctionner.

3.7
défaillance
perte de la capacité d'une structure, d'un système ou d'un composant de fonctionner conformément aux critères d'acceptation

Note 1 à l'article: La structure, le système ou le composant sont considérés comme défaillants lorsqu'ils ne fonctionnent plus, que l'on en ait besoin ou non à ce moment-là. Par exemple, la défaillance d'un système de secours peut ne pas se manifester jusqu'à ce que l'on ait recours à ce système, soit dans le cadre d'essais, soit lorsque le système principal est en panne.

Note 2 à l'article: Une défaillance est le résultat d'un défaut dans cette structure, ce système ou ce composant.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.8
réseau de portes programmable sur site
FPGA
circuit intégré qui peut être programmé sur site par le fabricant d'I&C. Il comprend des blocs logiques programmables (combinatoires et séquentiels), des interconnexions programmables entre ceux-ci, et des blocs programmables pour les entrées et/ou les sorties. La fonction est ensuite définie par le concepteur du contrôle-commande, et non par le fabricant du circuit intégré

Note 1 à l'article: Bien que les FPGA soient essentiellement des dispositifs numériques, certains peuvent inclure des entrées et sorties analogiques ainsi que des convertisseurs de signaux analogiques en numérique. Les FPGA peuvent inclure des fonctions numériques avancées telles que des multiplieurs, des mémoires dédiées et des cœurs de microprocesseurs.

Note 2 à l'article: L'abréviation «FPGA» est dérivée du terme anglais développé correspondant «Field Programmable Gate Array».

[SOURCE: IEC 62566:2012, 3.5]

3.9
langage de description de matériel
HDL
langage permettant de décrire formellement les fonctions et/ou la structure d'un composant électronique, à des fins documentaires, de simulation ou de synthèse

Note 1 à l'article: L'abréviation «HDL» est dérivée du terme anglais développé correspondant «hardware description language».

[SOURCE: IEC 62566:2012, 3.6]

3.10
circuit intégré programmé en HDL
HPD
circuit intégré configuré (pour des systèmes d'I&C de centrales nucléaires de puissance) avec des HDL et outils associés

Note 1 à l'article: L'abréviation «HPD» est dérivée du terme anglais développé correspondant «HDL-Programmed Device».

[SOURCE: IEC 62566:2012, 3.7]

3.11
conditions de fonctionnement
conditions correspondant au fonctionnement normal et aux incidents de fonctionnement prévus

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.12
signal de déclenchement partiel
signal logique produit par une voie du système de sûreté après traitement des signaux reçus des capteurs de cette voie, avant d'être filtré par la logique du vote final déclenchant l'arrêt d'urgence du réacteur ou les dispositifs motorisés de sauvegarde

3.13
réseau logique programmable
PLD
circuit intégré composé d'éléments logiques avec un motif d'interconnexions, dont des parties sont programmables par l'utilisateur

Note 1 à l'article: Différents types de PLD existent, par exemple les EPLD (PLD effaçables), et les CPLD (PLD complexes).

Note 2 à l'article: Les différences entre FPGA et PLD ne sont pas strictement définies, mais PLD désigne habituellement un dispositif plus simple que FPGA.

Note 3 à l'article: L'abréviation «PLD» est dérivée du terme anglais développé correspondant «programmable logic device».

[SOURCE: IEC 62566:2012, 3.13]

3.14
durée de vie qualifiée
période pour laquelle il a été démontré, par des essais, l'analyse ou l'expérience qu'une structure, un système ou un composant est capable de fonctionner dans les limites des critères d'acceptation, dans des conditions de fonctionnement spécifiques, tout en restant à même de remplir ses fonctions de sûreté en cas d'accident de dimensionnement ou de séisme de dimensionnement

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.15
redondance
mise en place de structures, systèmes ou composants (identiques ou différents) supplémentaires, afin qu'une structure, qu'un système ou qu'un composant quelconque puisse remplir la fonction requise indépendamment de l'état de fonctionnement ou de défaillance d'un autre élément

Note 1 à l'article: Cette définition doit être clarifiée pour les besoins du présent document:

- Redondance non diversifiée – pour répondre au risque de défaillance unique (aléatoire).
- Redondance diversifiée – pour répondre au risque de défaillance aléatoire ou de mode commun.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.16
fiabilité
probabilité qu'un dispositif, un système, un composant ou une installation satisfasse aux exigences minimales de performance lorsqu'il ou elle est sollicité(e)

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.17
sûreté (nucléaire)
protection des personnes et de l'environnement contre les risques associés aux rayonnements, et sûreté des installations et des activités donnant lieu à des risques associés aux rayonnements

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.18
fonction de sûreté
but particulier qui doit être atteint aux fins de la sûreté pour une installation ou dans le cadre d'une activité pour empêcher ou limiter les conséquences radiologiques d'un fonctionnement normal, des incidents de fonctionnement prévus ou des conditions accidentelles

Note 1 à l'article: Le document SSR2/1 de l'AIEA établit des exigences pour les fonctions de sûreté à accomplir au niveau de la conception d'une centrale nucléaire de puissance de façon à satisfaire aux trois exigences de sûreté générales:

a) la capacité à arrêter de façon sûre le réacteur et à le maintenir en condition d'arrêt sûr, durant et après des conditions de fonctionnement appropriées et dans des conditions accidentelles;

b) la capacité à évacuer la chaleur résiduelle du cœur du réacteur, du réacteur et du combustible nucléaire stocké, à l'arrêt et durant et après des conditions de fonctionnement appropriées et dans des conditions accidentelles;

c) la capacité à réduire la probabilité de rejet de matière radioactive et à assurer que tous les rejets se situent dans les limites prescrites durant et après les conditions de fonctionnement et dans des limites acceptables durant et après des accidents de dimensionnement.

Note 2 à l'article: L'IEC 61226 spécifie des recommandations relatives aux catégories des fonctions de sûreté.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.19
ensemble logique de sûreté
équipement faisant partie d'un système de protection réalisant une fonction logique de catégorie A simple, avec un très haut niveau de sûreté de fonctionnement et utilisé généralement pour transmettre des commandes aux actionneurs de sûreté ou des signaux à un autre ensemble logique de sûreté

Note 1 à l'article: Une fonction logique simple est combinatoire et/ou séquentielle. En conséquence une telle fonction est complètement testable.

3.20
système de sûreté
système important pour la sûreté destiné à garantir la mise à l'arrêt sûre du réacteur ou l'évacuation de la chaleur résiduelle du cœur du réacteur, ou à limiter les conséquences des incidents de fonctionnement prévus et des accidents de dimensionnement

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.21
arrêt d'urgence
mise à l'arrêt rapide d'un réacteur nucléaire en situation d'urgence

Note 1 à l'article: Le terme "arrêt d'urgence" est associé à l'unité d'arrêt rapide du réacteur qui commande l'interrupteur qui ouvre le circuit de maintien des absorbants. Un arrêt d'urgence est alors souvent appelé "arrêt rapide du réacteur".

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.22
défaillance unique
défaillance qui rend un système unique ou un composant impropre à remplir sa (ses) fonction(s) de sûreté prévue(s) et une ou d'autres défaillance(s) qui en résulte(nt)

Note 1 à l'article: Une défaillance unique est généralement causée par des effets tels que la corrosion, les contraintes thermiques et l'usure que subissent les composants matériels dans un système.

Note 2 à l'article: La défaillance unique est aussi appelée: «défaillance aléatoire».

Note 3 à l'article: Du fait de leur nature aléatoire, les informations statistiques peuvent être produites à partir d'essais et de données historiques. Ainsi, la probabilité moyenne, et donc le risque, associés à l'apparition d'une défaillance aléatoire peuvent être calculés.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.23
arrêt rapide
réduction rapide de la puissance d'un réacteur nucléaire

Note 1 à l'article: L'arrêt rapide d'un réacteur est également appelé "arrêt d'urgence".

