IEC 61500

Edition 2.0 2009-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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

IEC 61500:2009

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

About the IEC

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

About IEC publications

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

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 It also gives information on projects, withdrawn and replaced publications.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

A propos de la CEI

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

A propos des publications CEI

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

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

IEC 61500

Edition 2.0 2009-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

P

ICS 27.120.20

ISBN 978-2-88910-523-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

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

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

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

c) Recommendations and limitations regarding the application of the standard

It is important to note that this standard establishes no additional functional requirements for safety systems.

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

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

To ensure that the standard will continue to be relevant in future years, emphasis is placed on principles, rather than on specific technologies.

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

The top-level document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

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

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

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

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

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

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

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

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

1 Scope

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

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

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

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

[IEC 61784-3, 2007]

3.2
communication node

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

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

[IEC 61784-3, 2007]

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

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

[IEC 61784-3, 2007, modified]

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

[IEC 61784-3, 2007, modified]

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

[IEC 61158-3-19, 2007]

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

4 Symbols and abbreviations

CCF Common cause failure

EMC Electromagnetic compatibility

FMEA Failure mode and effects analysis

I&C Instrumentation and control

QA Quality assurance

5 General requirements

5.1 Principles of selection of data communication techniques and equipment

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

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

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

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

5.2 Functional requirements

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

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

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

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

Messages should have fixed length predefined by design.

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

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

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

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

5.3 Performance requirements

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

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

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

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

5.4 Failure detection

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

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

5.5 Communication within division

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

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

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

5.6 Interfaces to systems of lower importance to safety

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

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