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 It also gives information on projects, replaced and withdrawn publications.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

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~~