PD IEC/TR 62918:2014

BSI Standards Publication

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

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: PD IEC/TR 62918:2014

National foreword

This Published Document is the UK implementation of IEC/TR 62918:2014.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Reactor instrumentation.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014.
Published by BSI Standards Limited 2014

ISBN 978 0 580 85816 1
ICS 27.120.20

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 August 2014.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD IEC/TR 62918:2014

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XB

ICS 27.120.20

ISBN 978-2-8322-1750-4

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

® Registered trademark of the International Electrotechnical Commission

Documents
Document Sharing Hub

Full document details: PD IEC/TR 62918:2014

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 9
2 Normative references 9
3 Terms and definitions 9
4 Motivation 11
5 Generic applications 13
6 Technology 16
6.1 Wireless basics 16
6.2 Industrial wireless sensor networks 19
6.3 Radio frequency 20
6.3.1 Applications 20
6.3.2 802.11 (Wi-Fi), 802.15.1 (Bluetooth), 802.15.4 (sensors) 23
6.4 Satellite leased channels and VSAT 25
6.5 Magnetic field communications 26
6.6 Visual light communication (VLC) 27
6.7 Acoustic communication 27
6.8 Asset tracking utilizing IEEE 802.11 – Focus on received signal strength 28
6.9 Asset tracking (RFID/RTLS): ISO 24730 29
7 Current wireless technology implementations 30
7.1 General 30
7.2 Comanche Peak nuclear generating station 30
7.3 Arkansas Nuclear One (ANO) nuclear power plant 31
7.4 Diablo Canyon nuclear power plant 32
7.5 Farley nuclear power plant 33
7.6 San Onofre nuclear generating station 33
7.7 South Texas project electric generating station 34
7.8 High Flux Isotope Reactor (HFIR), Oak Ridge, TN 34
8 Considerations 36
8.1 General 36
8.2 Concerns regarding wireless technology 36
8.3 Wireless deployment challenges 37
8.4 Coexistence of 802.11 and 802.15.4 38
8.5 Signal propagation 40
8.6 Lessons learned from wireless implementations 41
8.6.1 General 41
8.6.2 Comanche Peak implementation 41
9 Concerns 42
9.1 Common reliability and security concerns for wired media and wireless media 42
9.2 Reliability and security concerns that are more of an issue for wired systems 42
9.3 Reliability and security concerns that are more of an issue for wireless systems 42
10 Standards 43
10.1 Nuclear standards 43

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

10.1.1 General ... 43
10.1.2 IEEE Std. 603-1998 ... 43
10.1.3 IEEE Std. 7-4.3.2-2003 ... 44
10.1.4 IEC 61500 ... 44
10.2 Other safety-related standards and guidelines ... 45
10.2.1 IEC 61784-3 ... 45
10.2.2 VTT research notes 2265 ... 46
10.2.3 European Workshop on Industrial Computer Systems – Technical Committee 7 (EWICS TC7) ... 47
11 Conclusions ... 47
11.1 Issues for wireless application to NPP ... 47
11.2 Recommendations ... 48
Annex A (informative) Use of 5 GHz in the world ... 50
Annex B (informative) Synopses of wireless technologies ... 51
B.1 802.11 ... 51
B.2 ISO 14443 Near Field Communications (NFC) ... 56
B.3 Real details of mesh networking ... 59
B.4 Not all mesh networks are created equal – Latency and indeterminism in mesh networks ... 62
B.5 ISA100.11a – “Mesh – When You Need It – Networking” ... 63
B.6 Security by non-routing edge nodes ... 66
B.7 Device and network provisioning methods ... 67
Bibliography ... 69

Figure 1 – Cost comparison – Wired versus wireless for an extensive building automation system ... 12
Figure 2 – Wireless use in nuclear power plants ... 12
Figure 3 – Possible application areas for wireless instrumentation in a nuclear power plant ... 13
Figure 4 – Bandwidth requirements for a variety of applications and the associated wireless technology that can support such requirements ... 14
Figure 5 – Structured fabric design of layered wireless for an industrial facility ... 15
Figure 6 – Inexpensive wireless sensors in a fossil-fuel plant ... 16
Figure 7 – Functional hierarchy ... 18
Figure 8 – Simplified diagram of a generic wireless sensor design ... 19
Figure 9 – Standard compliant network ... 20
Figure 10 – 802.15.1 (Bluetooth) frequency channels in the 2 450 MHz range ... 23
Figure 11 – 802.15.4 frequency channels in the 2 450 MHz range ... 24
Figure 12 – Overlapping channel assignments for 802.11 operation in the 2 400 MHz range ... 24
Figure 13 – 802.11n dual stream occupies 44 MHz of bandwidth. Dual stream 802.11n in the 2,4 GHz band ... 25
Figure 14 – VSAT mini-hub network configuration ... 26
Figure 15 – Spatial resolution is provided in multiple axes only if the tag (target in this Figure) is in communications with multiple APs ... 28
Figure 16 – ISO 24730-2 architecture ... 29
Figure 17 – Wireless vibration system at ANO ... 32
Figure 18 – ANO wireless tank level system ... 33

