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.™

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.

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

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

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.

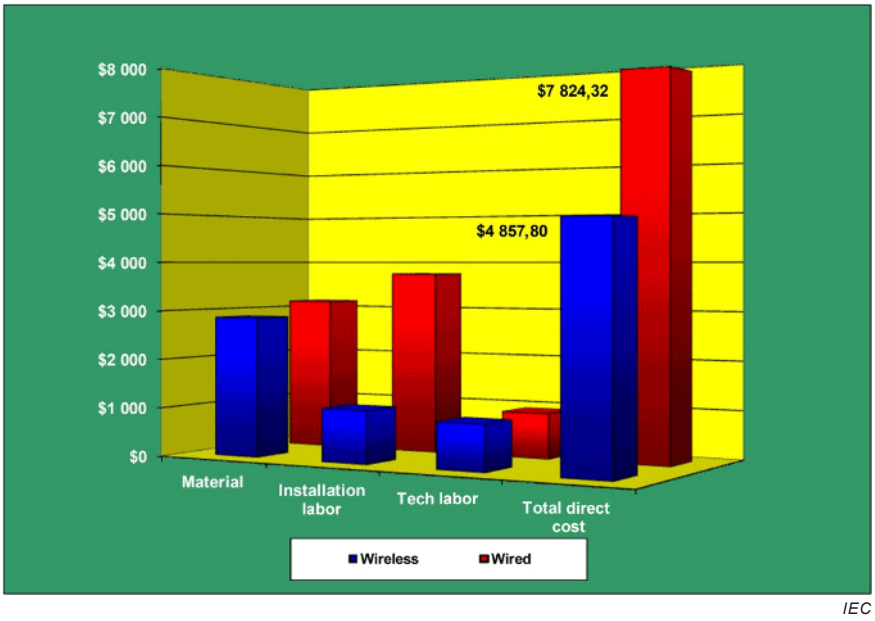


Figure 1 – Cost comparison – Wired versus wireless for an extensive building automation system

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.

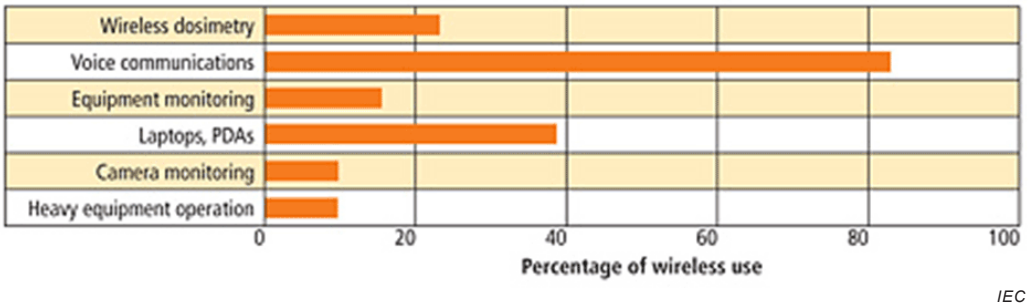


Figure 2 – Wireless use in nuclear power plants

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.

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

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.

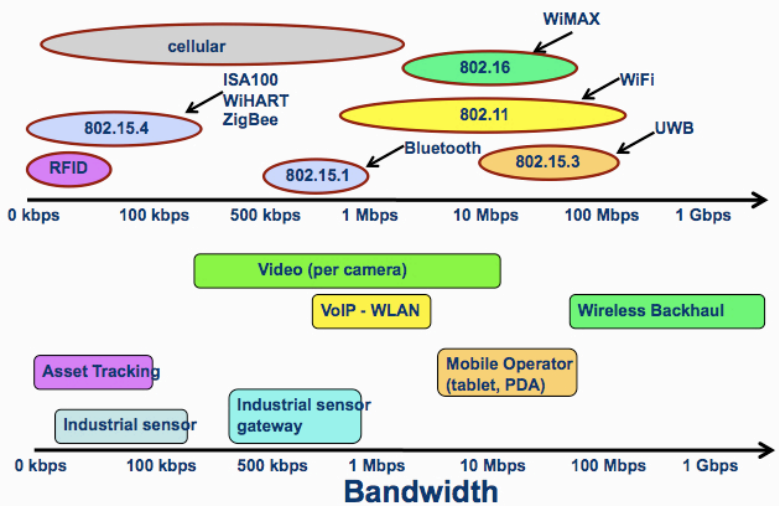


Figure 4 – Bandwidth requirements for a variety of applications and the associated wireless technology that can support such requirements

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.

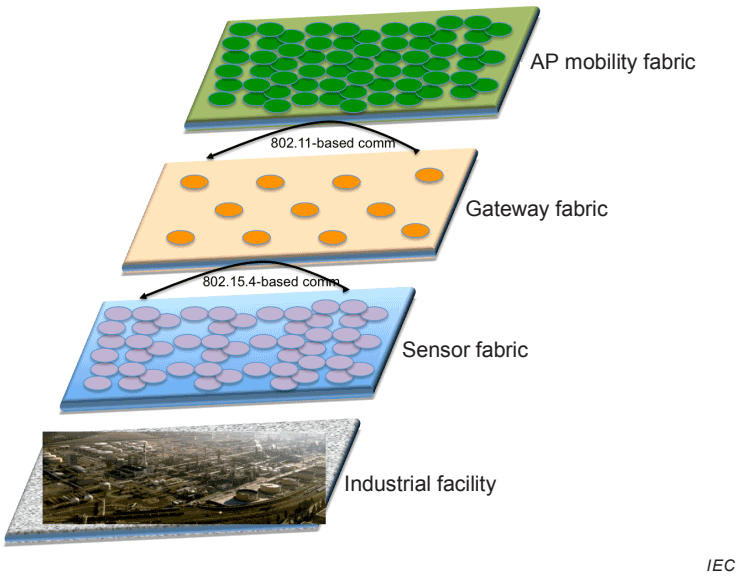


Figure 5 – Structured fabric design of layered wireless for an industrial facility

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

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.

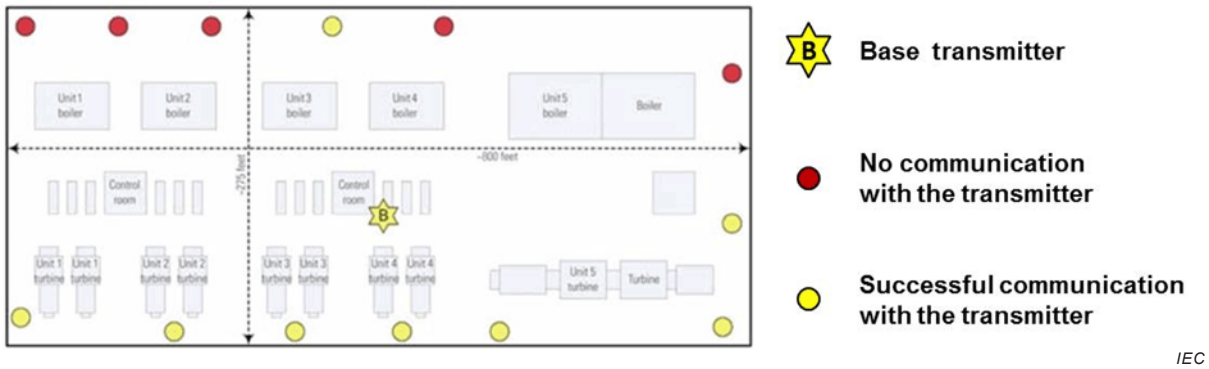


Figure 6 – Inexpensive wireless sensors in a fossil-fuel plant

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

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 $1/R^n$.

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.

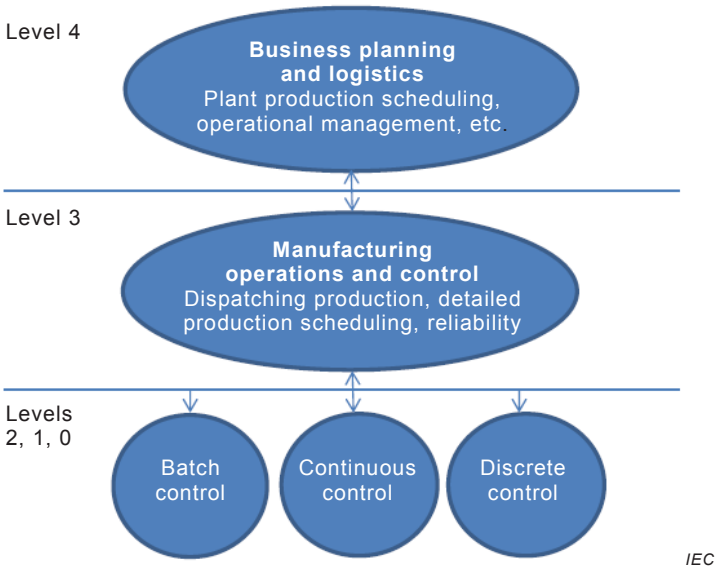


Figure 7 – Functional hierarchy

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.

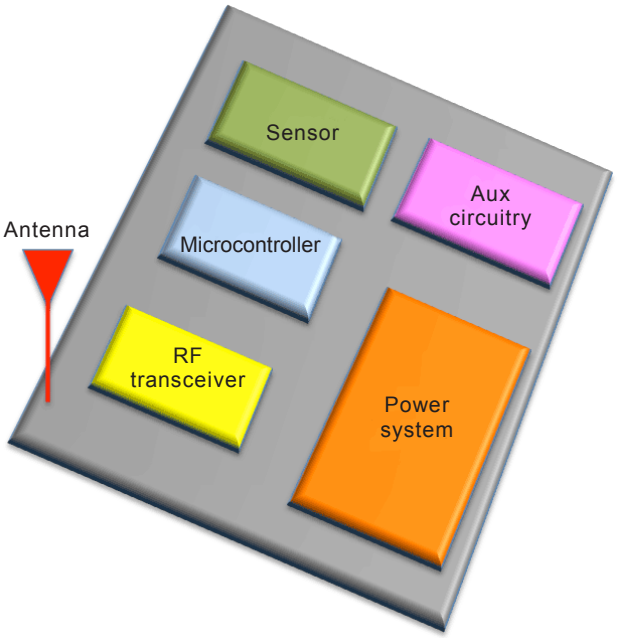


Figure 8 – Simplified diagram of a generic wireless sensor design

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.

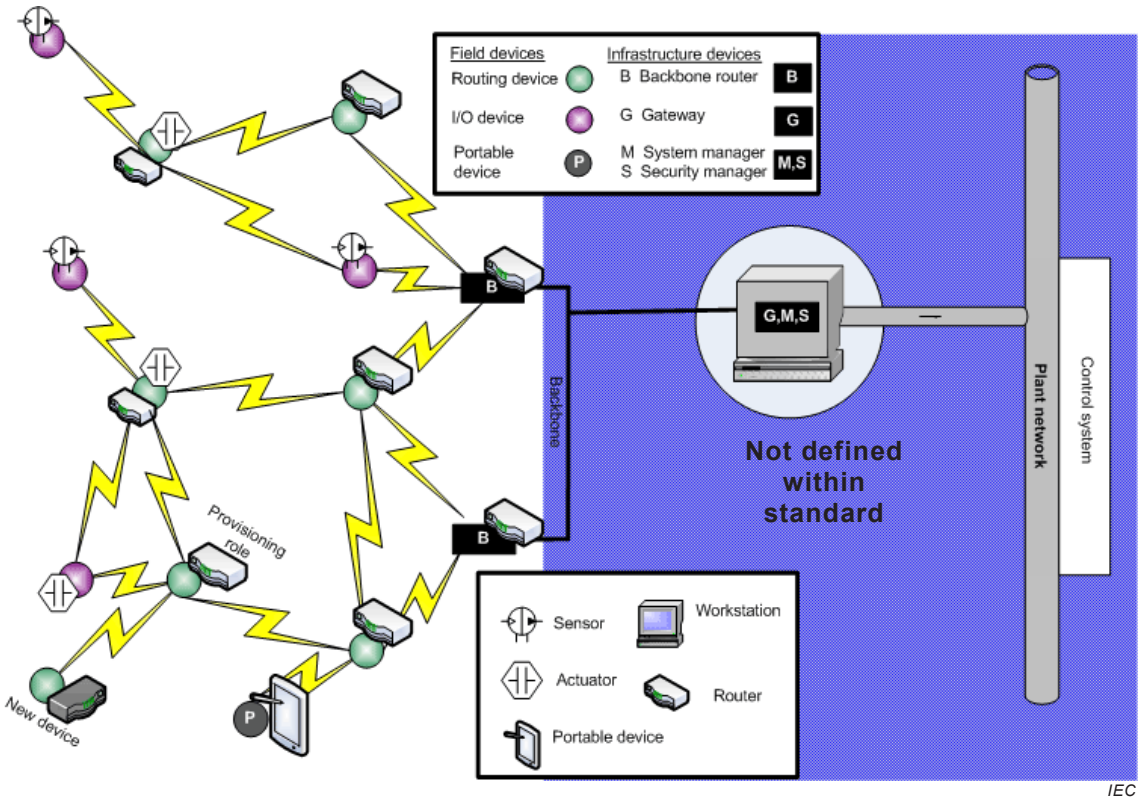


Figure 9 – Standard compliant network

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).

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

having a complete understanding of what is happening within that facility and wireless sensors/communications are the most cost effective means of providing that understanding.

The standards applicable to wireless technologies are presented in Table 1. The table lists the standard, its common name, the frequency range, whether or not the system/elements use an unlicensed (ISM; Industrial, Scientific and Medical) radio band as defined by ITU-T and the typical application of the technology.

When implementing wireless technologies one of the important considerations is the communication frequency range and what, if any, co-existence concerns may be created. The vast majority of wireless sensor networks (field transmitters) rely on radios that operate in the Industrial, Scientific, and Medical (ISM) license-free frequency bands. The International Telecommunications Union (ITU) specifies the ISM frequency bands available for use throughout the world in sections 5.138, 5.150 and 5.280 of the Radio Regulations.

Perhaps the most prevalent use of wireless technology at industrial facilities is associated with cellphones. There are significant differences between cellular systems operating in the US and the rest of the world. Even within an individual country there are multiple cellular technologies operating at multiple frequencies. The cellular systems and their associated operating frequencies for the US are presented in Table 2. The Global System for Mobile Communications (GSM) is the most prevalent mobile telephony technology deployed around the world (~80 % of all cellular systems deployed are GSM). GSM may operate in a wide variety of frequencies presented in Table 3.

Table 2 – Cellular telephony frequencies in the US

Current / planned technologies	Frequency MHz
SMR iDEN	806-824 and 851-869
AMPS, GSM, IS-95 (CDMA), IS-136 (D-AMPS), 3G	824-849, 869-894, 896-901, 935-940
GSM, IS-95 (CDMA), IS-136 (D-AMPS), 3G	1 850-1 910 and 1 930-1 990
3G, 4G, MediaFlo, DVB-H	698-806
Unknown	1 392-1 395 and 1 432-1 435
3G, 4G	1 710-1 755 and 2 110-2 170
4G	2 500-2 690

Table 3 – GSM frequency bands, channel numbers assigned by the ITU

System	Band	Uplink MHz	Downlink MHz	Channel number
T-GSM-380	380	380,2–389,8	390,2–399,8	dynamic
T-GSM-410	410	410,2–419,8	420,2–429,8	dynamic
GSM-450	450	450,4–457,6	460,4–467,6	259–293
GSM-480	480	478,8–486,0	488,8–496,0	306–340
GSM-710	710	698,0–716,0	728,0–746,0	dynamic
GSM-750	750	747,0–762,0	777,0–792,0	438–511
T-GSM-810	810	806,0–821,0	851,0–866,0	dynamic
GSM-850	850	824,0–849,0	869,0–894,0	128–251
P-GSM-900	900	890,2–914,8	935,2–959,8	1–124
E-GSM-900	900	880,0–914,8	925,0–959,8	975–1 023, 0-124
R-GSM-900	900	876,0–914,8	921,0–959,8	955–1 023, 0-124
T-GSM-900	900	870,4–876,0	915,4–921,0	dynamic
DCS-1800	1 800	1 710,2–1 784,8	1 805,2–1 879,8	512–885
PCS-1900	1 900	1 850,0–1 910,0	1 930,0–1 990,0	512–810

6.3.2 802.11 (Wi-Fi), 802.15.1 (Bluetooth), 802.15.4 (sensors)

A wealth of information pertaining to radios compliant with IEEE standards 802.11, 802.15.1, and 802.15.4 – excluding, personal communications devices, the most prevalent radio technologies found at nuclear power plants – is available online (e.g., www.wikipedia.org/wiki/802.11). The following information is provided as an overarching guide to these radio technologies.

In standards-compliant wireless operation, most devices have gravitated to using either an IEEE 802.15.4-compliant wireless channel or an IEEE 802.11b/g compliant channel. Note that not all of the exhibited devices operate under IEEE-compliance, rather they could be running their own protocol (etc.) and be broadcasting in the ISM bands (the beauty of an unlicensed wireless). The result is easy to predict, namely numerous sensors/instruments/transmitters all attempting to operate in the same 2 400 MHz channels resulting is considerable congestion and coexistence issues. The principal ISM radio transceivers encountered in industrial settings are based on 802.15.1, 802.15.4, and 802.11.

The 2 400 MHz channel assignments for 802.15.1 are shown in Figure 10. Figure 11 shows the channel assignments for 802.15.4 while the 2 400 MHz frequencies associated with 802.11 are shown in Figure 12.

