IEC 62988

Edition 1.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control systems important to safety – Selection and use of wireless devices

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils sans fil

IEC 62988:2018-05(en-fr)

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

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

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

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

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

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

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

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

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

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

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

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

IEC 62988

Edition 1.0 2018-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control systems important to safety – Selection and use of wireless devices

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils sans fil

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-5655-8

CONTENTS

FOREWORD 3
INTRODUCTION 5
1 Scope 7
2 Normative references 7
3 Terms and definitions 8
4 Symbols and abbreviations 11
5 Fundamental requirements 11
5.1 Safety classification 11
5.2 Physical separation and isolation 11
5.3 Cybersecurity 12
6 Wireless application: system requirements 12
6.1 General 12
6.2 Network architecture 12
6.3 Network performance 12
6.4 Network surveillance and monitoring 12
6.5 Power supply requirements 13
6.6 Physical security 13
6.7 Electromagnetic security 13
7 Device selection: evidence of correctness and device integration 13
7.1 General 13
7.2 Quality assurance 13
7.3 Functional and performance suitability 14
7.4 Integration into the application 14
7.5 Device self-monitoring 14
7.6 Solution preferences 14
8 Radio emissions 14
8.1 Electromagnetic compatibility 14
8.2 Radio coverage requirements 15
8.3 Spectrum management 15
8.3.1 General 15
8.3.2 Flexibility 15
8.3.3 Mobility 16
9 Cybersecurity 16
9.1 General requirements 16
9.2 Wireless-specific requirements 16
9.2.1 Data logging 16
9.2.2 Site topology 16
9.2.3 Connection to a wired network 16
9.2.4 Network surveillance 16
10 Qualification 17
10.1 Hardware qualification 17
10.2 Software qualification 17
11 Documentation 17
Bibliography 18

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SELECTION AND USE OF WIRELESS DEVICES

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 62988 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/1187/FDIS	45A/1198/RVD

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

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

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

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

INTRODUCTION

a) Technical background, main issues and organization of this document

This document sets out requirements applicable to wireless devices that are used to perform functions important to safety in nuclear power plants (NPPs).

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

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

IEC 62988 is a third level IEC SC 45A document covering the selection and use of wireless devices in instrumentation and control (I&C) systems important to safety used in NPPs.

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 this document

It is important to note that this document is applicable to all important to safety systems containing wireless devices, including systems performing category A and B functions (and in such systems, wireless devices are prohibited by this document). Therefore, only systems performing category C functions are required to follow the requirements of this document.

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

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

The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete, coherent et consistent 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 45 standard series, corresponds to the Technical Reports, which are not normative.

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

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SELECTION AND USE OF WIRELESS DEVICES

1 Scope

This document establishes requirements relevant to the selection and use of wireless devices in instrumentation and control (I&C) systems important to safety used in nuclear power plants (NPPs). Those I&C systems may fully consist of wireless devices.

NOTE The word “use” refers to the integration of the device, its qualification, administrative control, and every other activity that may be necessary to use the device in an important to safety application.

This document applies to the I&C of new NPPs and to backfit of I&C in existing NPPs. Every wireless device or wireless system that is important to safety is in the scope of this document. Both fixed and mobile devices and all data types (voice, process data, etc.) are included within the scope if they provide a safety classified function.

This document restricts the use of wireless devices to systems supporting category C functions according to IEC 61226, excluding explicitly their use for categories A and B.

Non-safety devices and systems may use this document as guidelines, for example to ensure that important to safety devices are not disturbed.

– Clause 5 describes the fundamental requirements regarding safety and cybersecurity.
– Clause 6 gives wireless-specific requirements that have to be included in the system design.
– Clause 7 describes the requirements for the selection and integration of wireless devices.
– Clause 8 deals with electromagnetic compatibility and spectrum management.
– Clause 9 gives wireless-specific requirements regarding cybersecurity.
– Clause 10 describes the requirements for the qualification of wireless devices and their environment.

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

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

IEC 61513:2011, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*

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

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

IEC 62671, *Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality*

3 Terms and definitions

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

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

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

3.1
authentication
provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2018, 3.5]

3.2
category of an I&C function
one of three possible safety assignments (A, B, C) of I&C functions resulting from considerations of the safety relevance of the function to be performed. An unclassified assignment may be made if the function has no importance to safety.

Note 1 to entry: See also "class of an I&C system".

Note 2 to entry: IEC 61226 defines categories of I&C functions. To each category there corresponds a set of requirements applicable on both the I&C function (concerning its specification, design, implementation, verification and validation) and the whole chain of items which are necessary to implement the function (concerning the properties and the related qualification) regardless of how these items are distributed in a number of interconnected I&C systems. For more clarity, this document defines categories of I&C functions and classes of I&C systems and establishes a relationship between the category of the function and the minimal required class for the associated systems and equipment.

[SOURCE: IEC 61513:2011, 3.4]

3.3
class of an I&C system
one of three possible assignments (1, 2 or 3) of I&C systems important to safety resulting from consideration of their requirement to implement I&C functions of different safety importance. An unclassified assignment is made if the I&C system does not implement functions important to safety.

Note 1 to entry: See also "category of an I&C function", "safety system".

[SOURCE: IEC 61513:2011, 3.6]

3.4
spectrum management
coexistence management
process to establish and to maintain coexistence that includes technical and organizational measures

[SOURCE: IEC 62657-2:2017, 3.1.15, modified – The preferred term "spectrum management" has been added.]

3.5
cybersecurity
set of activities and measures whose objective is to prevent, detect, and react to digital attacks that have the intent to cause:

- disclosures that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation (confidentiality),
- malicious modifications of functions that may compromise the delivery or integrity of the required service by I&C computer-based and HDL programmed device (CB&HPD) systems (including loss of control) which could lead to an accident, an unsafe situation or plant performance degradation (integrity),
- 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 which could lead to an accident, an unsafe situation or plant performance degradation (availability).

Note 1 to entry: This definition is tailored with respect to the scope of this document, focusing on the prevention of, detection of and reaction to malicious acts by digital means on I&C CB&HPD systems. 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, which are all out of the scope of this document (see Clause 1).

[SOURCE: IEC 62645:2014, 3.6]

3.6
electrical/electronic/programmable electronic item
E/E/PE item
item based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

[SOURCE: IEC 61508-4:2010, 3.3.2, modified]

Note 1 to entry: In this term and its definitions, the word “item” can be replaced by the words: system or equipment or device.