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

Figure 19 – Installation of accelerometers on ORNL HFIR cold source expansion engines (9-2010) 35
Figure 20 – Cold source expansion engine monitoring system software 35
Figure 21 – Installation of permanent wireless monitoring system at ORNL HFIR cooling tower (8-2011) 36
Figure 22 – System commissioned in August 2011 36
Figure 23 – Identification of containment in a nuclear facility 38
Figure 24 – Non-overlapping 802.11b/g channels and 802.15.4 channels 39
Figure 25 – Spectral analysis of Wi-Fi traffic for the case where a) minimal wi-fi channel "usage" and b) streaming video transfer across Wi-Fi channel 7 are analyzed 39
Figure 26 – Multipath is exemplified in this indoor environment as the signal from Source (S) to Origin (O) may take many paths 41
Figure B.1 – The Open Systems Interconnection (OSI) model defines the end-to-end communications means and needs for a wireless field transmitter to securely communicate with a distributed control system (DCS) 57
Figure B.2 – Operating frequencies for an IEEE 802.15.4 radio are 868 MHz, 902-926 MHz and 2 405-2 485 MHz. The worldwide license-free band at 2400 MHz is shown 58
Figure B.3 – Networking topologies take many forms with associated levels of complexity required for robust fault-tolerant data transport 58
Figure B.4 – Typical mesh network diagram 59
Figure B.5 – Requirement for mesh-networking communication of Figure B.4's topology 60
Figure B.6 – RF footprint map for a mesh network gateway and four nodes 61
Figure B.7 – The connectivity diagram for Figure B.6's RF footprint coverage map 61
Figure B.8 – Representation of the latency and indeterminism that it takes for a message to be transported through a mesh network that relies on time synchronization 63
Figure B.9 – The technical specifications associated with ISA100.11a end at the gateway. The area shaded falls within the Backhaul Work Group, ISA100.15 64
Figure B.10 – ISA100.11a utilizes the best topology for the application, in this case, a star 64
Figure B.11 – ISA100.11a allows for the deployment of multiple "hub and spoke" network elements with high speed interconnection to a gateway 65
Figure B.12 – The ISA100.11a network deployed at Arkema was a logical mix of wireless field transmitters and an ISA100.15 backhaul network 65
Figure B.13 – Networks deployed at neighbouring facilities will not "cross-talk" if non-routing nodes are deployed along the periphery of each facility 66
Figure B.14 – State transition diagram showing various paths to joining a secured network 68

Table 1 – List of "industrial" radio technology standards and their candidate applications 21
Table 2 – Cellular telephony frequencies in the US 22
Table 3 – GSM frequency bands, channel numbers assigned by the ITU 23
Table 4 – Specific uses of wireless technologies in the nuclear industry 30
Table A.1 – Use of 5 GHz in America, Asia/Pacific, and Europe 50

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

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

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

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.

Documents
Document Sharing Hub
Full document details: PD 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

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

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

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)

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

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

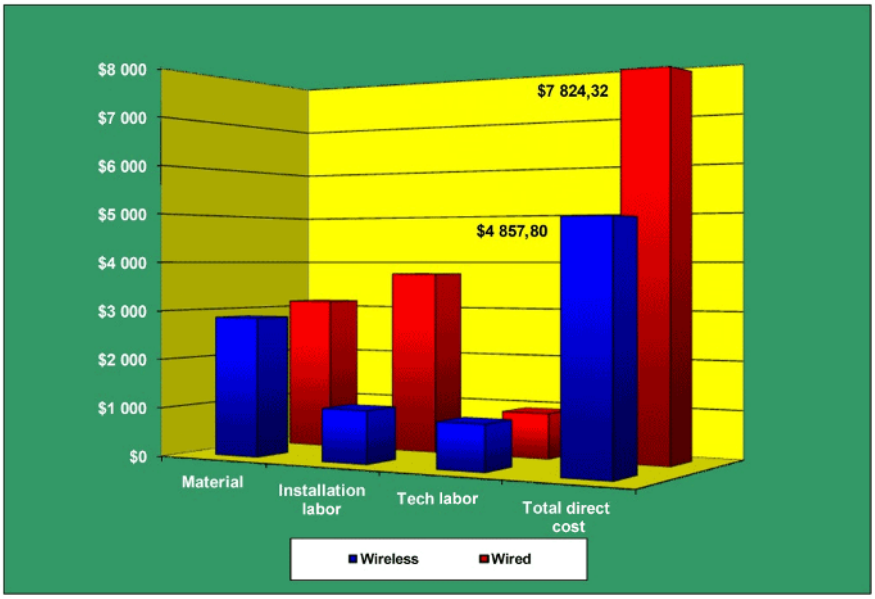
3.15
Virtual Private Network
VPN
VPN extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network, with all the functionality, security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