[SOURCE: IEC 60050-395:2014, 395-07-91]

4 Termes abrégés et acronymes

DCC	Défaillance de cause commune
CPLD	Complex Programmable Logic Device (Réseau logique programmable complexe)
CEM	Compatibilité électromagnétique
REM	Relais Electromagnétique
EMI/RFI	Electromagnetic Interference / Radiofrequency Interference (brouillage électromagnétique / brouillage radioélectrique)
ESF	Engineered Safety Feature (and post-trip actions and sequences) (Dispositif motorisé de sauvegarde (et séquences et actions après le déclenchement de l'arrêt rapide du réacteur))
ESFAS	Engineered Safety Feature Actuating System (Système d'actionnement du dispositif motorisé de sauvegarde)
AMDE	Analyse des Modes de Défaillance et de leurs Effets
FPGA	Field Programmable Gate Array (Réseau de portes programmable sur site)
HDL	Hardware Description Language (Langage de description de matériel)
HPD	HDL-Programmed Device (Circuit intégré programmé en HDL)
AIEA	Agence internationale de l'énergie atomique
I&C	Instrumentation and Control (Instrumentation et contrôle-commande)
MCR	Main Control Room (Salle de commande principale)
CNP	Centrale nucléaire de puissance (ou Centrale)
EIP	Événement initiateur postulé
PLD	Programmable Logic Device (Réseau logique programmable)
REP	Réacteur à eau pressurisée
AQ	Assurance qualité
PCS	Points de commande supplémentaires
SCR	Safety Control Room / Emergency Control Room (Salle de commande de secours)
SLA	Safety Logic Assembly (Ensemble logique de sûreté)
RS	Relais statique
V&V	Vérification et Validation
2oo3	Voting logic: 2 out of 3 (Logique de vote: 2 sur 3)
2oo4	Voting logic: 2 out of 4 (Logique de vote: 2 sur 4)

5 Ensemble logique de sûreté – Principes et description

5.1 Ensemble logique de sûreté

Le système de protection est généralement conçu avec des technologies programmées pour réaliser les fonctions de sûreté sur la base de moyens numériques.

Habituellement, il comprend des divisions redondantes multiples et parfois diversifiées, pour parmi d'autres aspects satisfaire au critère de défaillance unique, atteindre les objectifs de fiabilité et permettre les tests en ligne et la réalisation de la maintenance.

Les sorties des multiples divisions font l'objet de certains traitement supplémentaires, réalisés par les ensembles logiques de sûreté, avant que l'ordre final ne soit envoyé à un actionneur. Ceci dépend de la conception mais généralement comprend une forme de vote pour prendre en compte des divisions qui pourraient être défaillantes ou qui pourraient être inhibées pour raison de maintenance.

L'Annexe A donne de nombreux exemples de fonctions possibles réalisées par un ensemble logique de sûreté.

Du fait de la simplicité du traitement final (séquentiel et/ou combinatoire) et de son importance pour la sûreté (commande directe des actionneurs de sûreté), la technologie pour concevoir un ensemble logique de sûreté doit être extrêmement fiable et sûre. L'Annexe C clarifie les concepts relatifs à la sûreté de fonctionnement.

Les ensembles logiques de sûreté mettant en œuvre une technologie programmée ne sont pas traités dans ce document dans la mesure où d'autres normes traitent spécifiquement des systèmes programmés et du développement de logiciels.

En conséquence, dans ce document un ensemble logique de sûreté réalise des fonctions logiques de catégorie A afin de transmettre le signal de commande direct aux actionneurs de sûreté sans recourir à une technologie programmée.

L'ensemble logique de sûreté, comme partie intégrante du système de protection, doit être conçu conformément à l'IEC 61513.

5.2 Technologie applicable à l'ensemble logique de sûreté

La conception d'un ensemble logique de sûreté peut relever de n'importe quel type de technologie si la fiabilité des performances réalisées satisfait les exigences. Dans ce document deux types de technologies sont considérées: technologie câblée et technologie HPD.

a) Technologie câblée:

   la fonction est définie par les caractéristiques des composants et de leurs connexions internes. Les premiers systèmes électroniques étaient basés sur une technologie câblée pour assurer les fonctions de sûreté.

   Plusieurs types de composants technologiques sont pris en considération, tels que les relais, les composants à semiconducteurs ou la logique dynamique. Le terme "technologie analogique" se substitue parfois au terme "technologie câblée" afin de souligner que les signaux sont analogiques (tensions, courant, fréquence, etc.). Les signaux ne sont toutefois pas nécessairement analogiques du fait du caractère non programmable des premiers composants numériques. La technologie câblée est simple, solide et rapide. La fonction est fixe et stable.

   Après la validation et les essais, le risque résiduel de défaillance est associé uniquement aux défaillances aléatoires dues au vieillissement, à l'usure ou aux conditions d'environnement qui peuvent entraîner des dérives.

   Étant donné que la probabilité de défaillance peut être estimée, la probabilité de défaillance d'un système est plus ou moins prévisible.

   Avec une technologie câblée, la sûreté est obtenue en se protégeant contre les défaillances aléatoires grâce à une conception spécifique avec une redondance non diversifiée appropriée.

b) Technologie HPD:

La miniaturisation récente et importante des composants électroniques a produit un nouveau type de technologie basée sur des portes logiques haute densité, capables de réaliser des fonctions complexes mises en œuvre par le langage HDL. Cette technologie, désignée par l'expression "circuits intégrés programmés en HDL" (HPD), inclut les FPGA, PLD, CPLD ou ASIC. Sa conception repose sur les principes de technologie câblée du fait du "câblage" des fonctions par des connexions entre des portes logiques. Néanmoins, les applications pratiques sont très similaires à la technologie programmée. La conception peut notamment être affectée par des erreurs. Le respect des recommandations de l'IEC 62566 doit permettre d'évaluer spécifiquement le risque d'erreur dû à la complexité.

Du fait de la nécessité de satisfaire des performances de sûreté et de fiabilité très exigeantes lors de la conception des ELS, les composants HPD doivent être spécifiquement choisis pour ce faire.

Le Paragraphe B.4.3 de l'Annexe B fournit des recommandations et définit les limitations associées aux composants HPD.

5.3 Interfaces d'un ensemble logique de sûreté

La Figure 1 représente le montage typique d'une voie de contrôle-commande dans un système de protection utilisant un ensemble logique de sûreté pour commander les actionneurs de sûreté.

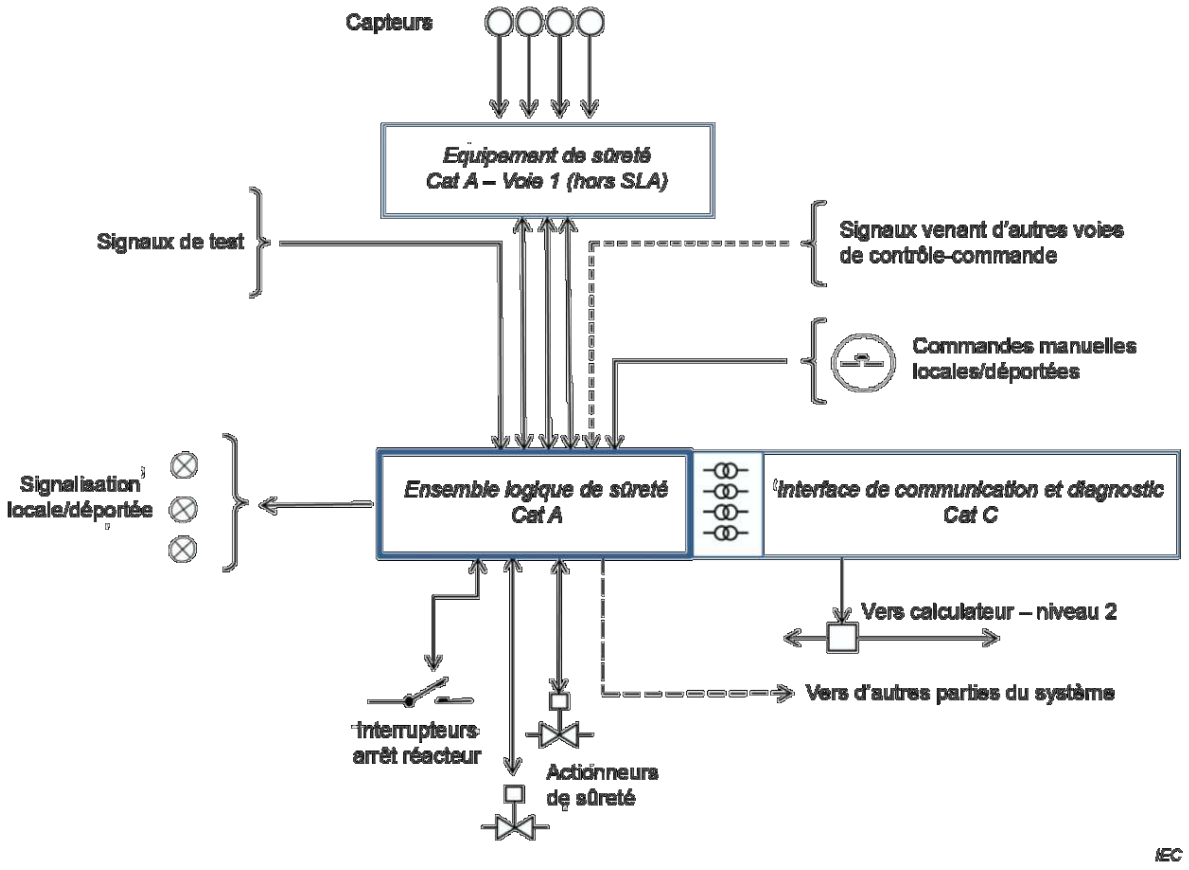

Figure 1 – Montage typique de l'interface d'un ensemble logique de sûreté dans un système de protection