3.7
encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e. to hide the information content of the data

[SOURCE: ISO/IEC 18033-1:2015, 2.21]

3.8
access point
gateway
network device containing at least one host interface such as serial or Ethernet, acting as ingress or an egress point enabling communication between host applications and wireless devices

[SOURCE: IEC 62591:2016, 3.2.47, modified – The preferred term "access point" has been added.]

3.9
I&C system
system, based on E/E/PE items, performing plant I&C functions as well as service and monitoring functions related to the operation of the system itself.

Note 1 to entry: The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices. The different functions within a system may use dedicated or shared resources.

Note 2 to entry: The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

Note 3 to entry: See also the definition of E/E/PE item and the associated notes.

Note 4 to entry: According to their typical functionality, IAEA distinguishes between automation/control systems, HMI systems, interlock systems and protection systems.

3.10
item important to safety
item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public

Note 1 to entry: Items important to safety include:

a) those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of the site personnel or members of the public;

b) those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions;

c) those features which are provided to mitigate the consequences of malfunction or failure of structures, systems or components.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.11
latency
time it takes for a packet to cross a network connection, from sender to receiver

[SOURCE: IEC 62591:2016, 3.2.57]

3.12
mesh network
network topology in which redundant physically-diverse routing paths are available between each pair of network nodes

Note 1 to entry: Wireless mesh topology is usable to extend coverage via multi-hop capability and/or to facilitate communication reliability by providing redundant paths between devices.

[SOURCE: IEC 62734:2014, 3.1.2.95, modified – The term "mesh topology" has been replaced by "mesh network".]

3.13
network
series of devices connected by some type of communication medium

[SOURCE: IEC 62591:2016, 3.2.70, modified – In the definition, "nodes" has been replaced by "devices". Note 1 to entry has been deleted.]

3.14
quality assurance
function of a management system that provides confidence that specific requirements will be fulfilled

Note 1 to entry: This definition is compatible with that of ISO 9000:2015, 3.3.6.

[SOURCE: IAEA Safety Glossary, 2016 Edition, modified – The term "quality management" has been replaced by "quality assurance".]

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

[SOURCE: IAEA Safety Glossary, 2016 Edition]

3.16
safety related system
system important to safety that is not part of a safety system

[SOURCE: IAEA Safety Glossary, 2016 Edition]

3.17
safety system
system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the reactor core, or to limit the consequences of anticipated operational occurrences and design basis accidents

[SOURCE: IAEA Safety Glossary, 2016 Edition]

3.18
wireless device
device that is able to establish a wireless communication with another wireless device, that may or may not be part of a wireless network

4 Symbols and abbreviations

CPU central processing unit
DMZ demilitarized zone
EMC electromagnetic compatibility
EMI electromagnetic interference
I&C instrumentation and control
NPP nuclear power plant
RFI radio frequency interference
SRS system requirement specification

5 Fundamental requirements

5.1 Safety classification

The wireless devices shall be limited to use in I&C systems performing category C functions and shall not be used in I&C systems supporting category A and B functions.

The safety class of the wireless communication systems shall be consistent with the I&C category C functions which they support and implement and should be safety class 3.

5.2 Physical separation and isolation

The wireless communication systems shall be electrically isolated and physically separated from wired communication channels of I&C systems supporting category A and B functions.

The wireless communication systems for category C functions shall be designed such that any fault is not propagated to wired communication channels in I&C systems performing category A and B functions.

5.3 Cybersecurity

Wireless communications shall not be used in systems that have been assigned an S1 or S2 security degree according to IEC 62645.

Each network connection with systems with a higher safety class shall be addressed within the overall security plan in order to take adequate measures regarding cybersecurity.

Additional information for cybersecurity can be found in Clause 9.

6 Wireless application: system requirements

6.1 General

The requirements of IEC 61513 shall be met. In particular, a system requirement specification (SRS) shall be written to support the system design.

6.2 Network architecture

Taking into account the intended application and functions of the wireless system, the SRS shall specify and give justification for:

– network topology,
– access point locations,
– network configuration.

Mesh networks should implement load balancing routing algorithms. This means that if several paths are available from node A to node B, the chosen path should avoid overloaded intermediate nodes.

The network routing algorithms should be capable of handling packets/messages with different priorities.

6.3 Network performance

In connection with the intended application, the SRS shall specify and give justification for:

– transmission delay between relevant locations of the network (typical and maximum),
– data transfer speed between relevant locations of the network (typical and minimum).

NOTE 1 IEC 62657-1 provides considerations regarding time behaviour of wireless communication systems, such as transmission time, update time and availability.

The network load should be context-independent. This means that if a monitored event occurs, the network load should not increase.

NOTE 2 A true context-independent design is difficult to achieve, thus a context-independent application layer is sufficient.

6.4 Network surveillance and monitoring

Means shall be provided for surveillance and monitoring of the wireless network. Those means shall be capable of detecting and correcting anomalies within the wireless network.

Data error rate shall be monitored. The SRS shall define the acceptable packet loss rate and state whether or not lost messages shall be resent.

NOTE To suppress the error rate of the communication system within the acceptable range specified by the system design, latency and/or jitter may be also monitored.

It shall be possible to monitor:

– the network status: load, transmission error rate, packet losses, latency;
– the comprehensive list of devices connected to the network;
– the network logs, including failed connections (unauthorized connection attempts, etc.);
– for each device:
  - its self-monitored variables (see 7.5),
  - its characteristics (software version, etc.),
  - its physical location if relevant.

6.5 Power supply requirements

If required by the application, redundant power supplies should be used.

If required by the application, wireless devices should be battery-powered. In that case:

– the SRS shall specify the minimum battery capacity for the intended application,
– remote devices shall be physically accessible in order to be able to replace a defective or discharged battery. If this is not possible, the battery capacity shall be dimensioned to last a predefined time that has been shown to be adequate.

A one-hour electrical power loss shall not alter the device configuration. This includes a mains electricity outage or a battery replacement. The SRS may specify a different duration for configuration retention.

6.6 Physical security

Wireless devices shall be protected by physical measures so that they are not tampered with or inadvertently damaged.

6.7 Electromagnetic security

Protection against intentional EMI shall be considered depending on the importance of the wireless system to the safety of the NPP.

