IEC TR 62918

Edition 1.0 2014-07

TECHNICAL REPORT

colour inside

Nuclear power plants – Instrumentation and control important to safety – Use and selection of wireless devices to be integrated in systems important to safety

IEC TR 62918:2014-07(en)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 - www.iec.ch/searchpub
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 It also gives information on projects, replaced and withdrawn publications.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 more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 55 000 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: csc@iec.ch.

IEC TR 62918

Edition 1.0 2014-07

TECHNICAL REPORT

Nuclear power plants – Instrumentation and control important to safety – Use and selection of wireless devices to be integrated in systems important to safety

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XB

ICS 27.120.20

ISBN 978-2-8322-1750-4

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 62918, which is a technical report, has been prepared by subcommittee 45A: Instrumentation, control and electrical systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
45A/947/DTR	45A/963/RVC

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

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

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

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

A bilingual version of this publication may be issued at a later date.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

a) Technical background, main issues and organisation of the Standard

The ad hoc meeting of the IEC Technical Working Group on Nuclear Power Plant Control and Instrumentation, held in Yokohama in May 2009, resulted in the recommendation to develop a technical report addressing the applicability of incorporating wireless technology throughout nuclear power plant systems, regardless of the categorizations such as non-safety, important to availability and important to safety.

This technical report addresses this recommendation and one of its main objectives is to pave the way for the development of a standard on the topic. The technical report addresses concerns regarding the application, safety and security of integrating wireless technologies into the systems of nuclear power plants. It reviews the motivation for use of wireless applications in nuclear power plants, wireless technology considerations, and the feasibility of incorporating wireless technology in nuclear power plants.

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

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

IEC 62918 as a technical report is a fourth level IEC SC 45A document.

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 Technical Report

It is important to note that a technical report is entirely informative in nature. It gathers data collected from different origins and it establishes no requirements.

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, defence 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. Regarding nuclear safety, it provides the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector, regarding nuclear safety. 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 and IAEA GS-G-3.1 and IAEA GS-G-3.5 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 SSR-2/1, 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.

NOTE 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, that are based on the requirements of a standard such as IEC 61508.

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

1 Scope

This Technical Report describes the state of wireless technology for industrial applications in fossil and chemical plants and discusses the specific issues to be addressed in order to apply wireless technologies to nuclear power plants.

The review of the technology behind wireless communication and the status of existing implementations are described in Clauses 7 and 8, respectively. Issues associated with wireless implementations in nuclear facilities are discussed in Clause 10, and final conclusions are presented in Clause 11 of this Technical Report.

2 Normative references

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

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

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

IEC 62591, *Industrial communication networks – Wireless communication network and communication profiles – WirelessHART™*

IEC PAS 62734, *Industrial communication networks – Fieldbus specifications – Wireless systems for industrial automation: process control and related applications (Based on ISA 100.11a)*

3 Terms and definitions

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

3.1
access control
protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy

3.2
authenticate
verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission

3.3
communications protocol
set of standard rules for data representation, signaling, authentication and error detection required to send information over a communications channel

3.4
cybersecurity
actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets

3.5
Defense in Depth
DiD
application of more than one protective measure for a given safety objective, such that the objective is achieved even if one of the protective measures fails

[SOURCE: IAEA Safety Glossary, edition 2007]

3.6
denial of service
prevention or interruption of authorized access to a system resource or the delaying of system operations and functions

3.7
Distributed Control System
DCS
type of control system in which the system elements are dispersed but operated in a coupled manner. A DCS is similar to a supervisory control and data acquisition (SCADA) system except that a DCS is usually located within a more confined area (such as a factory). It uses a high-speed communications medium, which is usually a separate wire (network) from the factory's primary local area network (LAN). A significant amount of closed-loop control can reside in the DCS

3.8
Electromagnetic Compatibility
EMC
capacity of electrical equipment or system to function satisfactorily in its electromagnetic (EM) surroundings without radiating EM disturbance variables that are unacceptable for other equipment in these surroundings. Requirements are balanced with regard to interface transmission and immunity in case of EMC.

3.9
encryption
cryptographic transformation of data (called plaintext) into a form (called ciphertext) that conceals the data's original meaning to prevent it from being identified or used by outsiders. Decryption is the corresponding reversal process

3.10
Industrial, Scientific and Medical band
ISM band
section of radio spectrum allocated by the International Telecommunication Union (ITU) and many national regulators to ISM use. Radio communication systems that use these frequency bands are typically free for use but typically operate under a "license- exempt" regime that sets limits on power, spectrum spreading techniques, or duty cycles. Any device that transmits in the ISM bands must be "type-approved."

3.11
interoperability
ability of diverse systems and organizations to work together (inter-operate)

3.12
Intrusion Detection System
IDS
type of security management service for computers and networks. An intrusion detection system (IDS) monitors, gathers, and analyses information from various areas within a device or a network to identify possible security breaches, including intrusions and misuse.