Un système de protection utilisant un ensemble logique de sûreté est divisé généralement en trois parties principales:

a) L'équipement de sûreté

Par exemple une voie d'I&C redondante du système de protection. La Figure 1 représente la voie d'I&C 1, réalisant des fonctions de catégorie A au moyen de traitement de signaux

analogiques et de comparaison aux valeurs de consigne avec des signaux fournis par des capteurs. Cet équipement produit des signaux binaires qui sont les entrées des ensembles logiques de sûreté.

b) L'ensemble logique de sûreté (câblée ou HPD)

L'ensemble réalise des fonctions de catégorie A sur les signaux logiques reçus de la partie programmée et d'autres signaux y compris les commandes manuelles, les signaux d'essai et éventuellement les signaux émis par les autres voies lorsqu'une logique de vote est exigée. De nombreux projets utilisent les ensembles logiques de sûreté pour transmettre directement les commandes finales pour déclencher les interrupteurs d'arrêt d'urgence ou les actionneurs de sûreté.

Des indicateurs d'affichage de sûreté sont disponibles (déportés ou en local). Certains signaux sont transmis à l'équipement d'interface, de communication et de diagnostic (de l'ensemble logique de sûreté) afin d'améliorer la surveillance du système avec le soutien du système informatique de la centrale.

Les signaux peuvent également être transmis à d'autres parties du système de sûreté (par exemple, à un autre ensemble logique de sûreté) selon les fonctions et l'architecture du système de sûreté.

Les fonctions réalisées par un ensemble logique de sûreté dépendent spécifiquement de chaque projet et peuvent être très différentes. Dans certains cas, un ensemble logique de sûreté peut recevoir des signaux transmis par les actionneurs tels que l'état ou la position.

c) L'équipement d'interface, de communication et de diagnostic

Cet équipement, associé à l'ensemble logique de sûreté, réalise des fonctions de catégorie C à l'aide des signaux transmis par ce même ensemble. Les signaux et les résultats des diagnostics peuvent être transférés aux ordinateurs et aux salles de commande, sous réserve que cet équipement soit correctement isolé de l'ensemble logique de sûreté.

5.4 Objectifs de la sûreté de fonctionnement

Du fait de la prise en compte de l'importance d'un ensemble logique de sûreté puisqu'il transmet directement le signal de commande aux actionneurs de sûreté, au-delà de la fiabilité, il doit être tenu compte de son comportement en cas de défaillance. La probabilité de défaillance doit alors être décomposée en probabilité de défaillance dans un état sûr (actionnement intempestif) et dans un état non sûr (actionnement bloqué).

La sûreté de fonctionnement (se reporter à l'Annexe C) est mieux adaptée à l'atteinte des objectifs de sûreté et de disponibilité de la centrale. La sûreté de fonctionnement inclut deux objectifs principaux relatifs au fonctionnement de la centrale: sûreté et disponibilité de la centrale.

Le rôle de l'ensemble logique de sûreté vis-à-vis de la sûreté de la centrale consiste à garantir la transmission des commandes vers les actionneurs de sûreté en cas de demande.

Une meilleure sûreté et disponibilité peut être atteinte en augmentant la fiabilité (probabilité de fonctionnement correct sans défaillance).

Mais en cas de défaillance d'un SLA deux cas sont à considérer:

- Défaillance pour laquelle le signal de sortie est dans un état déclenché (actionnement de sûreté intempestif). L'installation sera arrêtée, donc moins disponible, mais sûre. Pour augmenter la disponibilité, il est nécessaire de réduire la probabilité de défaillance en état sûr.
- Défaillance pour laquelle le signal de sortie est dans un état bloqué non sûr. L'installation est encore en fonctionnement, mais la sûreté est dégradée. Pour augmenter la sûreté il est nécessaire de réduire la probabilité de défaillance dans un état non déclenché.

La sûreté et la disponibilité sont des objectifs qui doivent être exprimés par deux probabilités:

- Probabilité de blocage d'une commande d'actionnement en cas de demande (probabilité de défaillance par demande)
- Probabilité de défaillance en provoquant une commande intempestive (probabilité de défaillance par année)

Ces probabilités doivent être allouées à l'ensemble logique de sûreté lors de la conception du système de protection comme cela est spécifié par l'IEC 61513.

Les probabilités effectives sont calculées lors de l'analyse de fiabilité qui doit être effectuée selon la procédure indiquée dans l'IEC 60812.

Les probabilités peuvent être ajustées lors de la conception: architecture interne, technologie, détection de défaillance.

5.5 Modes de fonctionnement

Les différents modes de fonctionnement d'un ensemble logique de sûreté suivants doivent être pris en compte pour démontrer que le fonctionnement de l'ensemble n'est pas compromis .

- Conditions normales:
  - Absence de défaillance, conditions d'environnement normales
  - Mode de défaillance
  - Mode d'essai
  - Mode de démarrage pour la technologie HDL
- Conditions anormales:
  - Conditions d'environnement anormales telles que spécifiées
- Erreur humaine: le risque d'erreur humaine lors de la mise en œuvre de certaines dispositions préventives est pris en compte.

5.6 Principes de réalisation des objectifs de sûreté

5.6.1 Fonctionnement sûr en mode de fonctionnement normal

Les recommandations suivantes s'appliquent au bon fonctionnement d'un ensemble logique de sûreté dans des conditions normales:

a) Pertinence des fonctions mises en œuvre dans l'ensemble logique de sûreté. Cette pertinence est obtenue par la qualité des spécifications et leur validation, ainsi que par la qualité de la conception.

b) Réalisation d'essais périodiques pour mettre en évidence toute défaillance qui ne serait pas détectée par un circuit de détection permanente. Si l'essai périodique entraîne la mise hors service de la partie de l'équipement soumise à l'essai, et si la réalisation de l'essai nécessite le fonctionnement de l'équipement, la conception doit comporter une redondance appropriée.

c) Fiabilité des composants afin de limiter le taux de défaillance dans les conditions de fonctionnement spécifiées. Le choix de composants appropriés lors de la conception permet d'obtenir cette fiabilité.

d) Prévision du comportement en cas de défaillance. Même si tous les composants ont un taux de défaillance faible, le comportement d'un ensemble logique de sûreté doit être compris en cas de défaillance. Il convient de prendre plusieurs dispositions pour traiter ce point:

   - Une conception orientée sûreté: une défaillance éventuelle entraîne le déclenchement des actions de sûreté ou mise en état sûr.
   - Une conception qui permet de limiter le temps de fonctionnement avec un composant ou une partie de l'équipement défaillant. Cette conception implique que l'équipement

comporte des circuits de détection permanente de défaillance, une alarme destinée à informer les opérateurs de maintenance et un plan de réparation rapide et aisée des modules défaillants.

- Une redondance interne de l'ensemble logique de sûreté pour faire face au risque de non-déclenchement en cas de défaillance.

5.6.2 Fonctionnement sûr en mode de fonctionnement anormal

Un ensemble logique de sûreté doit être capable de fonctionner dans les conditions d'environnement spécifiées. La conception doit inclure toutes dispositions pour favoriser la robustesse de l'équipement en choisissant des composants appropriés. Le fonctionnement sûr dans des conditions anormales est obtenu par un processus de qualification réalisé comme spécifié en 6.5.

5.6.3 Protection contre une erreur humaine

Un ensemble logique de sûreté reçoit des commandes manuelles conformément aux spécifications fonctionnelles, par exemple, pour placer l'équipement en mode essai ou pour déclencher manuellement une action de sûreté.

