NUREG/CR-6882
ORNL/TM-2004/317

Assessment of Wireless Technologies and Their Application at Nuclear Facilities

Oak Ridge National Laboratory

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

NUREG/CR-6882
ORNL/TM-2004/317

Assessment of Wireless Technologies and Their Application at Nuclear Facilities

Manuscript Completed: July 2005
Published: July 2006

Prepared by
B.J. Kaldenbach, M.R. Moore, P.D. Ewing, W.W. Manges,
C.L. Dillard, K. Korsah, R.A. Kisner

Oak Ridge National Laboratory
Managed by UT-Battelle, LLC
Oak Ridge, TN 37831-6283

C.E. Antonescu, NRC Project Manager

Prepared for
Division of Fuel, Engineering and Radiological Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code Y6475

Intentionally Left Blank

ABSTRACT

Oak Ridge National Laboratory (ORNL) has been engaged by the U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) to identify and assess the safety-related issues that may be posed by the implementation of wireless systems in nuclear facilities. This work is being performed in response to the Office of Nuclear Reactor Regulation (NRR) User Need Request NRR-2002-017 for investigating emerging technologies and their application in nuclear facilities. Currently, wireless technology is not used as an integral element of safety-related systems in nuclear facilities. The most prevalent introductory use is for in-facility communications among personnel and for supplemental information transmission. However, further system upgrades and implementations at new facilities may introduce wireless communication into safety-significant applications.

This report documents the technology considerations, deployment issues, and implementation considerations that could contribute to the technical basis for comprehensive guidance on wireless systems. It is expected to help future instrumentation and controls designers select compatible wireless systems for nuclear facilities. The report also provides considerations regarding wireless system deployments.

Intentionally Left Blank

FOREWORD

Wireless technology is not currently used as an integral element of safety-related systems in nuclear facilities. The most prevalent emerging uses at this time are in-facility communications among personnel and supplemental information transmission. However, future system upgrades and implementations at nuclear facilities may introduce wireless technology into safety-significant communication-related applications. Three primary regulatory issues that may result include (1) electromagnetic interference with safety-related systems, (2) dependability and reliability of system-level communications; and (3) security of information and functions. Moreover, no available consensus standards fully address these issues. As a result, comprehensive regulatory guidance regarding the application of wireless technology requires development of regulatory practices and criteria for the design, implementation, operation, and maintenance of such systems.

This report discusses research, sponsored by the U.S. Nuclear Regulatory Commission (NRC) and conducted by Oak Ridge National Laboratory, to document the technology considerations, deployment issues, and implementation considerations associated with introducing wireless technology into nuclear facilities. The significant findings from this research include (1) a description of the state of the technology and current/expected applications in nuclear facilities; (2) a discussion of deployment issues related to increasing use of wireless technology within nuclear facilities and, in particular, its impact on safety-related systems; and (3) suggestions regarding the potential resolution of those deployment issues. This report does recognize that there are security issues associated with the deployment of wireless technology, but does not provide a comprehensive discussion on wireless or cyber security issues. A follow-on project is anticipated that will provide a more comprehensive treatment of the security of wireless technology, as well as address guidance on cyber security issues. This report has potential regulatory value as it relates to how proposed wireless solutions can be evaluated during regulatory reviews. It may also contribute to the technical basis for comprehensive regulatory guidance regarding the use of wireless technology in nuclear facilities.

Brian W. Sheron, Director
Office of Nuclear Regulatory Research

Intentionally Left Blank

CONTENTS

Page

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

Table **Page**

Intentionally Left Blank

EXECUTIVE SUMMARY

Oak Ridge National Laboratory (ORNL) has been engaged by the U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) to identify and assess the safety-related issues that may be posed by the implementation of wireless systems in nuclear facilities. This work is being performed in response to the Office of Nuclear Reactor Regulation (NRR) User Need Request NRR-2002-017 for investigating emerging technologies and their application in nuclear facilities. Currently, wireless technology is not used as an integral element of safety-related systems in nuclear facilities. The most prevalent introductory use is for in-facility communications among personnel and for supplemental information transmission. However, further system upgrades and implementations at new facilities may introduce wireless communication into safety-significant applications. The purpose of this report is to document the technology considerations, deployment issues, and implementation considerations that can contribute to the technical basis for comprehensive guidance on wireless systems.