7 Device selection: evidence of correctness and device integration

7.1 General

It is common for pre-existing devices to be used to build a new wireless system. Clause 7 gives requirements for the selection and integration of such devices into the system.

7.2 Quality assurance

The selected device shall come with sufficient evidence that an adequate quality assurance programme was used to develop the device.

NOTE A wireless device developed in accordance with IEC 61513 or complying with IEC 62671 is a good example of a device with a good quality assurance programme.

7.3 Functional and performance suitability

The performance characteristics, the features and the capability of the candidate device to be selected shall be evaluated so that it is suitable to meet the system requirements (Clause 6).

NOTE For example, if the SRS specifies that encryption is used, the selected device provides an adequate encryption feature.

The device selection is deeply connected to the system requirements, thus most requirements are likely to have an associated device selection criterion. For example, power supply requirements of Clause 6 have a clear impact on the selection of the device (battery life, etc.).

7.4 Integration into the application

For the integration of pre-existing devices, the following requirements shall be applied:

– IEC 61513:2011, 6.2.3.2 (Selection of pre-existing components), or
– IEC 62671.

NOTE IEC 62671:2013, 5.3.2 provides requirements for building an Evaluation and Application Plan (EAP) in order to select and evaluate a pre-existing device in a nuclear power plant.

7.5 Device self-monitoring

The wireless device shall be able to monitor and transmit condition information such as:

– the power supply status;
– the battery status (if applicable);
– the wireless signal quality (uplink and downlink);
– data transfer speed;
– processor load;
– operative memory;
– processor temperature.

7.6 Solution preferences

Wireless protocols shall be based on a documented standard or a documented communication protocol.

8 Radio emissions

8.1 Electromagnetic compatibility

Electromagnetic compatibility (EMC) shall be considered prior to the implementation of wireless devices near equipment important to safety. This is to ensure the proper operation of the wireless device and to prevent interference with other equipment.

An impact analysis regarding EMC shall be conducted prior to the on-site installation of the system.

The impact analysis may include system reviews and evaluations in combination with laboratory/on-site testing according to IEC 62003, such as:

– review of EMC test reports of nearby NPP equipment;
– determination of exclusion zones based on industry guidance;
– characterization of the electromagnetic environment;
– susceptibility testing of wireless devices to verify they can withstand the NPP environment;

– immunity testing of nearby NPP equipment during maintenance programmes.

NOTE These requirements are intended to protect systems important to safety and key control systems from electromagnetic waves emitted by the wireless device.

Fixed wireless devices such as access points shall be installed at a pre-defined distance away from other equipment important to safety if that equipment is sensitive to signals from wireless devices. This exclusion zone distance shall be calculated based upon free-space propagation models and shall account for the output power and antenna gain of the wireless device as well as the demonstrated immunity level of the equipment performing category A and B functions. The demonstrated immunity level shall be 8 dB higher than the expected field strength of the wireless device at the exclusion distance boundary. If the equipment important to safety was not tested for radiated immunity according to IEC 61000-4-3 (or equivalent) at the transmitting frequency of the wireless device, then additional testing and/or evaluation shall be performed. Additional testing could include in-situ immunity testing of the important to safety equipment (or testing of equivalent equipment in a simulated environment) at a time when its trip/control function can be bypassed such as during a refuelling outage according to guidance in IEC 62003. This testing should determine the immunity of the NPP equipment and establish an associated exclusion distance for the wireless device (if any).

Mobile devices shall be addressed in a similar manner but shall include administrative controls such as training, signage, or other means, to ensure that the established exclusion distances are not violated.

8.2 Radio coverage requirements

The access point location shall be defined through the results of coverage mapping and/or EMI/RFI site survey.

The communication system coverage demands for the intended application shall be identified.

8.3 Spectrum management

8.3.1 General

A formal spectrum management programme shall be established and documented to ensure that all wireless devices used on the NPP or nuclear facility are formally controlled. This programme shall include provisions to ensure that:

– the wireless devices are evaluated and approved before implementation and use;
– the spectrum usage includes margins of safety in order to eliminate interference between channels;
– the spectrum usage considers the non-safety devices that may be operated in the same areas;
– the wireless devices are configuration managed throughout their life, particularly with respect to maintenance, modification and replacement.

This includes documentation of the frequency, power level, and other properties of the wireless transmitting devices, as well as routine monitoring of the spectrum usage to verify usage of the NPP environment. New wireless applications being implemented into the NPP should consider occupying unused frequencies instead of overcrowding existing channels.

Wireless devices applied throughout the NPP will require flexibility, mobility and failure management.

8.3.2 Flexibility

If multiple devices have to be available at different locations, adequate network coverage should be provided in the necessary areas of the plant.

8.3.3 Mobility

When necessary, any device should be able to access all necessary information in real-time at all locations identified. The device and the system shall be able to handle devices moving from area to area without losing communication if required by the intended application.

9 Cybersecurity

9.1 General requirements

The requirements of IEC 62645 shall be met.

Encryption should be used for wireless communications. The encryption methods – or lack of encryption – shall be consistent with the overall security plan.

Authentication of all messages should be used. The authentication process – or lack of authentication – shall be consistent with the overall security plan.

9.2 Wireless-specific requirements

9.2.1 Data logging

A data recording device should be available so that the wireless devices can log information such as:

– authentication and connection attempts,
– maintenance data (battery wear, CPU load, autotest results, etc.),
– system-specific process data (temperature, pressure, vibration level, etc.).

This data should be accessible for a cybersecurity audit in case of a suspected cybersecurity event.

9.2.2 Site topology

The site topology shall be considered when evaluating cybersecurity and writing the overall security plan.

One shall bear in mind that a network connection may be achieved from a remote location using specialized and/or modified devices, such as directional antennas, and/or higher-than-usual power outputs, etc.

9.2.3 Connection to a wired network

If a wireless network is connected to a wired network, a filtering device shall be installed between the two networks.

NOTE This filtering function may take the form of a DMZ, a hardware filtering device, etc.

9.2.4 Network surveillance

Failed connection attempts should be reviewed by the appropriate staff responsible for cybersecurity.

For fixed instrumentation networks, the following events should be monitored by the appropriate staff responsible for cybersecurity:

– new device connecting to the network;
– output power of wireless devices;

– transmission delay variations (especially for mesh networks);
– unusual battery discharge rate.

10 Qualification

10.1 Hardware qualification

An environmental qualification shall be performed. IEC 60987:2007, 5.4 and IEC/IEEE 60780-323 provide additional requirements for hardware design and qualification.

10.2 Software qualification

The requirements of IEC 62138 (for category C functions) shall be met.

11 Documentation

The startup and shutdown procedures of the wireless network shall be documented.

The procedure for inserting a new device in the wireless network shall be documented.

The procedure for replacing a defective device in the wireless network shall be documented. This includes the procedure for transferring all the relevant configuration parameters from the old to the new device into the wireless network.

Wireless devices, like any system, have obsolescence concerns that shall be considered during the design and implementation phase.

Bibliography

IEC 61000-4-3, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*

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

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

IEC 62657-1:2017, *Industrial communication networks – Wireless communication networks – Part 1: Wireless communication requirements and spectrum considerations*

IEC 62657-2:2017, *Industrial communication networks – Wireless communication networks – Part 2: Coexistence management*

IEC TR 62918:2014, *Nuclear power plants – Instrumentation and control important to safety – Use and selection of wireless devices to be integrated in systems important to safety*

SOMMAIRE

AVANT-PROPOS 21
INTRODUCTION 23
1 Domaine d'application 25
2 Références normatives 25
3 Termes et définitions 26
4 Symboles and abréviations 29
5 Exigences fondamentales 30
5.1 Classement de sûreté 30
5.2 Isolement et séparation physique 30
5.3 Cybersécurité 30
6 Application sans fil: exigences système 30
6.1 Généralités 30
6.2 Architecture réseau 30
6.3 Performance réseau 31
6.4 Suivi et surveillance réseau 31
6.5 Exigences pour l'alimentation électrique 31
6.6 Sécurité physique 32
6.7 Sécurité électromagnétique 32
7 Sélection de l'appareil: preuves de conformité et intégration de l'appareil 32
7.1 Généralités 32
7.2 Assurance qualité 32
7.3 Pertinence fonctionnelle et des performances 32
7.4 Intégration dans l'application 32
7.5 Auto surveillance de l'appareil 32
7.6 Solution préférée 33
8 Émissions radio 33
8.1 Compatibilité électromagnétique 33
8.2 Exigences portant sur la couverture radio 34
8.3 Gestion spectrale 34
8.3.1 Généralités 34
8.3.2 Flexibilité 34
8.3.3 Mobilité 34
9 Cybersécurité 34
9.1 Exigences générales 34
9.2 Exigences particulières pour le sans fil 35
9.2.1 Journalisation des données 35
9.2.2 Topologie du site 35
9.2.3 Connexion à un réseau câblé 35
9.2.4 Surveillance du réseau 35
10 Qualification 35
10.1 Qualification du matériel 35
10.2 Qualification du logiciel 35
11 Documentation 36
Bibliographie 37

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – SÉLECTION ET UTILISATION DES APPAREILS SANS FIL

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 62988 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.

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

FDIS	Rapport de vote
45A/1187/FDIS	45A/1198/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 du présent document

Le présent document établit des exigences applicables aux appareils sans fil qui sont utilisés pour réaliser des fonctions importantes pour la sûreté dans les centrales nucléaires de puissance (CNP).

L'objectif du présent document est d'être utilisée par les exploitants de centrales nucléaires de puissance, les évaluateurs de système et par les régulateurs.

b) Position du présent document dans la collection de normes du SC 45A de l'IEC

L'IEC 62988 est le document du SC 45A de l'IEC de troisième niveau qui traite de la sélection et de l'utilisation des appareils sans fil dans les systèmes d'instrumentation et de contrôle-commande (I&C) importants pour la sûreté employés dans les centrales nucléaires de puissance.

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 du présent document

Il est important de noter que le présent document est applicable pour tous les systèmes importants pour la sûreté intégrant des appareils sans fil, y compris ceux réalisant des fonctions de catégories A et B (et pour de tels systèmes l'emploi de dispositifs sans fil est prohibé par le présent document). Ainsi, il est demandé que seuls les systèmes réalisant des fonctions de catégorie C suivent les exigences du présent document.

Afin d'assurer la pertinence de la présente 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 de puissance. 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 de puissance, 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 de puissance, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires de puissance, avec le guide de sûreté SSG-39 qui traite de la conception de l'instrumentation et du contrôle-commande des centrales nucléaires de puissance, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires de puissance, 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 de l'IEC 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 série 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 – SÉLECTION ET UTILISATION DES APPAREILS SANS FIL

1 Domaine d'application

Le présent document établit les exigences applicables pour la sélection et l'utilisation des appareils sans fil intégrés dans les systèmes d'instrumentation et de contrôle-commande (I&C) importants pour la sûreté employés dans les centrales nucléaires de puissance (CNP). Ces systèmes d'I&C peuvent être intégralement constitués d'appareils sans fil.

NOTE Le mot «utilisation» fait référence à l'intégration de l'appareil, sa qualification, son contrôle administratif et toutes les autres activités qui peuvent être nécessaire pour utiliser l'appareil dans une application importante pour la sûreté.

Le présent document est applicable pour la construction des nouvelles CNP et pour la rénovation de l'I&C sur les CNP existantes. Tous les appareils sans fil ou les systèmes sans fil importants pour la sûreté relèvent du domaine du présent document. Les appareils fixes comme les appareils mobiles et tous les types de données (voix, données du procédé, etc.) sont couverts par le domaine du présent document s'ils réalisent une fonction classée de sûreté.

Le présent document restreint l'utilisation des appareils sans fil aux systèmes réalisant des fonctions de sûreté de catégorie C telle que définie par l'IEC 61226, et exclut explicitement leur utilisation pour les catégories A et B.

On peut utiliser le présent document comme un guide pour les appareils et les systèmes non classés de sûreté, par exemple pour s'assurer que les appareils importants pour la sûreté ne sont pas perturbés.

– L'Article 5 décrit les exigences fondamentales concernant la sûreté et la cybersécurité.
– L'Article 6 fournit des exigences spécifiques au sans fil qui doivent être couvertes au niveau conception système.
– L'Article 7 décrit les exigences pour la sélection et l'intégration des appareils sans fil.
– L'Article 8 traite de la compatibilité électromagnétique et de la gestion spectrale.
– L'Article 9 fournit des exigences propres au sans fil en matière de cybersécurité.
– L'Article 10 décrit les exigences de qualification des appareils sans fil et leur environnement.

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

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

IEC 61513:2011, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

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

IEC 62645, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences relatives aux programmes de sécurité applicables aux systèmes programmés*

IEC 62671, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils numériques à fonctionnalités limitées*

3 Termes et définitions

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

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

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

3.1
authentification
méthode permettant de garantir qu'une caractéristique revendiquée pour une entité est correcte

[SOURCE: ISO/IEC 27000:2018, 3.5]

3.2
catégorie d'une fonction d'I&C
l'une des trois affectations de sûreté possibles (A, B, C) des fonctions d'I&C résultant de l'évaluation de l'importance pour la sûreté de la fonction exécutée. Une affectation "non classée" peut être délivrée si la fonction n'est pas importante pour la sûreté.

Note 1 à l'article: Voir également "classe d'un système d'I&C".

Note 2 à l'article: L'IEC 61226 définit trois catégories de fonctions d'I&C. A chaque catégorie correspond un ensemble d'exigences relatives à la fois aux fonctions d'I&C (spécification, conception, intégration, vérification et validation) et à l'ensemble des composants nécessaires à la réalisation des fonctions (propriétés et qualification) indépendamment de la manière suivant laquelle ces composants sont distribués dans plusieurs systèmes d'I&C interconnectés. Pour davantage de clarté, le présent document définit des catégories de fonctions d'I&C et des classes de systèmes d'I&C. Elle établit une relation entre la catégorie d'une fonction et la classe minimale des systèmes et équipements associés.

[SOURCE: IEC 61513:2011, 3.4]

3.3
classe d'un système d'I&C
l'une des trois affectations possibles (1, 2, 3) des systèmes d'I&C importants pour la sûreté, résultant de la nécessité pour ces systèmes d'exécuter des fonctions d'I&C d'importances pour la sûreté différentes. Une affectation "Non Classé" est délivrée si le système d'I&C n'exécute pas de fonction importante pour la sûreté.

Note 1 à l'article: Voir également "catégorie d'une fonction d'I&C", "système de sûreté".

[SOURCE: IEC 61513:2011, 3.6]

3.4
gestion spectrale
gestion de coexistence
processus visant à établir et maintenir la coexistence comportant des mesures techniques et organisationnelles

[SOURCE: IEC 62657-2:2017, 3.1.15, modifiée – Le terme privilégié "gestion spectrale" a été ajouté.]

3.5
cybersécurité
ensemble des activités et des mesures dont l'objectif est d'empêcher, de détecter et de réagir aux attaques digitales dont l'intention est d'entrainer:

- la divulgation d'informations qui pourraient être utilisées pour réaliser des actes malveillants qui pourraient amener à un accident, une situation non sûre ou dégrader les performances de fonctionnement de la centrale,
- les modifications malveillantes de fonctions qui pourraient porter atteinte à la fourniture ou à l'intégrité d'un service demandé par des systèmes programmés-HPD d'I&C (y compris la perte de contrôle) qui pourraient avoir pour conséquence un accident, l'apparition d'une situation non sûre ou une dégradation des performances de l'installation (intégrité),
- la rétention, la prévention pour l'accès à ou la communication d'informations, de données ou de ressources (y compris la perte de vue) malveillantes qui pourraient compromettre la fourniture par un système d'I&C d'un service demandé qui pourrait avoir pour conséquence un accident, l'apparition d'une situation non sûre ou une dégradation des performances de l'installation (disponibilité).

Note 1 à l'article: Cette définition est taillée sur mesure par rapport au domaine du présent document, se concentrant sur la prévention, la détection et la réaction aux actes malveillants portant atteinte aux systèmes programmés-HPD d'I&C en utilisant des moyens numériques. Il est reconnu que terme «cybersécurité» à un sens plus large au niveau des autres normes et documents guide et souvent qu'il couvre les menaces non malveillantes, les erreurs humaines et la protection contre les risques naturels, qui sont en dehors du domaine du présent document (voir l'Article 1).

[SOURCE: IEC 62645:2014, 3.6]

3.6
élément électrique/électronique/électronique programmable
élément E/E/PE
élément réalisé à base de technologie électrique (E) et/ou électronique (E) et/ou électronique programmable (PE)

[SOURCE: l'IEC 61508-4:2010, 3.3.2, modifiée]

Note 1 à l'article: Pour ce terme et cette définition le mot "élément" peut être remplacé par les mots: système ou équipement ou dispositif.

3.7
chiffrement
transformation (réversible) des données par un algorithme de cryptographie pour produire une donnée chiffrée, à savoir pour cacher le contenu informatif des données

[SOURCE: In English, ISO/IEC 18033-1:2015, 2.21]

3.8
point d'accès
passerelle
dispositif de réseau contenant au moins une interface d'hôte telle qu'une interface série ou Ethernet, faisant office de point d'entrée ou de point de sortie permettant la communication entre des applications d'hôtes et des dispositifs de terrain

[SOURCE: IEC 62591:2016, 3.2.47, modifiée – Le terme privilégié "point d'accès" a été ajouté. Dans la définition, "appareil" a été remplacé par "dispositif".]

3.9
système d'I&C
système réalisé sur la base d'éléments E/E/PE, exécutant des fonctions d'I&C ainsi que des fonctions de service et d'affichage liées au fonctionnement du système lui-même.

Note 1 à l'article: Le terme est utilisé comme terme général comprenant tous les éléments du système, tels que les alimentations électriques, les capteurs et autres dispositifs d'entrée, les bus de données et autres chemins de communication, les actionneurs et autres dispositifs de sortie. Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées.

Note 2 à l'article: Les éléments contenus dans un système d'I&C donné sont définis dans la spécification des limites de ce système.

Note 3 à l'article: Voir aussi la définition d'élément E/E/PE et les notes associées.

Note 4 à l'article: Selon leurs fonctionnalités propres, l'AIEA fait la distinction entre les systèmes de contrôle et de commande, les systèmes d'IHM, les systèmes de verrouillage et les systèmes de protection.

3.10
constituant important pour la sûreté
constituant faisant partie d'un groupe de sûreté et/ou dont le mauvais fonctionnement ou la défaillance pourrait entraîner une exposition à des rayonnements du personnel du site ou de personnes du public

Note 1 à l'article: Les constituants importants pour la sûreté comprennent:

a) les structures, systèmes et composants dont le mauvais fonctionnement ou la défaillance pourraient entraîner une exposition indue à des rayonnements du personnel du site ou de personnes du public;

b) les structures, systèmes et composants qui empêchent les incidents de fonctionnement prévus d'aboutir à des conditions accidentelles;

c) les dispositifs prévus pour atténuer les conséquences d'un mauvais fonctionnement ou d'une défaillance de structures, systèmes ou composants.

[SOURCE: In English, IAEA Safety Glossary, 2016 edition]

3.11
latence
temps mis par un paquet pour franchir la connexion réseau, de l'expéditeur vers le destinataire

[SOURCE: IEC 62591:2016, 3.2.57]

3.12
topologie maillée
topologie de réseau dans laquelle des chemins redondants d'acheminement physiquement différents sont disponibles entre chaque paire de nœuds du réseau

Note 1 à l'article: La topologie maillée sans fil est utilisable pour étendre la couverture par une fonctionnalité de sauts multiples et/ou pour faciliter la fiabilité des communications par la fourniture de chemins redondants entre les appareils

[SOURCE: IEC 62734:2014, 3.1.2.95]

3.13
réseau
série de nœuds reliés par quelque type de support de communication

[SOURCE: IEC 62591:2016, 3.2.70, modifiée – Dans la définition, "un type donnée" a été remplacé par "quelque type". La Note 1 à l'article a été supprimée.]

3.14
assurance qualité
fonction d'un système de gestion qui garantit que des prescriptions spécifiques seront respectées

Note 1 à l'article: Cette définition est compatible avec celle de l'ISO 9000:2015, 3.3.6.

[SOURCE: In English, IAEA Safety Glossary, 2016 edition, modified – The term "quality management" has been replaced by "quality assurance".]

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

[SOURCE: In English, IAEA Safety Glossary, 2016 edition]

3.16
système lié à la sûreté
système important pour la sûreté qui ne fait pas partie d'un système de sûreté

[SOURCE: In English, IAEA Safety Glossary, 2016 edition]

3.17
système de sûreté
système important pour la sûreté destiné à garantir la mise à l'arrêt sûre du réacteur ou l'évacuation de la chaleur résiduelle du cœur du réacteur, ou à limiter les conséquences des incidents de fonctionnement prévus et des accidents de dimensionnement

[SOURCE: In English, IAEA Safety Glossary, 2016 edition]

3.18
appareil sans fil
appareil capable d'établir une communication sans fil avec un autre appareil sans fil, qui peut ou non faire partie d'un réseau sans fil

4 Symboles and abréviations

CPU processeur central (*central processing unit*)

DMZ zone démilitarisée (*demilitarized zone*)

CEM compatibilité électromagnétique

HPD circuit intégré programmé en HDL (*HDL programmed device*)

IEM interférence électromagnétique

I&C instrumentation et contrôle-commande

CNP centrale nucléaire de puissance

IFR interférences des fréquences radio

SES spécification d'exigences système

5 Exigences fondamentales

5.1 Classement de sûreté

L'utilisation des appareils sans fil doit être limitée aux systèmes d'I&C réalisant des fonctions de catégorie C et ils ne doivent pas être utilisés pour des systèmes d'I&C réalisant des fonctions de catégorie A ou B.

La classe de sûreté des systèmes de communication sans fil doit être cohérente avec les fonctions de catégorie C qu'ils supportent et réalisent et il convient qu'elle soit de classe 3.

5.2 Isolement et séparation physique

Les systèmes de communication sans fil doivent être électriquement isolés et physiquement séparés des canaux de communication câblés des systèmes d'I&C réalisant des fonctions de catégorie A ou B.

Les systèmes de communication sans fil pour les fonctions de catégorie C doivent être conçus de telle façon qu'aucun défaut ne se propage aux canaux de communication câblés des systèmes d'I&C réalisant des fonctions de catégorie A ou B.

5.3 Cybersécurité

Les communications sans fil ne doivent pas être utilisées dans des systèmes qui ont été affectés aux degrés de sécurité S1 ou S2 tels que définis par l'IEC 62645.

On doit considérer sur la base d'un plan d'ensemble de sécurité les connexions réseau avec les systèmes de classe de sûreté supérieure de façon à prendre les mesures appropriées en termes de cybersécurité.

Des informations complémentaires concernant la cybersécurité peuvent être trouvées à l'Article 9.

6 Application sans fil: exigences système

6.1 Généralités

Un document de spécification d'exigences systèmes (SES), tel que requis par l'IEC 61513 doit être écrit pour servir de base à la conception système.

6.2 Architecture réseau

Prenant en compte les fonctions et l'application prévues pour le système sans fil, le SES doit spécifier et justifier:

– la topologie réseau,

– la situation des points d'accès,

– la configuration réseau.

Il convient que les réseaux maillés implémentent des algorithmes d'équilibrage de charge pour le routage. Ceci signifie que si plusieurs sont disponibles pour aller d'un nœud A à un nœud B, alors il convient que le chemin choisi évite les nœuds intermédiaires surchargés.

Il convient que les algorithmes de routage réseau soient capables de gérer les paquets/messages avec différentes priorités.

6.3 Performance réseau

En relation avec l'application prévue, le SES doit spécifier et donner les justifications pour:

– les retards de transmission entre les différents points pertinents du réseau (habituel et maximum),
– les vitesses de transfert des données entre les différents points pertinents du réseau (habituel et maximum).

NOTE 1 l'IEC 62657-1 fournit des informations concernant le comportement des systèmes de communication sans fil, telles que le temps de transmission, le temps de mise à jour et de disponibilité.

Il convient que la charge réseau soit indépendante du contexte. Ceci signifie que si un évènement surveillé survient, il convient que la charge réseau n'augmente pas.

NOTE 2 Une conception complètement indépendante du contexte est difficile à réaliser, ainsi une couche application indépendante du contexte est suffisante.

6.4 Suivi et surveillance réseau

Des moyens permettant le suivi et de surveillance du réseau sans fil doivent être fournis. Ces moyens doivent être capables de détecter et de corriger les anomalies dans le réseau sans fil.

Le taux d'erreur de données doit être suivi. Le SES doit définir le taux de perte des paquets acceptable et indiquer si des messages perdus doivent être renvoyés ou pas.

NOTE Pour s'affranchir du suivi du taux d'erreur dans le système de communication dans la gamme spécifiée par la conception système, la latence et/ou les fluctuations peuvent être aussi surveillées.

Il doit être possible de suivre:

– l'état du réseau: charge, taux d'erreurs de transmission, perte des paquets, latence;
– la liste exhaustive des appareils connectés au réseau;
– les journaux réseau, couvrant les défauts de connexion (tentatives de connexions non autorisées, etc.);
– pour chaque appareil:
  - ses variables auto-surveillées (voir 7.5),
  - ses caractéristiques (version logiciel, etc.),
  - sa localisation physique, si pertinente.

6.5 Exigences pour l'alimentation électrique

Lorsque requis par l'application, il convient d'utiliser des alimentations électriques redondantes.

Lorsque requis par l'application, il convient que les appareils soient auto alimentés par batterie. Dans ce cas:

– le SES doit spécifier la capacité minimale des batteries pour l'application prévue,
– les appareils distants doivent être physiquement accessibles de façon à pouvoir remplacer les batteries déchargées ou défaillantes. Si cela n'est pas possible la capacité des batteries doit être dimensionnée pour tenir un temps donné prédéfini et dont on a montré qu'il est approprié.

Une perte de l'alimentation électrique d'une heure ne doit pas altérer la configuration d'un appareil. Ceci inclut la perte de l'alimentation secteur ou le remplacement de batterie. Le SES peut spécifier une durée différente pour le maintien de l'intégrité de la configuration.

6.6 Sécurité physique

Les appareils sans fil doivent être protégés physiquement pour qu'ils ne soient pas sabotés ou endommagés par inadvertance.

6.7 Sécurité électromagnétique

La protection contre les IEM malveillantes doit être mise en œuvre en prenant en compte l'importance du système sans fil pour la sûreté de la CNP.

7 Sélection de l'appareil: preuves de conformité et intégration de l'appareil

7.1 Généralités

Il est courant d'utiliser des appareils pré existants pour réaliser un nouveau système sans fil. L'Article 7 fournit des exigences portant sur la sélection et l'intégration de tels appareils dans le système.

7.2 Assurance qualité

L'appareil sélectionné doit être accompagné de preuves suffisantes portant sur le caractère approprié du programme d'assurance qualité suivi pour développer l'appareil.

NOTE Un appareil sans fil développé conformément à l'IEC 61513 ou conforme à l'IEC 62671 est un bon exemple d'appareil présentant un bon programme d'assurance qualité.

7.3 Pertinence fonctionnelle et des performances

Les caractéristiques des performances, des fonctionnalités et l'aptitude de l'appareil candidat à être choisi doivent être évaluées pour que celui-ci soit apte à satisfaire aux exigences système (voir Article 6).

NOTE Par exemple, si le SES spécifie que le chiffrement est utilisé, l'appareil sélectionné met en œuvre des mesures de chiffrement appropriées.

La sélection de l'appareil est étroitement liée aux exigences système, ainsi pour la plupart des exigences il est possible de les associer à un critère de sélection de l'appareil. Par exemple, les exigences de l'Article 6 portant sur l'alimentation électrique ont clairement un effet sur la sélection de l'appareil (durée de vie de la batterie, etc.).

7.4 Intégration dans l'application

Pour l'intégration d'appareils pré existants les exigences suivantes doivent être satisfaites:

– IEC 61513:2011, 6.2.3.2 (Sélection des composants pré existants), ou,

– IEC 62671.

NOTE Le paragraphe 5.3.2 de l'IEC 62671:2013 fournit des exigences pour établir un Plan d'Évaluation et d'Application (PEA) de façon à choisir et évaluer les appareils pré existants pour les centrales nucléaires de puissance.

7.5 Auto surveillance de l'appareil

L'appareil sans fil doit être capable de surveiller et de transmettre les informations relatives à l'état telles que:

– l'état de l'alimentation électrique;

– l'état des batteries, le cas échéant;

– la qualité du signal sans fil (émission et réception);

– la vitesse de transfert de données;

– la charge du processeur;
– mémoire opérationnelle;
– température processeur.

7.6 Solution préférée

Le protocole de transmission sans fil doit reposer sur une norme documentée ou sur un protocole de communication documenté.

8 Émissions radio

8.1 Compatibilité électromagnétique

La compatibilité électromagnétique (CEM) doit être prise en compte avant la mise en œuvre de l'appareil sans fil à proximité d'un équipement important pour la sûreté. Ceci pour garantir un fonctionnement correct de l'appareil sans fil et empêcher toute interférence avec les autres matériels.

Une analyse d'impact portant sur la CEM doit être réalisée avant l'installation sur site du système.

L'analyse d'impact peut comprendre des revues et évaluations système combinées à des essais site ou laboratoire conformément à l'IEC 62003 tels que:

– la revue des rapports d'essais CEM sur les matériels de la CNP situés à proximité,
– la détermination des zones d'exclusion reposant sur des recommandations industrielles,
– la caractérisation de l'environnement électromagnétique,
– les tests de susceptibilité des appareils sans fil pour vérifier leur résistance à l'ambiance d'exploitation,
– les tests d'immunité des matériels de la CNP à proximité lors des programmes de maintenance.

NOTE L'objectif de ces exigences est de protéger les systèmes importants pour la sûreté et les systèmes de conduite clé des ondes électromagnétiques émises par les appareils sans fil.

Les appareils sans fil fixes tels que les points d'accès doivent être installés à une distance prédéfinie des autres équipements importants pour la sûreté si ces derniers sont sensibles aux signaux des appareils sans fil. Cette distance de zone d'exclusion doit être calculée à partir des modèles de propagation en espace libre et doit prendre en compte la puissance d'émission et le gain d'antenne de l'appareil ainsi que le niveau d'immunité vérifié pour les équipements réalisant des fonctions de catégories A ou B. Le niveau d'immunité vérifié doit être supérieur de 8 dB par rapport à la puissance du champ attendu pour l'appareil sans fil à la limite de la distance d'exclusion. Si l'équipement important pour la sûreté n'a pas été testé pour l'immunité aux rayonnements conformément à l'IEC 61000-4-3 (ou à un équivalent) au niveau de fréquence de transmission de l'appareil sans fil alors des tests et/ou des évaluations supplémentaires doivent être réalisées. Les essais supplémentaires peuvent comprendre des essais sur site d'immunité pour les équipements importants pour la sûreté (ou des essais sur des équipements équivalents en environnement simulé) à un moment où les fonctions d'arrêt automatique et de conduite peuvent être contournées, par exemple durant les arrêts pour rechargement, et ceci conformément aux recommandations de l'IEC 62003. Il convient que ces tests déterminent l'immunité des équipements de la centrale et établissent la distance d'exclusion associée pour les appareils sans fil, le cas échéant.

Les appareils mobiles doivent être pris en charge de façon similaire, mais cela comprend en plus les contrôles administratifs tels que la formation, la signalisation et les autres moyens permettant de garantir que les distances d'exclusion seront respectées.

8.2 Exigences portant sur la couverture radio

La localisation des points d'accès doit être définie sur la base des résultats de cartographie et/ou sur les études site IEM/IFR.

On doit identifier les demandes concernant la couverture du système de communication pour l'application prévue.

8.3 Gestion spectrale

8.3.1 Généralités

Un programme formel de gestion spectrale doit être établi et documenté pour garantir que les appareils sans fil utilisés sur la centrale ou sur une installation nucléaire sont formellement contrôlés. Ce programme doit comprendre les dispositions permettant de garantir que:

– les appareils sans fil sont évalués et approuvés avant mise en œuvre et utilisation;
– le spectre d'utilisation comprend des marges de sécurité de façon à éliminer les interférences entre canaux;
– le spectre d'utilisation prend en compte les appareils non classés de sûreté qui peuvent fonctionner dans les mêmes zones;
– les appareils sans fil sont soumis à une gestion de configuration durant toute leur vie, en particulier pour ce qui concerne la maintenance, les modifications et les remplacements.

Ceci comprend la documentation pour la fréquence, le niveau de puissance et les autres propriétés des appareils sans fil transmetteurs, de même que les surveillances périodiques de l'utilisation du spectre pour vérifier l'utilisation de l'environnement de la CNP. Il convient que les nouvelles applications sans fil qui sont installées dans la CNP prennent en compte l'occupation des fréquences inutilisées plutôt que de surcharger les canaux existants.

Les appareils sans fil utilisés pour les applications dans la CNP doivent être flexible, mobile et capable de gérer les défaillances.

8.3.2 Flexibilité

Si de multiples appareils doivent être disponibles en différents endroits, il convient qu'une couverture réseau appropriée soit assurée dans les zones concernées de la CNP.

8.3.3 Mobilité

Lorsque nécessaire, il convient que tout appareil puisse avoir accès à toutes les informations nécessaires en temps réel à partir de tous les endroits identifiés. L'appareil et le système doivent être capables gérer les appareils se déplaçant d'une zone à une autre sans perdre la communication si cela est nécessaire à l'application prévue.

9 Cybersécurité

9.1 Exigences générales

Les exigences de l'IEC 62645 doivent être satisfaites.

Il convient d'utiliser le chiffrement pour la communication sans fil. Les méthodes de chiffrement – ou l'absence de chiffrement – doivent être cohérentes avec le plan d'ensemble de la sécurité.

Il convient de mettre en place une authentification de tous les messages. Le procédé d'authentification – ou l'absence d'authentification – doit être cohérent avec le plan d'ensemble de la sécurité.

9.2 Exigences particulières pour le sans fil

9.2.1 Journalisation des données

Un appareil de journalisation des données doit être disponible pour que les appareils sans fil puissent enregistrer les informations concernant:

– les tentatives d'authentification et de connexion,
– les données de maintenance (usure des batteries, charge CPU, résultats d'autotests, etc.),
– les données de procédé particulières au système (température, pression, niveau de vibration, etc.).

Il convient que ces données soient accessibles dans le cadre des audits de cybersécurité dans le cas où on suspecte qu'un événement de sécurité est survenu.

9.2.2 Topologie du site

La topologie du site doit être prise en compte lors de l'évaluation de la cybersécurité et lors de l'écriture du plan d'ensemble de sécurité.

On doit garder à l'esprit que les connexions réseau peuvent se faire à distance en utilisant des appareils spécialisés et/ou modifiés, tels que des antennes directionnelles, et/ou des émetteurs plus puissants que d'habitude, etc.

9.2.3 Connexion à un réseau câblé

Si un réseau sans fil est connecté à un réseau câblé, un appareil de filtrage doit être installé entre les deux réseaux.

NOTE Cette fonction de filtrage peut prendre la forme d'une DMZ, d'un filtrage matériel, etc.

9.2.4 Surveillance du réseau

Il convient que la revue des tentatives échouées de connexions soit faite par le personnel compétent responsable pour la cybersécurité.

Pour les réseaux d'instrumentation fixe, il convient que la revue des évènements suivants soit faite par le personnel compétent responsable pour la cybersécurité:

– connexion d'un nouvel appareil au réseau;
– puissance d'émission des appareils sans fil;
– variations des délais de transmission (spécialement pour les réseaux maillés);
– vitesse de décharge inhabituelle des batteries.

10 Qualification

10.1 Qualification du matériel

Une qualification environnementale doit être réalisée. L'IEC 60987:2007, 5.4 et l'IEC/IEEE 60780-323 fournissent des exigences complémentaires pour la conception et la qualification du matériel.

10.2 Qualification du logiciel

Les exigences de l'IEC 62138 doivent être satisfaites pour ce qui concerne les fonctions de catégorie C.

11 Documentation

Les procédures de démarrage et d'arrêt du réseau sans fil doivent être documentées.

La procédure pour ajouter un nouvel appareil dans le réseau sans fil doit être documentée.

La procédure pour remplacer un appareil défectueux dans le réseau sans fil doit être documentée. Ceci comprend la procédure de transfert des paramètres de configuration pertinents de l'ancien appareil vers le nouvel appareil dans le réseau sans fil.

Les appareils sans fil, comme tous les systèmes font face à l'obsolescence, qui doit être prise en compte durant les phases de conception et de mise en œuvre.

Bibliographie

IEC 61000-4-3, *Compatibilité électromagnétique (CEM) – Partie 4-3: Techniques d'essai et de mesure – Essai d'immunité aux champs électromagnétiques rayonnés aux fréquences radioélectriques*

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

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

IEC 62657-1:2017, *Réseaux de communication industriels – Réseaux de communication sans fil – Partie 1: Exigences de communication sans fil et considérations relatives au spectre*

IEC 62657-2:2017, *Réseaux de communication industriels – Réseaux de communication sans fil – Partie 2: Gestion de coexistence*

IEC TR 62918:2014, *Nuclear power plants – Instrumentation and control important to safety – Use and selection of wireless devices to be integrated in systems important to safety* (disponible en anglais seulement)

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

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

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