Il convient que la conception prenne en compte le risque d'une commande inappropriée de l'opérateur. Par exemple, la mise en mode essai simultanée de deux parties redondantes de l'équipement est interdite. Il convient de mettre en œuvre un circuit de verrouillage afin d'adapter la logique en fonction du nombre d'ensembles configurés en mode essai. Ces dispositions sont importantes et il convient qu'elles soient analysées avec soin lors de la conception de l'équipement.

5.7 Principes de réalisation des objectifs de disponibilité

5.7.1 Objectifs de disponibilité de la centrale

Les objectifs de disponibilité de la centrale sont compris et non limité aux SLA. Comme les SLA envoient les ordres de commande directement aux actionneurs, en cas de défaillance, les conséquences ont un impact sur le fonctionnement de la centrale et cet aspect est fondamental.

5.7.2 Disponibilité de la centrale en mode de fonctionnement normal

Il convient que la conception minimise le risque de déclenchement intempestif dû à une défaillance du matériel, une erreur de conception ou une commandé inappropriée de l'opérateur de conduite. Les principes sont identiques à ceux qui permettent d'atteindre les objectifs de sûreté, mais certaines solutions (notamment l'architecture interne avec une logique de vote) doivent être conçues avec soin pour ne pas compromettre la sûreté.

La probabilité qu'une défaillance aléatoire unique entraîne un déclenchement automatique doit respecter la valeur allouée à l'ensemble logique de sûreté.

La logique de vote en aval des parties redondantes de l'ensemble logique de sûreté doit être simple et extrêmement fiable.

5.7.3 Disponibilité de la centrale en mode de fonctionnement anormal

Les principes de réalisation des objectifs de sûreté en mode de fonctionnement anormal s'appliquent également pour atteindre la disponibilité de la centrale en mode de fonctionnement anormal.

5.7.4 Protection contre une erreur humaine

Il convient de mettre en œuvre des solutions permettant d'éviter les déclenchements intempestifs dus à une erreur de l'opérateur, par exemple:

- Affichage de l'état des autres voies redondantes afin d'informer clairement l'opérateur du risque de déclenchement en cas de commande manuelle, par exemple, lorsqu'une voie est déjà en mode essai.
- Mise en place d'un circuit de verrouillage afin d'éviter un déclenchement intempestif. Si le concepteur décide de mettre en place un tel circuit, la conception doit être analysée avec soin pour ne pas compromettre la fonction de sûreté.

6 Ensemble logique de sûreté – Exigences de conception

6.1 Généralités

Un ensemble logique de sûreté doit être conçu afin d'assurer:

- qu'il fonctionnera correctement dans toutes les conditions spécifiées,
- que les objectifs de sûreté de fonctionnement sont respectés,
- qu'il satisfait à toutes les exigences applicables aux systèmes de sûreté.

6.2 Fonctions

6.2.1 Spécification des fonctions

Les fonctions de sûreté d'un ensemble logique de sûreté sont spécifiques à chaque projet et doivent être spécifiées et validées comme exigé dans l'IEC 61513.

Les fonctions comportant des signaux logiques sont principalement combinatoires ou séquentielles. Les signaux de sortie sont transmis aux actionneurs ou à d'autres ensembles du système de sûreté.

Puisque les fonctions d'un ensemble logique de sûreté sont de catégorie A conformément à l'IEC 61226, elles doivent être soumises à des essais périodiques selon les recommandations indiquées dans l'IEC 60671.

Il convient qu'un circuit de diagnostic câblé permanent, lorsque cela est possible, soit mis en place dans l'ensemble logique de sûreté afin de détecter une défaillance hypothétique ou une mauvaise position des commandes manuelles.

Il convient qu'un signal d'alarme soit positionné et un signal de déclenchement automatique d'action de sûreté doit être généré si la position correspond à un état non sûr (conception orientée sûreté).

Lorsqu'un circuit de diagnostic câblé permanent est mis en place, ses principes doivent être établis avec soin lors de la conception d'un ensemble logique de sûreté. L'analyse de fiabilité et l'analyse de sûreté sont effectuées afin de faciliter la spécification des fonctions de diagnostic câblé permanent. La couverture des défaillances par ce circuit de surveillance doit être déterminée.

Un circuit de diagnostic câblé permanent ne doit pas compromettre le fonctionnement sûr du système.

La connexion correcte d'une carte, la surveillance des sources d'alimentation ou la position correcte des interrupteurs constituent quelques exemples de fonctions de diagnostic câblé permanent.

Lorsqu'elle est détectée, une défaillance entraîne la transmission du résultat de la fonction de diagnostic câblé vers:

- le système de sûreté s'il est nécessaire pour invalider les signaux de sûreté éventuels transmis par la voie défectueuse. Cette exigence doit être justifiée par analyse.

- l'opérateur, localement ou à distance – connexion directe pour l'affichage de sûreté ou par l'intermédiaire de l'équipement d'interface et de communication.

6.2.2 Commandes manuelles

Les commandes manuelles sont des signaux logiques transmis localement par l'équipement lui-même ou à distance par les postes de commande. Par exemple, ces commandes sont utilisées:

- pour commander manuellement soit un actionneur donné, soit une action de sûreté complète avec plusieurs actionneurs;
- pour placer une partie de l'équipement en position d'essai.

L'IEC 60965 spécifie des exigences concernant les commandes manuelles en cas d'indisponibilité de la salle de commande principale.

Les commandes manuelles de l'opérateur doivent être conçues conformément à l'IEC 61227.

6.2.3 Temps de réponse

Le temps de réponse d'un ensemble logique de sûreté doit être spécifié et défini de sorte que la valeur qui lui est associée doit lui permettre de satisfaire aux exigences du système de sûreté.

Le comportement en fonction du temps comporte deux aspects:

- le séquencement de chaque commande d'actionneur (toutes les commandes peuvent ne pas être déclenchées simultanément);
- le temps de réponse entre les signaux d'entrée et de sortie de chaque module.

Le séquencement et le temps de réponse d'un ensemble logique de sûreté doivent être validés et utilisés pour calculer le temps de réponse du système de sûreté dans son ensemble.

6.2.4 Affichage – Indicateurs-alarmes

On doit indiquer l'état du signal de sortie (normal ou déclenché) émis par chaque ensemble logique de sûreté (ou on doit prévoir des dispositifs d'avertissement). Il convient aussi d'indiquer l'état des signaux d'entrée importants.

L'IEC 62241 spécifie des recommandations et des exigences relatives aux fonctions d'alarme dans la salle de commande principale.

L'IEC 60964 spécifie des exigences de mise en œuvre des fonctions de signalisation dans les salles de commande.

Le retrait d'un module en vue de son remplacement doit être indiqué.

Toute modification d'une fonction logique de vote (par exemple, modification du vote de 2oo4 en 2oo3) dans l'ensemble logique de sûreté doit être indiquée (ou des dispositifs d'avertissement doivent être prévus), de manière à limiter le temps nécessaire pour détecter cette situation et réparer les composants défectueux.

6.2.5 Interface

Un ensemble logique de sûreté peut être connecté à un équipement d'interface, de diagnostic et de communication afin de fournir au système informatique de la centrale et aux opérateurs de la salle de commande tous les signaux importants émis par l'ensemble logique de sûreté. Ces signaux doivent être isolés comme spécifié en 6.7.

6.3 Architecture et redondance

L'architecture d'un ensemble logique de sûreté dédié à un ensemble d'actionneurs dans une voie du système de protection doit être conçue pour respecter les objectifs de sûreté de fonctionnement décrits en 5.4.

Pour atteindre les objectifs de sûreté et de fiabilité, il convient qu'un ensemble logique de sûreté présente une architecture interne redondante et il convient que les parties redondantes soient suivies par une logique de vote extrêmement fiable.

Les principales exigences concernant la conception de l'architecture d'un ensemble logique de sûreté sont spécifiées par l'IEC 61513.

6.4 Technologie

Diverses solutions technologiques sont possibles pour la conception d'un ensemble logique de sûreté.

L'Annexe B propose plusieurs types de technologies câblées possibles, ainsi que les conditions de leur utilisation pour la conception d'un ensemble logique de sûreté.

Le principal critère de sélection pour la technologie couvre l'aptitude à la réalisation de la fonction, l'atteinte de l'objectif de fiabilité (voir 5.4) et la satisfaction des conditions de qualification (voir 6.5).