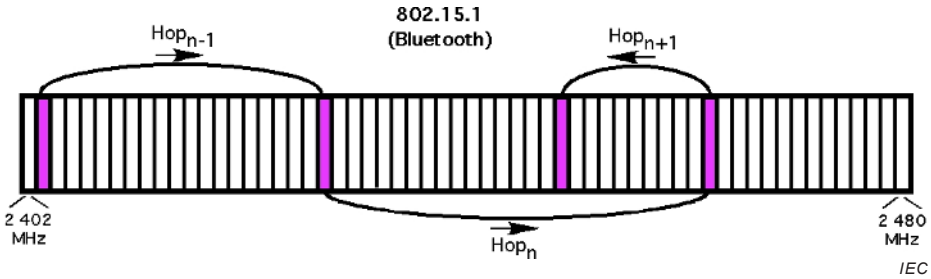


Figure 10 – 802.15.1 (Bluetooth) frequency channels in the 2 450 MHz range

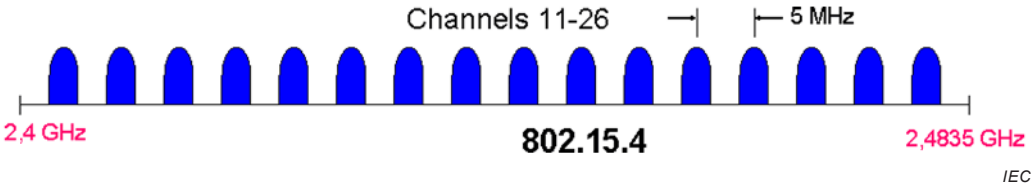


Figure 11 – 802.15.4 frequency channels in the 2 450 MHz range

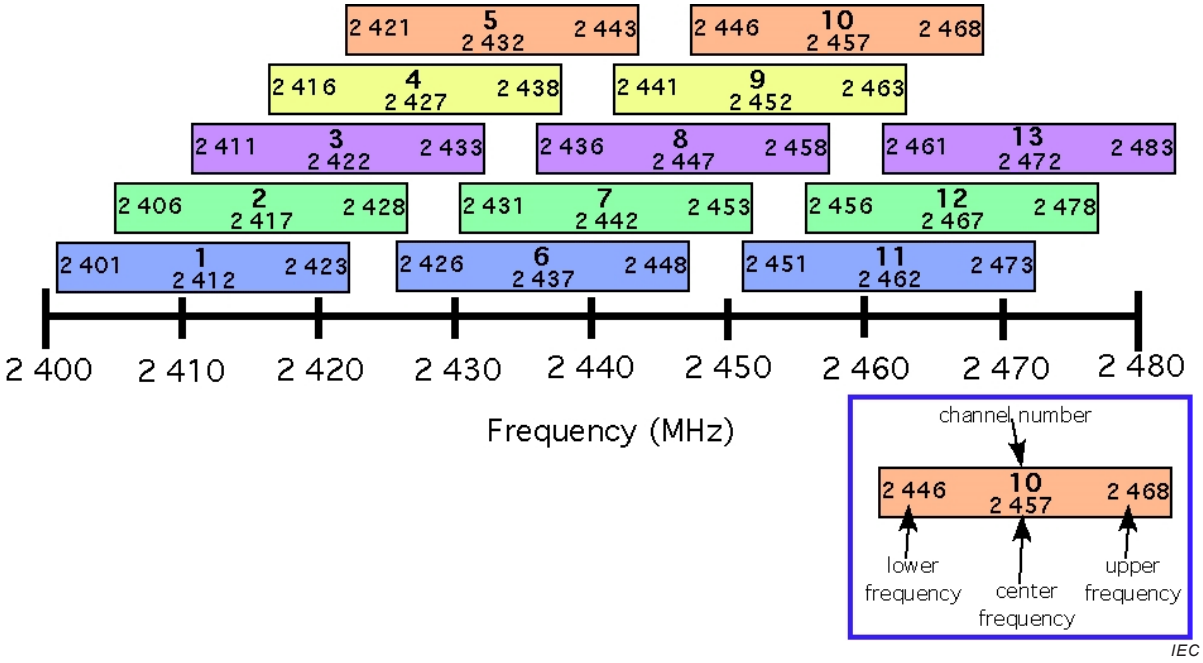


Figure 12 – Overlapping channel assignments for 802.11 operation in the 2 400 MHz range

The situation for 802.11 in industrial settings warrants further examination. The IT departments at many, if not all, organizations has or is contemplating deploying 802.11 (Wi-Fi) networks in support of a wide range of applications that cross multiple business units (e.g., video surveillance, mobile operator support, etc.). From a frequency perspective, 802.11b/g utilizes the 22 MHz channels that are listed in Figure 13. A higher data/throughput rate is achieved in 802.11n. 802.11n provides an option to double the bandwidth per channel to 40 MHz. 802.11n operating in the 20 MHz bandwidth is frequently referred to as single stream. The 40 MHz situation is referred to as dual stream and provides approximately twice the data/throughput rate of single stream 802.11n. 802.11n defines operation in the 2,4 GHz and 5,7 GHz bands. However, when in 2,4 GHz enabling the dual stream option takes up to 82 % of the unlicensed band, which in many areas may prove to be unfeasible.

The 802.11n specification calls for requiring one main 20 MHz channel as well as an adjacent channel spaced ±20 MHz away. The main channel is used for communications with clients incapable of 40 MHz mode. When in 40 MHz mode the center frequency is actually the mean of the main and auxiliary channel. 802.11n may operate in a “single stream” (20 MHz plus tones) bandwidth channel or “dual stream” (40 MHz plus tones) bandwidth channel. The 802.11n “dual stream” situation is shown in Figure 13.

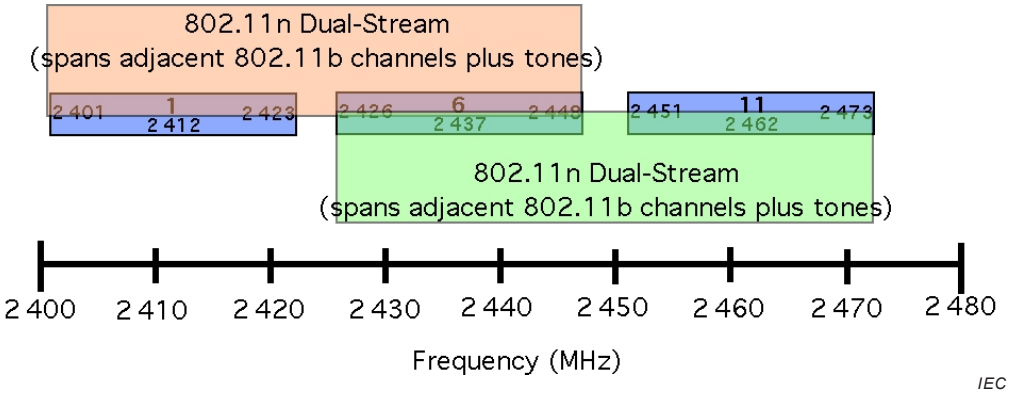


Figure 13 – 802.11n dual stream occupies 44 MHz of bandwidth. Dual stream 802.11n in the 2,4 GHz band

The industrial wireless sensor usage of battery-powered 802.15.4-based devices is based on low duty cycle operation with data readings delivered every few seconds, few minutes or even every few hours. This leads to bursty traffic that is infrequent.

The coexistence implications for co-channel interference of 802.11 and 802.15.4 signals are asymmetrical. Per the IEEE standards, a properly operating 802.15.4 transceiver shall not interfere with 802.11 – therefore there is no impact of a sensor network on an 802.11 Wi-Fi network. In the case of an 802.11 transceiver that is in the RF "proximity" of an 802.15.4 transceiver – again per the IEEE standards – the 802.15.4 is to use CCA to ascertain if there is an interfering signal. If there is, then the device is to wait a (pseudo) random amount of time and check the channel again, or move to a different 802.15.4 channel and again check CCA, or some combination of both actions. This arena is of intense academic research.

The probability of 802.11 broadcasting when an 802.15.4 transceiver is set to transmit is multivariate with a complete description outside of the bounds of this Technical Report[4]. A simple rule of thumb is that 802.11 channel is less active if video is not being streamed.

6.4 Satellite leased channels and VSAT

A satellite circuit has five elements – two terrestrial end points, an uplink, a downlink, and a satellite repeater circling the earth either in geosynchronous orbit at 22 241 miles (35 793 km) above the equator, or in low-earth orbits (LEOs) that travel faster than the earth's rotation and do not appear "stationary" over a specific location on earth, but suffer from less of a communications delay. Usually each LEO communicates with a network of LEOs that have been positioned to provide continuing coverage.

Satellites employ several techniques to increase the traffic carrying capacity and to provide access, namely: FDMA (frequency division multiple access), TDMA (time division multiple access), and DAMA (demand assigned multiple access).

The primary technical issue with geosynchronous satellite communications is the ¼ second time delay between two earth stations. Data communication circuits can experience unacceptably low throughput via a satellite if they use a block transmission protocol that requires a station to transmit a new block only after the receiver acknowledges the preceding block. Most protocols used with satellites now get around this problem either by sending very large blocks or by allowing multiple blocks to be transmitted before expecting acknowledgments.

---

4 Readers interested in further details of models used to predict 802.15.4 (CSMA-CA) performance in the presence of 802.11 signals – and verification studies of such models – should visit the communications and multimedia protocol section of www.prismmodelchecker.org.

A secondary issue is the “eclipsing” of the geosynchronous satellites twice a year in spring and autumn as the earth blocks the sun from providing power to the satellites. In addition, strong solar geomagnetic activity can disrupt communications and even drop satellites out of their normal orbits.

Several satellite-based services are available. The one most often used by utilities is called Very Small Aperture Terminal (VSAT) that uses a very small transmitting antenna (from 0,6 m to 3,8 m), and is star-connected with a hub at the center of the network and with dedicated lines running to the host computer (Figure 14). The hub has a large antenna aimed at the satellite. The hub is very expensive and is usually owned by the VSAT vendor. TDMA and spread spectrum technologies are the most common ways of allocating access to the hub by the VSATS. VSAT provides bandwidth as high as T1/E1 or as low as what the customer needs for video, voice and data, typically 9,6 kbps.

These VSAT systems are particularly cost-beneficial for accessing low volumes, but important data which is spread over wide territories. Rural coops or utilities with substations in very remote areas find VSAT systems particularly beneficial. They can also serve as backup communications for very critical systems, particularly in locations that might be affected by widespread terrestrial disasters, such as hurricanes and earthquakes.

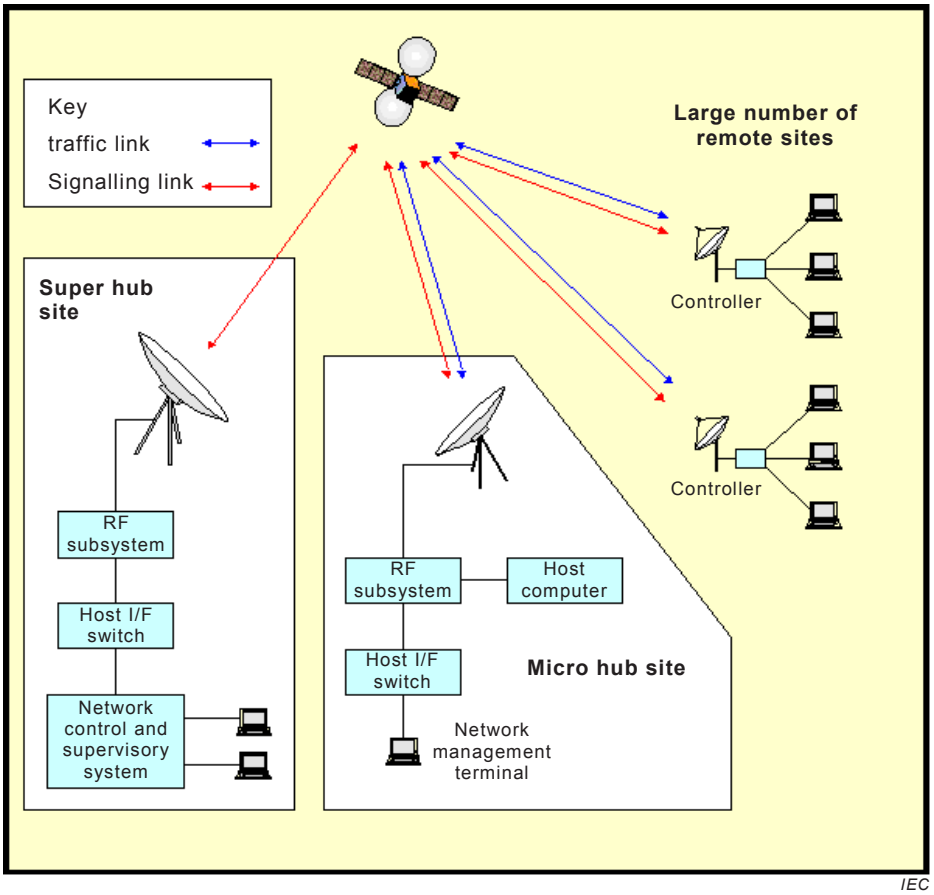


Figure 14 – VSAT mini-hub network configuration

6.5 Magnetic field communications

Another wireless communication technology for consideration uses magnetic fields, not radio frequencies. The magnetic field is the distance from radiating electromagnetic fields to the point at which the electromagnetic fields start to propagate. This distance is expressed mathematically as $l/2p$ (l: wavelength). In this range, the magnitude of magnetic fields is stronger than that of electric fields, so the strength of electric fields can be ignored. Thus, the

characteristics of the magnetic field are dominant. Using Maxwell's equations to construct a description of the electric and magnetic field generated by an infinitesimally small constant current loop element, expressed in spherical coordinated results in the following.

The wireless communication system usually uses a current loop antenna for radiating a low frequency signal and uses magnetic fields as a medium. This enables the system to provide a reliable communication service even in water and metal, compared to the conventional wireless communication systems.

The magnetic field wireless communication technology can be done in the magnetic field in several hundreds of kHz frequency band. The permeability of magnetic fields in water is almost the same as that of air. Thus, there is no difference between the attenuation rate in air and that in water. And the magnetic field communication system can receive magnetic energy even though surrounded by metal, if there is a slight gap.

6.6 Visual light communication (VLC)

Visible light communication (VLC) is characterized by a "line of sight" transfer of data between the transmitter and the receiver. The LED Standard document defines the relationship, necessity and basic structure of the LED interface between illumination and visible light communication. This standard specification plays a key role in supporting the visible light communication using LED illumination. And this standard will contribute to activation of many application services using the LED illumination.

The basic configuration of the light location information service model using VLC defines the scope of the function and the requirements for indoor location based service using VLC. This model also defines the location-based service which is composed of navigation services, indoor information services, push services and public safety services in an indoor VLC environment. Location or position information is obtained from each unique ID assigned illumination. VLC using location-based information is composed of two system models: one-way passive system and two-way dynamic system. This specification plays a key role in supporting the location-based service industry development using the VLC, and the navigation service, indoor information service, push service and public safety service.

Lighting identification for VLC defines the visible lighting ID standard for visible light communication and the object of the management and the management method. This standard also defines various services using the visible lighting ID. And this standard specification plays a key role in supporting the LBS (location-based service) industry development using the visible lighting ID, and other services.

6.7 Acoustic communication

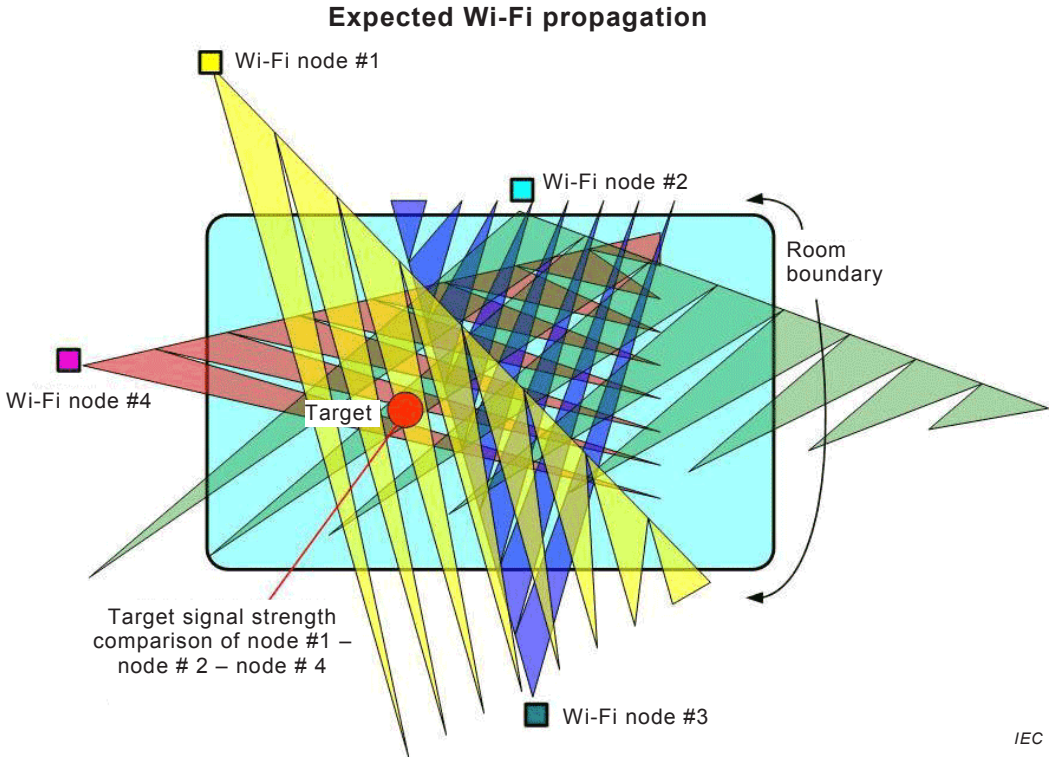
Underwater acoustic communication is a technique of sending and receiving messages below water. There are several ways of employing such communication but the most common is using hydrophones. Underwater communication is difficult due to factors like multi-path propagation, time variations of the channel, small available bandwidth and strong signal attenuation, especially over long ranges. In underwater communication there are low data rates compared to terrestrial communication, since underwater communication uses acoustic waves instead of electromagnetic waves.

Earlier underwater acoustic communication systems have been relying on scalar sensors only, which measure the pressure of the acoustic field. Vector sensors measure the scalar and vector components of the acoustic field in a single point in space and, therefore, can serve as a compact multichannel receiver. This is different from the existing multichannel underwater receivers, which are composed of spatially separated pressure-only sensors, which may result in large-size arrays. In general, there are two types of vector sensors: inertial and gradient. Inertial sensors truly measure the velocity or acceleration by responding to the acoustic medium motion, whereas gradient sensors employ a finite-difference approximation to estimate the gradients of the acoustic field such as velocity and acceleration.

6.8 Asset tracking utilizing IEEE 802.11 – Focus on received signal strength

Numerous techniques for RTLS are based on the strength of the signal received by the asset's attached radio changing – and associating that received signal strength variation with a change in the separation distance between the gateway/access point and the asset's receiver.

Infrastructure requirements for a WiFi RSSI-based asset tracking system are not dissimilar from that of any typical data or voice deployed wireless network (Figure 15). WiFi Tags are managed as any other wireless client, with the exception that Voice and Data solutions are given network priority to maintain Quality of Service and Production Application availability. WiFi Tags are maintained on separate VLANs to maintain separation from production Wireless Applications.



Note Node #3 is not in play as target is out of range.

Figure 15 – Spatial resolution is provided in multiple axes only if the tag (target in this Figure) is in communications with multiple APs

There are solutions that offer state-of-the art deployment tools for verifying that the infrastructure requirements are met, and in cases where the requirements are not met, problem areas are indicated with resolution options provided. It should be noted that a typical VoIP Wireless Network provides excellent location granularity and at least one solution provides software clients for tracking VoIP phones.

While the RF footprint is obviously dependent on the transmit power and antenna gain (directionality), the typical indoor specified WiFi-compliant range is on the order of ~50 m.

One advantage of the RSSI solutions is that the RF coverage for RTLS can be easily determined through utilization of the 'location coverage' visualization provided through specific site survey products. This in conjunction with the 'network requirements' visualizations make it easy to visualize and report on areas of strong coverage and to also identify areas where the network might be improved for RTLS location accuracy, if asset location requirements dictate increased accuracy. In essence some site survey products allow

you to manage your wireless network, while reporting and planning location performance for asset tracking.

ISO 24730-2 MODE: Various WiFi-tags are multi-use in the context that they may also deliver tag information via schemes that are not specifically IEEE 802.11-based. Of particular note is ISO 24730-2. This standard is a superset of the ANSI 371.1 Time-of-arrival location derivation protocol which was designed for asset tracking. When using this protocol, the tag transmits 0 dBm “blinks” with a 60 MHz bandwidth using a DSSS modulated 2,4 GHz ISM band carrier (this is not IEEE 802.11-based WiFi, but a proprietary system). Tags can be programmed using a magnetic data link, with a 2,4 GHz On-Off Keyed/Frequency-Shift-Key (OOK/FSK) modulation scheme for command acknowledgement. The tag also sends specific DSSS-modulated signals when receiving signals from a magnetic choke-point transmitter. A network architecture depicting this situation is provided as Figure 16.