The new technology of robust wireless communication has become available, and it is having a significant impact on how industrial operations are conducted. Wireless technology has already affected the business sector by introducing inexpensive wireless products (e.g., cell phones, personal digital assistants, and wireless network routers) into the marketplace. These products provide untethered (wire-free) access to computing in the workplace and at home and generally provide an adequate level of performance for the intended function. Industrial environments, and especially nuclear environments, are not as benign as business and home environments and present some unique issues for wireless devices that must be properly addressed to avoid operational problems. Industrial environments are characterized by extreme temperature and humidity changes; high noise levels (both electromagnetic and acoustic); and potential exposure to various chemicals, fumes, and dust. The nuclear environment also adds potential exposure to sources of ionizing radiation. In addition to the challenges that industrial environments present wireless devices, some industrial sensors and instruments may be sensitive to the electromagnetic emanations from wireless signals.

This study identifies and assesses wireless technologies, both current and emerging, that have the potential for deployment in nuclear facilities. The study explores the technology differentiators that need to be considered before deploying a wireless system. In addition, deployment issues are investigated and current wireless deployments in nuclear facilities are examined. Several security issues are briefly explored. (A more comprehensive treatment of wireless security is anticipated in a follow-on study. This study concludes by evaluating implementation considerations and offering suggested practices.

Stringent safety considerations in the nuclear environment will warrant stringent wireless-related security measures. In particular, (1) sensor data must be guarded against unauthorized snooping; (2) unauthorized sensors must be prevented from inserting data into the system; (3) the facility network must be guarded against infiltration through sensor networks; and (4) the facility network must be guarded against spoofing devices. To defend against attackers, wireless networks will need a robust and layered protection mechanism. These considerations should be reviewed in conjunction with the following documents that address cyber security in nuclear facilities: NUREG/CR-68476, *Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants*, and NEI 04-04, *Cyber Security Program for Power Reactors*.

Wireless-based systems have the potential for interference with facility systems. To put the probability of interference in perspective, it is important to realize that spread-spectrum technologies reduce the transmission distance, increase the quality of the signal, and transmit at lower power levels. The introduction of spread-spectrum wireless systems will likely have minimal impact on other facility equipment. Regarding the interference issue related to the coexistence of wireless devices, the potential for problems is still unknown. ORNL staff is conducting experimental studies to confirm the coexistence

issues, as well as developing coexistence simulation models. The results are expected to be reported in a future NUREG/CR report.

The locations of wireless transmitters must be given adequate thought and planning. The desired coverage area needs to be defined and a site analysis developed. If possible, a propagation analysis should be conducted; at a minimum, field tests should be conducted once the wireless equipment is identified.

User acceptance by facility personnel is a consideration that is often overlooked when implementing wireless systems. Most implementations will be centered around cost savings, efficiency, and remote operations, and the importance of these should not be underestimated. However, safety and security must always be considered with wireless applications at nuclear facilities and should be addressed early in the process. The users need to embrace the technology, yet remain receptive to the safety implications. User awareness of safety and security concerns is paramount, as both will be important to the implementation of wireless systems.

An important parameter for wireless networks is the ability to predict and/or guarantee performance. In the case of nuclear facilities, the probability that a message will get through, the probability that it will get through in a certain amount of time, and/or the probability that the system will know when a message did not get through are paramount. In safety-related systems, performance should be the most important parameter. Because absolute control of the transmission medium (the spectrum) is not possible, wireless systems by their very nature are not deterministic. Measures will have to be applied to increase the *probability*. The system must take into account the probabilities of success at each intervening node between the originator of the message and the final user. Prudent use of redundancy should be considered when deploying wireless systems.

This report documents the state of the technology from the perspective of possible use in nuclear facilities and the wireless standards presently in use, as well as new standards under development. It identifies present applications of wireless systems in nuclear facilities and describes deployment issues that could impact regulatory policy. The report also discusses the safety implications of implementing wireless systems and the lessons learned from recent deployments.

Suggested uses of the report include:

- An introduction to wireless systems for NRC staff,
- Background technical information on wireless technology and potential deployment issues for its implementation into nuclear facilities,
- Assistance in assessing wireless systems proposed for nuclear facilities that may require NRC review, and
- A knowledge base for operating simulation tools that can assess the performance of wireless devices in nuclear facilities.

ACKNOWLEDGEMENTS

The authors wish to thank Bill Kemper, Branch Chief, and Christina Antonescu and Tekia Govan, JCN Y6475 Project Managers, of the U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research for their help in initiating, planning, and implementing this research effort.