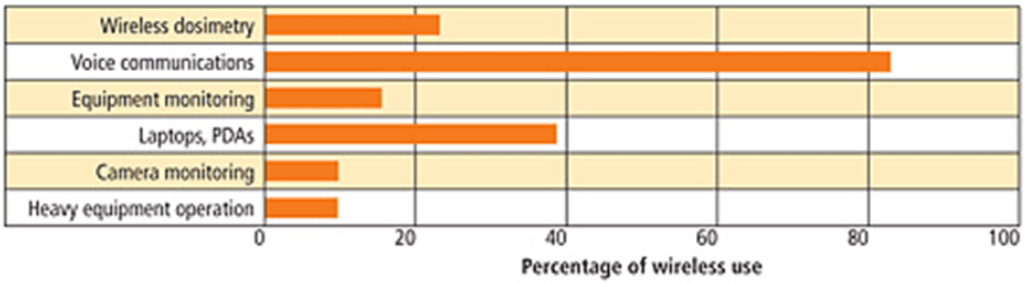
Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014



IEC

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.



IEC

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.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

In 2006, a study ascertained the state of the art in wireless technology and the implications for nuclear power facilities. The resulting document [30], presented a broad ranging examination of areas where wireless systems could benefit nuclear facilities. The following text, extracted from the report, sets the stage:

> *As the nuclear power industry moves to upgrade many of its older electronic systems, wireless technology may become an attractive alternative to wired systems. One of the largest costs in upgrading systems at nuclear facilities is the cost of running cables in this environment. When cost is considered, the perceived benefit of deploying wireless technology becomes clear. The benefits of using wireless systems in nuclear facilities could expand the argument for cost savings to include the possibility of ubiquitous (ever-present) sensing. To deploy an extensive number of sensors in the current nuclear environment would be cost-prohibitive because of cabling costs. However with wireless technology, additional types of sensors could be deployed to provide a more in-depth understanding of the area or process being monitored. In addition, the number of sensors of any given type could be increased, thereby improving redundancy. Also, with wireless technology, diversity in the types of sensors could be used to improve reliability.*

A specific tenor of that report is summarized in the following statement:

There could also be safety benefits.

Nuclear plant system	Wireless measurement(s)	Application
Heat exchangers	Temperature	Monitor ambient temperature to take into account the effects of such factors as seasonal changes in weather.
Secondary side valves	Position indication	Replace periodic, labor-intensive valve indication readings with continuously monitored wireless measurements.
Inlet water intake	Level, temperature, flow	Monitor factors that affect performance such as changes in level, seasonal temperature variations, and intake flow.
Rotating equipment (pumps, valves, motors, compressors, fans)	Temperature, vibration, motor current	Monitor temperatures, vibration signatures, and load fluctuations to assess condition and improve performance.
Diesel generators	Temperature, level, vibration, motor current	Augment existing sensor readings to provide redundancy and comprehensive performance assessment.
Spent fuel dry cask storage	Temperature, radiation	Eliminate need for underground cabling and conduit by monitoring temperature and radiation with wireless sensors.
Weather station	Temperature, wind velocity, pressure, humidity, etc.	Improve monitoring by replacing failure-prone equipment and cabling with wireless measurements.

IEC

Figure 3 – Possible application areas for wireless instrumentation in a nuclear power plant

In conclusion, the motivation for use of wireless technologies is strong, with several applications already seeing use in nuclear power plants currently. It is likely that the current pace of technology deployment will at least continue and may accelerate in the near term. This technical report includes information important to technology adopters and current users by showcasing the current technologies and applications available in this growing field.

5 Generic applications

The deployment and value of industrial wireless is based on two broad application classes; those requiring mobility and those derived from the reduced cost of attachment – not having

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

to run the wire. Such applications are best served by differing wireless technologies, typically based on response time and bandwidth requirements. An unscientific[2] mapping of applications-bandwidth-wireless technology is presented as Figure 4.

The diagram is meant to depict the (approximate) upper boundary of the delivered bandwidth for the shown technologies.

The diagram illustrates that, in the case of wireless sensor networks using 802.15.4-RF underpinnings, the bandwidth for the transmission is in the order of 256 kbps, less than optimal for video transmission. Similarly, the sensor networks are configured with typically up to 50 wireless field transmitters per gateway. The aggregate output bandwidth from the gateway is beyond the limits for efficient 802.15.4 transport and is more applicable for 802.11, 802.16 or similar backhaul technologies.

At the plant this results in a structured fabric design as depicted in Figure 5. The small circles on the fabric layers represent an RF footprint originating from, for example, a 100 mW output, omnidirectional antenna transceiver 802.15.4 or 802.11 device. The primary purpose of the diagram is to illustrate how a layer of wireless sensor devices are intertwined with a layer gateway device which, in turn, may communicate with an 802.11-based dense RF footprint which comprises the network fabric that mobility applications require.