6.5 Qualification

Les ensembles logiques de sûreté doivent être conçus et qualifiés en tant qu'équipements importants pour la sûreté afin de supporter les conditions d'environnement produites par les événements normaux ou les événements initiateurs postulés. Il doit être tenu compte des effets des paramètres suivants:

- température
- pression
- humidité
- vibrations mécaniques
- tremblement de terre
- rayonnement
- compatibilité électromagnétique (CEM)
- isolement électrique

Les essais de qualification et les normes applicables correspondantes sont indiqués en 7.2.4.

La spécification des ensembles logiques de sûreté doit définir la durée de vie qualifiée et le temps de mission de l'équipement par rapport aux conditions de fonctionnement exigées.

La durée de vie qualifiée doit être adaptée aux conditions de fonctionnement et au temps de mission nécessaires du système de sûreté.

6.6 Maintenance

Un ensemble logique de sûreté doit être réparé facilement et rapidement après la détection d'une défaillance et lors de la maintenance préventive. Cette exigence peut comprendre deux dispositions:

- détection des défaillances avec un circuit de détection spécifique afin d'indiquer à l'opérateur quel composant ou quel module est défaillant.
- remplacement rapide avec peu de réglages ou d'ajustements. Il convient qu'un composant défaillant soit remplacé rapidement et facilement. Ce remplacement n'est possible qu'après la détection et le signalement d'un composant défaillant. Cette solution est rendue possible par exemple en utilisant des cartes électroniques disposées dans des châssis normalisés.

Des dispositifs internes ou externes doivent être prévus pour l'identification rapide de l'état logique de l'ensemble logique de sûreté et des modules remplaçables afin de faciliter la maintenabilité.

Une pièce de rechange (module, carte) qui remplace une pièce défaillante doit être vérifiée et soumise à des essais préalablement à l'installation sur site. Le paragraphe 7.3.3 spécifie des exigences pour les essais de toutes les pièces installées.

En cas de retrait d'un module remplaçable, la probabilité d'une action sûre du système associé doit être maintenue à un niveau de sûreté et de disponibilité acceptable.

La maintenabilité étant spécifique à chaque type de solution technologique décrite à l'Annexe B, elle doit être préparée avec soin lors de la conception.

6.7 Séparation

La conception d'un ensemble logique de sûreté doit permettre de satisfaire aux critères d'indépendance applicables au système de sûreté dans son ensemble. Les exigences concernant la séparation entre les parties redondantes et les autres parties du système doivent satisfaire aux recommandations spécifiées dans l'IEC 60709.

Les ensembles logiques de sûreté d'une voie redondante doivent être conçus avec une indépendance électrique et une séparation physique suffisantes. Cette condition est nécessaire, mais pas suffisante pour réduire la probabilité de défaillances multiples à un niveau acceptable conforme aux exigences de fiabilité spécifiées pour le dimensionnement du système de protection.

Un ensemble logique de sûreté doit fonctionner correctement en présence d'un niveau d'interférence spécifié. De la même façon, il convient de prévoir une protection entre deux ensembles logiques de sûreté afin de satisfaire aux exigences CEM. Les principes de qualification sont donnés en 6.5 et ceux pour les essais de qualification en 7.2.4.

Les circuits d'entrée et de sortie doivent être protégés contre les tensions existantes dans l'environnement et contre tout contact électrique potentiel avec eux du fait d'un défaut.

Si la suppression d'arcs électriques exige l'utilisation de dispositifs, ces derniers ne doivent altérer ni la rapidité ni la fiabilité de l'ensemble logique de sûreté au-delà de valeurs acceptables.

Les signaux de commande manuelle reçus par un ensemble logique de sûreté (localement ou depuis la salle de commande) doivent être câblés, protégés contre les interférences CEM et séparés par un module d'isolement afin d'éviter les perturbations dues aux tensions parasites reçues par les câbles.

Un ensemble logique de sûreté peut être connecté à d'autres ensembles appartenant à d'autres voies. Tous les signaux doivent être transmis aux autres voies par l'intermédiaire de modules d'isolement.

Les exigences de séparation fonctionnelle et de communication concernant l'architecture de l'I&C de la centrale doivent être satisfaites au niveau des branchements internes de l'ensemble de sûreté.

6.8 Alimentation électrique

Les ensembles logiques de sûreté d'une voie redondante doivent être alimentés par la voie redondante.

L'alimentation électrique doit avoir une indépendance et une capacité suffisantes lorsqu'elle est nécessaire au maintien des fonctions de sûreté requises pour l'ensemble logique de sûreté.

L'alimentation électrique doit être conçue conformément à l'IEC 61225.

7 Essais des ensembles logiques de sûreté

7.1 Généralités

Il existe quatre types d'essais pour un ensemble logique de sûreté:

- essais de type destinés à valider la conception
- essais de production destinés à valider la fabrication
- essais sur site destinés à valider l'installation
- essais périodiques destinés à détecter les défaillances pendant l'exploitation

7.2 Essais de type

7.2.1 Généralités

Les essais de type doivent être effectués pour valider la conception d'un ensemble logique de sûreté et pour démontrer que les caractéristiques de performances observées de l'ensemble logique de sûreté respectent ou dépassent les caractéristiques de performances spécifiées dans le cadre de la conception générique et/ou spécifique.

La substitution d'une analyse théorique à certains essais de type est acceptable. Ce type d'analyse doit toutefois être justifié et documenté dans le programme de qualification.

7.2.2 Séquences d'essai

Les essais de type doivent être réalisés sur un ensemble logique de sûreté selon une séquence spécifiée qui doit faire partie intégrante de la procédure d'essai écrite.

Il est recommandé de réaliser deux séquences d'essai:

a) Essais de validation fonctionnelle et de performance: Essais destinés à valider les fonctions et leur exécution dans les conditions normales de fonctionnement.
b) Essais de qualification: Essais destinés à valider le fonctionnement de l'équipement dans des conditions d'environnement anormales et extrêmes.

7.2.3 Essais de validation fonctionnelle et de performance

Les ensembles logiques de sûreté constituent des parties d'un ensemble de sûreté. Il convient de ce fait que les essais de validation fonctionnelle soient inclus dans les essais de validation de ce système.

Les essais de validation doivent être effectués en suivant un programme d'assurance qualité et doivent être documentés.

Les ensembles logiques de sûreté doivent être soumis à des essais afin de vérifier les caractéristiques de performances suivantes:

- plage de signaux d'entrée (tolérance sur le 0 et le 1 logiques);
- plage de signaux de sortie (tolérance sur le 0 et le 1 logiques);
- fonction logique;
- temps de réponse (l'ensemble logique de sûreté doit produire son signal de sortie dans un délai spécifié après le lancement de la configuration d'entrée);
- contraintes de dépassement de plage à l'entrée;
- impédance d'entrée et de sortie;
- capacité de charge;
- caractéristiques admises du signal d'entrée;
- caractéristiques admises du signal de sortie le cas échéant;
- caractéristiques d'isolement et de découplage (pour chaque signal d'entrée et de sortie par rapport aux autres signaux d'entrée et de sortie);
- caractéristiques assignées des contacts (courant alternatif, courant continu, courant inductif et courant résistif);
- rapport signal/bruit (mesuré en décibels rapportés à la valeur la plus faible du signal correspondant au niveau logique 1).

7.2.4 Essais de qualification

Ces essais doivent vérifier que l'équipement réalise ses fonctions spécifiées avant, pendant et après un événement initiateur postulé. L'essai de type doit comporter une séquence prédéterminée de profils d'essai:

- essais de qualification dans les conditions d'environnement conformément à l'IEC/IEEE 60780-323,
- essais de qualification sismique conformément à l'IEC 60980,
- essais de qualification CEM conformément à la série IEC 61000 et à l'IEC 62003, et
- qualification d'irradiation, le cas échéant, conformément à l'IEC/IEEE 60780-323.

7.3 Essais de production

7.3.1 Généralités

Les essais suivants peuvent être effectués sur un nombre approprié d'échantillons afin de vérifier que les ensembles logiques de sûreté produits en usine demeurent totalement conformes aux ensembles utilisés pour les essais de type.

Les conditions et procédures des essais de production sont définies dans un programme d'assurance qualité du fabricant.