Intentionally Left Blank

ACRONYMS

AES	Advanced Encryption Standard
ALARA	as low as reasonably achievable
AP	access point
BER	bit error rate
BFSK	binary frequency shift keying
BPSK	binary phase shift keying
CCK	complementary code keying
CCP	centrifugal charging pump
CDMA	code division multiple access
CBM	conditioned-based maintenance
CSMA	carrier sense multiple access
CSMA-CA	CSMA with collision avoidance
CTS	clear to send
DBPSK	differential binary phase shift keying
DCF	distributed coordination function
DES	Data Encryption Standard
DSL	digital subscriber line
DSSS	direct sequence spread spectrum
EPRI	Electric Power Research Institute
EPSS	Electronic Performance Support System
FCC	Federal Communications Commission
FDMA	frequency division multiple access
FEC	forward error correction
FFH	fast frequency hopping
FHSS	frequency hopping spread spectrum
FIPS	Federal Information Processing Standard
GFSK	Gaussian frequency shift keying
GMSK	Gaussian minimum shift keying
I&C	instrumentation and controls
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IP	Internet protocol
IPv6	IP, version 6
ISA	Instrumentation Systems and Automation Society
ISM	Industrial, Scientific, and Medical
ISO	International Organization for Standardization
IT	information technology
ITU	International Telecommunication Union
LAN	local area network
LLC	logical link control
LMR	land mobile radio
LOS	line-of-sight
MAC	media access control layer
MAN	metropolitan area network
M-ary	multiple carrier signals
MFSK	M-ary frequency shift keying
MIMO	multiple input - multiple output
MPSK	M-ary phase shift keying
MSK	minimum shift keying
MTBF	mean-time-between-failure

NAV	network assignment variable
NIST	National Institute of Standards and Technology
NEI	Nuclear Energy Institute
NLOS	non-line-of-sight
n-QAM	multilevel quadrature amplitude modulation
NRC	Nuclear Regulatory Commission
NRR	NRC Office of Nuclear Reactor Regulation
OFDM	orthogonal frequency division multiplexing
OFDMA	orthogonal frequency division multiple access
OLA	overlap avoidance
O-QPSK	offset quadrature phase shift keying
ORNL	Oak Ridge National Laboratory
OSI	Open Systems Interconnect
PAN	personal area network
PBCC	packet binary convolutional coding
PC	personal computer
PCF	point coordination function
PDA	personal data assistant
PHY	physical layer
PN	pseudo-noise
PSEG	Public Service Enterprise Group
QoS	quality of service
QPSK	quadrature phase shift keying
RAM	reliability, availability, and maintainability
RES	NRC Office of Nuclear Regulatory Research
RF	radio frequency
RFID	radio frequency identification
RTS	request to send
Rx	receiver
SDR	software defined radio
SFH	slow frequency hopping
SSID	service set identifier
TDMA	time-division multiple access
TKIP	Temporal Key Integrity Protocol
Tx	transmitter
UNII	Unlicensed National Information Infrastructure
UWB	ultra-wideband
VPN	virtual private network
WAN	wide area network
WECA	Wireless Ethernet Compatibility Alliance
WEP	wired equivalent privacy
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
Wi-Media	Wireless Media
WINA	Wireless Industrial Networking Alliance
WLAN	wireless local area network
WPA	WiFi Protected Access
WPA2	WPA, version 2

GLOSSARY

AC—Alternating current.

Ad-hoc—Self-configuring. An ad-hoc network is one that self-configures based on the nodes that present themselves as members of the network. The result is a dynamic network; for example, static routing tables are not used.

Bandwidth—A range within a band of frequencies. In a digital communications system, the bandwidth is the amount of data that can be transmitted in a fixed amount of time.

Baseband—A bit stream which has not been modulated; i.e., its spectral content extends from DC to some finite value.

Beamform—A technique for increasing the directional gain of a system by introducing phase delay in each of several channels so that the signals in the direction of interest add constructively, while signals in other directions will suffer destructive interference and therefore be attenuated.

Bit—The finest breakdown of information in a digital computer. In binary, the value of a single bit is either zero (off) or one (on).

BER—Bit Error Rate—A measure of the likelihood that data transmitted will be successfully received. Bit error rate is usually expressed as a ratio such as 1 in 1000, meaning that 1 bit in 1000 will likely be in error; or as a probability like 10^{-3}, meaning that each bit has a 1 in a 1000 chance of getting through successfully.

BFSK—Binary Frequency Shift Keying—A technique for modulating a radio frequency carrier wave where the frequency of the carrier signal is switched between two possible message states corresponding to a "zero" and a "one."

BPSK—Binary Phase Shift Keying—a technique for modulating a radio frequency carrier wave where the carrier is transmitted with a certain phase for a "zero" and a phase difference of 180° for a "one."

Broadband—A type of transmission in which a single medium can carry several channels at once.

CCK—Complementary Code Keying—A modulation technique where data are transmitted by modulating a single carrier.

