IEC 61500

Edition 2.0 2009-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category A functions

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Communication de données dans les systèmes réalisant des fonctions de catégorie A

IEC 61500:2009

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

About the IEC

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

About IEC publications

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

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

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

A propos des publications CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 61500

Edition 2.0 2009-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category A functions

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Communication de données dans les systèmes réalisant des fonctions de catégorie A

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

P

ICS 27.120.20

ISBN 2-8318-1065-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – DATA COMMUNICATION IN SYSTEMS PERFORMING CATEGORY A FUNCTIONS

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 61500 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1996. This edition constitutes a technical revision.

The revision of the standard is intended to accomplish the following:

- To change the focus from multiplexed data transmission to data communication
- To restrict the scope to communication in systems performing category A functions
- To clarify definitions
- To up-date the reference to new standards published since the first issue.

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

FDIS	Report on voting
45A/772/FDIS	45A/783/RVD

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

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

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

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

INTRODUCTION

a) Technical background, main issues and organization of the standard

The equipment for data communication of on-line plant data can simplify the hardwired cables connecting distributed systems for instrumentation, control, protection and monitoring needed for safe Nuclear Power Plants operation. Such communication systems can have advantages over direct cables, for electrical isolation, for reduction of cable fire loads or other reasons. In a distributed computer based system, communication equipment is an essential part of the system. Data communication is usually essential for implementing I&C systems important to safety in nuclear power plants.

It is intended that the standard be used by operators of NPPs (utilities), manufacturers of data communication equipment, systems evaluators and by licensors.

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

IEC 61500 is the third level IEC SC 45A document tackling the generic issue of data communication for equipment performing category A functions.

IEC 61500 is to be read in association with IEC 61513, which is the appropriate IEC SC 45A document providing guidance on general requirements for instrumentation and control systems important to safety, IEC 60880, which is the appropriate IEC SC 45A document providing guidance on software aspects for computer based systems performing category A functions, and IEC 60987 which is the appropriate IEC SC 45A document providing guidance on hardware aspects for computer based systems .

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 standard establishes no additional functional requirements for safety systems.

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

- Requirements for data communication within systems performing category A functions.
- Requirements for data communication between divisions of a system performing category A functions.
- Requirements for data communication of systems performing category A functions with systems of lower safety importance.
- Reliability requirements for data communication.

To ensure that the standard will continue to be relevant in future years, emphasis is placed on principles, rather than on 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 document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

IEC 61513 refers directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems,

defense against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

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

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

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

IEC 61513 refers to ISO as well as to IAEA GS-R-3 for topics related to quality assurance (QA).

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

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – DATA COMMUNICATION IN SYSTEMS PERFORMING CATEGORY A FUNCTIONS

1 Scope

This International Standard establishes requirements for data communication which is used in systems performing category A functions in nuclear power plants.

It covers also interface requirements for data communication of equipment performing category A functions with other systems including those performing category B and C functions and functions not important to safety.

The scope of this standard is restricted to the consideration of data communication within the plant I&C systems. It does not cover communication by telephone, radio, voice, fax, email, public address etc.

The internal operation and the detailed technical specification of data communication equipment are not in the scope of this standard. This standard is not applicable to the internal connections and data communication of a processor unit, its memory and control logic. It does not concern the internal processing of instrumentation and control computer systems.

This standard gives requirements for functions and properties of on-line plant data communications by reference to IEC 60880 and IEC 60987, produced within the framework of IEC 61513. It requires classification of the communication functions in accordance with IEC 61226, which in turn requires environmental and seismic qualification (i.e., the environment where the safety function is required to operate) according to IEC 60780 and IEC 60980.

2 Normative references

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

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

IEC 60780:1998, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

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

IEC 60987:2007, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*

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

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

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

IEC 62340:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

IAEA safety guide No. NS-G-1.3:2002, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

3 Terms and definitions

For the purposes of this document, the terms and definitions of IEC 60880, IAEA safety glossary and safety guide No. NS-G-1.3 and the following definitions are applicable.

3.1
communication channel
logical connection between two end-points within a communication system

[IEC 61784-3, 2007]

3.2
communication node

connection point on a communication network, at which data is conveyed via communication channels to or from that point to other points on the network

3.3
communication system
arrangement of hardware, software and propagation media to allow the transfer of messages (ISO/IEC 7498 application layer) from one application to another

[IEC 61784-3, 2007]

3.4
data communication
exchange of data between communication nodes via communication channels

3.5
data communication equipment
embodiment of the media, modulation and coding-dependent portion of a bus-connected device, comprising the lower portions of the physical layer within the device

[IEC 61784-3, 2007, modified]

3.6
message
ordered series of digital states in defined groups, used to convey information

[IEC 61784-3, 2007, modified]

3.7
protocol
convention about the data formats, time sequences, and error correction in the data exchange of communication systems

[IEC 61158-3-19, 2007]

3.8
processing unit
one or more processing cores whose instructions are specialized to handle networking or communication-related functions, in this specific communication standard

4 Symbols and abbreviations

CCF Common cause failure

EMC Electromagnetic compatibility

FMEA Failure mode and effects analysis

I&C Instrumentation and control

QA Quality assurance

5 General requirements

5.1 Principles of selection of data communication techniques and equipment

The communications equipment shall meet requirements for systems performing category A functions.

NOTE To ensure acceptability for nuclear applications one of the following principles for selection of data communication techniques and equipment can be applied:

- use of protocols implementing safety features;
- use of industrial standard protocols with added safety layers;
- use of protocols where higher protocol layers implementing unsafe or not needed functionality are removed or replaced by ones with reduced and safe functionality.

The hardware and the software shall be qualified, see Clause 9.

5.2 Functional requirements

Generally each data communication channel is part of an overall system providing services of information gathering and presentation, control or protection of the nuclear power plant.

Equipment providing cyclic data over a communication channel shall not depend on the receipt of acknowledge messages from the receiver for continued operation.

Communication channels shall not be allocated dynamically during the run time of the system but shall be statically allocated and predefined by design.

All messages of application software shall be transmitted periodically within a pre-defined variation of cycle time.

Messages should have fixed length predefined by design.

The communication system shall enable messages from instruments or other outstation equipment using a communications channel to be sent and received within a specified time frame, together with data integrity status information (if implemented).

The data communication network topology and media access control shall be designed and implemented to avoid CCF of independent systems or subsystems (see 8.3).

Data may be distributed via data communication to redundant systems to enable continued operation if one system is damaged.

The security threats arising from the use of data communication shall be taken into consideration within the scope of the security plans according to IEC 61513.

5.3 Performance requirements

Data communication channels shall provide sufficient performance to ensure that any message sent from any communication node is received by the intended destination node in a timely manner.

Data communication shall meet the requirements of the functions. The mechanisms and protocols used shall guarantee that any delay which may occur during communication or during access to the communication equipment is known and bounded by design.

Communication channels shall be verified to meet the specified real time response requirements of the Category A functions to be performed, under credible worst-case conditions. The required real time response and the worst-case conditions shall be justified by analysis. Deterministic communications shall be used so that communications load does not vary, irrespective of plant conditions.

Where communication equipment is used for manual plant control and indication through a control room, the time from operating the physical switch or soft control until the confirmation of the action by indication of the changed state in the control room should be assessed under all potential circumstances including worst case conditions.

5.4 Failure detection

Hardware failures of Communication equipment shall be detected and reported. Detected failures of the communication equipment that result in unacceptable degradation of the nuclear safety functions of the I&C system shall be indicated to the plant operators in control rooms.

The data communication including operation of error response features (if used) shall be verified and validated prior to operational use of the equipment to perform category A functions.

5.5 Communication within division

The data communication within a segregated division (train) shall be protected from adverse influences from outside of the division. Thus messages in a division shall be passed directly from the sending communication node to the receiving one without involvement of the communication equipment outside the division.

Data communication in a division shall be separated from the other divisions

However, communication between divisions may be acceptable if it is required by voting logic.

5.6 Interfaces to systems of lower importance to safety

Communication equipment of systems performing category A functions shall be adequately segregated from communication equipment of systems performing only lower category functions.

When plant systems of different categories are required to communicate over communication channels, then the plant data flow should be from category A functions to lower category functions.

Data flow from lower categories to category A functions should be prevented unless the design of the communications channel is such that category A functions cannot be adversely affected by such a connection.

6 Physical separation and isolation

6.1 Electrical isolation

The electrical isolation of systems performing category A functions connected by communication channels to other systems shall be considered in accordance with IEC 60709. The degree of electrical isolation will depend on the station power supply voltages present, national practice, and plant-specific requirements.

NOTE A method of achieving a high degree of electrical isolation is by means of optical fibre connections or opto-electronic isolators.

Appropriate isolation shall be demonstrated between data communication equipment and connected equipment. This shall be sufficient to prevent faults of the connected equipment and cables from affecting the operation of the data communication equipment adversely. Connected equipment includes sensors, contacts, power supplies and other communication equipment.

6.2 Physical separation

The communication equipment should be designed such that faults are not propagated from one part of the equipment to another, or to another system. IEC 60709 gives requirements for this and specifically for communication from equipment performing functions of one category to equipment performing functions of another category.

The requirements of IEC 60709 shall be applied to the cables of communication channels important to safety.

The preferred method of physical separation and protection of the cables of communication channels, whether carrying electrical or optical signals, should be by the use of dedicated cable enclosures or trunking, providing adequate protection against hazards.

A system can require redundant paths for communication, which can be required to provide redundancy in the event of a hazard such as a fire which may affect a localized area. Redundant equipment which is providing protection against such a physical hazard shall be separated physically.

NOTE Requirements for coping with common cause failures are given in IEC 62340.

7 Functional independence

For receiving and transmitting data from and to separate processing units, software modules shall be provided which have specified interfaces with the communications network and with the system software and the application software of the related processing unit, to avoid fault propagation.

The design should use separate software modules for numerical and logical operations performed on signals and message contents, from those used for data transmission and message checking. This will reduce complexity and simplify verification and validation.

8 Reliability

8.1 Self-supervision and failure mitigation

8.1.1 Communication error detection

Communication equipment shall check the integrity of communicated data to confirm correct transmission, or to record/report transmission failures.

The communication equipment shall provide error detection facilities according to the relevant requirements of 4.2 d) of IEC 60987, and 4.8 of IEC 60880. These facilities shall provide appropriate assurance that data communication errors will be detected so that erroneous data will not affect the performance of category A functions. In particular, these should address:

a) faulty insertion of single bits or a group of bits in the transmitted message,

b) corruption of bits of the transmitted message,

c) transmission of out-of-date data,

d) message loss.

8.1.2 Response to failure

I&C systems performing category A functions shall take suitable actions, when communication faults are detected.

When failures of communication equipment are detected, appropriate automatic measures should be taken: e.g.

a) isolation of failed communication channels,

b) indication of the failed equipment to warn operators of failure (see also 5.4).

The action to be taken upon the detection of failures shall be specified, e.g., logging, warning to the maintenance team, alarm for immediate corrective or mitigation action.

As part of the design substantiation process, data communication equipment and processes shall be systematically analyzed using appropriate methods e.g. FMEA with respect to the consequences of failures upon category A functions.

Failures or malfunctions of a single communication node shall not affect the availability and reliability of the I&C system.

The potential affect upon the performance of category A functions of the failure of any communication node or channel shall be considered during the design process, and this analysis shall be documented. Any required actions to be taken by the system upon the detection of failure shall be defined, e.g. record the failure, produce an alarm, or drive plant to a safe state.

Communication channels should be tolerant of ‘soft’ errors, such as a missed message or an error in a single message, providing the frequency of such errors is not high enough to compromise the performance of category A functions; such ‘soft’ errors should not lead to the shutdown of a channel, but these errors should be logged by the system.

8.2 Test

The relevant testing requirements of IEC 60987, Clause 10, shall apply to class 1 communication channels. Also, the relevant subclauses 7.10 (testability), 7.11 (operational bypasses) and 7.12 (control of access to protection systems equipment) of IAEA safety guide No. NS-G-1.3 shall apply to communication channels of systems performing category A functions.

The performance of data communication functions shall be verified before equipment is placed in full operational service. The following aspects of system functionality shall be covered:

a) transmission error handling,

b) correct operation when under the maximum data transfer rates.

IEC 60880 and IEC 60987 require that the data communication system shall have self-test capabilities (see 8.1). Additional periodic tests as a supplement to self-tests should be possible during the lifetime of the equipment as required to reduce the probability of unrevealed hardware failures compromising the performance of category A functions, e.g.

1) alteration of the state or value of input signals, and monitoring of the alteration at the receiving equipment;

2) interruption of transmission, and confirmation that the receiving equipment will detect this and take correct actions.

NOTE Nuclear safety considerations may make such testing undesirable at power operation.

The communication equipment shall be qualified for operational use by functional testing in accordance with 4.79 to 4.96 of IAEA safety guide No. NS-G-1.3. Testing of the equipment modules shall be performed during factory tests or on-site commissioning tests, or evidence of previous type testing in accordance with 5.3 of IEC 60780 shall be provided.

8.3 Prevention of failures (including CCF)

Data communication equipment could be affected by conditions which cause several redundant parts of the system to fail at the same time. In order to eliminate or minimize the possibility of simultaneous failures of several modules by hazards which a system is required to survive, consideration shall be given to the following potential hazards:

- seismic disturbance or other relevant external hazards;
- fire, smoke or flooding in equipment or cable areas;
- loss of environmental control, heating and ventilation;
- excessive radiation or other factors external to the equipment, and
- factors internal to the equipment itself.

The cable trays which contain the cables for data communication between separated redundancies/trains shall be designed and separated in accordance with the requirements of IEC 60709, so that possible hazards are limited and the required fault tolerance for the overall I&C system is met.

Data communication shall be designed to prevent failure propagation, e.g. by transfer of corrupted data (see IEC 62340, 7.4).

The potential failures taken into account and the claimed features to prevent or mitigate these failures shall be analyzed and documented.

NOTE Requirements for coping with common cause failures are given in IEC 62340.

9 Qualification

Class 1 communication hardware of systems shall be qualified in accordance with the relevant requirements of IEC 60780 (environmental qualification), IEC 60980 (seismic qualification, if the equipment is to be seismically qualified), and an appropriate EMC Standard such as IEC 62003 or the IEC 61000 series (EMC Testing).

Communication software of system performing category A functions should be designed, verified and validated in accordance with nuclear standards (e.g. IEC 60880) or other appropriate standards (e.g. IEC 61508 series). The suitability of the selected qualification standard shall be analysed and justified by formal documentation.

10 Maintenance and modification

Communication hardware and software of systems performing category A functions shall be maintained and modified in accordance with IEC 61513, IEC 60880 and IEC 60987.

If one of the communication nodes fails, prompt replacement of a part should be possible at power. A communication node replacement should be accomplished in a simple manner without adversely affecting the operability of the system and within the targeted availability of the system.

Modifications of the data communication equipment shall be done under the strict procedures of the plant modification process.

Modifications shall be based on clear requirements. These modifications shall be confirmed to be in accordance with the original safety, functional and performance requirements of the data communication equipment by suitable verification consistent with IEC 61513, IEC 60880 or IEC 60987 as applicable.

When modifications have been made, the data communication shall be proven to meet their functional and performance requirements by testing prior to the installation at the plant (e.g., in a representative testbed regarding functional testing), and after installation into the target system (e.g., meet the system performance and interface requirements)(see 8.2).

Bibliography

IEC 60068 (all parts), *Environmental testing*

IEC 60721 (all parts), *Classification of environmental conditions*

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

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

IEC 61158-3-19, *Industrial communication networks – Fieldbus specifications – Part 3-19: Data-link layer service definition – Type 19 elements*

IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses*

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

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

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

ISO/IEC 7498, *Information processing systems – Open systems interconnection – Basic reference model*

———————

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – COMMUNICATION DE DONNÉES DANS LES SYSTÈMES RÉALISANT DES FONCTIONS DE CATÉGORIE A

AVANT-PROPOS

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

La Norme internationale CEI 61500 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Cette seconde édition annule et remplace la première édition publiée en 1996. Cette édition correspond à une révision technique.

L'objectif de la révision de la norme est de:

- Modifier le sujet et passer de la transmission multiplexée de données à la communication de données
- Restreindre le domaine à la communication au sein des systèmes réalisant des fonctions de catégories A
- Clarifier les définitions
- Mettre à jour les références avec les nouvelles normes publiées depuis la première édition.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/772/FDIS	45A/783/RVD

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

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

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

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

INTRODUCTION

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

Les équipements de communication de données utilisés en ligne pour les données de tranche peuvent permettre de simplifier le câblage en fil-à-fil reliant les systèmes répartis d'instrumentation, de régulation, de protection et de surveillance nécessaires à l'exploitation sûre d'une centrale nucléaire. De tels systèmes peuvent présenter des avantages par rapport aux câblages en fil-à-fil en terme d'isolement électrique, de volume de câblage en cas d'incendie ou pour d'autres raisons. Dans un système numérique réparti, les dispositifs de communication forment une partie essentielle de celui-ci. La communication des données est généralement primordiale pour la mise en oeuvre des systèmes d'instrumentation et de contrôle-commande importants pour la sûreté utilisés dans les centrales nucléaires de puissance.

L'objectif de cette norme est d'être utilisée par les exploitants de centrales nucléaires, les fabricants d'équipements de communication de données, les évaluateurs de système et par les régulateurs.

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

La CEI 61500 est le document de troisième niveau, du SC 45A de la CEI, qui traite du sujet de la communication des données pour les systèmes assurant des fonctions de catégorie A.

La CEI 61500 doit être lue avec la CEI 61513 du SC 45A de la CEI qui fournit des recommandations pour ce qui concerne les exigences générales applicables aux systèmes d'instrumentation et de contrôle-commande importants pour la sûreté, avec la CEI 60880, document du SC 45A, qui fournit des recommandations pour ce qui concerne les aspects logiciels des systèmes réalisant des fonctions de catégorie A et avec la CEI 60987, du même SC, qui fournit des recommandations applicables au matériel des systèmes informatisés .

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

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

Il est important de noter que cette norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté.

Cette norme fournit des recommandations particulières pour les aspects suivants:

- Exigences applicables à la communication de données dans les systèmes réalisant des fonctions de catégorie A.
- Exigences applicables à la communication de données entre voies d'un système réalisant des fonctions de catégorie A.
- Exigences applicables à la communication de données entre des systèmes réalisant des fonctions de catégorie A et des systèmes d'une importance moindre pour la sûreté.
- Exigences de fiabilité relatives à la communication de données.

Afin d'assurer la pertinence de cette norme pour les années à venir, l'accent est mis sur les questions de principes plutôt que sur les technologies particulières.

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

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

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

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

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

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

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA GS-R-3 pour ce qui concerne l'assurance de qualité.

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

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – COMMUNICATION DE DONNÉES DANS LES SYSTÈMES RÉALISANT DES FONCTIONS DE CATÉGORIE A

1 Domaine d'application

Cette Norme internationale établit des exigences applicables à la communication de données assurée pour des systèmes réalisant des fonctions de catégorie A dans les centrales nucléaires de puissance.

Cela comprend aussi les exigences relatives aux interfaces des équipements de communication de données assurant des fonctions de catégorie A, avec les autres systèmes y compris ceux qui assurent des fonctions de catégories B et C, ainsi que des fonctions non importantes pour la sûreté.

Le domaine d'application de cette norme est limité aux systèmes d'instrumentation et de contrôle-commande des centrales nucléaires. Il ne couvre pas les communications par téléphone, par radio, orales, par fax, par courrier électronique ou l'information au public, etc.

Le fonctionnement interne, ainsi que les spécifications techniques détaillées des équipements ne font pas partie du domaine d'application de cette norme. Cette norme n'est pas applicable aux connexions internes et à la communication de données entre les processeurs, leurs mémoires ou les logiques de commande. Elle ne concerne pas les traitements internes des systèmes numériques d'instrumentation et de contrôle-commande.

Cette norme fournit des exigences pour les fonctions et les propriétés afférentes à la communication de données en faisant référence aux CEI 60880 et CEI 60987, qui ont été développées sous couvert de la CEI 61513. Cela implique que les fonctions de communication soient classées conformément à la CEI 61226, qui à son tour nécessite de réaliser des qualifications d'ambiance et sismique (par exemple l'environnement dans lequel la fonction de sûreté est sollicitée) conformément aux CEI 60780 et CEI 60980.

2 Références normatives

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

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

CEI 60780:1998, *Centrales nucléaires – Equipements électriques de sûreté – Qualification*

CEI 60880:2006, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

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

CEI 60987:2007, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés*

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

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

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

CEI 62340:2007, *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)*

Guide de sûreté de l'AIEA NS-G-1.3:2002, *Système d'instrumentation et de contrôle-commande importants pour la sûreté des centrales nucléaires*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de la CEI 60880, du glossaire de sûreté et du guide de sûreté NS-G-1.3 de l'AIEA, ainsi que les définitions suivantes s'appliquent.

3.1
canal de communication
connexion logique entre deux points terminaux au sein d'un système de communication

[CEI 61784-3, 2007]

3.2
nœud de communication
point de connexion d'un réseau de communication, auquel sont envoyés les données véhiculées par les canaux de communication, à ce point ou à partir de ce point vers d'autres points du réseau

3.3
système de communication
ensemble formé de matériel, de logiciel et de moyen de transmission pour permettre le transfert de message (couche application de l'ISO/CEI 7498) d'une application vers une autre

[CEI 61784-3, 2007]

3.4
communication de données
échange de données entre nœuds de communication par les canaux de communication

3.5
équipement de communication de données
parties d'un appareil connecté par bus, liée au support de communication, à la modulation et au codage, y compris la partie basse de la couche physique dans l'appareil

[CEI 61784-3, 2007, modifiée]

3.6
message
série ordonnée de groupe de bits, utilisée pour transmettre de l'information

[CEI 61784-3, 2007, modifiée]

3.7
protocole
convention portant sur le format des données, les séquences temporelles, et la correction d'erreur lors de l'échange des données dans les systèmes de communication

[CEI 61158-3-19, 2007]

3.8
unité de traitement
pour cette norme particulière traitant de communication, un ou plusieurs processeurs dont les instructions sont spécialisées dans le domaine de la gestion réseau ou dans celui des fonctions liées à la communication

4 Symboles et abréviations

DCC Défaillance de cause commune

CEM Compatibilité electromagnétique

AMDE Analyse des modes de défaillance et de leurs effets

I&C Instrumentation et contrôle-commande

AQ Assurance qualité

5 Exigences générales

5.1 Principes de sélection des équipements et des techniques de communication de données

Les équipements de communication doivent satisfaire aux exigences applicables aux systèmes réalisant des fonctions de catégorie A.

NOTE Pour garantir qu'on puisse accepter l'emploi d'équipement et de techniques de communication dans le cadre d'application nucléaire, il convient d'appliquer pour leur sélection un des principes suivant:

- utilisation de protocoles présentant des caractéristiques de sûreté;
- utilisation de protocoles répondant à des normes industrielles auxquels ont été ajoutées des couches de sûreté;
- utilisation de protocoles dont les couches supérieures présentant des fonctionnalités non sûres ou non nécessaires ont été retirées ou remplacées par d'autres avec des fonctionnalités limitées et sûres.

Le matériel et le logiciel doivent être qualifiés, voir l'Article 9.

5.2 Exigences fonctionnelles

Généralement chaque canal de communication de données est une partie d'un système global assurant des services de collecte et de présentation de l'information, de régulation et de protection de la centrale nucléaire de puissance.

Les équipements produisant cycliquement des données sur les canaux de communication ne doivent pas être dépendants de la réception de messages d'acquittement du destinataire dans le cadre d'un fonctionnement continu.

L'allocation des canaux de communication ne doit pas se faire dynamiquement lorsque le système est en fonctionnement mais doit être statique et avoir été prédéfinie lors de la conception.

Tous les messages des logiciels d'application doivent être transmis périodiquement et en un temps de variation du cycle prédéfini.

Il convient que les messages aient une longueur fixe prédéfinie lors de la conception.

Le système de communication doit permettre que les messages des appareils ou des équipements périphériques utilisant les canaux de communication soient envoyés et reçus de façon ordonnée dans un intervalle de temps spécifié, avec l'information de l'état de l'intégrité des données (le cas échéant).

La topologie du réseau de communication des données et le contrôle d'accès aux médias doivent être conçus et mis en œuvre de façon à éviter les DCC dans les systèmes ou sous systèmes indépendants (voir 8.3).

Les données peuvent être distribuées par des systèmes redondants de communication de données pour permettre la continuité du fonctionnement en cas d'endommagement d'un des systèmes.

Les menaces portant sur la sécurité liées à la communication des données doivent être prises en considération dans le cadre des plans de sécurité conformément à la CEI 61513.

5.3 Exigences de performance

Les performances associées aux canaux de communication des données doivent être suffisantes pour garantir que tout message envoyé par un nœud de communication est reçu par le bon destinataire dans un laps de temps correct.

La communication de données doit satisfaire aux exigences des fonctions. Les mécanismes et protocoles utilisés doivent garantir que tout retard survenant dans la communication ou lors de l'accès aux équipements de communication est connu et borné par la conception.

Les canaux de communication doivent être vérifiés de façon qu'ils satisfassent aux exigences spécifiées portant sur le temps de réponse réel des fonctions de catégorie A dans les pires des conditions plausibles. Le temps de réponse réel exigé et les pires conditions doivent être justifiés par analyse. Des communications de type déterministe doivent être utilisées pour que les charges de communication ne varient pas par rapport aux conditions de la centrale.

Lorsqu'un équipement de communication est employé pour la commande manuelle de la centrale et la remontée d'information en salle de commande, il convient que le laps de temps séparant le basculement physique du commutateur ou le déclenchement de la commande logiciel et la confirmation de l'action par indication du changement d'état en salle de commande soit évalué pour des circonstances probables couvrant les conditions correspondant aux pires cas.

5.4 Détection des défaillances

Les défaillances matériel des équipements de communication doivent être détectées et signalées. Les défaillances détectées des équipements de communication qui ont pour conséquence une dégradation inacceptable des fonctions de sûreté nucléaire du système d'I&C doivent être signalées aux opérateurs en salles de commande.

La communication de données, y compris le fonctionnement des mécanismes de réponse aux erreurs (le cas échéant) doit être vérifiée et validée avant toute utilisation en exploitation de l'équipement pour réaliser des fonctions de catégorie A.

5.5 Communication entre voies

La communication des données au sein d'une voie séparée (train) doit être protégée des influences adverses provenant de l'extérieur de la voie. Ainsi les messages d'une voie doivent transiter directement du nœud de communication émetteur au nœud récepteur sans intervention d'équipement de communication externe à la voie.

La communication de données au sein d'une voie doit être séparée des autres voies.

Cependant la communication entre les voies peut être acceptable si elle est nécessaire à des logiques de vote.

5.6 Interfaces avec les systèmes d'une importance de sûreté moindre

Les équipements de communication des systèmes réalisant des fonctions de catégorie A doivent être adéquatement séparés des équipements de communication des systèmes réalisant seulement des fonctions de catégories inférieures.

Lorsque des systèmes de la centrale de différentes catégories de sûreté ont besoin de communiquer par les canaux de communication, alors il convient que la transmission de données soit orientée à partir des fonctions de catégorie A vers les fonctions de catégories inférieures.

Il convient d'empêcher la transmission de données des catégories inférieures vers la catégorie A à moins que la conception des canaux de communication soit telle que les fonctions de catégorie A ne puissent être mises en péril par de telles connexions..

6 Isolement et séparation physique

6.1 Isolement électrique

L'isolement électrique des systèmes réalisant des fonctions de catégorie A connectés au travers de canaux de communication à d'autres systèmes doit être pris en compte conformément à la CEI 60709. Le niveau d'isolement électrique dépend des tensions d'alimentations employées sur la centrale, des pratiques nationales et des exigences propres à la centrale.

NOTE Une méthode pour obtenir un haut niveau d'isolement électrique consiste à utiliser des connexions par fibre optique ou des coupleurs optoélectroniques.

On doit démontrer que l'isolement entre les équipements de communication de données et les équipements connectés est approprié. Ceci doit être suffisant pour éviter que les défaillances des équipements et câbles connectés n'aient un impact dommageable sur le fonctionnement des équipements de communication de données. Les équipements connectés comprennent les capteurs, les relais de contact, les alimentations électriques et les autres équipements de communication.

6.2 Séparation physique

Il convient de concevoir les équipements de communication pour que les pannes ne se propagent pas d'une partie d'un équipement à une autre, ou à un autre système. La norme CEI 60709 fournit des exigences pour cela et plus particulièrement pour les communications à partir d'équipements réalisant des fonctions d'une catégorie à des équipements réalisant des fonctions d'une autre catégorie.

Les exigences de la CEI 60709 doivent être appliquées aux câbles des canaux de communication importants pour la sûreté.

Il convient que la méthode préférée de protection et de séparation physique des câbles des canaux de communication qui transportent des signaux électriques ou optiques, soit l'utilisation d'armoires, de tableaux ou de goulottes dédiés assurant une protection adéquate contre les risques.

Un système peut avoir besoin de chemins redondants de communication, qui peuvent être nécessaires pour assurer la redondance en cas de risque tel que l'incendie qui peut toucher une zone localisée. Les équipements redondants assurant la protection contre de tels risques physiques doivent être séparés physiquement.

NOTE Les exigences pour faire face aux défaillances de cause commune sont fournies par la CEI 62340.

7 Indépendance fonctionnelle

Afin d'assurer la réception et l'émission de données en provenance et à destination des unités de traitement séparées, il convient de mettre en oeuvre des modules logiciel qui possèdent des interfaces propres avec le réseau de communication et avec le logiciel système et le logiciel d'application des unités de traitement concernées, pour éviter la propagation des pannes.

Il convient que des modules logiciel différents de ceux employés pour la vérification des messages et des données transmises, soient utilisés au niveau de la conception pour les opérations numériques et logiques réalisées sur le contenu des messages et des signaux. Ceci limitera la complexité et simplifiera la vérification et la validation.

8 Fiabilité

8.1 Auto-surveillance et limitation des conséquences des défaillances

8.1.1 Détection des erreurs de communication

Les équipements de communication doivent vérifier l'intégrité des données transmises pour confirmer que la transmission était correcte, ou signaler/enregistrer les défaillances de transmission.

Les équipements de communication doivent offrir des fonctionnalités de détection d'erreur conformément aux exigences pertinentes de 4.2 d) de la CEI 60987 et de 4.8 de la CEI 60880. Ces dispositifs doivent permettre d'assurer de façon appropriée que les erreurs seront détectées pour que les données erronées n'affectent pas les performances des fonctions de catégorie A. En particulier, il convient que ceci couvre:

a) l'insertion par erreur d'un bit isolé ou d'un groupe de bits dans un message transmis,

b) la corruption de bits dans un message transmis,

c) la transmission de données périmées,

d) perte de message.

8.1.2 Réponse aux défaillances

Les systèmes d'I&C réalisant des fonctions de catégorie A doivent déclencher des actions appropriées, lorsque des pannes de communication sont détectées.

Lorsque des défaillances d'équipements de communication sont détectées, il convient de prendre les mesures automatiques appropriées, par exemple:

a) isolement des canaux de communication en défaut,

b) indication de l'équipement défaillant pour alerter les opérateurs de la défaillance (voir aussi 5.4).

Les actions à déclencher suite à la détection des défaillances doivent être spécifiées, par exemple, compte-rendu, alerte de l'équipe de maintenance, alarme pour le déclenchement immédiat d'une action corrective ou de limitation.

Au titre du processus de justification de la conception, les équipements et les processus de communication de données doivent être systématiquement analysés en utilisant des méthodes appropriées, par exemple des AMDE en prenant en compte les conséquences des défaillances sur les fonctions de catégorie A.

Les défaillances ou les disfonctionnements d'un simple nœud de communication ne doivent pas avoir d'impact notable sur la disponibilité et la fiabilité du système d'I&C.

L'effet potentiel sur les performances des fonctions de catégorie A des défaillances de tout nœud ou de tout canal de communication doit être pris en compte au niveau du processus de conception, et cette analyse doit être documentée. Toute action que le système doit nécessairement réaliser lors de la détection de la défaillance doit être définie, par exemple enregistrer la défaillance, produire une alarme ou amener la centrale dans un état sûr.

Il convient que les canaux de communication tolère les « petites » erreurs telle que la perte d'un message ou une erreur dans un simple message, considérant que la fréquence de telles erreurs n'est pas suffisamment élevée pour mettre en péril les performances des fonctions de catégorie A; il convient que de telles erreurs n'entraînent pas l'arrêt d'un canal de communication, mais que ces erreurs soient enregistrées par le système.

8.2 Essais

Les exigences pertinentes de la CEI 60987, Article 10, portant sur les essais, doivent être appliquées aux canaux de communication de classe 1. De plus, les paragraphes pertinents 7.10 (aptitude aux essais), 7.11 (inhibition en exploitation) et 7.12 (contrôle d'accès aux équipements du système de protection) du guide de sûreté NS-G-1.3 doivent être appliqués aux canaux de communication des systèmes réalisant des fonctions de catégorie A.

Les performances des fonctions de communication de données doivent être vérifiées avant que l'équipement soit mis en service opérationnel courant. Les aspects des fonctionnalités système suivant doivent être couverts:

a) traitement des erreurs de transmission,

b) fonctionnement correct avec le taux de transfert de données maximal.

Les CEI 60880 et CEI 60987 exigent que les systèmes de communication de données présentent des fonctionnalités d'auto-surveillance, voir 8.1. Il convient que l'on puisse réaliser des essais périodiques complémentaires de la fonctionnalité d'auto-surveillance pendant la durée de vie de l'équipement tels que nécessaires pour réduire la probabilité de présence de défaillances matériel non révélées compromettant les performances des fonctions de catégorie A, par exemple:

1) altération de l'état ou de la valeur de signaux, et surveillance de celle-ci au niveau de l'équipement récepteur;

2) interruption de la transmission et confirmation que l'équipement récepteur détectera celle-ci et réagira correctement.

NOTE On peut considérer au niveau sûreté nucléaire que de tels essais ne sont pas souhaitables pour des tranches en puissance.

Les équipements de communication doivent être qualifiés pour une utilisation en exploitation par des essais fonctionnels conformément aux paragraphes 4.79 à 4.96 du guide de sûreté NS-G-1.3 de l'AIEA. Les essais des modules des équipements doivent être réalisés durant les

recettes usine ou durant les essais de mise en service sur le site, ou les preuves d'essais de type réalisés précédemment conformément à 5.3 de la CEI 60780, doivent être apportées.

8.3 Prévention des défaillances (y compris les DCC)

Les équipements de communication peuvent être affectés par des conditions qui entraînent la défaillance de plusieurs parties redondantes du système au même moment. De façon à limiter ou à éliminer la possibilité de défaillances simultanées de plusieurs modules suite à l'apparition des risques auxquels le système doit survivre, on doit prendre en compte les risques potentiels suivant:

- les perturbations sismiques et les autres risques externes pertinents;
- l'incendie, les entrées de fumée ou l'inondation des zones d'installation des équipements et des câbles;
- la perte du contrôle d'ambiance, du chauffage et de la ventilation;
- un niveau de rayonnement excessif ou d'autres facteurs externes à l'équipement, et
- les facteurs internes à l'équipement lui-même.

Les chemins de câbles qui contiennent les câbles utilisés pour la communication des données entre les redondances de voies doivent être conçus et séparés conformément aux exigences de la CEI 60709, de façon à limiter les risques possibles, et pour que les exigences de tolérance aux défaillances de l'ensemble du système d'I&C soient satisfaites.

La communication des données doit être conçue pour éviter la propagation des défaillances, par exemple par les mécanismes de synchronisation ou par le transfert de données corrompues, voir 7.4 de la CEI 62340.

Les défaillances possibles prises en compte et les fonctionnalités déclarées mises en place pour cela doivent être analysées et documentées.

NOTE Les exigences pour faire face aux défaillances de cause commune sont fournies par la CEI 62340.

9 Qualification

Le matériel des systèmes de communication de classe 1 doit être qualifié conformément aux exigences pertinentes de la CEI 60780 (qualification d'ambiance), de la CEI 60980 (qualification aux séismes, s'il est nécessaire de qualifier les équipements par rapport aux séismes) et des normes CEM adaptées telles que la CEI 62003 ou la série CEI 61000 (essais CEM).

Il convient de concevoir, vérifier et valider le logiciel de communication de système réalisant des fonctions de catégorie A conformément aux normes du nucléaire (par exemple la CEI 60880) ou à d'autres normes adaptées (par exemple la série CEI 61508). Le fait que les normes de qualification choisies soient adaptées doit être analysé et justifié dans une documentation formalisée.

10 Maintenance et modification

Le matériel et le logiciel de communication des systèmes réalisant des fonctions de catégorie A doivent être maintenus et modifiés conformément aux CEI 61513, CEI 60880 et CEI 60987.

Si un des nœuds de communication est défaillant, il convient qu'un remplacement rapide de la partie en cause soit possible centrale en puissance. Il convient que le remplacement d'un nœud de communication puisse être réalisé de façon simple sans porter atteinte au caractère opérationnel du système et en respectant les objectifs de disponibilité du système.

Les modifications des équipements de communication de données doivent être réalisées en suivant les procédures rigoureuses employées pour les modifications du procédé de la centrale.

Les modifications doivent reposer sur des exigences claires. Ces modifications doivent être confirmées par rapport aux exigences d'origine en matière de sûreté, de fonctionnalités et de performances de l'équipement de communication de données et ceci par une vérification appropriée et cohérente avec les CEI 61513, CEI 60880 et CEI 60987 lorsqu'elles sont applicables.

Lorsque les modifications ont été faites, la communication de données doit être mise à l'épreuve par des essais précédant l'installation sur la centrale (par exemple, sur un banc de test représentatif pour ce qui est des essais fonctionnels) et après installation dans le système cible (par exemple, satisfaction des exigences portant sur les interfaces et les performances du systèmes), pour s'assurer qu'elle satisfait à ses exigences fonctionnelles et de performances (voir 8.2).

Bibliographie

CEI 60068 (toutes les parties), *Essais d'environnement*

CEI 60721 (toutes les parties), *Classification des conditions d'environnement*

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

CEI 60965, *Centrales nucléaires de puissance – Salles de commande – Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)*

CEI 61158-3-19, *Industrial communication networks – Fieldbus specifications – Part 3-19: Data-link layer service definition – Type 19 elements* (disponible en anglais seulement)

CEI 61508-1, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 61508-2, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

CEI 61508-3, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels*

CEI 61508-4, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses* (disponible en anglais seulement)

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

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

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

ISO/CEI 7498, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base*

———————

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