3.13
risk assessment
process of systematically identifying potential vulnerabilities to valuable system resources and threats to those resources; quantifying loss exposures and consequences based on probability of occurrence; and [optionally] recommending how to allocate resources to countermeasures to minimize total exposure

3.14
trustworthiness
likelihood that an entity will behave as expected. In the context of industrial automation, attributes of trustworthiness include reliability, security, and resiliency

3.15
Virtual Private Network
VPN
VPN extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network, with all the functionality, security and management policies of the private network

3.16
vulnerability
flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy

4 Motivation

Aging nuclear power plant equipment and systems can benefit from additional instrumentation to detect and prevent equipment faults. Installing wired sensors into existing plant can be costly, cumbersome, and time consuming. In addition, as shown in Figure 1, the cost of installing wired sensor is often higher than the actual sensor itself. A wireless sensor network can eliminate cost of installing wires for the transmission of sensed data.

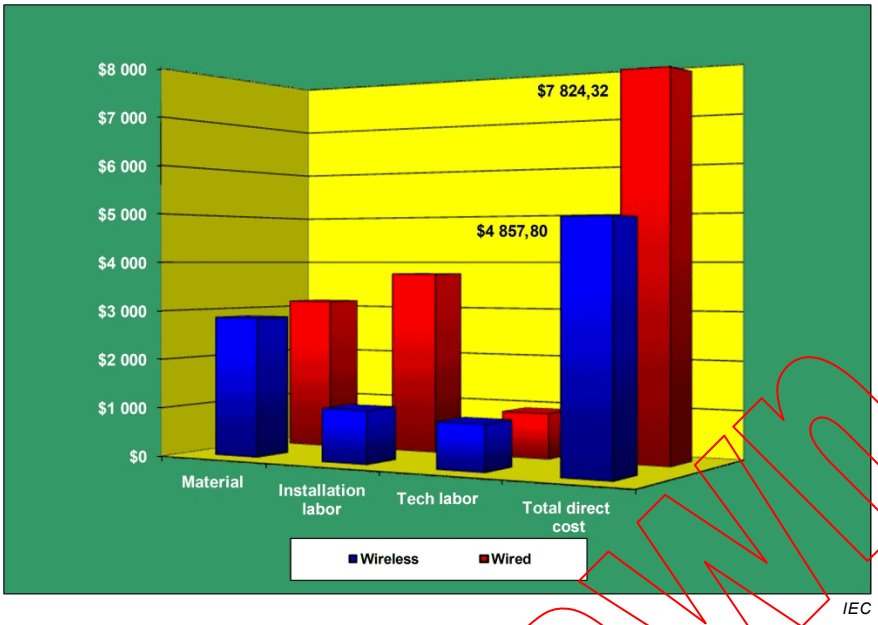

Figure 1 – Cost comparison – Wired versus wireless for an extensive building automation system

In many instances, a sensor network may be installed in one area of a facility while the sensor readings are to be used somewhere else at the facility (i.e., not within the RF coverage of the sensor network). In such a situation, some form of backhaul network is to be used to get the readings from point A to point B. Both nuclear and traditional fossil power plants have found it financially beneficial to use the same backhaul for the transport of differing types of information (such as security video, sensor readings (from condition monitoring instrumentation), and voice). Such "triple play" usage may further enhance the return on investment (ROI) associated with any or all aspects of such a wireless installation. Process and/or Important to Safety wireless networks shall have a documented specification and only carry data that complies with this specification. Wireless technology enhances facility maintainability since wireless devices are easily upgraded or replaced without major infrastructure impact as technology and or needs change. The general application of wireless technologies in power generation facilities – and in particular nuclear power plants – is far from static. In a 2009 article [3][1], the results of a survey yielded the wireless usage assessment, shown here as Figure 2.

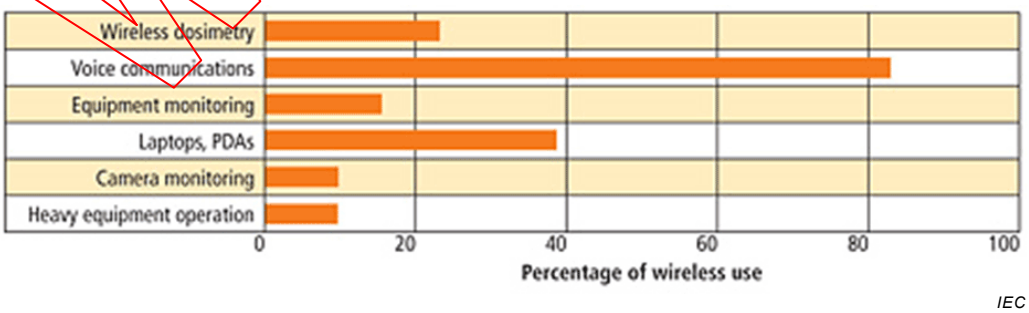

Figure 2 – Wireless use in nuclear power plants

Furthermore, this article related the wide range of possible applications of wireless technology within the nuclear power plant setting. The associated graphic is presented as Figure 3.

1 Number in square brackets refer to the Bibliography.