7.3.2 Essais des pièces de rechange

Les pièces de rechange sont fournies sous forme de modules ou de cartes électroniques. Elles peuvent être fabriquées à tout moment au cours de la durée de vie de l'équipement et doivent être soumises à des essais selon les procédures de fabrication.

Il est recommandé d'utiliser un banc d'essai spécifique qui représente toutes les interfaces dans des conditions réelles afin de contrôler le fonctionnement.

Au cours de la durée de vie de la centrale, les problèmes d'obsolescence doivent pris en compte et la conception de nouvelles pièces de rechange peut être nécessaire. Ainsi la

qualification des nouvelles pièces de rechange doit être faite conformément aux exigences fournies en 7.2.4.

La qualification fonctionnelle et la qualification aux conditions d'environnement doivent être analysées afin de déterminer la séquence d'essai à exécuter afin de maintenir la validité de la qualification.

7.3.3 Essais de production sur des ensembles logiques de sûreté fabriqués

Ces essais effectués sur les ensembles logiques de sûreté doivent inclure:

- inspection visuelle;
- contrôle des soudures, des brasures des connexions par enroulement ou autres méthodes;
- contrôle des tolérances mécaniques;
- essais électriques (essai diélectrique, contrôle de la résistance d'isolement);
- essais de l'alimentation électrique;
- essais fonctionnels. Un déverminage préliminaire de l'équipement peut être spécifié.

Les essais susmentionnés doivent être effectués sur la totalité des ensembles logiques de sûreté qui ont été fabriqués.

7.3.4 Essais sur des pièces ou des modules de substitution

Il convient que toutes les pièces approvisionnées soient du type utilisé avec l'équipement qualifié. Toutefois, lorsque des composants doivent être remplacés, une documentation de qualification appropriée doit être fournie. Celle-ci doit prendre en considération le procédé de fabrication, les procédures d'assurance qualité et la différence constatée dans les performances attendues lors du fonctionnement de l'équipement.

Quand le programme d'assurance qualité prévoit des essais par échantillonnage, le nombre de pièces ou de modules peut être choisi conformément aux exigences relatives au niveau d'assurance qualité, aux règles d'échantillonnage et au niveau d'inspection.

7.3.5 Essais sur les armoires montées

Les essais suivants doivent être effectués sur chaque armoire montée:

- essais fonctionnels de préférence avec un équipement automatique, au moins de toutes les configurations d'entrée et de sortie nécessaires pour identifier une panne dangereuse;
- contrôle du bon fonctionnement de la ventilation et des autres dispositifs de refroidissement;
- contrôles par échantillonnage de l'isolement entre les bornes d'entrée et de sortie et entre les bornes et le châssis. Le nombre de bornes peut être choisi conformément à la spécification.

7.4 Essais sur site

7.4.1 Contrôles de l'équipement avant installation

Un ensemble logique de sûreté doit, préalablement à l'installation sur site, faire l'objet d'un contrôle destiné à démontrer qu'il n'a pas subi de dommage pendant le transport.

Le contrôle doit être effectué selon une procédure écrite et un rapport doit être produit afin de certifier que toutes les parties de l'ensemble logique de sûreté sont conformes avant l'installation.

7.4.2 Essais de validation de l'installation

Après l'installation, des essais doivent être effectués afin de démontrer que l'ensemble logique de sûreté est correctement installé et qu'il fonctionne de manière satisfaisante.

Les essais sont effectués selon une procédure écrite qui tient particulièrement compte de toute l'influence possible des conditions sur site sur les performances de l'ensemble logique de sûreté, par exemple:

- L'adressage et le raccordement des câbles
- L'ancrage des armoires
- Le raccordement à la terre

Après les essais d'installation, des essais de mise en service sont effectués dans le cadre des essais de mise en service du système de protection.

Des essais diélectriques ou des essais CEM sur site doivent être considérés avec attention et avec des restrictions particulières afin d'éviter toute perturbation sur les autres systèmes.

7.4.3 Essais périodiques

Les essais périodiques doivent être effectués en fonctionnement normal afin de détecter toute défaillance qui ne peut pas l'être par des circuits de diagnostic permanent.

Les ensembles logiques de sûreté réalisent les fonctions de catégorie A conformément à l'IEC 61226. Ils font partie intégrante du système de protection et sont utilisés pendant de nombreuses années. Ils doivent être soumis à des essais et satisfaire au critère de défaillance unique pendant les essais.

Les intervalles de temps entre les essais périodiques sont définis lors de l'analyse de sûreté de fonctionnement afin de satisfaire aux exigences probabilistes de sûreté.

L'utilisation d'un moyen d'essai automatique avec édition d'un rapport est recommandée.

Les méthodes et procédures des essais de surveillance doivent satisfaire aux exigences de l'IEC 60671.

8 Assurance qualité

Un plan d'assurance qualité propre à l'ensemble logique de sûreté et spécifique à l'industrie nucléaire doit exister et satisfaire aux exigences du document GSR Part 2 de l'AIEA.

L'IEC 61513 donne un ensemble important de recommandations portant sur la conception et la mise en œuvre des systèmes, y compris l'assurance qualité.

Annexe A
(informative)

Exemples d'applications des ensembles logiques de sûreté

Les applications possibles des ensembles logiques de sûreté sont variées et peuvent couvrir des parties plus ou moins importantes des systèmes de sûreté. Lorsque les exigences de sûreté et de disponibilité sont importantes, le choix d'une technologie câblée s'avère essentiel pour obtenir les performances exigées en termes de sûreté et de disponibilité.

La liste suivante fournit des exemples d'applications réalisables avec les ensembles logiques de sûreté:

a) l'arrêt rapide du réacteur sur un paramètre spécifique dans une voie;

b) la logique interne à une voie telle que les traitements logiques sur de nombreux paramètres d'arrêt rapide normalement présents; le traitement logique dans un sous-groupe sur les entrées d'une voie afin de s'assurer qu'un paramètre se situe dans une plage correcte. Les exemples incluent les bipasses de fonctionnement pour le flux et la température de sortie du cœur. Une logique de dérivation est nécessaire sur certains réacteurs afin de s'assurer que les pompes primaires fonctionnent dans leur domaine nominal, sans blocage ni cavitation;

c) la logique de priorité: Interface logique entre la sortie des voies et les interrupteurs d'arrêt rapide ou les contacteurs, et entre la sortie des voies et les actionneurs de sauvegarde. Il est nécessaire que cette interface respecte l'ordre de priorité entre les commandes des systèmes de différentes catégories de sûreté;

d) la logique des séquences après le déclenchement de l'arrêt rapide du réacteur et des actions de sauvegarde;

e) la commande manuelle de l'arrêt rapide du réacteur et son interface avec les interrupteurs, les actionneurs et les contacteurs;

f) les commandes manuelles du système de sûreté pour les séquences consécutives au déclenchement de l'arrêt rapide du réacteur et des actions de sauvegarde;

g) le déclenchement manuel de l'arrêt rapide du réacteur depuis la salle de commande principale, et l'interface avec les autres commandes d'action;

h) lorsque cela est admis ou exigé, le raccordement entre deux systèmes de sûreté diversifiés afin de garantir l'arrêt rapide du réacteur par les deux systèmes en cas de commande émise par l'un des deux;

i) la génération des commandes «à manque» ou «à émission» pour déclencher l'arrêt rapide du réacteur ou pour actionner un dispositif motorisé de sauvegarde ou une séquence après le déclenchement de l'arrêt rapide du réacteur;

j) les dispositifs pour mettre en place ou retirer les bipasses de fonctionnement, permissifs et verrouillages;

k) l'utilisation d'un bipasse de maintenance;

l) l'utilisation d'un bipasse pour éviter le déclenchement sur un capteur ou un paramètre;

m) les indications et les alarmes nécessaires pour un système de sûreté;

n) les logiques de vote entre voies redondantes.

Annexe B
(normative)

Ensemble logique de sûreté – Solutions technologiques câblées

B.1 Vue d'ensemble

B.1.1 Généralités

Aucune technologie électronique n'est fiable à 100 %. Toute solution comporte un taux de défaillance. La technologie et la logique finale appliquée aux signaux de commande redondants doivent être choisies avec une attention particulière afin de réaliser les objectifs de sûreté très exigeants d'un système de protection.

Les ensembles logiques de sûreté peuvent être mis en œuvre avec différentes solutions technologiques afin d'obtenir le niveau de sûreté spécifié. Le choix des systèmes logiques (statiques ou dynamiques) doit être conforme aux exigences de fiabilité concernant le système de protection dans son ensemble.