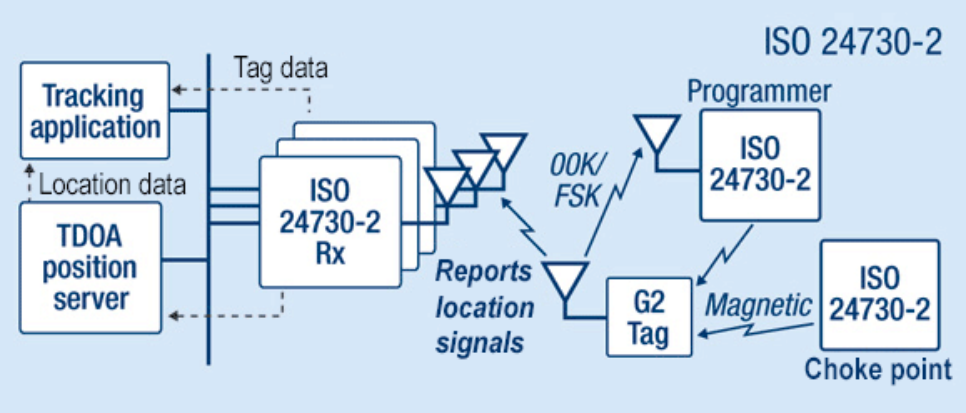


Figure 16 – ISO 24730-2 architecture

EPC MODE: The electronic product code (EPC) activities are related to the aforementioned ISO 24730-2 effort in the sense that various vendors are offering products that may support WiFi-based tags, ISO 24730-2 based tags and EPC tags. Of specific note is that many but not all EPC tags communicate in the 868/900 MHz band.

6.9 Asset tracking (RFID/RTLS): ISO 24730

ISO 24730 defines two air interface protocols and a single application program interface (API) for real-time locating systems (RTLS) for use in asset management. Marketing material from this group states that ISO 24730 is intended to allow for compatibility and to encourage interoperability of products for the growing RTLS market. ISO 24730 has specific details already defined, such as “To be fully compliant with this standard, RTLS shall comply with ISO 24730-1:2006 and at least one air interface protocol defined in ISO 24730”. In the ISO 24730 parlance, RTLS are wireless systems with the ability to locate the position of an item anywhere in a defined space (local/campus, wide area/regional, global) at a point in time that is, or is close to, real time. Position is derived by measurements of the physical properties of the radio link.

They have conceptually organized RTLS functionality into four classifications:

a) Locating an asset via satellite (requires line-of-sight) – accuracy to 10 m.

b) Locating an asset in a controlled area, e.g. warehouse, campus, airport (area of interest is instrumented) – accuracy to 3 m.

c) Locating an asset in a more confined area (area of interest is instrumented) – accuracy to <1 m (typically tens of centimetres).

d) Locating an asset over a terrestrial area using a terrestrial mounted receiver over a wide area, e.g. cell phone towers – accuracy to 200 m.

In trying to delineate between the RFID-BASED (i.e., portal-based) method, ISO 24730 defines two methods of locating an object which are really RFID-BASED rather than RTLS:

a) Locating an asset by virtue of the fact that the asset has passed point A at a certain time and has not passed point B.

b) Locating an asset by virtue of providing a homing beacon whereby a person with a handheld can find an asset.

In b) the method of location is through identification and location, generally through multi-lateration using one (or more) of these different techniques: Time of Flight Ranging Systems, Amplitude Triangulation, Time Difference of Arrival (TDOA), Cellular Triangulation, Satellite Multi-lateration, Angle of Arrival.

Of special note is that ISO/IEC 24730-1:2006 defines an API needed for utilizing an RTLS. This API describes the RTLS service and its access methods, to enable client applications to interface with the RTLS.

7 Current wireless technology implementations

7.1 General

The following is a detailed description of interviews conducted with different facilities on their use of wireless technology (Table 4).

Table 4 – Specific uses of wireless technologies in the nuclear industry

Nuclear Plant, Type, and Location	Voice Communication	Laptop/PDAs Communication	Equipment Monitoring	Camera Monitoring	Wireless Dosimetry	Heavy Equipment Operation	Process Monitoring
Arkansas Nuclear One (ANO) B&W PWR Russellville, AR	✓	✓		✓	✓		
Comanche Peak Westinghouse PWR Glen Rose, TX	✓	✓	✓	✓			
Diablo Canyon Westinghouse PWR San Luis Obispo, CA	✓	✓			✓		
Farley Westinghouse PWR Dothan, AL	✓	✓		✓	✓		
San Onofre C-E PWR San Clemente, CA			✓				✓
South Texas Project Westinghouse PWR Bay City, TX	In Development						

7.2 Comanche Peak nuclear generating station

One of the most extensive deployments of wireless technology in the US nuclear industry can be found at the Comanche Peak nuclear generating station. To upgrade their voice communications system, Comanche Peak installed a wireless data network (based on the IEEE 802.11b standard), in conjunction with Voice over Internet Protocol (VoIP) phones, provides the necessary coverage to ensure plant personnel are accessible throughout the entire plant. Once the network was implemented for voice communications, it has also been leveraged for other applications such as laptop computers, wirelessly-enabled devices for viewing and uploading real-time data, and wireless camera feeds. These camera feeds are used to view areas during outages, monitor personnel traffic, or to obtain analog gauge readings in remote locations.

Another significant wireless application at Comanche Peak is condition monitoring. This includes adding vibration and temperature sensors to monitor the condition of pumps and motors throughout the secondary side of the unit. Working in conjunction with EPRI and Azima DLI, Comanche Peak's parent company, Luminant, operates a condition monitoring office in Dallas, TX which receives data from wireless vibration and temperature sensors and analyzes the condition of equipment at Comanche Peak and Luminant's other fossil fuel sites. Data from the wireless sensors are analyzed and integrated with the Luminant PI data historian for viewing alongside other plant equipment. Installing wireless sensors for equipment condition monitoring at Comanche Peak has significantly improved the manual predictive maintenance program that was used at the facility. Direct savings can be realized from a number of sources which include improved data collection, reduction in human error, time savings from unnecessary labor, and improved data analysis resulting in better prediction of equipment failure. The initial annual savings calculated as a result of the joint effort between EPRI, Azima DLI, and Comanche Peak was $ 24 900 [14]. This was reported in late 2005.

To address EMI/RFI concerns associated with a wireless network, Comanche Peak performed qualification testing and EMI/RFI site mapping for both the wireless system as well as sensitive equipment within the plant. As a result, precautionary exclusion zones were established around sensitive equipment to ensure that the wireless systems would not interfere or interrupt existing equipment. During EMI testing, Comanche Peak noted that, when their protective cover was removed, transmitters were often susceptible to spiking when in the presence of high frequency signals.

7.3 Arkansas Nuclear One (ANO) nuclear power plant

Arkansas Nuclear One (ANO) is a two-unit nuclear power plant located in Russellville, Arkansas. Unit One, that started its commercial operation in December 1974, is a Babcox & Wilcox Pressurized Water Reactor with 843 MWe of capacity. Unit Two, that started its commercial operations in March 1980, is a Combustion Engineering Pressurized Water Reactor with 995 MWe of capacity.

Like Comanche Peak, ANO has an extensive wireless network. ANO is using the wireless network for voice communications using VoIP technology in lieu of walkie-talkie systems, which have been shown to interfere with sensitive equipment. ANO's wireless network also provides workers with online access to plant documents when performing in-field procedures (e.g., equipment calibration). Electronically available information aids in performing a job more efficiently and correctly, while reducing waste and costs associated with generating printed references, drawings, and instructions.

During outages prior to 2011, the wireless network was temporarily expanded inside the nuclear containment. This expansion allowed technicians to conveniently use their VoIP phones for work inside containment, as well as enabling ANO to temporarily install and use wireless cameras to observe in-containment work. Lastly, ANO uses their wireless network in containment with their Radiation Survey System. The system allows the Radiation Protection technicians to wirelessly update radiation readings in real-time using a tablet computer or PC.

In 2011, through a partnership with a wireless equipment provider, ANO installed a wireless access point and a wireless vibration monitoring system inside the containment structure of Unit 1 that is functional during refueling outages and, more importantly, while the plant is at power. The system records vibration data at 20 kHz for 10 s twice a day and wirelessly transmits the data outside of the containment. Over the full operating cycle, the ANO vibration experts have been basing maintenance planning decisions on >2 000 data points per fan, where previously they were forced to make planning decisions on four data values over the same timeframe. The system consists of one or more remote units and a communications hub (Figure 17). The remote unit powers and reads data from up to 4 standard industry accelerometers, wirelessly transmitting the data to the communications hub. The hub transitions the data from the wireless transmission onto the plant's wired network and sends the data outside the containment wall.

Based on the successful installation in Unit 1, ANO engineers performed a second installation in Unit 2 to monitor the four containment cooling fans and the four CEDM cooling fans. The second system was completed, tested, and successfully installed in Unit 2 in September 2012. With the new systems, maintenance personnel can more effectively monitor the condition of the equipment, significantly reducing the risk of being 'surprised' by equipment failure. In addition to providing vibration data to the maintenance group, the system also feeds data to the plant historian, satisfying tech spec requirements.

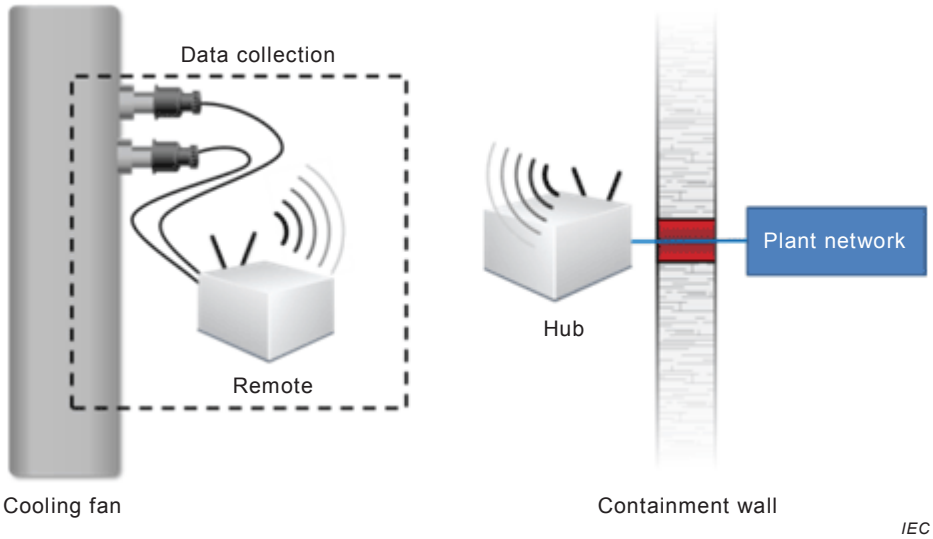


Figure 17 – Wireless vibration system at ANO

Based on the success of the wireless vibration systems, ANO worked to identify and develop an additional wireless application to monitor the oil level in their reactor coolant pump (RCP) oil collection tanks). This system was successfully installed in the summer of 2013 while Unit 1 is on extended outage (Figure 18).

According to ANO, the initial implementation cost for the wireless network was $ 280 000, which included the engineering work, all components, and the installation work in the power block. Since the first implementation, ANO estimates that they have invested ~$ 450 000 – $ 500 000 in their wireless network through coverage expansion and device upgrades.

7.4 Diablo Canyon nuclear power plant

Pacific Gas and Electric Company's Diablo Canyon nuclear power plant is located in San Luis Obispo County, California. Situated along the Central Pacific Coast, it is a vital part of the electricity produced in and for California. The plant contains two Westinghouse Pressurized Water Reactors. Both units are capable of generating over 1 100 MWe of electricity.

Diablo Canyon limits the use of wireless technology onsite, due to an incident in the late 1980s. During routine work, RF interference associated with a walkie-talkie caused a nearby Barton DP feedflow transmitter output to fluctuate, resulting in a plant trip. Since that time, Diablo Canyon has been hesitant to implement wireless technology. The plant currently has restrictions preventing the use of most wireless systems within the power block. Additionally, cell phones have not been allowed in the power block, even when they are turned off.

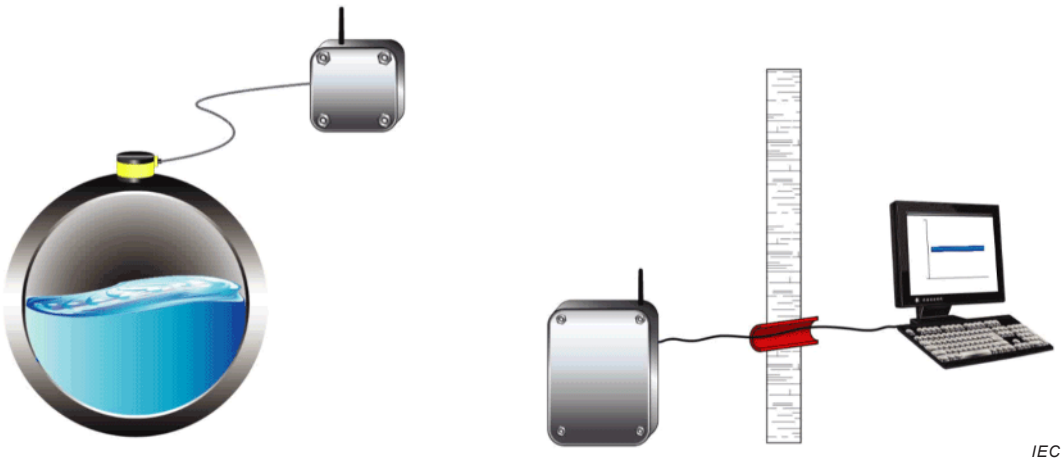


Figure 18 – ANO wireless tank level system

There are, however, some uses of wireless technologies in the plant, including wireless dosimetry, a wireless paging system, and walkie-talkies for use outside known exclusion zones. Lastly, there is a Wi-Fi wireless network in buildings outside the power block. This system is primarily used to support on-site supply delivery personnel when transporting materials throughout the plant. Using the wireless network and wireless hand-held devices, supplies can be validated and reconciled in real-time. Previously, supply delivery personnel would have to deliver all supplies, return to the warehouse, and manually log each delivery, requiring significant time and effort.

7.5 Farley nuclear power plant

The Joseph M. Farley Nuclear Plant is located on 1850 acres along the Chattahoochee River in southeast Alabama near Dothan. The plant is owned by Alabama Power and operated by Southern Nuclear Operating Company. Plant Farley consists of two units. Unit 1 achieved commercial operation in December 1977, and Unit 2 began commercial operation in July 1981. It is powered by two Westinghouse Pressurized Water Reactors (PWRs), and each reactor unit is capable of generating 888 megawatts (MW) for a total capacity of 1 776 MW. The plant generates approximately 19 percent of Alabama Power's electricity.

Farley nuclear power plant uses wireless technology in many areas of the plant. Farley performed EMI/RFI site surveys to establish guidelines and exclusion zones for using voice and data communication devices. They have wireless two-way radios and VoIP phones in use throughout the plant, as well as a low power, wireless digital paging system. Farley is also using wireless web cameras for various applications including providing a quick assessment of the fluctuating water level in the circulating water canal, and monitoring the gauge voltage readings at the switch house. Finally, Farley's Health Physics department uses wireless dosimetry to track and record radiation levels inside and outside of containment.

7.6 San Onofre nuclear generating station

The San Onofre Nuclear Generating Station (SONGS) is jointly owned by Southern California Edison (SCE), San Diego Gas & Electric, and the city of Riverside. The site consists of three Units; all are no longer in service. Units Two and Three are Combustion Engineering pressurized water reactors which generate 1 170 MWe and 1 180 MWe, respectively. Unit 2 operated from February 1982 to 2013 and Unit 3 operated from November 1982 until 2013.

During operation, San Onofre Nuclear Generating Station (SONGS) benefitted substantially from installing wireless devices for equipment condition monitoring. Repeated failures of circulation control motors prompted an investigation, revealing that clogged motor intakes caused overheating and, ultimately, damaged the motors. In response, a Wi-Fi 802.11b network was installed to communicate data from condition monitoring sensors. The system

provides the plant with enough forewarning to plan repairs or replace these motors, if needed, during an outage or low power operations. Since the wireless installation was deployed in 2003, not a single pump has failed during plant operations, significantly reducing expensive downtime, as well as the cost of maintenance for these motor-pump sets. Furthermore, the plant has seen a 60 % reduction in labor costs associated with maintenance on the motor pump systems due to the ability to schedule motor repair and replacement.

To address cyber security concerns, the plant used several methods to protect the data on the wireless network. Specialized wireless bridges are employed which use proprietary encryption and authentication protocols. In addition, an Access Control List (ACL) limits network access to only approved personnel, while MAC address filtering monitors the devices/platforms trying to access the network. Lastly, the IT department uses static IP addresses for all network clients, essentially reserving access for only pre-approved equipment.

7.7 South Texas project electric generating station

The South Texas Project (STP) Electric Generating Station is a two-unit nuclear power plant located near Bay City, Texas. Unit One, which was brought on-line in August 1988, is a four-loop Westinghouse Pressurized Water Reactor with ~1 350 MWe of capacity. Unit Two, which was brought on-line in June 1989, is also a four-loop Westinghouse Pressurized Water Reactor with ~1 350 MWe of capacity. A license application for two additional Advanced Boiling Water Reactors was submitted in September 2007 which would eventually be Unit Three and Unit Four of the facility.

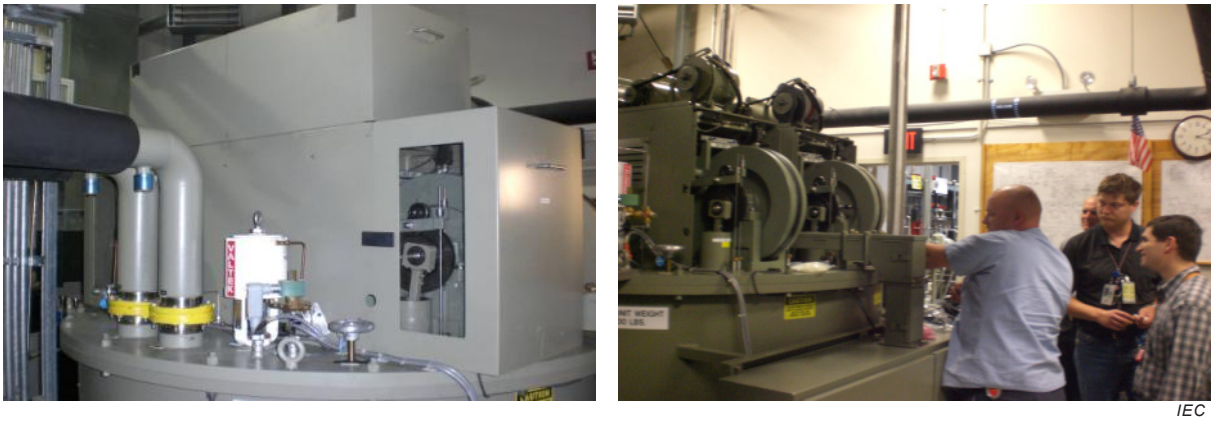
The South Texas Project site currently uses radios and pagers typical in most other nuclear facilities and currently allows the use of cell phones and blackberry devices onsite. Due to the location and structure of the Reactor Building, however, there is a lack of coverage for personal cell phone and blackberry devices. In addition, they extensively use wireless dosimeters for personnel and area/process radiation monitoring. These radiation monitoring devices use different radio transmitters/antennae than the Wi-Fi 802.11 backbone being implemented at STP.

South Texas has made significant progress in the installation of an 802.11 wireless backbone at the facility. There are ~125 access points in all administrative buildings which include the Turbine Building, Isolation Valve Cubicles, Diesel Building, Fuel Handling Buildings, Electrical Auxiliary, and Reactor Building. By the end of 2009, more than 300 access points will be installed. Like Arkansas Nuclear One, this will not just be on the plant campus or secondary side of the plant but will include the power block as well.