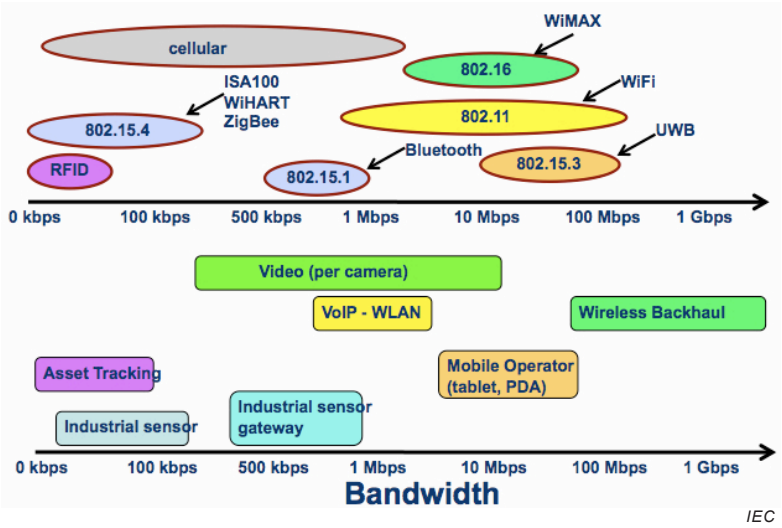


Figure 4 – Bandwidth requirements for a variety of applications and the associated wireless technology that can support such requirements

2 "Unscientific" in the sense that this is not an all-inclusive list of candidate RF technologies. Also note that, for example, the bandwidth for 802.11 is depicted as roughly 1 Mbps to 200 Mbps. The actual bandwidth may be as low as essentially 0 Mbps. Similar variations in the depiction of applicable bandwidths for the other technologies exist.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

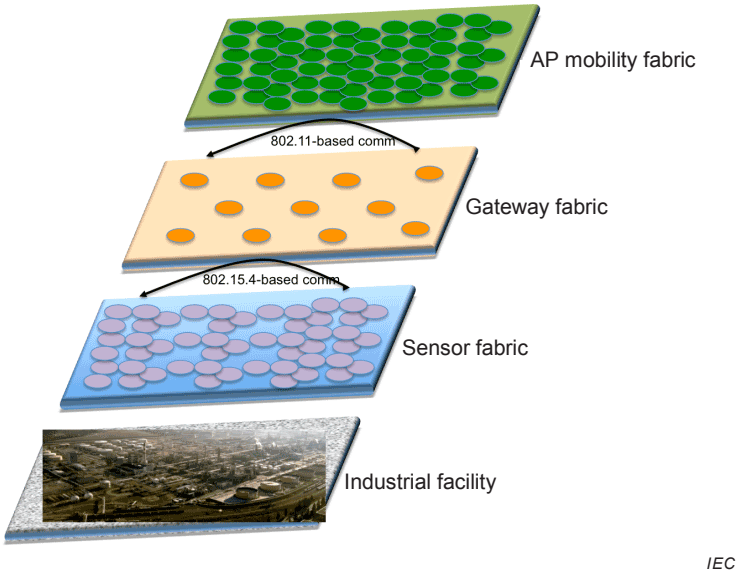


Figure 5 – Structured fabric design of layered wireless for an industrial facility

Using a designed solution – versus haphazard deployment – the result is an industrial site that may have a wide assortment of wireless technologies operating side-by-side at the plant with minimal (if any) RF coexistence.

In existing nuclear power plants, it may be impossible, impractical, or cost-prohibitive to add new sensors if they are to be hardwired to a monitoring location. Furthermore, the perception is that the cost and difficulty in hardwiring new sensors in a nuclear power plant is often not worth the benefits that can be gleaned from additional condition monitoring. As such, advanced predictive maintenance techniques have not served the industry as well as would be possible. Wireless sensors will help resolve this issue. Additionally, wireless technology for extending the plant network has shown promise in the US nuclear industry resulting in improved dissemination of information and overall personnel efficiency.

Voice communications can include the use of two-way radios, Voice over Internet Protocol (VoIP) telephony, etc. VoIP phones are becoming more prevalent in some nuclear industries offer a great degree of flexibility for voice communications throughout the plant.

Communications include the use of laptops or PDAs for the upload of data to the plant network, general network access, and data communications. Typically, Wi-Fi 802.11 networks are used for this purpose with strategically placed access points in necessary locations.

There are several nuclear plants which are using wireless sensors for asset condition monitoring. This can include wireless vibration sensors for traditional condition monitoring of rotating equipment, facilities monitoring, and more. This is seen as one of the most beneficial uses of wireless technology in the nuclear power industry. As an example of test relating to the in-service inspection in nuclear power plants, it is required that many sensors are temporarily installed for gathering the data for plant integrity checks in the case of the integral leak rate test.