CDMA—Code Division Multiple Access—A transmission protocol used to transmit data on a shared line. It can be wired or wireless but is most often used in wireless communication, including cell phones. CDMA is one of the only communication technologies that allows multiple transmitters to be "on" at the same time and not interfere with each other.

Chip—The finest breakdown of information as transmitted in a digital communications system.

Chipping—The process of high-speed sampling of individual bits in the data stream for transmission over the channel to accomplish the spreading in a spread spectrum radio—as in "IEEE 802.11 uses 11 chips per bit in its spreading code."

Chip Rate—The number of subsamples taken on each bit in the transmission.

DC—Direct current.

Diffraction—The phenomenon whereby waves traveling in straight paths bend around an obstacle.

Diversity—a technique where information is transmitted using multiple modalities, thus increasing the likelihood of error-free reception. Spread spectrum signals are inherently spectrally diverse since the information is spread over a range of frequencies. Other techniques are used to make the signal temporally (spread over time), spatially (spread in space), and polarity (polarization of the carrier wave) diverse.

DSSS—Direct-Sequence Spread Spectrum—A communication technology where each bit in the transmitted signal is combined with a higher-speed chipping pattern using a modulo-2 adder before being modulated onto an RF carrier for transmission. The resulting RF signal has significantly wider bandwidth than the original "baseband" signal had. This has some advantages in high-interference environments. The DSSS "process gain" is equal to 10 dB log (chip rate).

FCC—The Federal Communications Commission regulates the radio transmissions in the United States. It authorizes specific types of transmissions in specific radio bands for the overall welfare of the nation as well as international treaties.

FDMA—Frequency Division Multiple Access—A technique for allocating channels in a particular space by assigning a specific frequency to each transmitter so that they can all transmit at the same time.

FEC—Forward Error Correction—A technique whereby additional information is transmitted with the signal so bits that are received in error can be corrected without requiring a retransmission.

FHSS—Frequency Hopping Spread Spectrum—A communication technology where the transmitter and receiver change frequencies every so often so that the entire bit stream is not on a single frequency. The transmitter and receiver are synchronized so that they can stay locked and the bit stream is retrieved. This technology has some advantages in a high multipath environment.

ft—Feet, unit of length.

GFSK—Gaussian Frequency Shift Keying—A frequency shift keying modulation technique where the baseband pulses are first passed through a gaussian filter to make the pulses smoother to limit their spectral width.

GHz—Gigahertz, 10^9 Hertz or cycles per second, a unit of frequency. For example, a 2.4-GHz radio transmission is an electromagnetic signal that oscillates at 2.4×10^9 cycles per second. These ultra-high-frequency (UHF) signals have very good noise immunity but are useful for line-of-sight transmissions only. In general, the higher the frequency, the more the radio signal is like visible light—line of sight, sensitive to fog, immune to most electrical interferers.

GMSK—Gaussian Minimum Shift Keying—derivative of MSK that is most attractive for its power efficiency and spectral efficiency.

IEEE—The Institute of Electrical and Electronic Engineers is a professional society involved in establishing standards for various technical areas (www.ieee.org).

IEEE 1451—This smart sensor standard defines the electrical and logical interfaces for communicating between industrial sensors and computers.

IEEE 802—This is the standard for computer local area networks (LANs). "Regular" Ethernet (802.3) is included in this standard, as well as 802.11, the wireless Ethernet standard. Bluetooth and Zigbee wireless communications are defined under 802.15.

ISM—The FCC has allocated a collection of frequencies in the radio spectrum for use by "industry, science, and medicine." Radios in these bands don't require licenses but are "type accepted" under FCC regulations so that individual transmitter licenses are not required. The 900-MHz, 2.4-GHz, and 5.8-GHz bands are the most commonly used in wireless sensor networks.

kb/s—Kilobits per second–10^3 bits/second, unit of data rate.

km—Kilometers—1000 (or 10^3) meters, unit of length. 1 km = 0.6214 mile.

km/h—Kilometers per hour—10^3 meters/hour, unit of speed.

LAN—A Local Area Network (as opposed to a Wide Area Network—WAN) usually comprises a collection of computers tied together over some network technology (like Ethernet) and managed by a single organization to provide computing services to a community of users such as at a university or company.

Line-of-sight—In radio, line of sight refers to the need for transmission between transmitter and receiver to occur without intervening structures or obscurers. Lower-frequency radio transmissions (like commercial AM broadcasts) can "bend" around buildings and even the horizon or bounce off the ionosphere, but higher-frequency transmissions (like TV) require that the transmitter tower be able to "see" the receiver antenna.

m—Meter, unit of length.

M-ary—A signaling scheme where two or more bits are grouped together to form symbols. One of M possible signals, where M is a multiple of 2, is transmitted for each symbol.