The applications will be similar to Arkansas Nuclear One and will most likely be used for voice and data communications. The plan is to also temporarily extend this wireless network inside containment during outages. The program is in the beginning stages so multiple applications have not yet been implemented; however, several have already been envisioned. Some of these include VoIP phones, plant network access in isolated areas using tablet PCs, paperless gauge calibration, and wireless data transmission from plant personnel in the field. For the latter example, an application is envisioned where data that is currently logged into a performance monitoring database via handheld PC docking stations could be uploaded to the plant network using a wirelessly-enabled handheld PC. Information like temperature, level, and flow gauge readings could be uploaded in real-time to the plant computer from anywhere in the plant. Additionally, STP plans to investigate fire detection using IP cameras to augment resources for fire watch. Lastly, in the summer of 2009, STP deployed IP cameras in their auxiliary feed-pump cubicles for elevated temperature monitoring.

7.8 High Flux Isotope Reactor (HFIR), Oak Ridge, TN

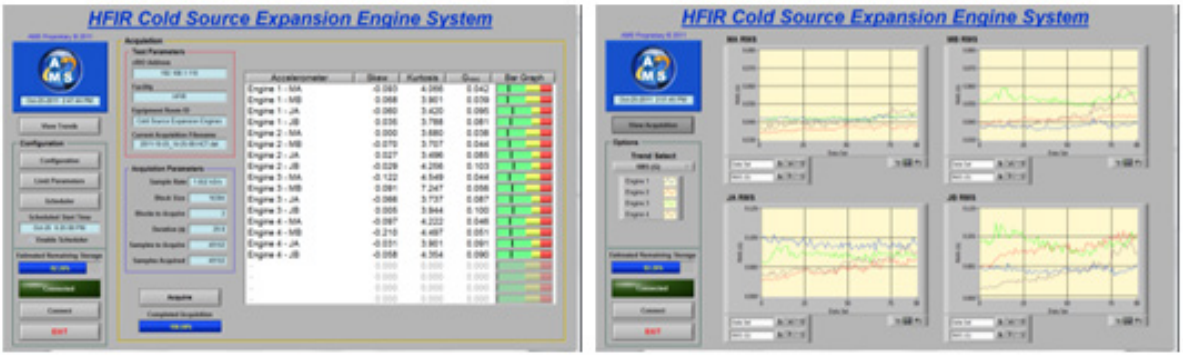
In an application at Oak Ridge National Laboratory’s High Flux Isotope Reactor (ORNL HFIR), the portable version has been installed as a permanent system. It monitors multiple test points on four cold source expansion engines (Stirling-type engines) that are vital for maintaining the cryogenic temperature of the neutron cold source (Figure 19).



IEC

Figure 19 – Installation of accelerometers on ORNL HFIR cold source expansion engines (9-2010)

The monitoring system routinely collects data every 4 h, performing real-time calculation of vibration acceleration RMS, skew, and kurtosis. These parameters are automatically trended and displayed for cold source operators (Figure 20). The operators and system engineer use this data and other process parameters such as temperature and pressure to make informed decisions regarding the health of the engines and when to schedule repairs.



IEC

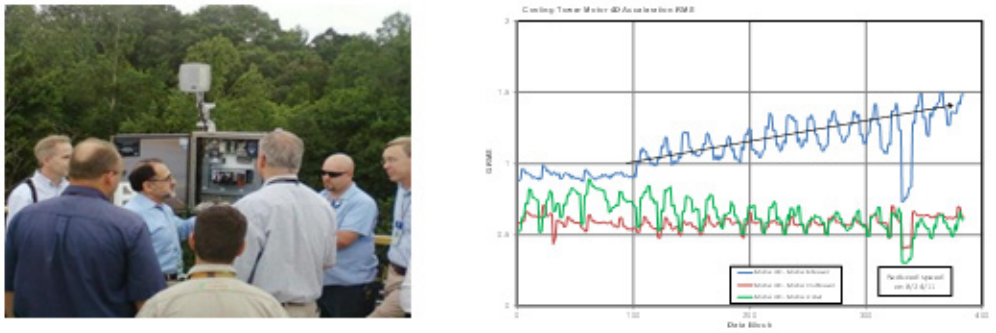
Figure 20 – Cold source expansion engine monitoring system software

The operators and system engineer use this data and other process parameters such as temperature and pressure to make informed decisions regarding the health of the engines and when to schedule repairs.

ORNL installed the permanent configuration of the wireless vibration system at ORNL's HFIR cooling tower. The cooling tower fan motors have been problematic for close to a decade and the gearboxes (which may provide valuable diagnostic information) have not been previously monitored, as they are inaccessible during tower operation (Figure 21). The system provides automated periodic monitoring, data collection on demand, trending of vibration parameters and bearing noise, and delivery of data and trends to the desktop of HFIR's condition monitoring expert (Figure 22).

IEC

Figure 21 – Installation of permanent wireless monitoring system at ORNL HFIR cooling tower (8-2011)



IEC

Figure 22 – System commissioned in August 2011

8 Considerations

8.1 General

One of the main considerations when considering the use of wireless technology in a nuclear power plant is the speed of development and evolution of the wireless standards. Maintaining system integrity and operability can be a challenge in the face of the rapid development and upgrades of wireless components. For instance, early adopters of IEEE 802.11b are faced with maintaining the lower bandwidth system or performing a wholesale change out of the wireless infrastructure to one of the more recent, higher speed protocols such as IEEE 802.11g, n, or ac. Other concerns regarding wireless technology are discussed below.

8.2 Concerns regarding wireless technology

There are a number of common concerns about utilizing wireless technologies within nuclear power plants. Most notable ones are:

- The radiation in a nuclear power plant will damage the microelectronic chips onboard the wireless sensors and modules or temporarily render them useless.
- The radiation field will ionize the air media so that the electromagnetic waveforms will no longer propagate.
- The transmitted electromagnetic waves from a wireless sensor transmitter may interfere with sensitive equipment in the plant causing a false trip. And
- The background electromagnetic noise emitted from major plant electrical systems, such as motors, pumps, or electric relay contacts, will make the wireless sensor network inoperable.

Even though these are legitimate concerns, extensive studies have been conducted to demonstrate these concerns are manageable.

It is true that the radiation level in certain parts of a nuclear power plant can be higher than ambient level. However, during normal plant operation, the radiation has relatively mild effects to the electronics onboard the sensor nodes. With proper shielding, wireless sensor nodes can safely operate within a nuclear power plant.

However, in the event of an accident, the radiation level could increase significantly. In such situations, the sensor nodes could be damaged with time. Hence, if wireless sensor nodes are intended for post-accident applications, proper protection mechanisms should be utilized.

Radiation can be divided into two types: ionizing radiation and non-ionizing radiation. The ionizing radiation includes x-ray, α, β, and ϒ particles, while the non-ionizing radiation is related to those in radio waves and wireless sensor transmitting signals. It is true that both types of radiations carry energy, but they are often at different spectrum range. Experimental studies have been carried out within hot cells to investigate the interplay of these two types of radiations. It is concluded that, at extremely high levels of radiation, the ionizing radiation does have limited influence on the propagation of the non-ionizing radiation. However, during normal operation of a nuclear power plant, or even during a limited scale accident, the radiation would not normally reach to the level that the ionizing radiation can have significant influence on the propagation properties of the non-ionizing radiation, i.e. the radio waves between wireless sensor nodes.

It is true that there are many sensitive instruments within nuclear power plants. Some may not be completely shielded from the influence of electromagnetic interference. However, a typical transmitting power level of a wireless sensor node is at milli-watt level. Such low level of radio wave has no effects on any safety system equipment, because the power decays at a rate inversely proportional to the quadratic power of the distance of the emitting site. However, one has to be extremely careful if mobile devices (such as walkie-talkie, cell phones, and tablets) are used in the plant, as their emitting power can be several Watts. They could have significant influence on the sensitive equipment if placed sufficiently close to the equipment.

In any industrial environment, including nuclear power plants, there are electromagnetic pollutions emitted by equipment, such as electric machines, relay contacts and power tools. Furthermore, extensive use of digital control systems also contributes to potential emission of high frequency noise from switching actions. Several experimental studies have demonstrated that the spectrum of the noise from those emitting sources are typically much lower than 2,4 GHz central frequency used by most of the wireless sensor nodes. Therefore, such noise has little impact on the operation of wireless sensor node systems.

8.3 Wireless deployment challenges

While there are numerous instances of wireless sensors and systems being used in a utility environment, there are challenges in wide spread adoption – and secure deployment and integration – of wireless sensor technology in power plants. Some of these limitations are listed as follows:

- Cyber security
- Barrier penetration capability
- Power requirements
- Bandwidth requirements
- Plug and play capability
- Multiple standards
- Interoperability
- Compatibility

The questions may seem daunting – even intimidating – but are worthwhile having vendors complete thereby allowing IT to determine the security "rankings" of the sensors, systems, and networks. As a reminder, apart from the financial incentive, there are several key objectives for deploying a wireless sensor network in a NPP, namely:

- Uptime improvement
- Improved utilization of assets (including people)
- Impact/backup on safety systems
- Improving quality assurance with on-line, continuous monitoring/qualification
- Enhanced accountability
- Enhanced automation of non-critical functions
- Expert system support – event driven
- Knowledge management – capture wisdom (implemented as an expert system)
- Life cycle cost management
- Improved job satisfaction or less frustration.

However, wireless sensor networks in nuclear power plants pose a unique challenge. The commercially available devices are not radiation hardened. RF devices cannot be enclosed in a lead box (Faraday cage). The antenna should be mounted outside the protective shell for the electronics to minimize exposure to radiation. Depending on the placement of the wireless devices, the lifetime of the constituent materials and electronics will vary. Figure 23 shows various regions of a typical NPP.

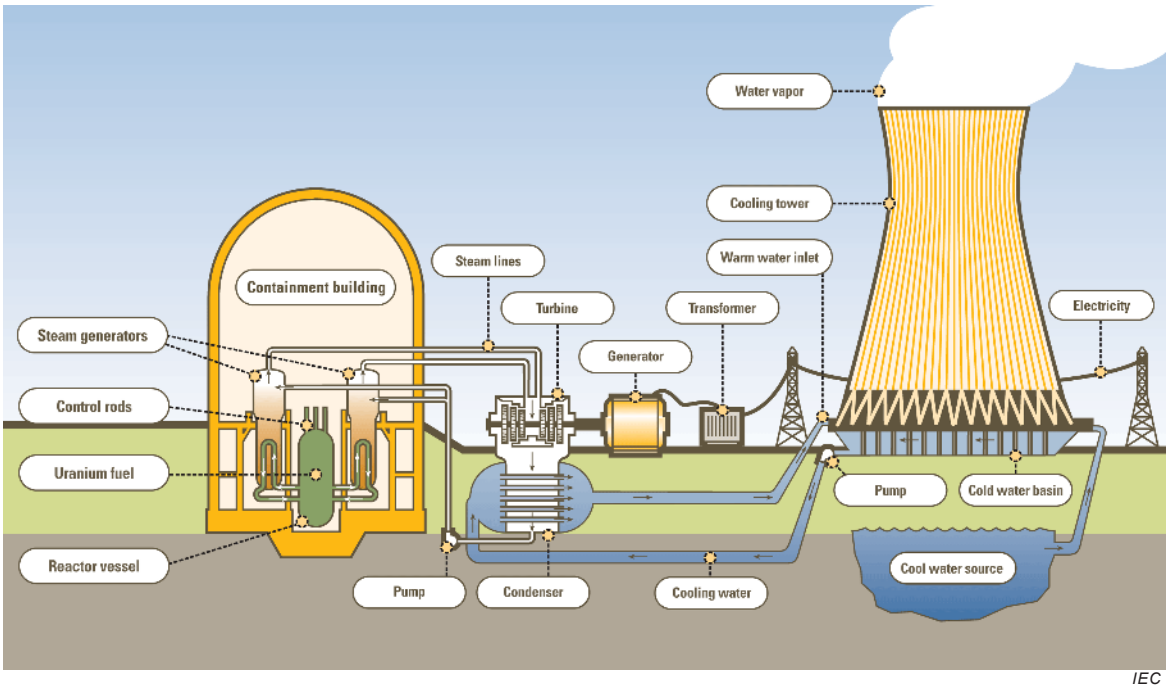


Figure 23 – Identification of containment in a nuclear facility

8.4 Coexistence of 802.11 and 802.15.4

The IEEE 802.15.2 Coexistence WG as well as the 802.19 RF Coexistence WG are tasked with addressing the coexistence issues associated with 802.11 and 802.15.1/802.15.4 transceivers. Coexistence between different wireless short-range devices, such as wireless sensors, using the 2,4 GHz and 5,8 GHz ISM bands is becoming increasingly more difficult and more important. Interference is increasingly an issue as wireless consumer devices proliferate. The IEEE specifications have stated that such 802.15-based devices are

"secondary," which means that they may not interfere with 802.11, and shall tolerate any interference received.

An 802.15.4 transceiver employs a Clear Channel Assessment (CCA) mechanism to "determine" if there is interference on the frequency channel that it is attempting to broadcast on. Restated, CCA is used to determine if the channel is busy. The second part of the 802.15.4 specification is that Collision Sensing Multiple Access (CSMA) is also available for use. The standard defines 3 modes of CCA/CSMA operation:

Mode 1 Energy above threshold. CCA reports a busy medium upon detecting energy above the ED (energy detection) threshold.

Mode 2 Carrier sense only. CCA reports a busy medium only upon detection of a signal with the modulation and spreading characteristics of IEEE 802.15.4. This signal may be above or below the ED threshold.

Mode 3 Carrier sense with energy above threshold. CCA reports a busy medium only upon detection of a signal with the modulation and spreading characteristics of IEEE 802.15.4 and with energy above the ED threshold.

Regardless of which CCA mode is used, if the CCA reports a busy medium, then the transceiver can employ multiple methods in an attempt to send the message including the two primary methods: a) wait a (pseudo) random amount of time and try the channel again, b) change channel and check CCA.

The frequency and channel assignments for 802.11 and 802.15.4 operation in the 2,4 GHz band are shown in Figure 24. Of particular note are the non-overlapping 802.11 channels. The frequency/channel assignments for 802.15.4 were originally specified such that there would "always" be a channel that would fall within the non-overlapping frequency bands of 802.11.

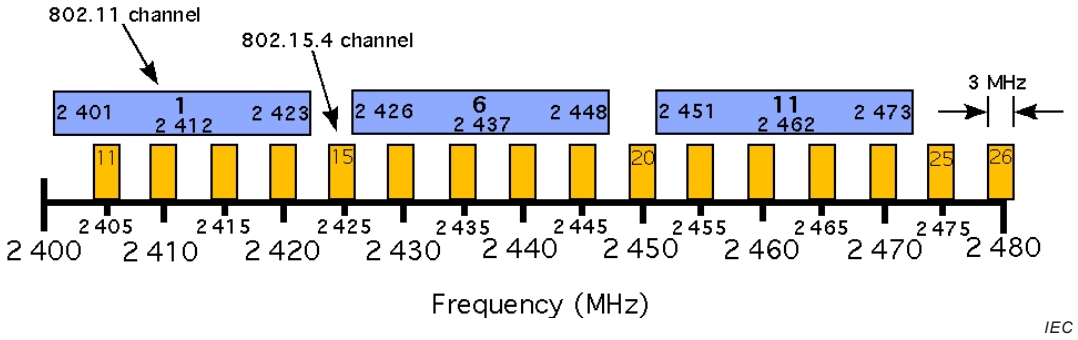
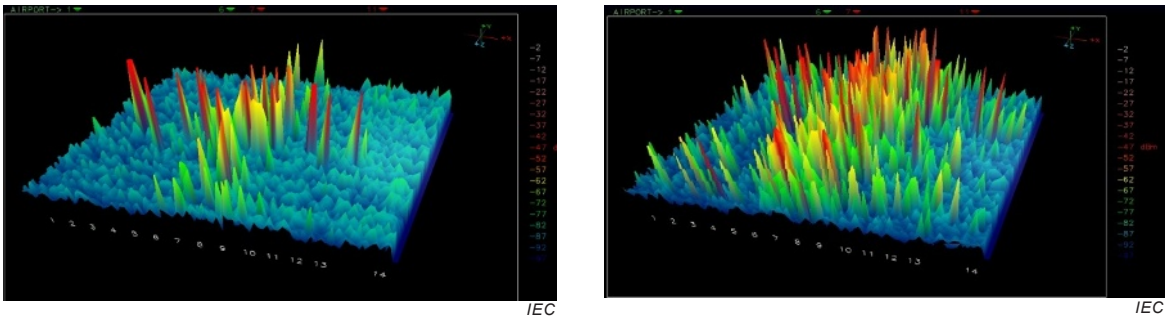


Figure 24 – Non-overlapping 802.11b/g channels and 802.15.4 channels



a) b)

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

Frequency charts such as Figure 24 do not depict the “bursty-channel” aspects of system performance for 802.11 and 802.15.4 communications. Consider the situations shown in Figure 25. In Figure 25 a) a simple spectrum analyzer’s depiction of a few seconds of traffic is shown for the case where there is minimal traffic on channel 7 – simple web surfing. Figure 25 b) illustrates the same spectrum analyzer depiction where video content is being streamed across 802.11 channel 7.

The highest signal strength is depicted in red; 802.11 2,4 GHz channels are on the horizontal axis; time progresses from bottom to top in the graph.

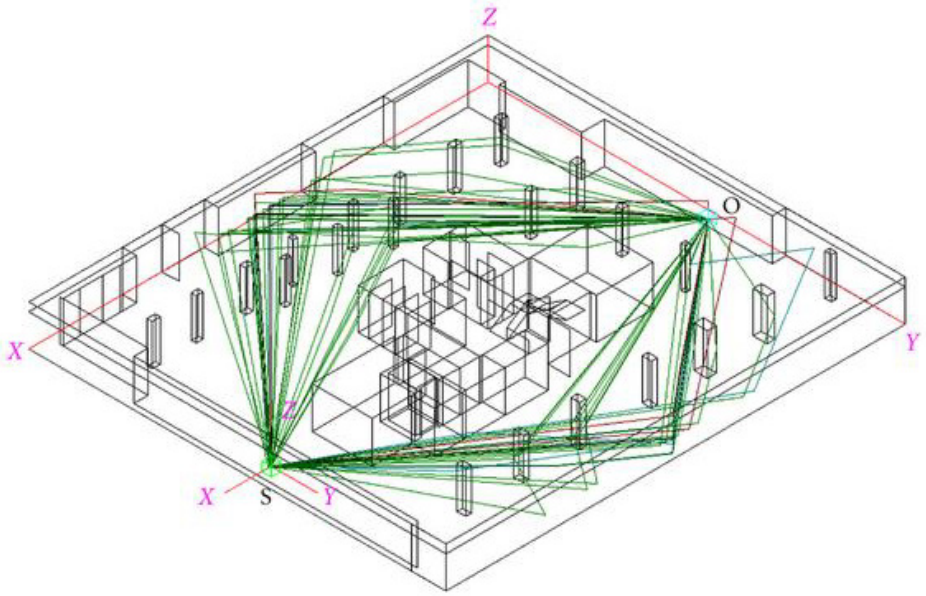
8.5 Signal propagation

RF signals have two common measurements: frequency and “strength.” Many signals are a mixture of different frequencies and different strengths. Frequency is measured in Hertz (Hz), meaning 1 cycle per second. The radio spectrum is broken into groups, with names such as HF (high frequency), VHF (very high frequency), and UH (ultra-high frequency). Graphically, the radio spectrum is illustrated using a logarithmic scale rather than linear. Most industrial wireless products are located in the upper VHF and UHF frequencies.

RF systems communicate by transmitting a signal made of EM energy from one antenna to another. This EM energy travels in the form of waves. This is called the signal path. As it is travelling from the transmitting antenna to the receiving antenna, some of the energy in the signal is lost. It can be lost for a number of reasons: absorption into the surrounding ground, environment, or materials that it may be passing through, such as walls or people. The amount of signal absorption also is dependent on the frequency of the RF signal. Typically, the higher the frequency, the more easily it is absorbed.