The wireless smart transmitter composed of an RF transmitter at 424 MHz, a sufficient battery power supplies, RTD and humidity sensors and enclosures has been used in the integrated leak rate tests at nuclear power plants, with its specific ad hoc communication network. Each test has been successfully performed at pressurized water reactors.

In certain facilities, wireless cameras are being used for physical security purposes, analog gauge readings, personnel monitoring and so on. This has proven to be a simple and effective

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

use of the technology. Specifically, it is obvious to help reducing operators' workload for the periodic recording of any local panel indication.

Wireless personnel dosimeters have become fairly conventional in some nuclear power industry. There are some plants that use wireless controls for crane operation.

One site has placed wireless pressure transmitters on the HP turbine to monitor its performance as a baseline for comparison to a new turbine which will be installed in the future. Entergy Nuclear adopted the wireless technology at its River Bend Nuclear Station and saved $ 4 million US in the process. The traditional system would have been to install fiber optic cables. The move to wireless, the cost of the project dropped from an initial projection of $ 7 to $ 3 million US.

River bend is one of the first nuclear power plants to implement wireless technology for the continuity of a power project. The closed network that River Bend is using for indication and control is the Motorola canopy advantage wireless data network. The system operates at an unlicensed bandwidth and offers a 128-bit encryption algorithm. The project was designed with multiple, redundant secure networks to ensure high reliability. Snow and heavy rains have not affected on signal reliability. Over the years, optical fibers largely replaced copper wire communications in core networks and now fiber optics are being replaced by wireless technology.

There have been numerous case studies presenting all sorts of information regarding the use of wireless sensors in a utility environment. For example, the situation described in [7] – while titled as only pertaining to fossil-fueled power plants – is indicative of the deployment strategies and application areas for wireless sensors, systems and networks. A diagram showing the deployed wireless system is presented as Figure 6.

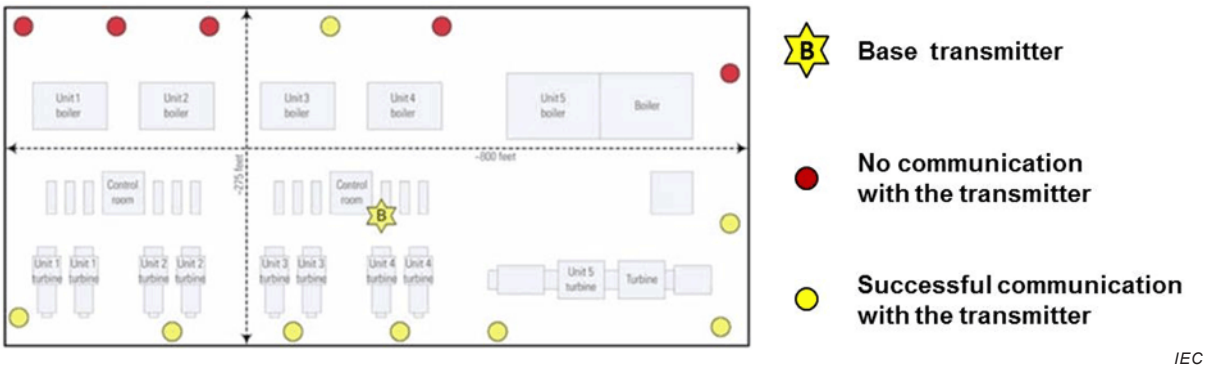


Figure 6 – Inexpensive wireless sensors in a fossil-fuel plant

6 Technology

6.1 Wireless basics

The pervasive use of wireless technology in nuclear power plants is inevitable. The technology is maturing at an extremely rapid pace due to the commercial market explosion over the last few decades of wireless-based products for personal and home use. This personal, widespread usage has generated a huge commercial wireless market with a never-ending list of new product offerings from very large corporations. This competitiveness has caused the wireless component technologies to standardize and improve in terms of reliability, security, and power management, which are the basic functional needs for use in the industrial markets.

Wireless communication is the transfer of information over a distance without the use of electric wires or conductors. How does it actually work? In its simplest form, a source device

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

creates EM waves that travel through air at close to the speed of light to reach a destination device. The source device can be any wire or conducting object (such as an antenna) that conducts alternating current creating EM radiation or "waves" propagated at the same frequency as the electric current. The wave is characterized by the wavelength and frequency, which are inversely proportional, so the shorter the wavelength, the higher the frequency. Thus, the wavelength for a 900 MHz device is longer than that of a 2,4 GHz device. In general, signals with longer wavelengths travel a greater distance and penetrate through and around objects better than signals with shorter wavelengths. An interesting artefact is that the closer the frequency is to visible light, the more it behaves like visible light. For that reason, 900 MHz radio has better barrier-penetrating properties than 2,4 GHz. As a general rule, the higher the frequency, the shorter the range, but the higher the available throughput so trade-offs are inevitable.