Mb/s—Megabits per second–10^6 bits/second, unit of data rate.

MFSK—M-ary Frequency Shift Keying—a modulation technique where M transmitted signals are of equal energy and equal duration and signal frequencies are orthogonal to one another.

MHz—Megahertz, 10^6 Hertz or cycles per second, a unit of frequency. For example, a 900-MHz radio transmission is an electromagnetic signal that oscillates at 900×10^6 cycles per second. These ultra-high-frequency (UHF) signals have very good noise immunity but are useful for line-of-sight transmissions only. In general, the higher the frequency, the more the radio signal is like visible light—line of sight, sensitive to fog, immune to most electrical interferers.

Mobile, Ad Hoc Networking—A technique for ensuring a robust connection in a local area network by allowing a dynamic routing table (i.e., a routing table in network routers that changes as the possible routes change) that can be updated when nodes enter and leave the network.

MPSK—M-ary Phase Shift Keying—A modulation technique where the carrier phase takes on one of M possible values and the amplitude of the transmitted signal remains constant. Example: If M=4, it is called QPSK.

MSK—Minimum Shift Keying—A special type of continuous phase frequency shift keying where the peak frequency deviation is ¼ the bit rate.

Multipath—Multiple radio signals arriving at the receiver along a trajectory that includes reflections are said to exhibit multi-path.

mW—Milliwatts–10^{-3} watts, a unit of power.

Noise—A term used to signify extraneous signals that do not convey any useful information for the problem at hand, and which can be described only by their statistical properties.

n-QAM—multilevel Quadrature Amplitude Modulation—A modulation technique where both the amplitude and phase vary to form a unique constellation of 2^n possible signal states, where n=1,2,3...

O-QPSK—Offset Quadrature Phase Shift Keying—A modified form of QPSK where even and odd bit streams are offset in their relative alignment by one bit period.

Packet—Packet radio implies that the data are being transmitted into bundles before being transmitted. This allows multiple users to access the physical media simultaneously. Traditional phone lines have been line switched, implying that the line is allocated to the connection until the connection is broken. Packet switched networks (as are now used for phone service) actually break the data up for transmission and then reassemble it for delivery.

PBCC—Packet Binary Convolutional Coding—A method of forward error correcting that reduces the bit error rate without increasing transmission power.

Process Gain—A signal-to-noise advantage gained by the modulation and demodulation process.

QPSK—Quadrature Phase Shift Keying—An update to the older RF modulation technique known as binary phase shift keying. Phase shift keying varies the phase of the RF carrier to represent the information desired. In binary, phase shift keying one phase would represent a zero and another phase a one. In quadrature phase shift keying, each sine wave in the carrier can be shifted to four different phases representing the data to be transmitted.

Refraction—The change in direction of propagation of a wave front due to its passing obliquely from one medium to another in which its speed is different.

Reflection—The phenomenon in which a wave that strikes a medium of different characteristics is returned to the original medium with angles of incidence and reflection equal and lying in the same plane.

Repeater—This type of radio receives a signal and retransmits it in such a way as to extend the range of the transmission.

RF—Radio Frequency—Usually considered to be any electromagnetic signal above 30 kHz. Electromagnetic signals under 30 kHz are considered acoustic (i.e., sound waves).

RFID—Radio Frequency Identification—A device used to locate and identify objects by transmitting a radio signal containing hard-coded information (like a bar code).

Rx—The abbreviation sometimes used to represent the receiver in a radio.

Scatter—A disordered change in the direction when radio waves encounter matter.

Signal-to-noise—A ratio, usually expressed in dB, representing the relative strength of the desired signal to the undesired noise. The expression for signal to noise ratio (SNR) is signal/(signal+noise).

Spread Spectrum—Telecommunication techniques in which a signal is transmitted with a bandwidth considerably greater than the frequency content of the original information and then collected onto the original frequency at the receiver. This frequency spreading can improve the signal-to-noise properties of the transmission. Common spread spectrum systems are of the "direct sequence" (see DSSS) or "frequency hopping" (see FHSS) type, or some combination of these two types (called a "hybrid").

Symbol—A pair of data bits representing a particular waveform.

Symbol period—A fixed number of output samples that can be transmitted across the communication channel.

TDMA—Time Division Multiple Access—A technique for allocating channels in a particular frequency band by assigning a specific time slot to each transmitter so that they can all use the same frequency.

Transceiver—A transceiver is a single unit that combines the functions of transmitter and receiver.

Tx—The abbreviation sometimes used to represent the transmitter in a radio.