The signal can also take many different paths to the receiving antenna. This is called multipath (Figure 26). It can be reflected off metal surfaces that exist around either of the antennas. These waves are all added together when they meet at the receiving antenna. Due to the different lengths of the paths each reflection of the signal takes to the antenna, the relative phase of the waves will change. Depending on the phase difference between the waves, they can enhance or attenuate the signal, and this attenuation appears as a loss of signal. Given exactly the same reflection paths, signals of different frequencies will have different phase differences. Multipath may prove to be beneficial if the delays exceed one bit period.

When installing an RF system, the signal path analysis can determine how much loss will occur due to the environment, antenna type and height, and radio performance; this is called a path-loss study. Path-loss studies are typically only done for longer-range outdoor installations. Indoor installations are almost impossible to predict because of the multipath considerations.



IEC

Figure 26 – Multipath is exemplified in this indoor environment as the signal from Source (S) to Origin (O) may take many paths

Wireless technologies are being rapidly adopted for communications, equipment monitoring, and supervisory control and data acquisition (SCADA) systems. Several communication technologies have been developed for industrial wireless applications, such as radio frequencies, magnetic field, visible light and acoustic wave. Wireless networking technologies are being applied to industrial processing engineering areas because of their reduced installation costs, improved reliability, easy installation, increased flexibility, and simple maintenance.

8.6 Lessons learned from wireless implementations

8.6.1 General

During the implementation of wireless networks at the facilities above, several key lessons were documented. The most pertinent lessons are listed below.

8.6.2 Comanche Peak implementation

The following is a list of lessons learned, benefits, problems, etc., as reported by EPRI for the initial Comanche Peak Installation.

Key lesson: Treat wireless equipment sensors as an “early warning system” and not a real-time monitoring system.

Key lesson: Order several extra sensors early on in your project to allow for “floater” monitoring of unanticipated components on a temporary basis.

Key lesson: Do not always believe the conventional wisdom regarding wireless coverage; instead, perform detailed coverage surveys to determine your site’s ability to employ wireless equipment sensors.

Key lesson: It always takes longer than you think it will. Plan for extra time to coordinate activities across different groups.

9 Concerns

9.1 Common reliability and security concerns for wired media and wireless media

Some reliability and security concerns/problems/issues are the same for both wired and wireless media. These need to be identified so that only the differences can be compared:

- Data protocols. Robustness and security of data are related to the actual protocol, not to the media it goes over. The security (or lack of security) of Modbus is the same whether it goes over fiber optic cable or a wireless system.
- Internet hackers. Hackers trying to access systems through the Internet do not care or even know about the media.
- Overloading of the communications network by the utility. The data volume that a network can handle is related to the bit-per-second rate of the media, as well as configuration, response requirements, the degree of “bursty” data, and other network parameters. Again, this is media-independent.
- Single points of failure. The network configuration, not the type of media, is responsible for possible single points of failure.
- Utility security policies. If authorization procedures are not solid or are not followed, it does not matter what media you use. This includes not updating default passwords, vendor “backdoors” into their equipment, lost or stolen equipment, bypassing security checks, etc.

9.2 Reliability and security concerns that are more of an issue for wired systems

Wired systems can have reliability and security issues that are not a factor in wireless systems.

- Cutting or breaking the cable. Cables can always be cut or broken, whether by a backhoe, by corrosion, by repeated bending, or by a disgruntled employee with a large pair of wire cutters.
- Poorly connected wires or stressed wires. Poor connections on wires can lead to noisy or intermittent communications and could potentially lead to breakage of the wire.
- Physical theft of wire. Long stretches of wire in unsecured areas may pose a problem of physical theft of the cable, a rampant problem in many countries in the world.
- Eavesdropping on metallic wires. If physical access is available, metallic wires can easily permit eavesdropping with very simple techniques.
- Ground potential rise on metallic wires. Metallic wires are susceptible to ground potential rise in substations due to power equipment and lightning strikes.
- Lack of mobility for additions, changes, upgrades, and movement of equipment. Wired networks are more difficult to move or modify as new equipment is added and the configurations are changed, particularly if parts of the wiring are in inaccessible ducts or trenches.

9.3 Reliability and security concerns that are more of an issue for wireless systems

Wireless systems can have reliability and security issues that are not a factor in wired systems. These are often associated with denial-of-service and/or the unreliability of time-sensitive interactions.

- Eavesdropping on non-secured channels. Since wireless signals can be received by users outside the immediate environment, their data can be listened to, and if not encrypted, can be understood. However, if the data is adequately encrypted (IEEE 802.11i) or authenticated (SHA-1), then the information does remain secure.
- Disruption of the wireless signal due to electromagnetic interference (EMI). Substations and power plants are very electrically noisy environments, particularly during breaker operations and other equipment actions.

- Faded signals. Many factors can cause the wireless signal to fade, including too long a distance between wireless transmitter and receivers, atmospheric conditions, metallic surfaces that reflect the wireless radio waves, obstacles in the line-of-sight, and other factors.
- Overloading of bandwidth. Nearby users can overload the available bandwidth in the frequencies being used in the substation, thus causing delays and the potential need to retransmit data.
- Immaturity of wireless lower layer protocols. Wireless lower layer protocols (as opposed to data protocols like Modbus and DNP) have only been developed recently and are still undergoing significant upgrades, modifications, and testing.

10 Standards

10.1 Nuclear standards

10.1.1 General

There are a number of applicable IEC standards that relate to installation, operation and maintenance of instrumentation within nuclear power plants (see Bibliography). In addition to those IEC standards, there are a number of other standards that have implications specifically for wireless at nuclear power plants. The most relevant are summarized in this clause.

10.1.2 IEEE Std. 603-1998

The Institute of Electrical and Electronics Engineers (IEEE) Std. 603, “Standard Criteria for Safety Systems for Nuclear Power Generating Stations”, establishes minimum functional and design requirements for the power, instrumentation, and control portions of safety systems (including their interfaces) for nuclear power generating stations. The criteria established cover the following areas:

- safety system criteria,
- single failure criterion,
- completion of protective action,
- quality of components and modules,
- equipment qualification,
- system and channel integrity,
- independence,
- information displays,
- control of access and security,
- repair,
- identification,
- auxiliary features,
- human factors considerations,
- reliability, and
- common cause failure.

Because of the nature of wireless systems to potentially interfere with other safety systems, some of the items listed above need to be considered when developing guidance for wireless systems in nuclear facilities. These items are discussed below:

Quality of components and modules – Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates.

Equipment qualification – Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis.

Independence – Relevant criteria involve independence between safety systems and other systems:

- The safety system design shall be such that credible failures in and consequential actions by other systems shall not prevent the safety systems from meeting the requirements of IEEE Std. 603.
- No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

Reliability – For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed to confirm that such goals have been achieved.

- IEEE Std. 603 endorses IEEE Std. 352 and IEEE Std. 577 for use in reliability analysis.
- IEEE Std. 603 endorses the use of IEEE Std. 7-4.3.2 for equipment employing digital computers and programs or firmware.

Common cause failure – Plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure. In addition, IEEE Std. 603 requires that data communication between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function. IEEE Std. 603 also requires that safety functions be separated from non-safety functions such that the non-safety functions cannot prevent the safety system from performing its intended functions. In digital systems, safety and non-safety software may reside on the same computer and use the same computer resources. Either of the following approaches may be acceptable to address these issues:

Barrier requirements shall be identified to provide adequate confidence that the non-safety functions cannot interfere with performance of the safety functions of the software or firmware. The barriers shall be designed in accordance with the requirements of this standard. The non-safety software is not required to meet these requirements.

If barriers between the safety software and non-safety software are not implemented, the non-safety software functions shall be developed in accordance with the requirements of this standard.

10.1.3 IEEE Std. 7-4.3.2-2003

IEEE Std. 7.4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”, provides additional requirements beyond IEEE Std. 603 for digital (computer-based) systems. Thus, consideration should also be given to this standard when developing guidance for wireless systems because many wireless systems contain embedded software. The criteria established in the standard include software development quality assurance and tools and verification and validation (V&V) procedures. It also provides guidance on identification and evaluation of hazards during the detailed design phase, as well as guidance on diversity and how to meet communication independence criteria.

10.1.4 IEC 61500

IEC 61500: “*Nuclear power plants – Instrumentation and control systems important to safety – Data communications in systems performing category A functions*", establishes the functional

requirements for multiplexed on-line plant data transmissions and data communications that are used between equipment, providing functions important to safety, or between the equipment of these systems and equipment of systems not important to safety in nuclear facilities. This standard gives requirements for data transmission where a fixed cycle of messages is sent, mainly in one direction, repeatedly and with no significant variation of quantity. It covers only data transmission equipment used to send data from one piece of equipment to another, in a broadcasting or point-to-point mode, and integration between equipment and displays using LAN, metropolitan area network (MAN), wide area network (WAN), broadcasting, and like methods for operation. It lists broad requirements for the following categories: function, performance, safety class, and network topology; communications protocols, communications media, reliability and independence, operation and maintenance, and qualification.

Also related, IEC TR 61508-0: *Functional safety of electrical/electronic/programmable safety-related systems – Part 0: Functional safety and IEC 61508*, is a generic process standard for the development of safety-related systems, and IEC 61513: *Nuclear power plants – Instrumentation and control for systems to safety – General requirements for systems*, is the specialization of IEC TR 61508-0 for the nuclear industry. IEC 61513 provides high-level requirements for the safety system.

10.2 Other safety-related standards and guidelines

10.2.1 IEC 61784-3

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*, describes the basic principles for implementing the requirements of IEC 61508 for safety-related data communications, including possible transmission faults, remedial measures and considerations affecting data integrity.

Individual descriptions of functional safety profiles for several communication families are described in IEC 61784-1: *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*, and IEC 61784-2: *Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3*. Several data communication parameters for safety measure and influence are presented below.

Subclause 5.4 of IEC 61784-3 lists measures commonly used to detect deterministic errors of communication systems. A brief description of the measures is as follows:

Sequence number – A sequence number is appended to the body of the message as additional bits in a predetermined way before transmission. After reception, this unique number is used to identify the actual message. Generally, these are known sequences of bits, with very good cross-correlation properties under channel corruption.

Time stamp – In most cases the content of the message is only valid for a particular time window. The time information in a message in the form of time of day and date is stamped before the transmission. Relative time stamps (w.r.t. message sequences) or absolute time stamps can be used. Time stamping requires a reference time for synchronization. Note that “synchronization” itself is a part of the message estimation (detection and decoding), which is different from the time stamp.

Time expectation – The message sink verifies the time elapsed between two consecutive received messages against the maximum predetermined allowed delay. If this delay exceeds the maximum delay, an error is reported. For example, with the time-division multiple access (TDMA) technique, each user (source) is allowed a time slot to transmit information. No one else can interfere with the designated users signal during that allotted slot.

Connection authentication – Message has a unique source and/or destination identifier that describes the logical address of the safety-related participant.

Feedback message – The message sink returns a feedback message to the source to confirm the reception of the original message. The feedback message has to be verified by the safety communication layers. The feedback messages can be a short acknowledgement or an acknowledgment with a copy of the original message.

Data integrity assurance – No communications system is error free, so error detection/correction is the key to reliable communications. The quality of error detection schemes is based on trading off two antagonistic factors: minimizing the redundant information transmitted vs maximizing the error detection capability.

The CRC error detection method is widely used in many communication protocols. A check sequence (typically 16 or 32 bit) is calculated by modulo-2 division of the message by a binary polynomial. The check sequence is appended as redundant bits (not part of the actual information bits) before modulation. At the receiver, these CRC bits determine the number of bits in error. The various protocols using CRC differ only by the polynomial chosen for the calculation. CRC does not add the bandwidth constraint of the modern error correction techniques and also does not offer powerful error correction capability. CRCs are generally used for serial communications because of their sensitivity to burst error bits, a type of error occurring in packet based, wireless, or interference limited channels. Addition techniques such as interleaving can be augmented to overcome the burst error.

Typical error detection or correction techniques, designed to protect data transmissions against corruption, are not acceptable for safety-related applications if they are not designed from the point of view of functional safety. Therefore, redundant data are included in a message to permit data corruptions to be detected by the redundancy checks. Instead of the CRC type error detection techniques, communication systems used for safety-related applications may use other methods, such as cryptography or a combination of powerful error correction coding (convolutional type coding) and cryptography, to ensure data integrity.

Redundancy with cross-checking – In safety-related applications, the safety data may be sent twice within one or two separate messages, using identical or different integrity measures. At the sink, the transmitted safety data are cross-checked for validity. If a difference is detected, an error is determined. There can be various fault detection models for safety devices connections and protocols. Four different scenarios follow:

a) One channel is connected to the bus. Data from both safety communication layers are checked and cross-checked. If cross-checking shows any discrepancy, an appropriate action is initiated to maintain safety.
b) All safety communication layers, transmission layers, and transmission media exist twice. Note that transmission layers and transmission media can be of different types.
c) Everything is the same as in b) except with one transmission medium.
d) Similar to the model in a) except both safety communication layers can access the transmission layers independently.

Different data integrity assurance systems – If safety-relevant (SR) and non-safety-relevant (NSR) data are transmitted using the same transmission medium, different data integrity assurance systems should be used, and more importantly better encoding should be used for SR transmission to make sure that NSR information cannot influence any safety function in a SR receiver.

The safety measures outlined in 5.4 of IEC 61784-3 can be related to the set of possible errors defined in 5.3. Each safety measure can provide protection against one or more errors in the transmission. The evaluation process is to demonstrate that there are one or more corresponding safety measures for the defined possible errors in accordance.

10.2.2 VTT research notes 2265

VTT Research Notes 2265, “Safety of Digital Communications in Machines,” covers safety related serial communications in machine automation. The message error types relating to

serial mode data transmission and their remedies are derived from other safety-related communication standards, as many of these parameters are also presented in 4.1.4 of IEC 61874-3. Although most of the safety bus solutions are commercially available, additional safety bus solutions from standards are also suggested in the report. Each bus solution has its own merits and poses specific challenges for safety applications. Hence, a thorough safety analysis and testing are required when using a bus for safety applications. There is a tendency to integrate multiple buses and even integrating the normal bus with the safety bus to improve the overall performance. The safety bus and the normal bus should be separated for the following reasons. If the system changes from time to time for different application purposes, the validation of the integrated system is quite cumbersome and risky. Individual sanity checks and “what if” analyses are much more tractable for separated systems where the normal bus and the safety bus are isolated. Also, any new addition or modification of the system changes the overall safety requirement, which then should be reevaluated as if it were a new system.

A generic safety analysis tool for bus-based communication systems at various signal levels was developed for the VTT report. The tool consists of a test flowchart, a database consisting of possible safety failure causes, and various action items in stages. This tool is a general procedural methodology that can be adapted for the analysis of safety buses in power plants.

10.2.3 European Workshop on Industrial Computer Systems – Technical Committee 7 (EWICS TC7)

The EWICS TC7 report, “Guideline on Achieving Safety in Distributed Systems”, concentrates on industrial systems that may suffer catastrophic consequences if their safety-critical, distributed systems fail. This report provides guidance on achieving safety in industrial computer-based distributed systems over the system life cycle. The focus of the EWICS TC7 report is exclusively on those aspects of distributed computer systems that influence the safety of the system. Distribution may result from different design considerations, such as redundancy or diversity, functional partitioning, adaptation to a geographically distributed process, and an increase of system time response through local intelligence at system peripheral levels. Diversity and functional partitioning result in better safety performance. Distributed processes and longer system time response increase complexity of the system. This increase in complexity and underlying functionality leads to an increase in failure modes that also have to be considered within the system safety analysis. Many of these safety properties are applicable to communication systems in nuclear facilities.

The EWICS TC 7 report presents various aspects of the basic activities of distributed systems throughout the life cycle, for example, safety analysis, system requirements specification, system design, hardware design, software design, software implementation, integration, installation, operation, maintenance and modification, and replacement. Some generic aspects of distributed systems that may have an impact on safety are also listed. These are security, project management, verification and validation, assessment, and human factors. Safety aspects, constraints, qualities, and guidelines are listed for each of these parameters.

11 Conclusions

11.1 Issues for wireless application to NPP

As a result of the analysis that has been done so far, the following issues should be discussed and considered to pick the requirements for wireless application into nuclear power plants.

a) The communication media selection

b) The communication protocol selection

c) The dynamic topology in relation to network security

d) In-line, on-line, off-line real time monitoring of network itself

e) The security for physical as well as information

f) Coexistence management in wireless world

g) Failure management and recovery requirements

h) Power supply consumption management requirements

i) Equipment qualification in the world of nature, i.e. dust, sand, moving objects, etc.

j) Close-loop real-time control performance requirements through jitter, or delay

11.2 Recommendations

This technical report has provided a complete and thorough background on the application of wireless technologies to nuclear facilities. After a careful review of the material in this report, it is expected that the reader will conclude that wireless technologies are appropriate for use in nuclear power plants and that applications and standards are in place to help guide in the deployment of these technologies at nuclear facilities. It is expected that national and international standards for communications, security, and equipment protection will be respected.

In specific, the following guidance is also provided:

a) General limits assigned to wireless systems

Wireless communications shall not be used in systems supporting Category A and B functions according to IEC 61226.

A suitability analysis shall be conducted prior to the selection of wireless systems supporting Category C functions according to IEC 61226.

Wireless systems shall not disturb I&C functions and other important for safety systems.

b) Verification & Validation requirements, qualification

IEC 61513 “General requirements for systems” requirements shall be met.

IEC 62138 “Software aspects” requirements shall be met.

IEC 60780 “Qualification” requirements shall be met.

c) Network architecture

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

d) Systems running on batteries

Remote devices running on batteries shall be physically reachable in order to be able to replace a defective or discharged battery. If this is not possible, the battery capacity shall be properly dimensioned to last a sufficient time, according to the system specification.

Battery level of remote devices running on batteries shall monitored.

e) Electromagnetic compatibility (EMC)

Any wireless device shall be installed at least 30 cm (1 foot) away from important for safety equipment. Additional distance may be required based upon the output power of the wireless device and the susceptibility of the plant equipment.

An impact analysis regarding EMC shall be conducted prior to the on-site installation of the system. The impact analysis can include system reviews and evaluations in combination with laboratory/on-site testing, such as:

1) Review of plant equipment functions and system characteristics

2) Review of EMC test reports for plant equipment

3) Determination of exclusion zones based on industry guidance

4) Electromagnetic Environment Characterization

5) Immunity testing of training/simulator equipment

6) In-situ immunity testing of plant equipment during times when the impact to plant safety and operability can be managed.

f) Irradiation

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

g) Computer security

Requirements of IEC 62645: *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems* shall be met.

Encryption should be used for wireless communications. The encryption methods – or lack of encryption – shall be consistent with IEC 61513 overall security plan.

Authentication of all messages should be used. The authentication process – or lack of authentication – shall be consistent with IEC 61513 overall security plan.

h) Solution durability

Wireless protocols using a documented standard should be preferred.

Annex A
(informative)

Use of 5 GHz in the world

The fragmented nature and jurisdictional differences of operation in the 5 GHz region are illustrated in Table A.1.