It is well understood that the further a receiver is from a transmitter, the less they received signal strength. This fundamental principle is based on the $1/r^2$ EM field law (sometimes referred to as the inverse square-law). In terms of communication systems, this means that the received signal strength (RSS) follows, for a line of site instance,

$$RSS\ x\ \frac{1}{R^2}$$

where R is the receiver-transmitter separation distance.[3]

Data are modulated or coded using conventional binary data (1s and 0s) onto an RF carrier. The wireless information is transmitted as a radio message using these 1s and 0s to represent the payload or actual message, plus additional data that control the message handling and/or the synchronization.

All industrial communication networks, whether wired or wireless, shall interconnect to other systems where sensor data are displayed, recorded, or fed back into control loops. In a world without wireless systems, the multi-level Purdue architecture reference model helped distinguish between categories of systems and their networks. However, in the de-parameterized wireless world, all systems share the same medium, often all in the same ISM band, and often geographically overlapping, and thus competing. The prime destination of wirelessly captured data from wireless systems in plants is also not clearly map-able on the Purdue model. In the wired world, it is common to look at DCS or SCADA systems as the landing point for all plant sensor data: a tag and an entry in the plant historian, with asset management and maintenance systems accessing plant instrument diagnostics via the DCS. Wireless systems, however, tend to produce data that is occasionally relevant to operators but more often relevant to optimization and maintenance staff or systems. Those applications reside more on the business networks and increasingly with third party contractors, i.e., on the internet.

Cyber security brings an additional challenge. Relative to Purdue, domain segregation was straightforward in the wired world, with firewalls between office and plant automation networks and firewalls between office networks and the internet. Disruptive perimeter-less wireless undermines that classical line of defense. Wireless offers the opportunity to provide sensor data at all levels of the Purdue model, with minimal deployment complexity while maintaining the appropriate level of cyber security. Figure 7 gives guidance on how to maintain domain segregation between internet, business, and plant networks without prohibiting wireless systems to receive or deliver data to the internet, the office, or the plant automation resident systems.

---

3 In general situations, the received signal strength decreases as $1/R^n$.

Documents
Document Sharing Hub

Full document details: PD IEC/TR 62918:2014

Wireless systems are either providers of wireless connectivity or users of that connectivity. Connectivity providers are, for example, plant-wide WiFi™ access points or cell phone towers. Connectivity users can be wireless sensors, tablet personal computers (PCs), video cameras, people-tracking and -tracing systems, or in-field wired control or safeguarding loops that can only be diagnosed and configured over wireless. Connectivity users are also tunnels that may be used within the classic Purdue model—for example, the microwave link that relays L2 between an offshore production platform and a satellite wellhead. Sometimes, a single field device can act as both a connectivity provider and a connectivity user. Mesh-to-the-edge wireless sensor networks are an example.

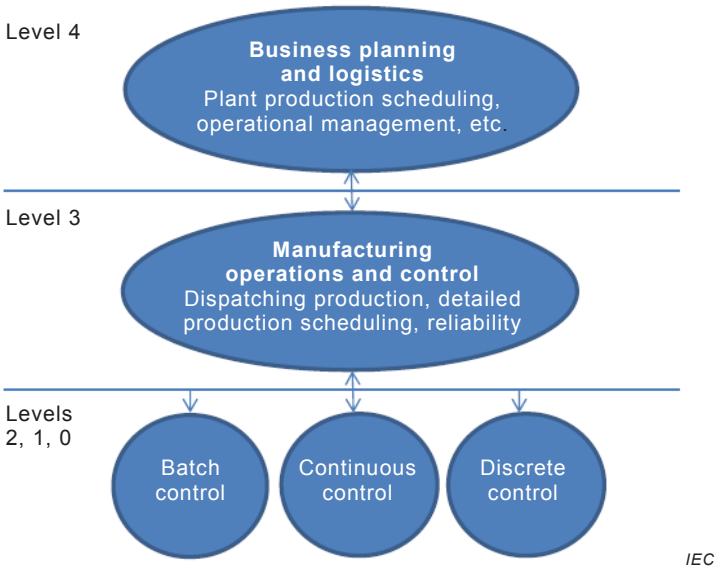


Figure 7 – Functional hierarchy

Walking counterclockwise (CCW) around the diagram (Figure 8), the top left component is the sensor. In the process arena, this tends to be of the temperature, pressure, vibration, etc. variety. The generic design makes no distinction is the sensor is “intrinsic” (on the board) or “extrinsic” (cabled to the board). Continuing CCW, the auxiliary circuitry block may support the sensor – perhaps as an Application Specific Integrated Circuit (ASIC). The details of the circuitry are tightly coupled to the sensor and manufacturer’s design. Power for the wireless sensor comes from the Power System (PS) block. The PS may simply be a battery or it may involve an energy/power harvesting function with associated storage means.

At this point we have described a generic sensor, or field transmitter, design with no details of the wireless functions.