UWB—Ultra-wideband—A relatively new term to describe a technology that has been known since the early 1960s as "carrier-free, "baseband", or "impulse" technology. The basic concept is to develop, transmit, and receive an extremely short-duration pulse of RF energy—typically a few tens of picoseconds to a few nanoseconds in duration. The resultant waveforms are extremely broadband, typically on the order of a few GHz.

Intentionally Left Blank

1. INTRODUCTION

Oak Ridge National Laboratory (ORNL) has been engaged by the U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) to identify and assess the safety-related issues that may be posed by the implementation of wireless systems in nuclear facilities. This work is being performed in response to the Office of Nuclear Reactor Regulation (NRR) User Need Request NRR-2002-017 for investigating emerging technologies and their application in nuclear facilities. Currently, wireless technology is not used as an integral element of safety-related systems in nuclear facilities. The most prevalent introductory use is for in-facility communications among personnel and for supplemental information transmission. However, further system upgrades and implementations at new facilities may introduce wireless communication into safety-significant applications.

The JCN Y6475 project is intended to encompass a systematic evaluation of the prospective role of wireless systems in nuclear facilities and is divided into two phases. The objective of Phase 1 is to identify and assess the state of wireless systems and investigate potential deployment issues. The Phase 2 objective is to conduct confirmatory research to validate the Phase 1 findings. The purpose of this report is to document the Phase 1 effort. Technology considerations, deployment issues, and implementation considerations that can contribute to the technical basis for comprehensive guidance on wireless systems are discussed. The Phase 2 effort has commenced with the development of simulation models for wireless systems and experimental measurements are expected to follow. Results of the Phase 2 effort will be reported in a future NUREG/CR.

The new technology of robust wireless communication has become available, and it is having a significant impact on how industrial operations are conducted. Wireless technology has already affected the business sector by introducing inexpensive wireless products (e.g., cell phones, personal digital assistants, and wireless network routers) into the marketplace. These products provide untethered (wire-free) access to computing in the workplace and at home and generally provide an adequate level of performance for the intended function. Based on the promulgation of wireless technology in the business sector and in users' personal lives, one can easily imagine the increase in productivity that is possible by providing users of computer-based products with wire-free capabilities. However, convenience almost always comes with a cost, and wireless access is no exception. Entire hacking communities and Web sites have sprung up with tips and tools for exploiting wireless technology, especially poorly configured wireless networks. In spite of this fact, the deployment of wireless devices in businesses and homes has been phenomenal.

Industrial environments, and especially nuclear environments, are not as benign as business and home environments and present some unique issues for wireless devices that must be properly addressed to avoid operational problems. Industrial environments are characterized by extreme temperature and humidity changes; high noise levels (both electromagnetic and acoustic); and potential exposure to various chemicals, fumes, and dust. The nuclear environment also adds potential exposure to sources of ionizing radiation. In addition to the challenges that industrial environments present wireless devices, some industrial sensors and instruments may be sensitive to the electromagnetic emanations from wireless signals. Many industrial organizations, like the Instrumentation Systems and Automation Society (ISA) (www.isa.org), the Electric Power Research Institute (EPRI) (www.epri.org), and the Wireless Industrial Networking Alliance (WINA) (www.wina.org), are working to advance wireless solutions for industrial environments.

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. However, there could also be safety benefits.

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.

The first goal of this study is to identify and assess wireless technologies that have the potential for deployment in nuclear facilities. The second goal is to consider the numerous applications in the nuclear environment where wireless systems could be applied without risking safety. This report begins with a brief overview of the wireless technologies, both current and emerging, that may be appropriate for the nuclear environment. The overview is intended to be somewhat tutorial, in an attempt to orient the reader to the germane technology. The report then explores technology differentiators that need to be considered before deploying a wireless system. Deployment issues are discussed, and current wireless deployments in nuclear facilities are examined. The report concludes with a discussion of implementation considerations and subsequent conclusions.

2. WIRELESS TECHNOLOGY OVERVIEW

2.1 Elements of a Wireless System

The essential elements of a wireless communications system are shown in Fig. 2.1. They are the transmitter, a transmission path, and the receiver. The transmitter processes the input signal or message being sent to produce a transmitted signal suitable for transmission. Signal processing is applied involving modulation and coding. Modulation is invoked at the transmitter and entails a modulating signal that represents the message being sent and a carrier wave. Demodulation is invoked at the receiver to strip off the carrier wave and present the original message. Coding is a processing operation that makes the communications between the transmitter and receiver more robust. The message is encoded into a new sequence of symbols for the transmission and then decoded back to the original message in the receiver. Modulation and coding techniques help the desired signal to maintain its integrity or fidelity when exposed to noise (random and unpredictable signals produced by natural processes) and interference (man-made exogenous signals). Along with demodulating and decoding the received signal, the receiver might also amplify and filter it in preparation for delivery to the intended recipient.