Table A.1 – Use of 5 GHz in America, Asia/Pacific, and Europe

Spectrum GHz -->	5,03 – 5,09	5,15 – 5,25	5,25 – 5,35	5,470 – 5,725	5,725 – 5,825/5,850
Bandwidth-->	60 MHz	100 MHz	100 MHz	255 MHz	100 MHz – 125 MHz
Argentina			Indoor/Outdoor		Indoor/Outdoor
Brazil					Indoor/Outdoor
Canada		Indoor	Indoor/Outdoor		Indoor/Outdoor
Columbia		Indoor	Indoor/Outdoor		Indoor/Outdoor
Mexico		Indoor	Indoor		Indoor/Outdoor
USA		Indoor	Indoor/Outdoor		Indoor/Outdoor
Australia		Indoor	Indoor		Indoor/Outdoor
China					Indoor/Outdoor (125 MHz)
Hong Kong		Indoor	Indoor		Indoor/Outdoor (125 MHz)
Japan	Indoor /Outdoor	Indoor			Indoor/Outdoor
Korea					Indoor/Outdoor
New Zealand		Indoor	Indoor		Indoor/Outdoor (125 MHz)
Singapore		Indoor /Outdoor			Indoor/Outdoor (125 MHz)
Taiwan			Indoor		Indoor/Outdoor
Austria		Indoor	Indoor		
Belgium		Indoor	Indoor		
Denmark		Indoor	Indoor	Indoor/Outdoor	
Finland		Indoor	Indoor	Indoor/Outdoor	
France		Indoor	Indoor		
Germany		Indoor	Indoor	Indoor/Outdoor	
Italy		Indoor	Indoor	Indoor/Outdoor	
Netherlands		Indoor	Indoor	Indoor/Outdoor	
Norway		Indoor	Indoor	Indoor/Outdoor	
Portugal		Indoor	Indoor	Indoor/Outdoor	
Switzerland		Indoor			
UK		Indoor	Indoor	Indoor/Outdoor	

Annex B
(informative)

Synopses of wireless technologies

NOTE The information presented in this Annex is based in large part on Wikipedia entries (www.wikipedia.org).

B.1 802.11

While devices using the 802.11b standard appear quite successful, these wireless standards come in several varieties with similar data layer protocols, for example:

802.11b is an IEEE standard (ratified in 1999) for high-speed wireless LAN/MAN operating on three non-overlapping or 11 overlapping 5 MHz-wide channels in the 2,4 GHz ISM band. Devices following this standard use the same frequency spectrum as Bluetooth devices, but employ a different modulation technique. The essential technical requirements include:

- Data rate per channel: 11 Mb/sec maximum
- Operating frequencies: 2,40 – 2,4835 GHz ISM band
- Modulation method: Direct-Sequence Spread Spectrum (DSSS)
- Nominal ERP of +10 to +20 dBm, typically 15 dBm
- Medium range, typically 30 m (100 m with +20 dBm transmitter)
- Supported stations: Up to 256 per Access Point, roaming between APs

802.11a is an IEEE standard (ratified in 1999) for high-speed wireless LAN/MAN operating in the in the 5 GHz band. Devices conforming to this standard are likely to be more expensive than 802.11b. Exact spectrum allocations vary from country to country/region. The essential characteristics include:

- Data rate: 54 Mb/sec maximum
- Operating frequencies include 5,15-5,35 GHz UNII band in U.S., 5,47-5,725 GHz in Europe, 5,725-5,85 GHz ISM
- Modulation: Orthogonal Frequency Division Multiplex (OFDM)
- Nominal ERP of +16 dBm +6 dBi antenna
- Medium range, typically 30 m
- Supported stations: Up to 256 per Access Point, roaming between APs
- Channel Capacity: Up to 12 non-overlapping 54Mb/s networks

802.11g is an IEEE standard compatible with 802.11b, but with a much higher data rate. Essential technical criteria include:

- Data rate: 54 Mb/sec maximum
- Operating frequencies: 2,40 – 2,4835 GHz ISM band
- Modulation: Orthogonal Frequency Division Multiplex (OFDM)
- Nominal ERP of +10 to +20 dBm, typically 15 dBm
- Medium range, typically 30 m (100 m with +20 dBm transmitter)
- Supported stations: up to 256 per Access Point, roaming between APs
- Channel capacity: 3 overlapping 54 Mb/s networks on channels 1,6, and 11
- Seen as an easier migration path than 802.11a.

802.11n is an IEEE standard compatible with 802.11g but with a much higher data rate. Essential technical criteria include:

- Data rate: 54 Mb/sec maximum
- Operating frequencies: 2,40 – 2,4835 GHz ISM band
- Modulation: Orthogonal Frequency Division Multiplex (OFDM)
- Nominal ERP of +10 to +20 dBm, typically 15 dBm
- Medium range, typically 30 m (100 m with +20 dBm transmitter)
- Supported stations: up to 256 per Access Point, roaming between APs
- Channel capacity: 3 overlapping 54 Mb/s networks on channels 1, 6, and 11

Cellular telephony is, not surprisingly, complicated with over 20 different radio standards and specifications used throughout the world.

IEEE 1901 (RuBee): (IEEE 1902.1) is a two way, active wireless protocol that uses Long Wave (LW) magnetic signals to send and receive short (128 bytes) data packets in a local regional network. The protocol is similar to the IEEE 802 protocols which are also known as WiFi (IEEE 802.11), WPAN (IEEE 802.15.4) and Bluetooth (IEEE 802.15.1), in that RuBee is networked by using on-demand, peer-to-peer, active radiating transceivers. RuBee is different in that it uses a low frequency (131 kHz) carrier. One result is that RuBee is very slow (1 200 bauds) compared to other packet based network data standards. 131 kHz as an operating frequency provides RuBee with the advantages of ultra-low power consumption (battery life measured in years), and normal operation near steel and/or water. These features make it easy to deploy sensors, controls, or even actuators and indicators. Because RuBee uses long wavelengths (131 kHz is 7 508 feet, see calculator) and works in the near field (under 100 feet) it is possible to simultaneously transmit and receive from many adjacent antennas, without interference providing the signals are synchronized.

IEEE 802.15.1(ULP Bluetooth, originally named WiBree): WiBree is a digital radio technology (intended to become an open standard of wireless communications) designed for ultra-low power consumption (button cell batteries) within a short range (10 m/ 30 ft) based around low-cost transceiver microchips in each device.[1] As of June, 2007 WiBree is known as Bluetooth ultra-low power, in 2008 renamed Bluetooth low energy.

Bluetooth is a wireless transport specification for interconnecting portable and fixed telecom, computing, and consumer equipment using low-cost, miniaturized RF components. Transport of either data or voice is supported. Originally conceived as a way to connect cellular or PCS telephones to other devices without wires, other applications include USB "dongles," peripheral interconnections, and PDA extensions. Bluetooth-enabled devices will allow creation of point-to-point or multipoint wireless personal area networks (WPANs) or "piconets" on an ad hoc or as needed basis. Bluetooth is intended to provide a flexible network topology, low energy consumption, robust data capacity and high quality voice transmission. The essential technical specifications include:

- Data rate: 1 Mb/sec maximum or gross, 721 kbps practical (if interference free)
- Operation limited to 2,40 – 2,4835 GHz ISM band
- Nominal ERP of –30 to +20 dBm, typically 0 dBm, segregated by classes:
- Class 1: from 4 dBm to 20 dBm (2,5 – 100 mW), power control mandatory
- Class 2: from 0 dBm to 4 dBm (1,0 – 2,5 mW), power control optional
- Class 3: Up to 0 dBm (1,0 mW)
- Short range, typically 10 m (100 m with 20 dBm transmitter)
- Frequency hopping spread spectrum modulation, with >75 hop frequencies with 1 MHz channel spacing, 1 600 hops/s (625 μs dwell time)
- Supported devices: 8 devices per piconet, 10 piconets for each coverage area

- Channel capacity: Max 3 voice channels per piconet, 7 per piconet for data

IEEE 802.15.3 (UWB, WiMedia). Ultra Wideband (formerly, 802.15.3a): Wireless USB. Wireless USB is based on the WiMedia Alliance's Ultra-WideBand (UWB) common radio platform, which is capable of sending 480 Mbit/s at distances up to 3 m and 110 Mbit/s at up to 10 m. It was designed to operate in the 3,1 to 10,6 GHz frequency range, although local regulatory policies may restrict the legal operating range for any given country.

IEEE 802.15.4 (Wireless low data rate Personal Area Network, ZigBee, ISA100.11a, WiHART, proprietary): Multiple proprietary or standards-based protocols exist in these areas that are intended for industrial wireless sensor networks, usually mesh based. These have been discussed in the body of the article. A general overview of IEEE 802.15.4 follows: IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices (in contrast with other, more end user-oriented approaches, such as Wi-Fi). The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more.

The basic framework conceives a 10 m communications area with a transfer rate of 250 kbit/s. Tradeoffs are possible to favor more radically embedded devices with even lower power requirements, through the definition of not one, but several physical layers. Lower transfer rates of 20 and 40 kbit/s were initially defined, with the 100 kbit/s rates being added in the current revision.

Even lower rates can be considered with the resulting effect on power consumption. As already mentioned, the main identifying feature of 802.15.4 among WPAN's is the importance of achieving extremely low manufacturing and operation costs and technological simplicity, without sacrificing flexibility or generality.

Important features include real-time suitability by reservation of guaranteed time slots, collision avoidance through CSMA/CA and integrated support for secure communications. Devices also include power management functions such as link quality and energy detection.

802.15.4-conformant devices may use one of three possible frequency bands for operation.

- 868,0-868,6 MHz: Europe, allows one communication channel (2003, 2006)
- 902-928 MHz: North America, up to ten channels (2003), extended to thirty (2006)
- 2400-2483,5 MHz: worldwide use, up to sixteen channels (2003, 2006)

The original 2003 version of the standard specifies two physical layers based on direct sequence spread spectrum (DSSS) techniques: one working in the 868/915 MHz bands with transfer rates of 20 and 40 kbit/s, and one in the 2 450 MHz band with a rate of 250 kbit/s.

The 2006 revision improves the maximum data rates of the 868/915 MHz bands, bringing them up to support 100 and 250 kbit/s as well. Moreover, it goes on to define four physical layers depending on the modulation method used. Three of them preserve the DSSS approach: in the 868/915 MHz bands, using either binary or offset quadrature phase shift keying (the second of which is optional); in the 2 450 MHz band, using the latter. An alternative, optional 868/915 MHz layer is defined using a combination of binary keying and amplitude shift keying (thus based on parallel, not sequential spread spectrum, PSSS). Dynamic switching between supported 868/915 MHz PHY's is possible.

Beyond these three bands, the IEEE802.15.4c study group is considering the newly opened 314-316 MHz, 430-434 MHz, and 779-787 MHz bands in China, while the IEEE 802.15 Task Group 4d is defining an amendment to the existing standard 802.15.4-2006 to support the new 950 MHz-956 MHz band in Japan. First standard amendments by these groups were released in April 2009.

In August 2007, IEEE 802.15.4a was released expanding the four PHYs available in the earlier 2006 version to six, including one PHY using Direct Sequence Ultra-wideband (UWB) and another using Chirp Spread Spectrum (CSS). The UWB PHY is allocated frequencies in three ranges: below 1 GHz, between 3 and 5 GHz, and between 6 and 10 GHz. The CSS PHY is allocated spectrum in the 2 450 MHz ISM band.

In April, 2009 IEEE 802.15.4c and IEEE 802.15.4d were released expanding the available PHYs with several additional PHYs: one for 780 MHz band using O-QPSK or MPSK[2], another for 950 MHz using GFSK or BPSK.

IEEE 802.16 (WiMAX): The 802.16 specification applies across a wide swath of the RF spectrum, and WiMAX could function on any frequency below 66 GHz (higher frequencies would decrease the range of a base station to a few hundred metres in an urban environment).

There is no uniform global licensed spectrum for WiMAX, although the WiMAX Forum has published three licensed spectrum profiles: 2,3 GHz, 2,5 GHz and 3,5 GHz, in an effort to decrease cost: economies of scale dictate that the more WiMAX embedded devices (such as mobile phones and WiMAX-embedded laptops) are produced, the lower the unit cost. (The two highest cost components of producing a mobile phone are the silicon and the extra radio needed for each band). Similar economy of scale benefits apply to the production of Base Stations.

In the unlicensed band, 5.x GHz is the approved profile. Telecommunication companies are unlikely to use this spectrum widely other than for backhaul, since they do not own and control the spectrum.

In the USA, the biggest segment available is around 2,5 GHz and is already assigned. Elsewhere in the world, the most-likely bands used will be the Forum approved ones, with 2,3 GHz probably being most important in Asia. Some countries in Asia like India and Indonesia will use a mix of 2,5 GHz, 3,3 GHz and other frequencies. Pakistan's Wateen Telecom uses 3,5 GHz.

Wireless Broadband (WiBro, also called Portable Internet Service): WiBro is the South Korean service name for IEEE 802.16e (mobile WiMAX) international standard. WiBro adopts TDD for duplexing, OFDMA for multiple access and 8,75 MHz as a channel bandwidth. WiBro was devised to overcome the data rate limitation of mobile phones (for example CDMA 1x) and to add mobility to broadband Internet access (for example ADSL or Wireless LAN). In February 2002, the Korean government allocated 100 MHz of electromagnetic spectrum in the 2,3 – 2,4 GHz band, and in late 2004 WiBro Phase 1 was standardized by the TTA of Korea and in late 2005 ITU reflected WiBro as IEEE 802.16e (mobile WiMAX). Two South Korean Telcom (KT, SKT) launched commercial service in June 2006, and the tariff is around US$ 30.

WiBro base stations will offer an aggregate data throughput of 30 to 50 Mbit/s per carrier and cover a radius of 1–5 km allowing for the use of portable internet usage. In detail, it will provide mobility for moving devices up to 120 km/h (74,5 miles/h) compared to Wireless LAN having mobility up to walking speed and mobile phone technologies having mobility up to 250 km/h.

Long Term Evolution (LTE): The 802.16 specification applies across a wide swath of the RF spectrum, and WiMAX could function on any frequency below 66 GHz (higher frequencies would decrease). While 3GPP Release 8 is an ungratified, formative standard, much of the Release addresses upgrading 3G UMTS to 4G mobile communications technology, which is essentially a mobile broadband system with enhanced multimedia services built on top.

The standard includes: For every 20 MHz of spectrum, peak download rates of 326,4 Mbit/s for 4x4 antennas, 172,8 Mbit/s for 2x2 antennas and peak upload rates of 86,4 Mbit/s for every 20 MHz of spectrum using a single antenna. Five different terminal classes have been

defined from a voice centric class up to a high end terminal that supports the peak data rates. All terminals will be able to process 20 MHz bandwidth.

At least 200 active users in every 5 MHz cell. (Specifically, 200 active data clients) Sub-5ms latency for small IP packets Increased spectrum flexibility, with spectrum slices as small as 1,5 MHz (and as large as 20 MHz) supported (W-CDMA requires 5 MHz slices, leading to some problems with roll-outs of the technology in countries where 5 MHz is a commonly allocated amount of spectrum, and is frequently already in use with legacy standards such as 2G GSM and cdmaOne). Limiting sizes to 5 MHz also limited the amount of bandwidth per handset.

Optimal cell size of 5 km, 30 km sizes with reasonable performance, and up to 100 km cell sizes supported with acceptable performance. This statement should be treated with caution. Comment: Without considering the radio propagation environment and the frequency used (looks like it will be 2,6 GHz in EU), it is meaningless to talk about cell size. For a given power budget, the higher the frequency, the more challenging range becomes in a mobile cellular system.

Co-existence with legacy standards (users can transparently start a call or transfer of data in an area using an LTE standard, and, should coverage be unavailable, continue the operation without any action on their part using GSM/GPRS or W-CDMA-based UMTS or even 3GPP2 networks such as cdmaOne or CDMA2000).

Support for MBSFN (Multicast Broadcast Single Frequency Network). This feature can deliver services such as Mobile TV using the LTE infrastructure, and is a competitor for DVB-H-based TV broadcast. PU^{2}RC as a practical solution for MU-MIMO. The detailed procedure for the general MU-MIMO operation is handed to the next release, e.g., LTE-Advanced, where further discussions will be held.

A large amount of the work is aimed at simplifying the architecture of the system, as it transits from the existing UMTS circuit + packet switching combined network, to an all-IP flat architecture system. An "All IP Network" (AIPN).

Next generation networks are based upon Internet Protocol (IP). See, for example, the Next Generation Mobile Networks Alliance (NGMN).

In 2004, 3GPP proposed IP as the future for next generation networks and began feasibility studies into All IP Networks (AIPN). Proposals developed included recommendations for 3GPP Release 7(2005), which are the foundation of higher level protocols such as LTE. These recommendations are part of the 3GPP System Architecture Evolution (SAE). Some aspects of All-IP networks, however, were already defined as early as release 4.

IEEE 802.20 (Mobile-Fi): 802.20 was aimed at developing an interface that would allow the creation of low-cost, always-on, and truly mobile broadband wireless networks, nicknamed Mobile-Fi. The standard was constructed according to a layered architecture, which is consistent with other IEEE 802 specifications. The scope of the working group consists of the physical (PHY), medium access control (MAC), and logical link control (LLC) layers. The air interface will operate in bands below 3,5 GHz and with a peak data rate of over 1 Mbit/s.

The goals of 802.20 and 802.16e ("mobile WiMAX") are similar. Core components of 802.20 were to allow IP roaming and handoff (at more than 1 Mbps) with a mobile component accommodating vehicular speeds up to 250 km/h. This is to operate in licensed bands below 3,5 GHz with channel bandwidths of 5, 10, and 20 MHz providing peak data rates of 80 Mbps. 802.20 specifies a frequency-hopping OFDM modulation method with good spectral efficiency allowing up to 100 low data rate phone calls per MHz.

IEEE 802.20 has been wracked by allegations of dominance and lack of transparency of the process. Many feel that this was since from the start Qualcomm saw ArrayComm’s iBurst “standard” – upon which 802.20 is based – and its standardization as 802.20 as a competitive

threat; they did all they could to thwart the progress of the standard. The dominance charges caused IEEE 802 Executive Committee suspending 802.20, then establishing an 802.20 Oversight Committee which after looking at the voting rights and records changed the voting mechanics from an individual voting member to an entity based system. With some of those procedural issues possibly again being an issue the IEEE 802 management groups took this proactive step in another attempt to secure the IEEE process for this particular standard.

The IEEE approved 802.20-2008, Physical and Media Access Specification on 12 June 2008.

B.2 ISO 14443 Near Field Communications (NFC)

Like ISO/IEC 14443, NFC communicates via magnetic field induction, where two loop antennas are located within each other's near field, effectively forming an air-core transformer. It operates within the globally available and unlicensed radio frequency ISM band of 13,56 MHz, with a bandwidth of 14 kHz.

Working distance with compact standard antennas: up to 20 cm

Supported data rates: 106 kb/s, 212 kb/s, 424 kb/s or 848 kb/s

There are two modes:

Passive communication mode: The initiator device provides a carrier field and the target device answers by modulating existing field. In this mode, the target device may draw its operating power from the initiator-provided electromagnetic field, thus making the target device a transponder. Active communication mode: Both initiator and target device communicate by alternately generating their own field. A device deactivates its RF field while it is waiting for data. In this mode, both devices typically need to have a power supply.

Wireless High Definition (Wireless HD): The Wireless HD specification is based on the 7 GHz of continuous bandwidth around the 60 GHz radio frequency and allows for uncompressed, digital transmission of full HD video and audio and data signals, essentially making it equivalent, in theory, to wireless HDMI. The specification has been designed and optimized for wireless display connectivity, achieving in its first generation implementation high-speed rates from 4 Gbit/s for the CE, PC, and portable device segments. Its core technology promotes theoretical data rates as high as 25 Gbit/s (compared to 10,2 Gbit/s for HDMI 1.3), permitting it to scale to higher resolutions, color depth, and range.

Wireless Home Display Interface (WHDI): WHDI uses 20/40 MHz of bandwidth in the 5 GHz unlicensed band, offering lossless video and achieving equivalent video data rates of up to 3 Gbit/s.

Comparison of Wireless Sensor Networks Based on 802.15.4 Transceivers. Much has been stated in the popular press of the fact that ISA100.11a, Wireless HART, ZigBee and various proprietary systems all rely on the IEEE 802.15.4-2006 radio transceiver. Frequently, such articles then state how if it is the same radio, then the integration between these devices should be very easy. The situation is not quite that simple.

Walking counterclockwise (CCW) around the diagram, 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.

a) Wireless sensors – Circa 2010

This standard defines service access points (SAPs) throughout the protocol layers to allow.

Modern devices achieve a high degree of performance and flexibility by adopting networking functionality and tightly tying the transceiver to the Microcontroller. As previously mentioned, ISA100.11a, WiHART (HART 7.1), ZigBee and other proprietary methods use the 2006 version of an IEEE 802.15.4 radio. This radio is flexible in terms of power, frequency, and – perhaps most importantly – in how it integrates with the wireless sensor's Microcontroller. While seemingly complicated, by adopting the design rules associated with the Open Systems Interconnection model (OSI), shown in Figure B.1, a compartmentalization of performance functions are logically defined. The goal of the component blocks of Figure B.1's generic wireless sensor are to perform these functions.

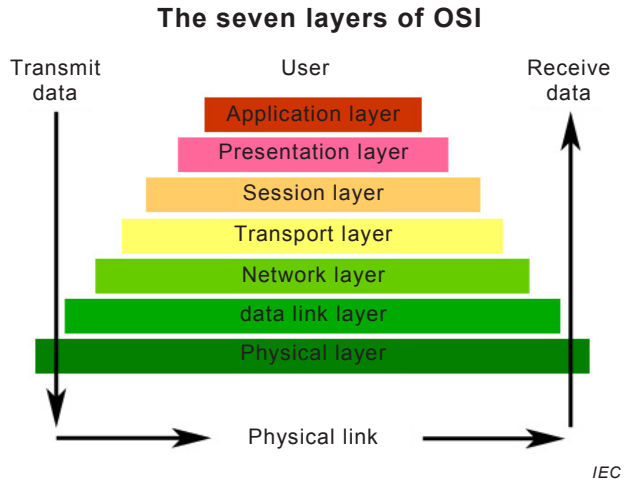


Figure B.1 – The Open Systems Interconnection (OSI) model defines the end-to-end communications means and needs for a wireless field transmitter to securely communicate with a distributed control system (DCS)

The situation may seem complicated, but in reality, by defining how the OSI layers are to communicate with each other – through Application Programming Interface (API) descriptors – different groups, different vendors may bring their specialty in a certain layer.

Returning to Figure B.2, the generic wireless sensor design as applied to ISA100.11a, WiHART (HART 7.1), and ZigBee stipulates that an IEEE 802.15.4 radio be used. In addition, while the 802.15.4 radio could be operated at a number of different frequencies, see Figure B.3, only the 2 450 (+/-) MHz frequency range is available – license free – worldwide.

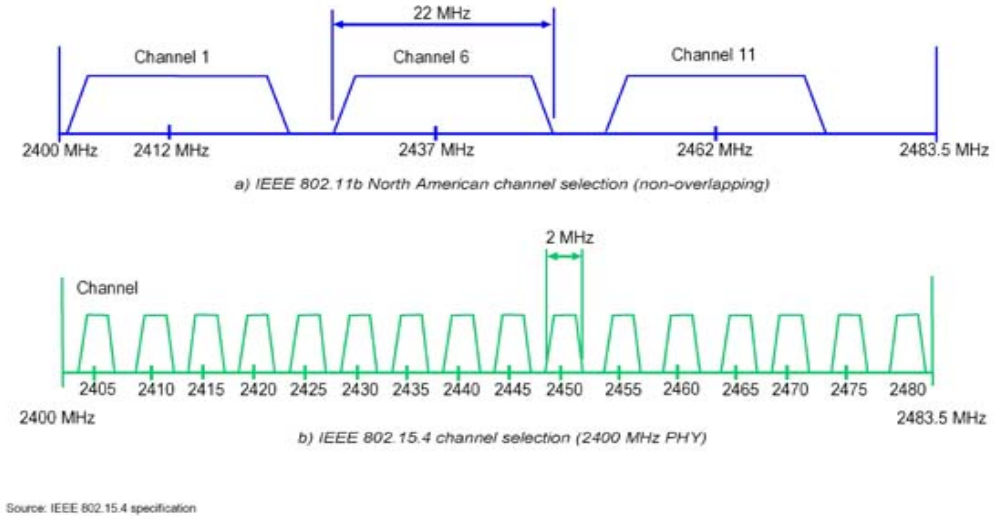


Figure B.2 – Operating frequencies for an IEEE 802.15.4 radio are 868 MHz, 902-926 MHz and 2 405-2 485 MHz. The worldwide license-free band at 2400 MHz is shown

The selection of the IEEE 802.15.4 radio dictates which frequency bands are “available” for use. The ISA100.11a standard stipulates that the radio shall operate in the 2 400 MHz band.

b) Network topologies – Circa 2010

In olden times, field transmitters were directly connected to an input/output (I/O) box. The signal transmission could be via pressure variations (3-15PSI) or electrical signaling, of many varieties but typically via variations in current (4-20 mA) or voltage (0-5 V, 0-10 V, etc.). The logistics associated with wiring thousands or tens of thousands of devices led to network developments where the field transmitters could (somehow) share a common transport medium. This idea, in turn, led to a wide variety of network designs and protocols with the vast majority being proprietary. Field transmitters (devices) would have identifiers that were transmitted within the data frame allowing those network elements with some level of intelligence to sort out the readings and process/transport them accordingly. Improvements in network protocols and the robustness requirement of minimal or even zero, single points of failure led to the variety of network topologies used today. Figure B.3 provides a graphical representation of such network topologies.

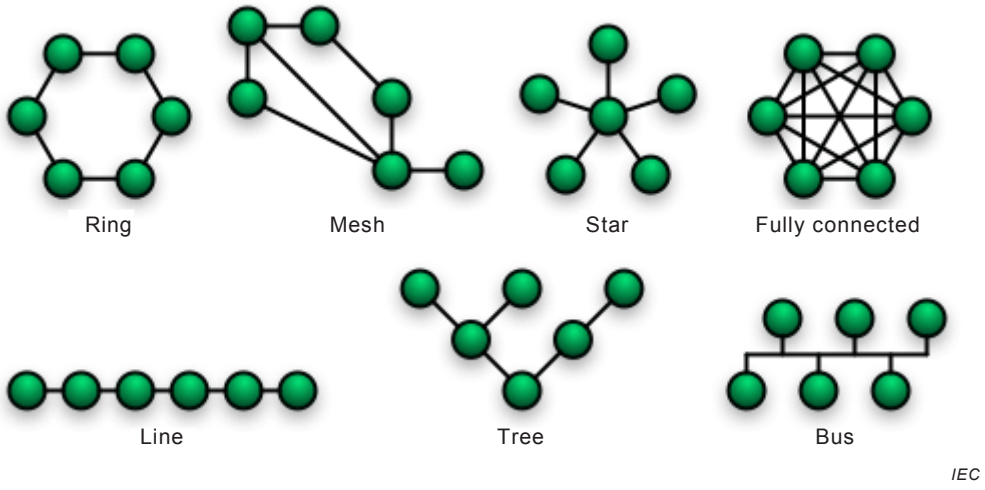


Figure B.3 – Networking topologies take many forms with associated levels of complexity required for robust fault-tolerant data transport

B.3 Real details of mesh networking

There is a vast amount of “how mesh networks work” information circulating in the ether. In the context of an industrial setting, it is not always so simple as to just move the wireless transmitters around to get better coverage – a frequent “fix” by academia and various vendors – but rather the sensors need to be at specific locations to provide useful information to the process engineer. A typical mesh network topological diagram is shown in Figure B.4. In the situation shown, each node is able to communicate with each other node.

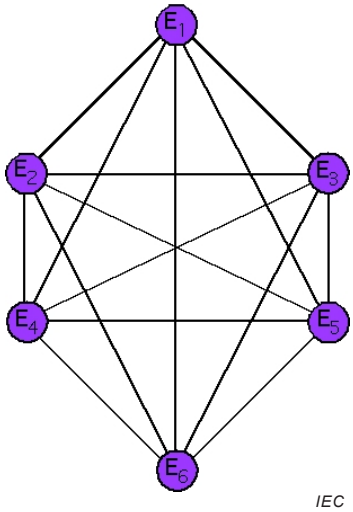


Figure B.4 – Typical mesh network diagram

While Figure B.5 is a nice diagram for discussion purposes indicating that each node can communicate with every other node, the reality is that this would require each node to project its RF signal over every other node. Assuming circular radiation patterns and that each wireless sensor transmits at the same power with the same omnidirectional antenna, the footprint scenario is as shown in Figure B.5.

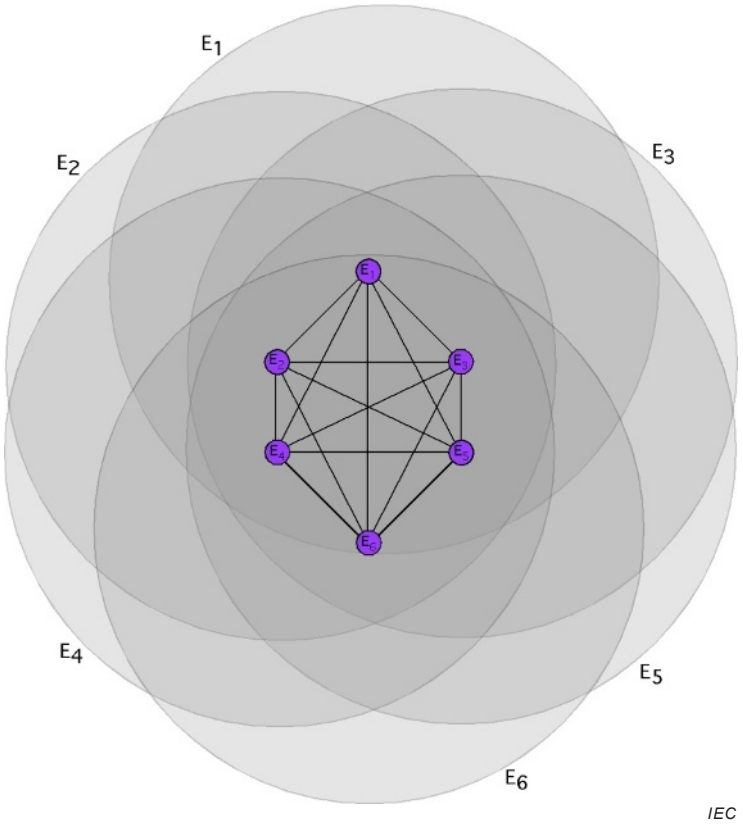


Figure B.5 – Requirement for mesh-networking communication of Figure B.4's topology

While Figures B.6 and B.7 show the principles of mesh networks, the reality of industrial wireless sensors operating in mesh network topologies is slightly different. Consider the following situation: the circles shown in Figure B.7 represent the idealized RF "footprint" of each radio-enable device. The "canyons of metal" and general reflective surfaces found throughout an industrial site can significantly vary the actual RF footprint from circular. The implications on the mesh requiring overlapping RF footprints when they may vary significantly from circular – and from each other – are: from an industrial deployment perspective, a fully-integrated mesh, as shown in Figure B.6 therefore requires a number of transmitters to be located in (relatively) close proximity.

The more realistic deployment scenario involves a cloud or cluster of wireless field transmitters that are controlled by a wireless gateway device. The gateway serves multiple roles, including:

a) coordinating the mesh routing table,

b) keeping track of the data transmission and network timing functions,

c) the network security (frequently working with a companion security manager), and

d) administration of any frequency channel "blacklisting/whitelisting".

The practical situation is that as shown in Figure B.6, a gateway and four nodes that, for this illustration, have been deployed in the industrial site resulting in the RF footprints shown.

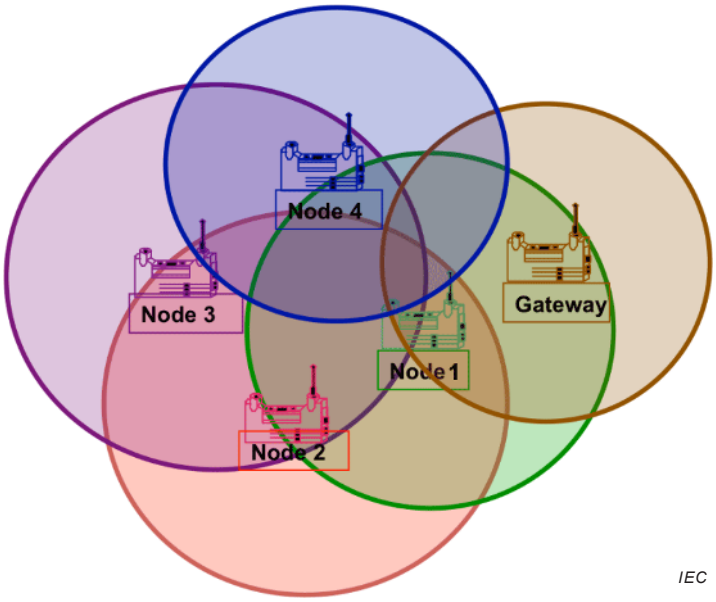


Figure B.6 – RF footprint map for a mesh network gateway and four nodes

Similar to Figures B.4 and B.5, the Figure B.6 diagram is meant to show how the radio transceiver (gateway/node) shall be within the RF footprint of its neighbors to be able to communicate with them. In Figure B.7's case, the Gateway can only communicate with Node #1. Node #1 lies within the RF footprint of the Gateway, Node #2 and Node #4 and is therefore – from an RF "coverage" perspective – able to relay messages from those neighbors. The associated mesh network connectivity diagram is shown in Figure B.7 (which is quite different from the idealized situation of Figure B.4).

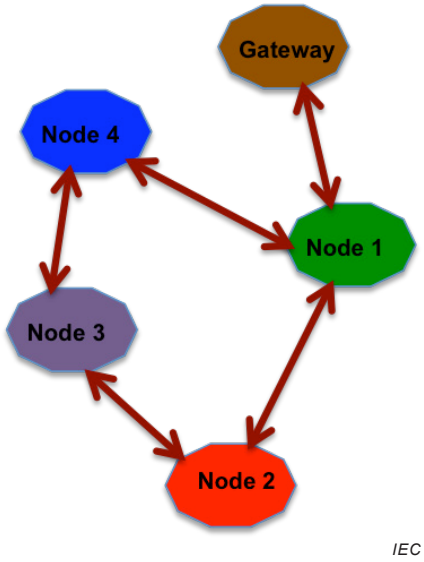


Figure B.7 – The connectivity diagram for Figure B.6's RF footprint coverage map

Please note that in this hypothetical deployment scenario, this is a non-robust communications network for a catastrophic network failure will happen if the link between the Gateway and Node #1 fails. The single-point of failure may be alleviated by moving the Gateway or the Nodes – a situation that the RF engineer may suggest, but that may not be feasible due to the actual locations of where the measurements are to be made.

B.4 Not all mesh networks are created equal – Latency and indeterminism in mesh networks

The mesh network diagrams of Figure B.4 and B.6 show how there is not a single path of communications through a mesh network and therefore is no single point of failure (except for the gateway). This is one of the key attributes of mesh networking, however, in establishing and maintaining a mesh network some rules shall be adopted – and abided with. At least 40 different mesh networking “rules” have been devised by industry and academia. Many of these rules are associated with placing an emphasis on, for example:

a) battery-operated lifetime,

b) algorithmic ease – in terms of computational complexity in the node firmware,

c) security/authentication/encryption of over the air traffic,

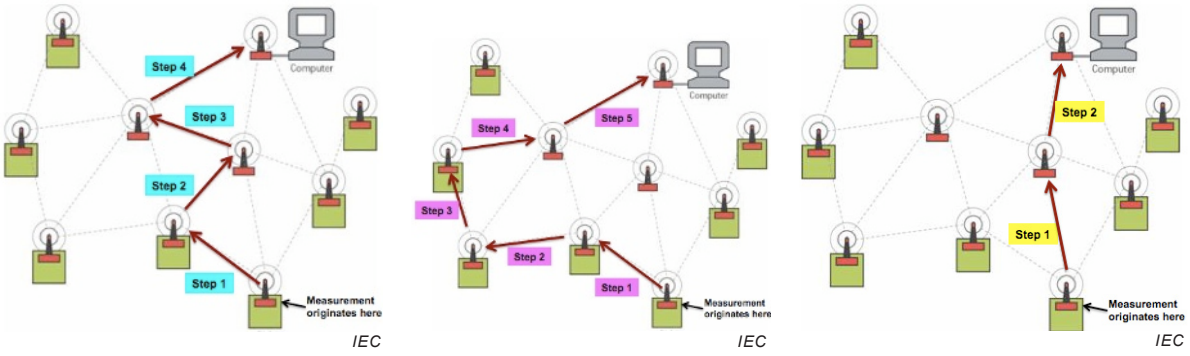
d) latency (data transport) minimization.

Each of these are noble causes but lead to substantially different “mesh networks” that, when implemented, do not allow interoperability.

Consider the mesh network shown in Figure B.8 and how a message (data) is transported through the network to the gateway. A philosophy used by a very prominent mesh networking group is that the devices are always in listening mode. Therefore when a node needs to transmit its message to its neighbors and on to the gateway, it checks if the communications channel (radio frequency) is busy (by monitoring the Received Signal Strength (RSS) value within its circuitry). If the channel is available it passes the message on to its neighbors (and so on) – the data transport (latency) is minimized. However, with listening taking a sizable percentage of the power as transmitting does, the batter-operated lifetime is relatively short (days, maybe months). Once again, the nodes are always listening, so if a message to be forwarded pops up, the node will concatenate that message with any other messages (traffic) and broadcast it to the nodes in proximity.

A very different mesh networking philosophy views the aforementioned scenario as consuming too much power listening – for probably infrequent messages – and looks to minimize listening and thereby increase battery-operated lifetime. In this scenario, the nodes in Figure B.4 or B.8 have time-synchronized precise clocks onboard and wake up at prescribed intervals. In essence, the nodes then check to see if there are any messages to transmit and/or receive, perform that data transfer/reception (if necessary), and then go back to sleep. By using this scheme, as the duty cycle is typically reduced to ~1 % and, given realistic batteries, the operational lifetime may be extended to over a year. In this time-synchronized mesh protocol method the data is transmitted from node-to-node with each clocking interval. Again referencing Figure B.8, consider a message that originates in Node 2. Depending on the network’s routing table, the message may take the Node 2 → Node 1 → Gateway path (2 hops) or it could take the Node 2 → Node 3 → Node 4 → Node 1 → Gateway path (4 hops).

While the Node 2 message may be time-stamped, the latency in getting the message from Node 2 to the Gateway – and beyond – is indeterminate. In a realistic situation where the nodes wake up once every 15 s, this means that the message may take 30 s to arrive at the gateway or 60 s to arrive at the gateway. The indeterminism comes from the message being able to take Paths (a), (b) or (c). The mesh networking algorithm being used in the nodes will dictate path variability.



a) b) c)

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

B.5 ISA100.11a – "Mesh – When You Need It – Networking"

The core networking tenet in ISA100.11a is to minimize the message latency. This means deploy a network topology that allows the wireless field transmitter to get to a high speed, low-latency backhaul network as quickly as possible. Figure B.9 illustrates the network topology for the ISA100.11a system. In most instances, the End User community (ISA100.8) is showing that a connection to some form of backhaul network is highly advantageous. The definitions for such a backhaul network are delivered by ISA100.15.

Figure B.9 depicts the communication areas addressed by ISA100.11a, as well as those areas (shaded in blue) that are not in scope of this standard. In Figure B.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 network infrastructure backbone network. A backbone is a data network (preferably high data rate) that is being defined by ISA100.15. This backbone could be an industrial Ethernet (802.3), Wi-Fi (802.11), WiMAX (802.16) or any other network within the facility interfacing to the plant's network.

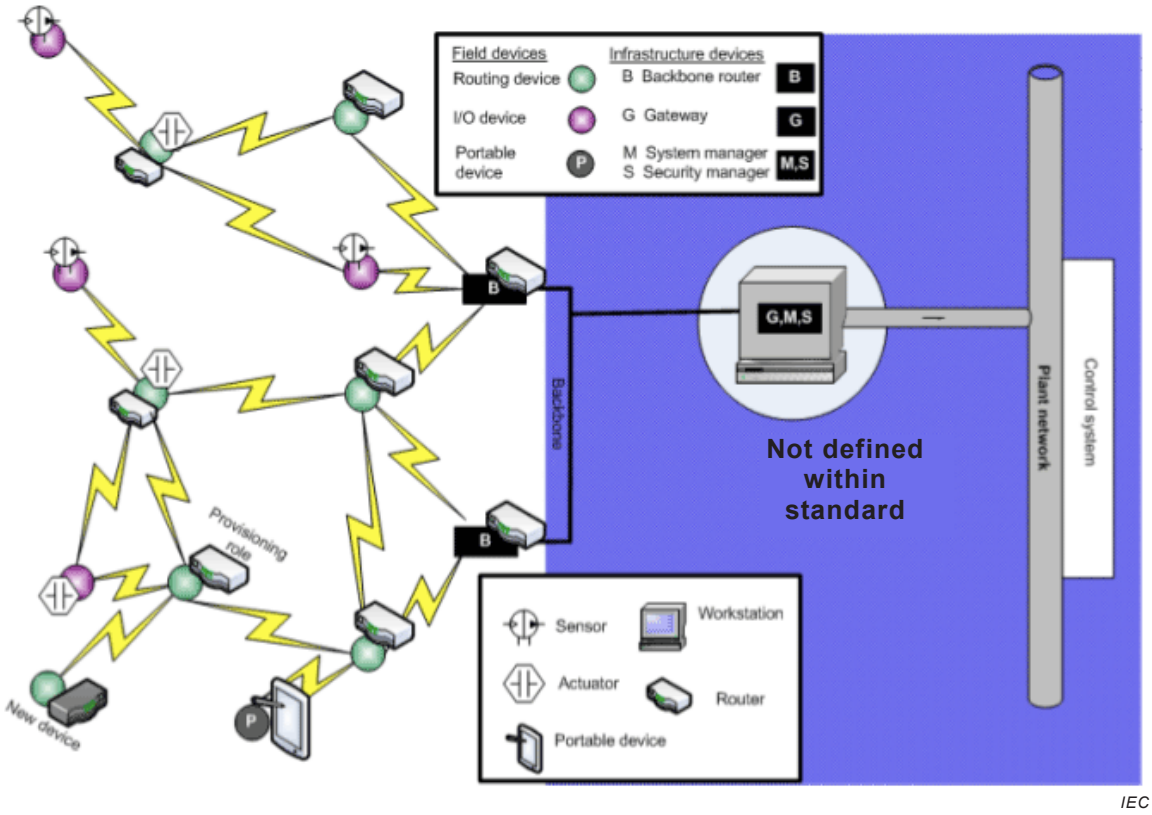


Figure B.9 – The technical specifications associated with ISA100.11a end at the gateway. The area shaded falls within the Backhaul Work Group, ISA100.15

As was described in Clause B.2 – and shown in Figure B.3 – there are a wide range of network topologies. ISA100.11a was designed to support such a variety of network topologies with an optimal system configuration yielding the lowest possible latency across the transport of device to control system. The simplest case, illustrated in Figure B.10, is where the field devices each have a direct link to the gateway. The message takes a single “hop” to the gateway and onto the high speed plant network.

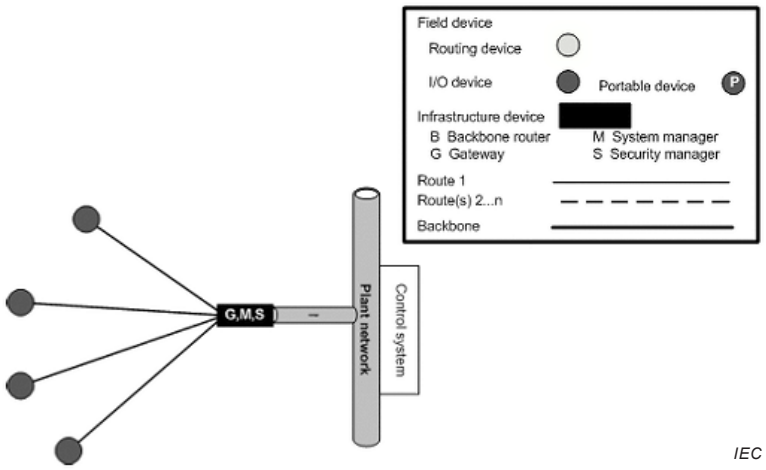


Figure B.10 – ISA100.11a utilizes the best topology for the application, in this case, a star

Another supported architecture is shown in Figure B.11. In this configuration two star networks are deployed with a high speed backbone network used to connect the backbone

routers to the gateway. The latency and indeterminism are minimized in each network segment.

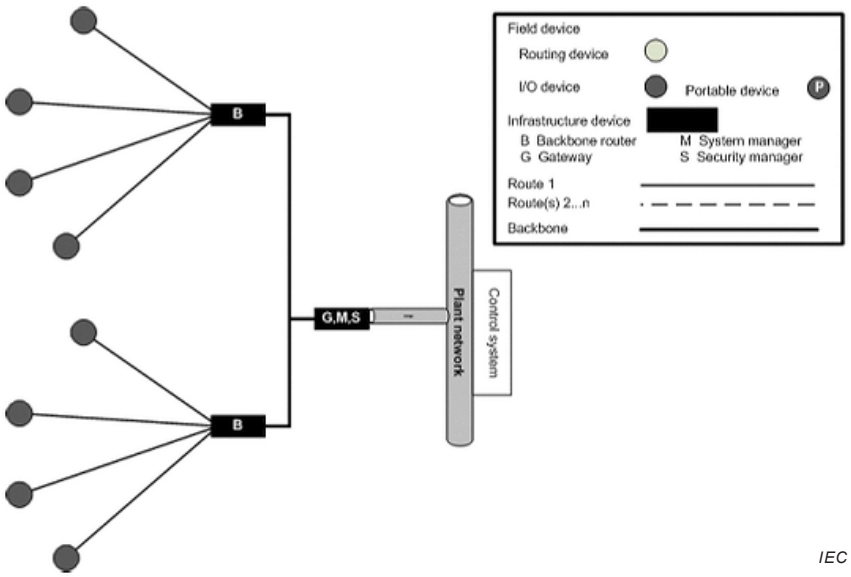


Figure B.11 – ISA100.11a allows for the deployment of multiple "hub and spoke" network elements with high speed interconnection to a gateway

Redundant, fault-tolerant, architectures employing dual gateways and multiple network segments are also supported. (An extensive array of supported network architectures and topologies are presented in the 700+ page ISA100.11a Standard itself.)

Technical drawings, such as those of Figures B.9, B.10 and B.11 are nice, but seeing the architecture for a deployed ISA100.11a network is, perhaps, more appropriate. Consider the network that was deployed at the Arkema chemical plant in Crosby TX. The network topology is shown in Figure B.12.

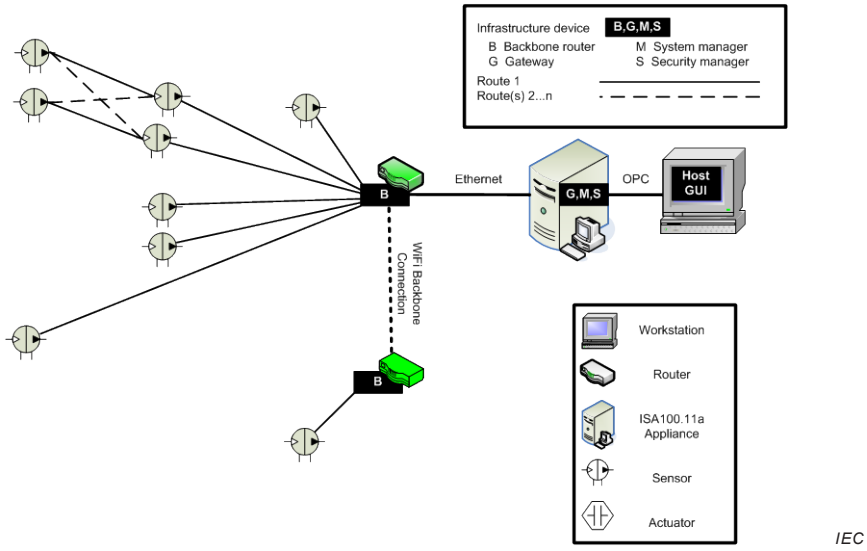


Figure B.12 – The ISA100.11a network deployed at Arkema was a logical mix of wireless field transmitters and an ISA100.15 backhaul network

An overlay of the chemical plant with the (approximate) location of the deployed suite of sensors and network elements is shown in Figure B.13. The diagram shows the ISA100.11a devices that were deployed in different locations within the plant, and then integrated with an 802.11 (Wi-Fi) backhaul network for long(er) distance transport across the plant.

Notice that this ISA100 network architecture allows for a wireless sensor mesh network – if it is necessary. Why not always a wireless mesh network? For the latency, indeterminism, and performance reasons previously stated.

B.6 Security by non-routing edge nodes

Mesh networks have some excellent characteristics for data transport in RF/physical environments where the attenuation and multipath circumstances may vary. This requires that the nodes be capable of routing traffic from their neighbors (in accordance with the network algorithm being used). From an implementation perspective, this allows the maintenance crew to deploy the nodes where they need to be.

But from a security perspective, this is not acceptable.

ISA100.11a addressed this specific security vulnerability by defining edge nodes (ISA100.11a devices deployed along the plant perimeter) to be non-routing. From a practical perspective, this implies that devices/systems/"bad guys" trying to access the plant network via their use of a device that is on the outside of the perimeter are not capable of doing so (for they would have to connect to the Edge Nodes, but the Edge Nodes do not allow such access (non-routing). Another situation where non-routing edge nodes are useful is depicted in Figure B.13. In this diagram (the aerial view was provided by members of the ISA Texas City chapter), chemical plants are neighbors of each other and require that their wireless sensor network not "talk to" the similar neighboring network. This situation may be taken care of by proper settings inside the gateways (using unique IDs for each plant's networks), but more importantly, it is readily achieved in ISA100.11a by the use of non-routing edge nodes.

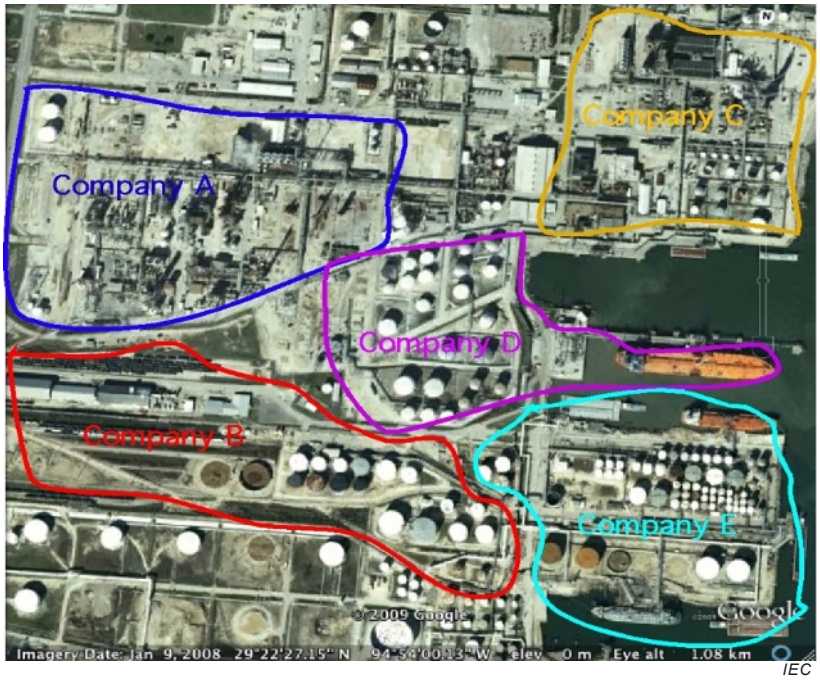


Figure B.13 – Networks deployed at neighbouring facilities will not "cross-talk" if non-routing nodes are deployed along the periphery of each facility

Other specifications, such as Wireless HART, may imply that they can achieve similar functionality by disabling their routing functions, but doing so makes such a device not compliant with their own specification.

The non-routing edge node functionality is a core tenet of ISA100.11a – in direct response to the requirements of the end users (ISA100.8).

B.7 Device and network provisioning methods

The end users requested that ISA100.11a meet their needs for a variety of secure provisioning methods. In response the technical gurus worked with sister organization ISA99 (Control System Security) to architect secure network elements to provide this capability. The result is a dizzying array of intersecting security methodologies aligned into the Standard. While those most interested in this aspect should refer to the 119 pages that comprise the Security and Provisioning sections of the Standard, the guiding State diagram for provisioning devices is shown in the following Figure B.1.

Under the ISA100.11a hood are the following end user provisioning methods:

- Provisioning over-the-air using pre-installed join keys.
- Provisioning using out of band mechanisms.
- Provisioning over-the-air using PKI certificates.
- Provisioning over-the-air using dual role advertisement routers.
- Provisioning backbone devices.

The net result is a system that allows the end user to choose from a number of secure provisioning methods based on the method(s) that best align with their business practices.

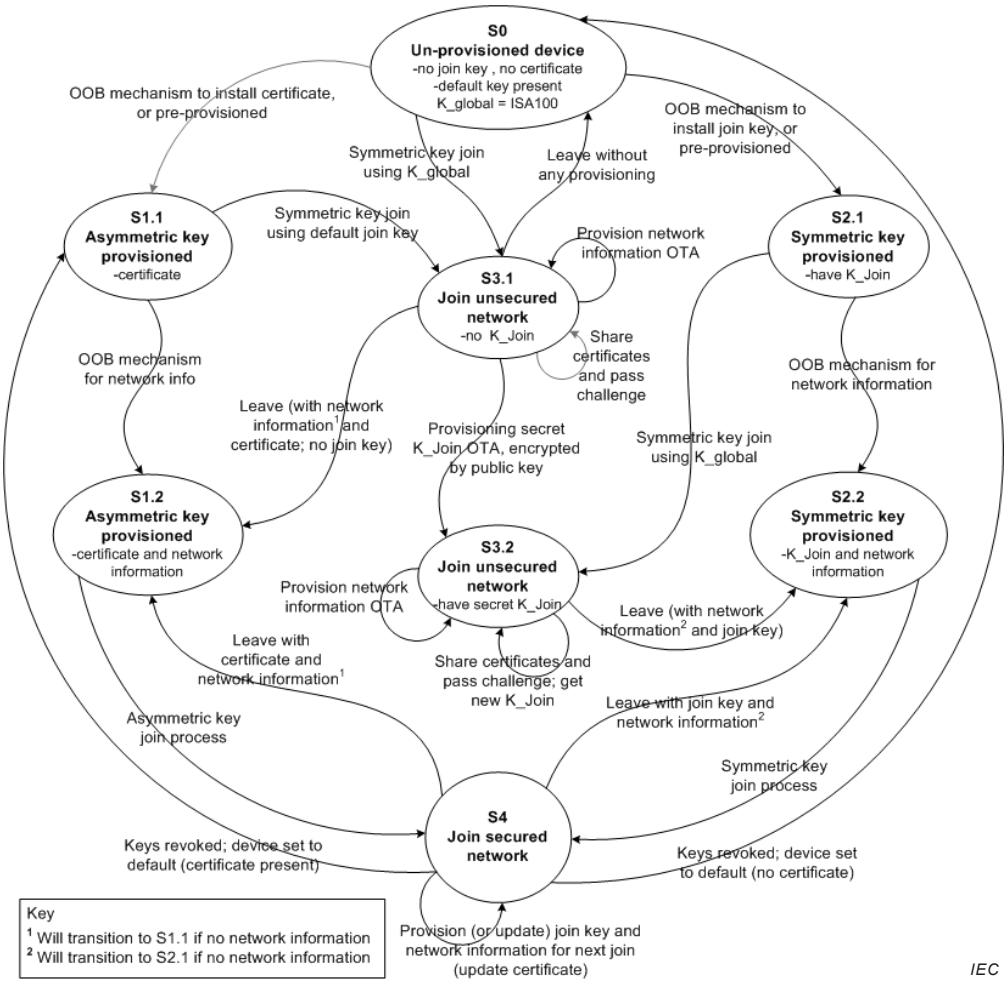


Figure B.14 – State transition diagram showing various paths to joining a secured network

Bibliography

[1] O'Hara, Bob, *The IEEE 802.11 Handbook: A Designer's Companion*

[2] Gast, Matthew, *802.11 Wireless Networks: The Definitive Guide (O'Reilly Networking)*

[3] Hashemian, H.M., Morton, G.W., Shumaker, B.D., and Kiger, C.J., "Nuclear Power Comeback Sure to Employ Wireless Tools", *InTech Magazine*, an ISA publication, January 2009

[4] Agar, Jon, Constant Touch, *A Global History of the Mobile Phone*, 2004 ISBN 1840465417

[5] Ahonen, Tomi, *m-Profits: Making Money with 3G Services*, 2002, ISBN 0-470-84775-1

[6] Ahonen, Kasper and Melkko, *3G Marketing*, 2004, ISBN 0-470-85100-7

[7] C. A. Balanis, *Antenna Theory Analysis and Design*, Second Edition, John Wiley & Sons, Inc., New York, 1997

[8] W. L. Stutzman and G. A. Thiele, *Antenna Theory and Design*, Second Edition, John Wiley & Sons, Inc., New York, 1997

[9] H. Mott, *Antennas for Radar and Communications*, John Wiley & Sons, Inc., New York, 1992, pp. 115-180

[10] D. K. Cheng, *Field and Wave Electromagnetics*, Addison Wesley, Reading, Massachusetts, 1989, p. 84

[11] http://www.ce-mag.com/archive/01/05/lansford.html

[12] IEC 60780, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

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

[14] IEC 60987, *Nuclear power plants – instrumentation and control important to safety – Hardware design requirements for computer-based systems*

[15] IEC 61000 (all parts), *Electromagnetic compatibility*

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

[17] IEC 62138, *Nuclear power plants – instrumentation and control important for safety – software aspects for computer-based systems performing category B or C functions*

[18] IEC 62657 (all parts), *Industrial communication networks – Wireless communication network*

[19] IAEA NS-G-1.3, *Instrumentation and control systems important to safety in nuclear power plants*

[20] IAEA GS-R-3, *The Management System for Facilities and Activities*

[21] IAEA GS-G-3.1, *Application of the Management System for Facilities and Activities*

[22] IAEA GS-G-3.5, *The Management System for Nuclear Installations*

[23] ISO/IEC 15149, *Information technology – Telecommunication and information exchange between systems – Magnetic field area network (MFAN)*

[24] IEC 62827, *Management protocol of wireless power transfer for multi-devices* (to be published)

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

[26] IEC 61784 (all parts), *Industrial communication networks – Profiles*

[27] ISO 24730-5, *Information technology – Real-time locating systems (RTLS) – Part 5: Chirp spread spectrum (CSS) at 2,4 GHz air interface*

[28] ISO/IEC 14443-1, *Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics*

[29] NUREG/CR-6882, *Assessment of Wireless Technologies and Their Application at Nuclear Facilities*

_____

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™