Les niveaux de protection les plus élevés sont généralement obtenus avec des systèmes conçus avec un mode de défaillance prédéfini (conception orientée sûreté). Pour cela, si l'on utilise des composants logiques à base de semiconducteurs en mode dynamique ou des composants magnétiques, les modes de défaillance des composants choisis doivent être étudiés pour garantir que tous respectent l'exigence de défaillance sûre (habituellement l'absence de signaux logiques dynamiques).

La redondance peut servir à améliorer la sûreté et/ou la disponibilité et peut être appliquée à des systèmes logiques statiques ou dynamiques.

Les essais réalisés sur les systèmes logiques statiques améliorent la fiabilité par la réduction de la durée moyenne de fonctionnement avant défaillance et de ce fait la durée pendant laquelle une défaillance non sûre demeure non révélée dans le système. L'IEC 60671 spécifie des recommandations.

La technologie électronique se limite aux composants à faible puissance pour la réalisation des fonctions de contrôle commande.

La conception d'un ensemble logique de sûreté peut utiliser des composants de différentes technologies. Les alinéas suivants présentent les solutions technologiques câblées possibles accompagnées de leurs caractéristiques principales et des exigences concernant la conception de l'ensemble logique de sûreté.

B.1.2 Relais

Un ensemble logique de sûreté qui commande en final l'arrêt rapide du réacteur ou les actions de sauvegarde peut être réalisé avec des relais.

Les relais sont des composants simples et robustes utilisés pour réaliser des fonctions logiques par des connexions appropriées entre les contacts et les bobines. Il existe deux technologies principales pour les relais:

- Les relais électromécaniques (REM)
- Les relais statiques (RS)

Pour les applications avec ensemble logique de sûreté, seuls sont pris en compte les relais fonctionnant avec des tensions et des courants faibles.

B.1.3 Relais électromécaniques

Un relais électromécanique (REM) est un interrupteur à commande électrique dont les contacts sont déplacés par l'application d'une force magnétique commandée par un courant.

Les relais utilisés dans un système de sûreté doivent être conçus pour fonctionner en continu conformément aux normes de la série IEC 60255. Les conditions suivantes doivent s'appliquer:

- la tension d'essai diélectrique des bobines de relais doit être spécifiée,
- la tension d'isolement nominale des contacts doit être spécifiée,
- les contacts de relais doivent être dimensionnés avec une marge de fonctionnement.

Les caractéristiques spécifiques des REM présentent un intérêt particulier dans la conception des ensembles logiques de sûreté:

- L'isolement entre le signal de commande et les circuits commandés, et l'isolement entre les contacts. Le maintien, même en cas de défaillance, de l'isolement électrique entre les signaux provenant de plusieurs voies redondantes est important. Ainsi, les relais électromécaniques sont privilégiés pour réaliser des fonctions logiques simples avec des signaux logiques isolés.
- L'impédance de la bobine permet d'intégrer à la conception une surveillance de la continuité. Un courant faible inférieur au courant de manœuvre ou des impulsions de courant dont la durée est inférieure au temps de manœuvre peuvent convenir pour cela. Dans les cas exceptionnels pour lesquels l'essai risque de provoquer un déclenchement, il convient que le courant d'essai soit égal à un dixième du courant minimum de manœuvre. Cette dernière recommandation ne s'applique pas nécessairement à l'essai ou à la surveillance de la continuité par impulsion.
- Le temps de commutation des REM peut être important et doit être spécifié. Il doit être pris en compte pour évaluer le temps de réponse de l'ensemble logique de sûreté.
- La conception des REM, du fait de leur structure mécanique, doit être robuste pour résister aux chocs et aux accélérations lors d'un séisme.
- Les REM à plusieurs pôles et contacts isolés permettent de concevoir des fonctions logiques entre plusieurs signaux.

Sur la durée, les parties mobiles s'usent et peuvent présenter des défaillances. Les arcs électriques modifient la résistance et contribuent à l'érosion des contacts, ce qui raccourcit la durée de vie du relais en le rendant inopérant. La fiabilité des REM dépend de plusieurs paramètres dont le nombre de manœuvres, la tension et le courant au niveau des contacts.

Les relais doivent être qualifiés vis-à-vis de leur temps de réponse et de leur fonctionnement dans les conditions spécifiées pour le système de sûreté. Bien que l'exigence sur le temps de réponse des relais dépende de leur type et/ou de leur structure mécanique, elle doit être justifiée afin de démontrer que le temps de réponse est approprié pour déclencher l'arrêt rapide du réacteur et les actions de sauvegarde. La justification doit couvrir l'adaptation aux conditions d'environnement conformément aux normes de la série IEC 60255.

B.1.4 Relais statiques

Un relais statique (RS) est un composant électronique qui fournit une fonction analogue à un relais électromécanique, mais ne comporte aucun composant mobile, améliorant ainsi sa fiabilité à long terme.

Un relais statique utilise un thyristor ou un autre dispositif de commutation statique, activé par un signal de commande, remplaçant ainsi le solénoïde pour commuter la charge commandée.

Un isolateur optique (une diode électroluminescente (LED) couplée à un phototransistor) peut être utilisé pour isoler les circuits de commande et les circuits commandés. Cette disposition nécessite toutefois l'installation d'une alimentation électrique séparée.

Le temps de commutation d'un RS est très court et son inductance propre est négligeable, ce qui complique la mise en place d'un circuit de surveillance de continuité.

B.2 Amplificateurs magnétiques

Un amplificateur magnétique est un dispositif électromagnétique constitué d'un petit nombre de composants très simples tels que des bobines, un noyau ferromagnétique et des diodes. Il ne comporte ni pièce mobile ni mécanisme d'usure, mais présente une tolérance satisfaisante aux chocs et aux vibrations mécaniques. Des enroulements de commande supplémentaires isolés peuvent être ajoutés sur les noyaux magnétiques. Les enroulements d'un amplificateur magnétique ont une plus grande tolérance aux surcharges momentanées que des composants comparables à semiconducteurs. Les noyaux des amplificateurs magnétiques résistent aux rayonnements. Ceci justifie leur utilisation dans les applications de puissance nucléaire.

Compte tenu de sa structure simple, un amplificateur magnétique présente un taux de défaillance très faible et peut être utilisé sur une longue période sans défaillance.

L'emploi des amplificateurs magnétiques se limite à des fonctions simples, compatibles avec les dimensions et la masse de ce type de composants. La qualification sismique doit être prise en compte dès le début de la conception en consolidant la fixation des composants lourds.

B.3 Défaillance sûre – logique dynamique

La logique dynamique est une technologie électronique réalisée avec des composants discrets et des transformateurs, utilisant un signal d'horloge périodique à plusieurs cellules pour réaliser une fonction logique. Le signal de sortie est correct tant que le signal d'horloge est présent. En cas de défaillance, le signal d'horloge s'interrompt et le signal de sortie est nul. Cette caractéristique est intéressante pour une conception orientée sûreté en raison de la nature prévisible du signal de sortie qui permet ainsi d'améliorer les performances de sûreté d'un ensemble logique de sûreté.

La conception doit faire l'objet d'une analyse formelle et documentée afin de confirmer sa conformité aux exigences de sûreté de fonctionnement et l'absence de modes de défaillance inconnus.

B.4 Circuits à semiconducteurs

B.4.1 Généralités

Les circuits à semiconducteurs traitent généralement des signaux plus faibles que les relais. Par conséquent, une attention particulière doit être portée pour réduire le plus possible les signaux (bruit) parasites émis par les rayonnements électromagnétiques, les décharges électrostatiques, les courants de terre ou les surtensions d'alimentation.

Des méthodes appropriées pour mesurer la marge de fonctionnement en présence du niveau d'interférence le plus défavorable doivent être spécifiées.

En respectant les exigences susmentionnées, il est peu probable que les composants d'un ensemble logique de sûreté soient endommagés du fait d'interférences électriques. Les composants utilisés aux interfaces d'entrée et de sortie de l'ensemble logique de sûreté (par

exemple, isolateurs optiques) doivent toutefois être capables de résister sans dommage aux niveaux d'interférences électriques postulés les plus défavorables induits dans les câbles.

B.4.2 Composants discrets

Les circuits à semiconducteurs utilisent des composants électroniques discrets tels que des transistors, des condensateurs, des diodes, etc., pour produire en sortie des signaux électriques à partir de signaux d'entrée et réaliser les fonctions exigées.