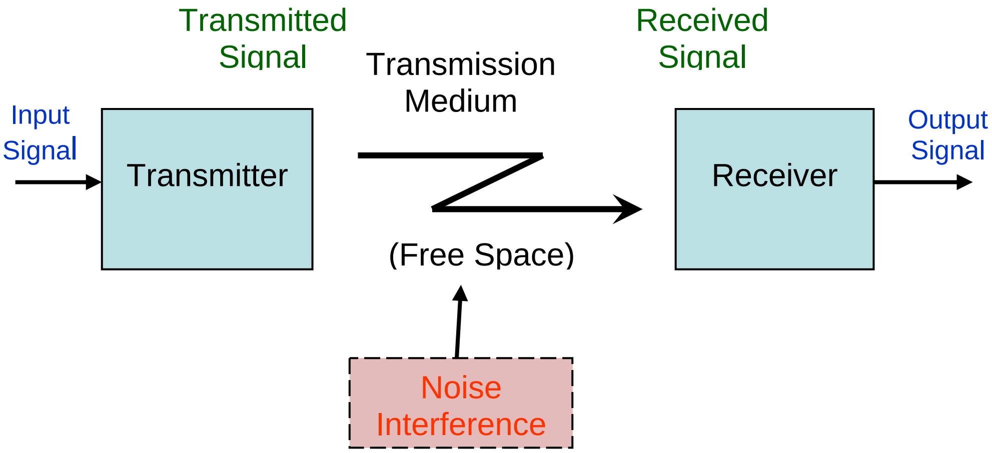

Figure 2.1. Elements of a wireless system.

2.2 Technology Description

The wireless technology thought to be best suited to be applied in nuclear facilities is the digital wireless data network because of the data types encountered. Wireless networks are now prevalent in industrial environments and are typically defined by their nominal transmission distances. Wireless personal area networks (PANs) operate over a coverage area (or range) of a few tens of meters, wireless local area networks (LANs) operate over a coverage area of hundreds of meters, and metropolitan area networks (MANs) operate over a coverage area of several kilometers. Characteristics of the different types of networks will vary based on their specific applications, but many wireless networks share commonly distinguishable attributes. These attributes could include spectrally efficient modulation techniques, multiple access techniques, and geographically distributed access points (APs). Detailed discussions of applicable techniques can be found in engineering textbooks;[1–3] the intent in this report is to succinctly summarize the current techniques of wireless technology.

Bandwidth is typically a major issue for wireless networks, and efficient use of the available frequency spectrum is directly related to network capacity. Hence, spectrally efficient modulation techniques are essential. Additional factors that influence the selection of modulation techniques include bit error rate

(BER), signal-to-noise ratio, multipath and fading conditions, and cost to implement. The selection of a modulation technique will depend on the desired fidelity (i.e., an acceptable BER), the available bandwidth in a particular frequency band, the desired data rate, the multipath environment (i.e., conditions where the wireless signal travels via multiple paths), and the complexity of the network hardware. Tradeoffs are made depending on the specific application.

Digital modulation techniques fall into several classifications: linear, constant envelope, combined linear and constant envelope, and spread spectrum. Linear modulation techniques vary the amplitude of the transmitted signal linearly with the modulating signal and are bandwidth-efficient. They are used in applications where there is a high demand for multiple users within a limited bandwidth. These techniques include binary phase shift keying (BPSK), quadrature phase shift keying (QPSK), and offset quadrature phase shift keying (O-QPSK).

Constant envelope modulation techniques keep the amplitude of the carrier constant despite variations in the modulating signal. They are not as bandwidth efficient as linear techniques, but they are power efficient. These techniques include binary frequency shift keying (BFSK), minimum shift keying (MSK), and Gaussian minimum shift keying (GMSK).

Combined linear and constant envelope techniques generate multiple carrier signals by varying both the envelope and phase and are called M-ary modulation. They are particularly useful in bandwidth-limited applications. These techniques include M-ary phase shift keying (MPSK), M-ary frequency shift keying (MFSK), and multilevel quadrature amplitude modulation (n-QAM). Descriptions of the individual modulation techniques are provided in the Glossary.

Spread spectrum modulation techniques occupy a large bandwidth by spreading the data transmission over the entire band. This spreading allows the transmitted signal to be more resistant to cancellation problems in multipath environments and enables many users to employ the same bandwidth without interfering with each other. Spread spectrum modulation includes direct sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS). DSSS spreads the baseband signal in the transmitter by multiplying its data pulses with a pseudo-noise (PN) sequence and then despreads it on the receiver side. FHSS involves hopping a series of modulated data bursts over a sequence of carrier frequencies chosen pseudo-randomly.