Continuing the CCW walkabout, the core component of the wireless transport method is seen, namely, the RF transceiver – the radio. A wide array of arcane operational and performance matters come into play with the RF transceiver, including modulation format, operating frequency, transmit power, receiver sensitivity – the list goes on and on. Obviously, wireless sensors (field transmitters) have been around for years. In the old days, the transceiver was coupled to complex hybrid (analog + digital) circuitry to achieve the (somewhat) stable wireless transmission.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

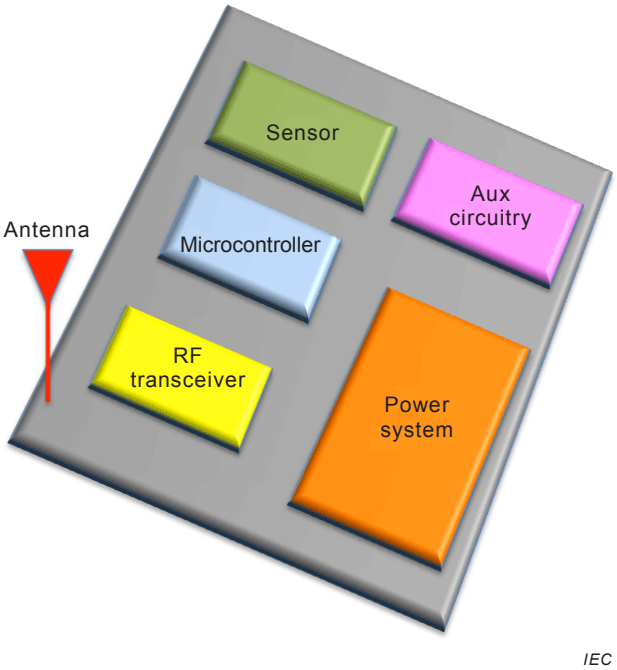


Figure 8 – Simplified diagram of a generic wireless sensor design

6.2 Industrial wireless sensor networks

In this subclause, field edge devices and the network that provides connectivity for them are detailed. Figure 9 depicts the communication areas addressed by IEC PAS 62734 or IEC 62591 (formally referred to as WirelessHART® standards, as well as those areas [shaded in blue] that are not in the scope of these standards). In Figure 9, circular objects represent field devices (sensors, valves, actuators, etc.), and rectangular objects represent infrastructure devices that communicate to other network devices via an interface to the infrastructure backbone network. A backbone is a data network (preferably high data rate) not defined by this standard. This backbone could be an industrial Ethernet, IEEE 802.11, or any other network within the facility interfacing to the plants network. A complete network, as defined in this standard, includes all components and protocols required to route secure traffic, manage network resources, and integrate with host systems. A complete network consists of one or more field networks connectable to a plant network via an infrastructure device. A field network consists of a collection of field devices that wirelessly communicate using a protocol stack defined by this standard. As shown in Figure 9, some field devices may have routing capabilities, enabling them to forward messages from other devices.