L'essentiel est le caractère non prévisible de l'état du signal de sortie d'un circuit à semiconducteurs, en cas de défaillance. Son niveau de tension n'est pas déterminé. De plus dans certains cas particuliers, une défaillance peut avoir pour conséquence un état non stable des signaux de commande.

La conception d'un ensemble logique de sûreté avec des circuits à semiconducteurs doit comporter des concepts redondants afin de limiter les conséquences des défaillances. Les signaux de sortie redondants doivent être combinés avec une fonction logique très simple et fiable.

B.4.3 Circuits intégrés – HPD

Les composants électroniques évoluent naturellement vers une miniaturisation plus importante pour proposer des composants à haut niveau d'intégration: Circuits intégrés programmés en HDL (HPD), tels que les composants FPGA, PLD, CPLD.

Il s'agit fondamentalement de composants câblés (assemblage d'un grand nombre de portes logiques), mais leur complexité est telle que leur conception nécessite des moyens de calcul, par exemple, la configuration d'un composant FPGA est généralement spécifiée avec un programme logiciel en langage HDL. Ces composants peuvent par ailleurs reproduire le comportement de certains microprocesseurs.

La récente et rapide miniaturisation des technologies submicroniques CMOS pour les composants HPD fait apparaître trois problèmes fondamentaux, liés à l'utilisation de ces composants pour les fonctions de sûreté, et ces problèmes augmentent avec le degré de miniaturisation:

- Ils sont susceptible de produite un évènement singulier dû aux interférences de particule.
- Ils peuvent être endommagés par des phénomènes d'électro-migration qui peuvent réduire leur durée de vie.
- La complexité des composants à haute intégration n'est pas un avantage pour établir des justifications de sûreté.

Ainsi l'utilisation de composants HPD intégrés pour la conception de SLA doit être limitée à des fonctions logiques simples, et ils doivent être choisis parmi ceux dont les performances sont éprouvées pour un fonctionnement dans la durée compatible avec l'objectif de durée de vie, et les besoins de justification de sûreté. Pour ces raisons l'utilisation de composants HPD hautement miniaturisés n'est pas recommandée.

Les composants HPD haute densité sont conçus pour réaliser des fonctions complexes et ce n'est pas le cas des fonctions réalisés par les SLA. Les composants HPD doivent être choisis avec une complexité limitée.

Les performances sûreté et de fiabilité des SLA doivent être soigneusement évaluées et cohérentes avec les objectifs de sûreté et de fiabilité du système de protection dans lequel ils sont à mettre en œuvre. Ces composants peuvent être utilisés pour réaliser des fonctions de catégorie A en appliquant les exigences de l'IEC 62566.

Annexe C
(informative)

Sûreté de fonctionnement et attributs

C.1 Généralités

Un ensemble logique de sûreté se caractérise principalement par sa capacité à fonctionner correctement pour commander des actionneurs en cas de demande. La sûreté de fonctionnement inclut des méthodes et des dispositions pour réduire le risque de défaillance lorsqu'une commande d'action est demandée. Le concept de sûreté de fonctionnement ne se limite pas à la fiabilité. Deux objectifs principaux sont associés aux conséquences des défaillances:

- Non-actionnement en cas de demande (défaillance non sûre): en conséquence, la sûreté de la centrale est compromise.
- Actionnement intempestif (défaillance sûre): en conséquence, la centrale s'arrête dans un état sûr mais elle n'est plus disponible.

Chacun de ces événements a sa probabilité propre.

C.2 Attributs qualitatifs et quantitatifs associés à la sûreté de fonctionnement

Le diagramme suivant, basé sur les définitions de l'AIEA et de l'IEC, présente la relation entre les différents attributs quantitatifs et qualitatifs de sûreté de fonctionnement concernant les risques finaux relatifs aux actionneurs: ne pas fonctionner en cas de demande (sûreté) ou fonctionner en l'absence de demande (disponibilité), voir Figure C.1.

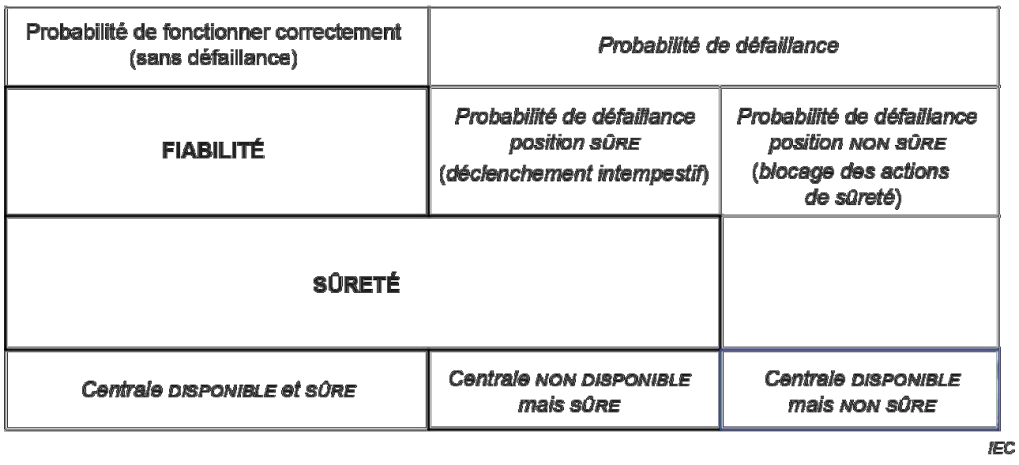

Figure C.1 – Attributs de la sûreté de fonctionnement – Relation entre la fiabilité et le risque final concernant la sûreté

L'attribut principal et fondamental est la fiabilité. Un ensemble logique de sûreté est fiable si sa probabilité de défaillance est faible (fiabilité). L'absence de défaillance signifie la disponibilité de l'ensemble logique de sûreté (disponibilité).

La probabilité d'une défaillance aléatoire est un attribut quantitatif qui peut être calculé à partir de diverses bases de données prenant en compte la description des composants et de leurs conditions d'environnement (température, vibrations, etc.). Cette probabilité permet d'obtenir de façon simple la probabilité de non-défaillance directement associée à la fiabilité.

La fiabilité peut être améliorée en utilisant des méthodes de détection des défaillances et de réparation facile et rapide pour minimiser le temps de fonctionnement avec une défaillance. La testabilité et la maintenabilité constituent les attributs correspondants. Ces attributs sont essentiellement qualitatifs.

En cas de défaillance d'un ensemble logique de sûreté, le signal de sortie ne correspond pas à une commande réelle. L'état du signal peut être:

- Soit état commandé (actionnement intempestif) qui entraîne alors le déclenchement de l'arrêt de la centrale (interrupteurs d'arrêt d'urgence) de manière automatique ou par une commande manuelle des opérateurs. La centrale est sûre, mais n'est plus disponible;
- Soit état de blocage (commande bloquée) qui signifie alors que la centrale n'est pas sûre, mais reste toujours disponible. Cet état correspond généralement à une défaillance non détectée.

La conception est généralement orientée vers la sûreté dans la mesure où les ensembles logiques de sûreté assurent la sûreté.

Ainsi, les deux types de risques (actionnement intempestif et commande de sûreté bloquée) peuvent être atténués par des dispositions de conception spécifiques telles que la redondance avec une logique de vote appropriée.

Bibliographie

IEC 60050-395, *Vocabulaire Electrotechnique International – Partie 395: Instrumentation nucléaire: Phénomènes physiques, notions fondamentales, instruments, systèmes, équipements et détecteurs*

IEC 60300 (toutes les parties), *Gestion de la sûreté de fonctionnement*

IEC 60706 (toutes les parties), *Maintenabilité de matériel*

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

IEC 62340, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences permettant de faire face aux défaillances de cause commune (DCC)*

IAEA Safety fundamentals – SF-1, *Fundamental safety principles* (disponible en anglais seulement)

Glossaire de sûreté de l'AIEA – édition 2016

IAEA Specific Safety Guide – SSG-30, *Safety classification of structures, systems and components in nuclear power plants* (disponible en anglais seulement)

IAEA – SSG-39, *Design of Instrumentation and Control Systems for NPP- (Specific Safety Guide)*

IAEA – SSR-2/1 Rev1, *Safety of Nuclear Power Plants Design (Specific Safety requirements)*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch