IEC 61500

Edition 3.0 2018-04
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

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

IEC 61500:2018-04 RLV(en)

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 It also gives information on projects, replaced and withdrawn publications.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.

IEC 61500

Edition 3.0 2018-04
REDLINE VERSION

INTERNATIONAL STANDARD

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20

ISBN 978-2-8322-5625-1

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS 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.

This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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

This third edition cancels and replaces the second edition published in 2009. This edition constitutes a technical revision.

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

a) the changes introduced to previously referenced standards have been confirmed to apply;
b) relevant newly published standards have been referenced;
c) lessons learned from several industrial applications have been incorporated.

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

FDIS	Report on voting
45A/1183/FDIS	45A/1194/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 stability 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.

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 publication using a colour printer.

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 the safe operation of Nuclear Power Plants (NPP). 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 document 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 documents of the IEC SC 45A standard series ~~is~~ are IEC 61513 and IEC 63046. ~~It~~ IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPP. IEC 63046 provides general requirements for electrical power systems of NPP; 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 ~~of systems~~, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects ~~of computer-based systems~~ 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 45A standard series, corresponds to the Technical Reports which are not normative.

~~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.~~

~~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 standard 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, the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPP, 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 the IEC 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. Also at level 2, 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 requirements 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 will be 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 – DATA COMMUNICATION IN SYSTEMS PERFORMING CATEGORY A FUNCTIONS

1 Scope

This document 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 document is restricted to the consideration of data communication within the plant I&C safety 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 document. This document is not applicable to the internal connections and data communication of a processor unit, its memory and control logic. It does not address the internal processing of instrumentation and control computer based systems.

This document gives requirements for functions and properties of on-line plant data communication by reference to IEC 60880 and IEC 60987, produced within the framework of IEC 61513. It requires ~~classification~~ categorisation 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/IEEE 60780-323 and IEC 60980.

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 60671:2007, *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 60780:1998, *Nuclear power plants – Electrical equipment of the safety system – Qualification*~~

IEC/IEEE 60780-323:2016, *Nuclear facilities – Electrical equipment important to safety – 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 60987:2007/AMD1:2013

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

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

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

IEC 62645:2014, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*

IEC 62859, *Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity*

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

IAEA safety guide No. SSG-39:2016, *Design of instrumentation and control systems for nuclear power plants*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60880, IAEA safety glossary, IAEA safety guide No. ~~NS-G-1.3~~ SSG-39 and the following 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
communication channel
logical connection between two end-points within a communication system

[SOURCE: IEC 61784-3:~~2007~~ 2016, 3.1.8]

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 7498-1 application layer) from one application to another

[SOURCE: IEC 61784-3: ~~2007~~ 2016, 3.1.9]

3.4
cybersecurity
set of activities and measures the objective of which is to prevent, detect, and react to:

– malicious disclosures of information (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation;

– malicious modifications (integrity) of functions that may compromise the delivery or integrity of the required service by I&C programmable digital systems (incl. loss of control) which could lead to an accident, an unsafe situation or plant performance degradation;

– malicious withholding or prevention of access to or communication of information, data or resources (incl. loss of view) that could compromise the delivery of the required service by I&C systems (availability) which could lead to an accident, an unsafe situation or plant performance degradation

Note 1 to entry: This definition is tailored with respect to the IEC 62645 scope and overall IEC SC 45A document structure. It is recognized that the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors and protection against natural disasters. Those aspects – except human errors degrading cybersecurity – are not included in the concept of cybersecurity used in the IEC SC 45A standard series. See Annex A of IEC 62645:2014 for more detail about such exclusions.

Note 2 to entry: Computer security, security and cybersecurity are considered synonymous in this document.

[SOURCE: IEC 62645:2014, 3.6, modified: "disclosures" replaced by "malicious disclosures", and notes 1 and 2 modified]

3.5
data communication
exchange of digital data between communication nodes via communication channels

3.6
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

[SOURCE: ~~IEC 61784-3, 2007~~ IEC 61158-2, 2014, 3.1.9, modified:"fieldbus" replaced by "bus"]

3.7
division
collection of items, including their interconnections, that form one redundancy of a redundant system or safety group. Divisions may include multiple channels

[SOURCE: IAEA SSG-39, 2016]

3.8
message
ordered series of digital states in defined groups, used to convey information

[SOURCE: IEC 61784-3:~~2007~~ 2016, 3.1.26, modified:"octets" replaced by "digital states in defined groups"]

3.9
protocol
convention about the data formats, time sequences, and error correction in the data exchange of communication systems

[SOURCE: IEC 61158-3-19:~~2007~~ 2014, 3.3.29]

~~**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 abbreviated terms

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 communication 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~~ shall 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 do it in a cyclic way that is not dependent on the receipt of acknowledge messages from the receiver for continued operation.

Communication channels including the memory mapping and allocation for sending/receiving data shall not be allocated dynamically during the run time of the system but shall be statically allocated and predefined by design.

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

Messages should have a 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)~~ provide communication channels for data exchange with instruments and other equipment allowing transfer within a specified time frame.

Messages should have data integrity information.

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~~ fails.

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~~ IEC 62645.

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~~ within a predefined maximum period.

Data communication shall meet the performance requirements in terms of response time and data capacity which result from the ~~functions~~ functional requirements and the architectural design of the I&C systems. 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 specified values of the required real time response and the worst-case conditions shall be justified by analysis. Deterministic communication shall be used so that the communication 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.

For monitoring functions and manually initiated functions that are needed in accident conditions to bring the plant back into a safe state, the worst-case time response and limited usage of resources shall be justified by analysis.

~~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.~~

5.4 Communication within and between 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~~ any 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~~ for voting logic.

5.5 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 performing functions 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 only.

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

If communication equipment of systems performing category A functions is interfaced to systems of lower importance to safety then cybersecurity measures shall be applied in accordance with IEC 62645 and IEC 62859.

6 Electrical isolation and physical separation

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.

NOTE 1 The degree of electrical isolation will depend on the station power supply voltages present, national practice, and plant-specific requirements.

NOTE 2 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 addressed in ~~IEC 62340~~ 8.3.

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.~~

The requirements below are intended to inhibit fault propagation:

a) Independent processing modules shall be designed so that they continue operation even if a communication partner fails.

NOTE 1 This implies use of measures such as the avoidance of handshake.

b) Processing modules shall provide separate communication interfaces for independent communication links.

The design should use separate software modules for processing of application data and for communication handling.

NOTE 2 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 should incorporate self-monitoring features. Detected failures shall be signalled to the control room. 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~~ 6.2 of IEC 60880:2006 or 8.3.9 of IEC 62566:2012. These facilities shall provide appropriate assurance that data communication ~~errors~~ failures will be detected so that ~~erroneous~~ faulty 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 (relating to either a valid or unknown / unexpected source),

b) corruption of bits of the transmitted message,

c) transmission of out-of-date data (arising from unintended repetition of an old message),

d) message loss,

e) incorrectly addressed message,

f) unacceptable message delay,

g) incorrect message sequence.

8.1.2 Response to failure

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

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 the control rooms.

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~~ verification 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~~ impact of the failure of any communication node on the performance of category A functions or channels 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~~ to transient faults, such as a missed message or a soft error in a single message, provided the frequency of such ~~errors~~ faults is not high enough to compromise the performance of category A functions; such ~~'soft' errors~~ transient faults should not lead to the shutdown of a channel, but they should be logged by the system.

8.2 Testing

~~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 relevant surveillance testing requirements of IEC 60987:2007, Clause 11, and IEC 60671 shall apply to class 1 communication channels. Also, the relevant subclauses 7.35 to 7.38 (protection system – operational bypasses) and 6.153 to 6.158 (control of access to systems

important to safety) of IAEA safety standard SSG-39:2016 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 data communication including operation of fault handling features shall be verified and validated prior to operational use of the equipment to perform category A functions. 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, IEC 60987 and IEC 62566 require that the data communication system shall have self-test capabilities (see 8.1.1). 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.

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

d) 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 of the plant.

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~~ subclauses 6.78, 6.79 and 6.92 of IAEA safety standard SSG-39:2016. 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~~ 7.4.1 of IEC/IEEE 60780-323:2016 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:

a) seismic disturbance or other relevant external hazards;

b) fire, smoke or flooding in equipment or cable areas;

c) loss of environmental control, heating and ventilation;

d) excessive radiation or other factors external to the equipment, and

e) 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 62340:2007, 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.

8.4 Cybersecurity

Data communication shall be planned, designed, implemented and operated in accordance with IEC 62645 and IEC 62859 through the whole lifecycle of their security features.

9 Qualification

Class 1 communication hardware of systems shall be qualified in accordance with the relevant requirements of IEC/IEEE 60780-323 (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 systems performing category A functions ~~should~~ shall be designed, verified and validated in accordance with nuclear standards ~~(e.g. IEC 60880) or other appropriate standards (e.g. IEC 61508 series)~~ IEC 61513, IEC 60880, IEC 60987, IEC 62645 and IEC 62566. 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, IEC 60987, IEC 62645 and IEC 62566.

If one of the communication nodes fails, prompt replacement of a part should be possible ~~at~~ during power operation of the plant. 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. In such cases, means shall be provided to confirm the correct operation of the replacement node.

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, IEC 60987, IEC 62645 and IEC 62566 ~~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~~ room 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 61226, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

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 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

~~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*

IEC TR 62987, *Nuclear power plants – Instrumentation and control systems important to safety – Use of Failure Mode and Effects Analysis (FMEA) and related methods to support the justification of systems*

ISO/IEC 7498 (all parts), *Information ~~processing systems~~ technology – Open Systems Interconnection – Basic reference model*

IEC 61500

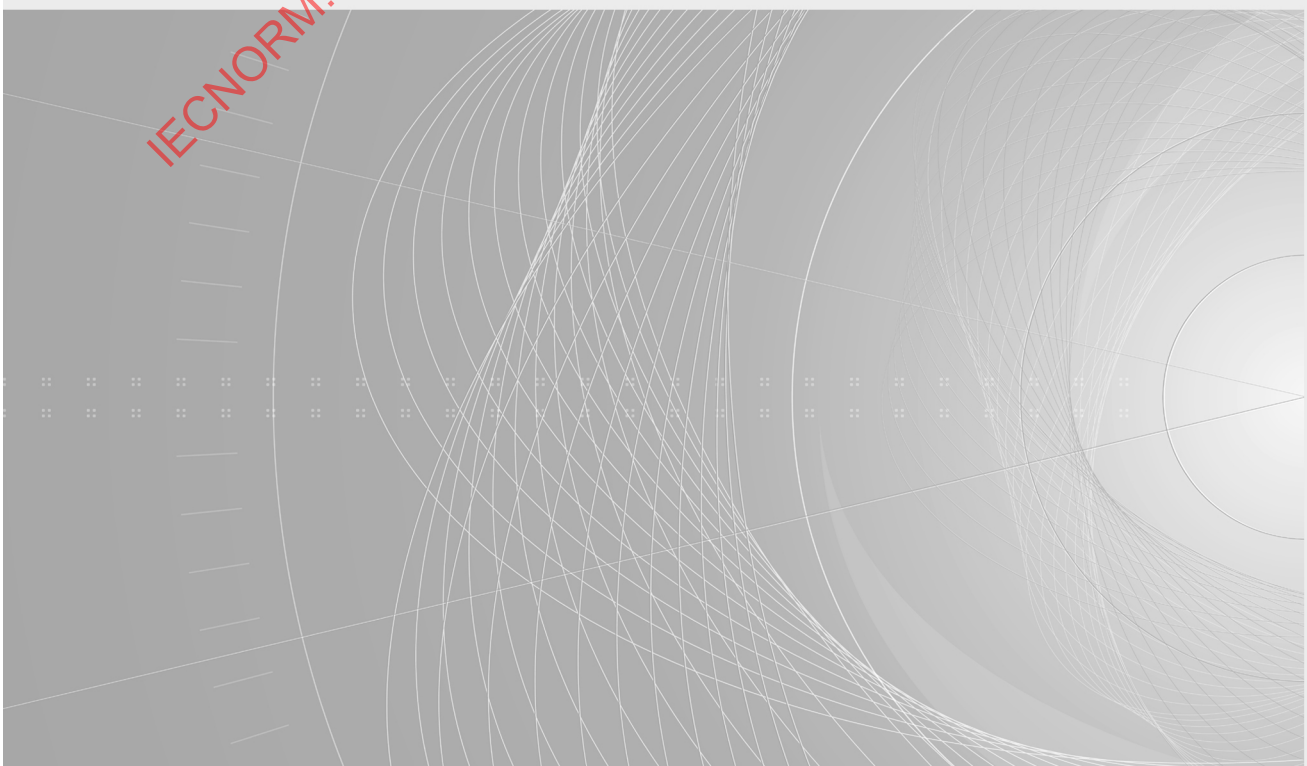
Edition 3.0 2018-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Communications de données dans les systèmes réalisant des fonctions de catégorie A



IEC 61500:2018-04(en-fr)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS 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, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This third edition cancels and replaces the second edition published in 2009. This edition constitutes a technical revision.

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

a) the changes introduced to previously referenced standards have been confirmed to apply;
b) relevant newly published standards have been referenced;
c) lessons learned from several industrial applications have been incorporated.

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

FDIS	Report on voting
45A/1183/FDIS	45A/1194/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 stability 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 the safe operation of Nuclear Power Plants (NPP). 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 document 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 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 NPP. IEC 63046 provides general requirements for electrical power systems of NPP; 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, defence 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 45A standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standard 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, the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPP, 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 the IEC 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. Also at level 2, 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 requirements 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 will be 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 – DATA COMMUNICATION IN SYSTEMS PERFORMING CATEGORY A FUNCTIONS

1 Scope

This document 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 document is restricted to the consideration of data communication within the plant I&C safety 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 document. This document is not applicable to the internal connections and data communication of a processor unit, its memory and control logic. It does not address the internal processing of instrumentation and control computer based systems.

This document gives requirements for functions and properties of on-line plant data communication by reference to IEC 60880 and IEC 60987, produced within the framework of IEC 61513. It requires categorisation 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/IEEE 60780-323 and IEC 60980.

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 60671:2007, *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 60780-323:2016, *Nuclear facilities – Electrical equipment important to safety – 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 60987:2007/AMD1:2013

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

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

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

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

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

IEC 62645:2014, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*

IEC 62859, *Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity*

IAEA safety guide No. SSG-39:2016, *Design of instrumentation and control systems for nuclear power plants*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60880, IAEA safety glossary, IAEA safety guide No. SSG-39 and the following 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
communication channel
logical connection between two end-points within a communication system

[SOURCE: IEC 61784-3:2016, 3.1.8]

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 7498-1 application layer) from one application to another

[SOURCE: IEC 61784-3:2016, 3.1.9]

3.4
cybersecurity
set of activities and measures the objective of which is to prevent, detect, and react to:

– malicious disclosures of information (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation;

– malicious modifications (integrity) of functions that may compromise the delivery or integrity of the required service by I&C programmable digital systems (incl. loss of control) which could lead to an accident, an unsafe situation or plant performance degradation;

– malicious withholding or prevention of access to or communication of information, data or resources (incl. loss of view) that could compromise the delivery of the required service by I&C systems (availability) which could lead to an accident, an unsafe situation or plant performance degradation

Note 1 to entry: This definition is tailored with respect to the IEC 62645 scope and overall IEC SC 45A document structure. It is recognized that the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors and protection against natural disasters. Those aspects – except human errors degrading cybersecurity – are not included in the concept of cybersecurity used in the IEC SC 45A standard series. See Annex A of IEC 62645:2014 for more detail about such exclusions.

Note 2 to entry: Computer security, security and cybersecurity are considered synonymous in this document.

[SOURCE: IEC 62645:2014, 3.6, modified: "disclosures" replaced by "malicious disclosures", and notes 1 and 2 modified]

3.5
data communication
exchange of digital data between communication nodes via communication channels

3.6
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

[SOURCE: IEC 61158-2, 2014, 3.1.9, modified:"fieldbus" replaced by "bus"]

3.7
division
collection of items, including their interconnections, that form one redundancy of a redundant system or safety group. Divisions may include multiple channels

[SOURCE: IAEA SSG-39, 2016]

3.8
message
ordered series of digital states in defined groups, used to convey information

[SOURCE: IEC 61784-3:2016, 3.1.26, modified:"octets" replaced by "digital states in defined groups"]

3.9
protocol
convention about the data formats, time sequences, and error correction in the data exchange of communication systems

[SOURCE: IEC 61158-3-19:2014, 3.3.29]

4 Symbols and abbreviated terms

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 communication equipment shall meet requirements for systems performing category A functions.

To ensure acceptability for nuclear applications one of the following principles for selection of data communication techniques and equipment shall 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 data over a communication channel shall do it in a cyclic way that is not dependent on the receipt of acknowledge messages from the receiver for continued operation.

Communication channels including the memory mapping and allocation for sending/receiving data shall not be allocated dynamically during the run time of the system but shall be statically allocated and predefined by design.

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

Messages should have a fixed length predefined by design.

The communication system shall provide communication channels for data exchange with instruments and other equipment allowing transfer within a specified time frame.

Messages should have data integrity information.

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 fails.

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 62645.

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 within a predefined maximum period.

Data communication shall meet the performance requirements in terms of response time and data capacity which result from the functional requirements and the architectural design of the I&C systems. 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 specified values of the required real time response and the worst-case conditions shall be justified by analysis. Deterministic communication shall be used so that the communication 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.

For monitoring functions and manually initiated functions that are needed in accident conditions to bring the plant back into a safe state, the worst-case time response and limited usage of resources shall be justified by analysis.

5.4 Communication within and between 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 any communication equipment outside the division.

Data communication in a division shall be separated from the other divisions. However, communication between divisions may be acceptable for voting logic.

5.5 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 performing functions 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 only.

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

If communication equipment of systems performing category A functions is interfaced to systems of lower importance to safety then cybersecurity measures shall be applied in accordance with IEC 62645 and IEC 62859.

6 Electrical isolation and physical separation

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.

NOTE 1 The degree of electrical isolation will depend on the station power supply voltages present, national practice, and plant-specific requirements.

NOTE 2 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. 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 addressed in 8.3.

7 Functional independence

The requirements below are intended to inhibit fault propagation:

a) Independent processing modules shall be designed so that they continue operation even if a communication partner fails.

   NOTE 1 This implies use of measures such as the avoidance of handshake.

b) Processing modules shall provide separate communication interfaces for independent communication links.

The design should use separate software modules for processing of application data and for communication handling.

NOTE 2 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 should incorporate self-monitoring features. Detected failures shall be signalled to the control room. 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 6.2 of IEC 60880:2006 or 8.3.9 of IEC 62566:2012. These facilities shall provide appropriate assurance that data communication failures will be detected so that faulty 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 (relating to either a valid or unknown / unexpected source),
b) corruption of bits of the transmitted message,
c) transmission of out-of-date data (arising from unintended repetition of an old message),
d) message loss,
e) incorrectly addressed message,
f) unacceptable message delay,
g) incorrect message sequence.

8.1.2 Response to failure

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

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 the control rooms.

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.

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 verification 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 of the I&C system.

The potential impact of the failure of any communication node on the performance of category A functions or channels 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 to transient faults, such as a missed message or a soft error in a single message, provided the frequency of such faults is not high enough to compromise the performance of category A functions; such transient faults should not lead to the shutdown of a channel, but they should be logged by the system.

8.2 Testing

The relevant surveillance testing requirements of IEC 60987:2007, Clause 11, and IEC 60671 shall apply to class 1 communication channels. Also, the relevant subclauses 7.35 to 7.38 (protection system – operational bypasses) and 6.153 to 6.158 (control of access to systems important to safety) of IAEA safety standard SSG-39:2016 shall apply to communication channels of systems performing category A functions.

The data communication including operation of fault handling features shall be verified and validated prior to operational use of the equipment to perform category A functions. 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, IEC 60987 and IEC 62566 require that the data communication system shall have self-test capabilities (see 8.1.1). 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.

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

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

Nuclear safety considerations may make such testing undesirable at power operation of the plant.

The communication equipment shall be qualified for operational use by functional testing in accordance with subclauses 6.78, 6.79 and 6.92 of IAEA safety standard SSG-39:2016. 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 7.4.1 of IEC/IEEE 60780-323:2016 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:

a) seismic disturbance or other relevant external hazards;

b) fire, smoke or flooding in equipment or cable areas;

c) loss of environmental control, heating and ventilation;

d) excessive radiation or other factors external to the equipment, and

e) 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 62340:2007, 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.

8.4 Cybersecurity

Data communication shall be planned, designed, implemented and operated in accordance with IEC 62645 and IEC 62859 through the whole lifecycle of their security features.

9 Qualification

Class 1 communication hardware of systems shall be qualified in accordance with the relevant requirements of IEC/IEEE 60780-323 (environmental qualification), IEC 60980 (seismic qualification), and an appropriate EMC Standard such as IEC 62003 or the IEC 61000 series (EMC Testing).

Communication of systems performing category A functions shall be designed, verified and validated in accordance with nuclear standards IEC 61513, IEC 60880, IEC 60987, IEC 62645 and IEC 62566. The suitability of the selected qualification standard shall be analysed and justified by formal documentation.

10 Maintenance and modification

Communication of systems performing category A functions shall be maintained and modified in accordance with IEC 61513, IEC 60880, IEC 60987, IEC 62645 and IEC 62566.

If one of the communication nodes fails, prompt replacement of a part should be possible during power operation of the plant. 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. In such cases, means shall be provided to confirm the correct operation of the replacement node.

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, IEC 60987, IEC 62645 and IEC 62566.

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

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 61784-2, *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

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*

IEC TR 62987, *Nuclear power plants – Instrumentation and control systems important to safety – Use of Failure Mode and Effects Analysis (FMEA) and related methods to support the justification of systems*

ISO/IEC 7498 (all parts), *Information technology – Open Systems Interconnection – Basic reference model*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

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 61500 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 troisième édition annule et remplace la seconde édition publiée en 2009. Cette édition constitue une révision technique.

Les principales modifications techniques par rapport à l'édition précédente sont les suivantes:

a) les modifications introduites dans les normes précédemment référencées sont applicables;
b) des normes pertinentes récemment publiées sont référencées;

c) le retour d'expérience obtenu au niveau de plusieurs applications industrielles a été pris en compte.

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

FDIS	Rapport de vote
45A/1183/FDIS	45A/1194/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.

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 termes 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 œuvre des systèmes d'instrumentation et de contrôle commande importants pour la sûreté utilisés dans les centrales nucléaires de puissance.

L'objectif de ce document est d'être utilisé 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 collection de normes du SC 45A de l'IEC

L'IEC 61500 est le document du SC 45A de l'IEC de troisième niveau qui traite du sujet de la communication des données pour les systèmes assurant des fonctions de catégorie A.

L'IEC 61500 doit être lue avec l'IEC 61513 du SC 45A de la IEC 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 IEC 60880 qui fournit des recommandations pour ce qui concerne les aspects logiciels des systèmes réalisant des fonctions de catégorie A et avec la IEC 60987 qui fournit des recommandations pour applicable au matériel des systèmes informatisés.

Pour plus de détails sur la collection de normes du SC 45A de l'IEC, 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 suivant:

- Exigences applicables aux systèmes réalisant des fonctions de catégorie A.
- Exigences applicables à la communication de données entre divisions 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 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 cybersécurité. Elle est élaborée sur 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 du SC 45A de l'IEC a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015 des discussions ont eu lieu au sein du SC 45A de l'IEC pour décider de la façon et de l'endroit pour établir les exigences générales portant sur la conception des systèmes électriques. Les experts du SC 45A de l'IEC 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 – COMMUNICATIONS DE DONNÉES DANS LES SYSTÈMES RÉALISANT DES FONCTIONS DE CATÉGORIE A

1 Domaine d'application

Le présent document 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 du présent document est limité aux systèmes d'instrumentation et de contrôle commande de sûreté 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 de ce document. Ce document n'est pas applicable aux connexions internes et à la communication de données entre les processeurs, leurs mémoires ou les logiques de commande. Il ne concerne pas les traitements internes des systèmes numériques d'instrumentation et de contrôle commande.

Ce document fournit des exigences pour les fonctions et les propriétés afférentes à la communication de données en faisant référence aux IEC 60880 et IEC 60987, qui ont été développées sous couvert de l'IEC 61513. Cela implique que les fonctions de communication soient classées conformément à l'IEC 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 normes IEC/IEEE 60780-323 et IEC 60980.

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 60671:2007, *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 60780-323:2016, *Installations nucléaires – Equipements électriques importants pour la sûreté – Qualification*

IEC 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*