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

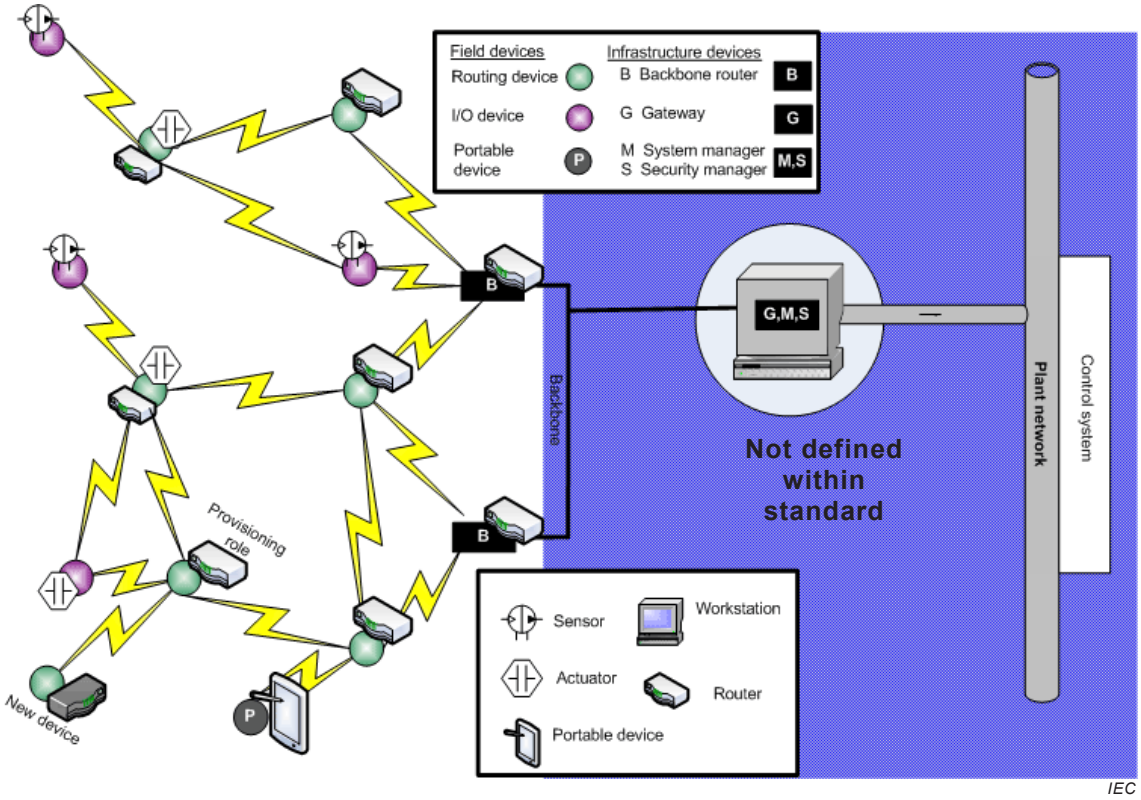


Figure 9 – Standard compliant network

Characteristics of a wireless industrial sensor network (WISN) include:

a) Scalable
b) Extensible
c) Support for simple operation
d) Unlicensed operation
e) Robustness in the presence of interference and with non-WISNs
f) Determinism or contention-free media access
g) Self-organizing network with support for redundant communications from field device to plant network
h) IP-compatible network layer
i) Coexistence with other 5 wireless devices in the industrial workspace
j) Security, including data integrity, encryption, data authenticity, replay protection, and delay protection
k) System management of all communication devices
l) Support for application processes using standard objects
m) Support for tunnelling, i.e., transporting other protocols through the wireless network

6.3 Radio frequency

6.3.1 Applications

The deployment and value of industrial wireless is based on two broad application classes: those enabling personnel mobility and those derived from the reduced cost of installation (e.g., not having to run wires).

Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014

Enabling process operators to traverse the facility while staying connected to plant information systems enables operators to be more efficient in their work as well as providing stationary operators with a more precise understanding of what is happening in different parts of the facility. While in the field, plant personnel can receive real-time alarms, alerts, process displays, streaming video, voice communication, and have full access to enterprise applications that track and locate material, equipment, staff, visitors, contractors, and first responders.

Table 1 – List of "industrial" radio technology standards and their candidate applications

Number	"Common" name	Operational frequency	Unlicensed (Yes/No)	Typical application
802.11 a-z	Wi-Fi	2,4 GHz, 5,7 GHz	Yes	Wireless LAN
802.15.1	Bluetooth	2,4 GHz	Yes	Wireless PAN
802.15.3	WiMedia	~5 GHz	*	High data rate, short distance
802.15.4	ZigBee/ISA100.11a/ WiHART	2,4 GHz	Yes	Low rate industrial sensors
802.15.4a	"chirped"	2,4 GHz	Yes	Low rate sensors and position
Sat Comm	Satellite Communications	Ku, K, Ka bands (12 GHz-40 GHz)	No	Broadband, data transport
802.16	WiMAX (WiBro)	2 GHz-11 GHz, 10 GHz-60 GHz	No	Broadband wireless
802.20	MBWA	<3,5 GHz	No	IP-based data transport
1451	Sensors	900 MHz, 2,4 GHz	Yes	Sensor transport using 802.15.4 and 802.11
1901	RuBee	135 kHz	Yes	location
Wi-Di	Wireless Display	5,7 GHz	Yes	HD displays using 802.11n
RF SCADA	Wireless SCADA	<1 GHz	No/Yes	SCADA transport
FRS/GMRS PMR446(Europe)	Walkie-Talkies	27, 49, 462-467 MHz, 446 MHz (E)	Yes/No	Personal communication
IS95/IS136/others (cellular)	CDMA/TDMA	Multiple Bands	No	Telephony
3GPP TS 45.005	GSM	Multiple Bands	No	Telephony
ISO 18000-7	DASH7	433 MHz	Yes	Wireless sensors, RFID
ISO/IEC 14443	Near Field Communications	13,56 MHz	Yes	Short distance (10 cm) data transfer
UWB	Wireless USB	3,1 GHz – 10,6 GHz	Yes*	High data rate, <10 m
Wireless HD		60 GHz	Yes	High def transmission
WHDI	Wireless Home Display Interface	5,7 GHz	Yes	Up to 3 Gbps, short distance

Since most plants operate under a fixed budget, reducing installation and maintenance costs provides additional resources to increase the number of measurement points within a process. Additional process measurements can improve process efficiency and optimization, saving resources, energy and increasing throughput. Added condition monitoring measurements can dramatically increase maintenance efficiency, reducing equipment costs and preventing downtime due to asset failures. The industrial facility of the future is built on

AVA Documents
Document Sharing Hub
Full document details: PD IEC/TR 62918:2014