Multiple access techniques are used to allow a number of users to simultaneously share the same frequency spectrum. The three major types of access techniques are frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA). FDMA assigns a user to an unshared frequency channel for a particular transmission, while TDMA allows users to transmit over the same frequency channel in allocated time slots. CDMA allows all users to transmit simultaneously in the same frequency channel by assigning each user a unique pseudorandom codeword. The receiver is set to detect only the desired codeword, and all other codewords appear as noise.

Another technique of interest for expanding the number of users is orthogonal frequency division multiplexing (OFDM). OFDM is not strictly a modulation technique, because modulation is added to each of its carriers; and it is not strictly a spectrum-spreading technique, because it is a combination of narrowband channels. OFDM uses a group of *n* closely spaced, orthogonal carrier frequencies, each of which carries 1/*n* of the total bits in a message. In FHSS, the carrier hops to each of these frequencies one at a time; in OFDM, all carriers are used simultaneously. OFDM systems adapt to the channel by avoiding the specific frequencies that exhibit a BER.

Geographically distributed APs allow wireless devices to communicate with other parts of the network, both wireless and wired. The topology of the wireless network is usually determined by the capabilities of the network components. Figure 2.2 shows common topologies for wireless networks. The most common wireless network topology is the star cluster, where the AP is at the center of the wireless devices and all of the devices communicate only with the AP. The AP then communicates with the wired network. Two other wireless network topologies are the tree and the mesh. In the tree topology, each wireless device is assigned to a specific AP, and that AP is connected to another AP closer to the wired network. This setup, presented graphically, looks similar to branches on a tree. In the mesh topology, each wireless device is both an end device and a network forwarding component and is responsible for forwarding any network transmissions not intended for itself to other wireless devices in transmission range. This wireless device is essentially a network router, and the mesh network is inherently redundant and self-healing. The star and mesh topologies appear to be best suited for industrial applications.

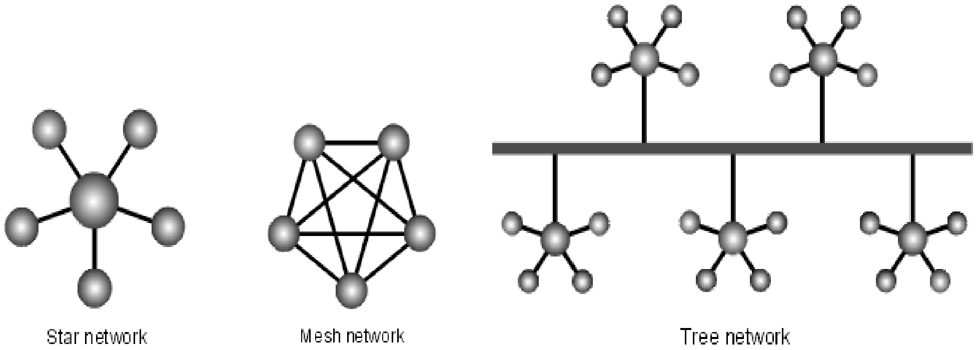

Figure 2.2. Wireless network topologies.

2.3 Components of a Network

Several types of components (e.g., servers with bridges, wireless LAN cards, gateways, routers, sensors, and actuators) can be used in setting up a network infrastructure for an industrial application. Figure 2.3 shows some representative components for a diverse network that includes wireless and wired components. These components provide generic data access, sensor-specific communications, and asset visibility.[4] Radio frequency identification (RFID) equipment is also included in the figure, showing operations at the levels of pallet, container, and individual item (commonly called "eaches," as shown in the figure).

2.4 Wireless Standards

Much of the success of wireless networks can be directly attributed to the successful development and adoption of the Institute of Electrical and Electronics Engineers (IEEE) 802 standards. Wireless LANs are covered by the IEEE 802.11 series of standards. These are typically called the Wireless Fidelity (WiFi) standards. Wireless PANs are covered by the IEEE 802.15 series of standards and include the Zigbee and Bluetooth technologies. IEEE 802.16 discusses the development of wireless MANs and incorporates broadband wireless access technology, typically referred to as Worldwide Interoperability for Microwave Access (WiMAX). Figure 2.4 illustrates the relationship of the IEEE 802 wireless standards and their associated technologies. Table 2.1 summarizes the characteristics of the standards. These include the modulation/multiplexing technique, frequency of operation, size, and data rate. Overviews of the individual standards are provided below.

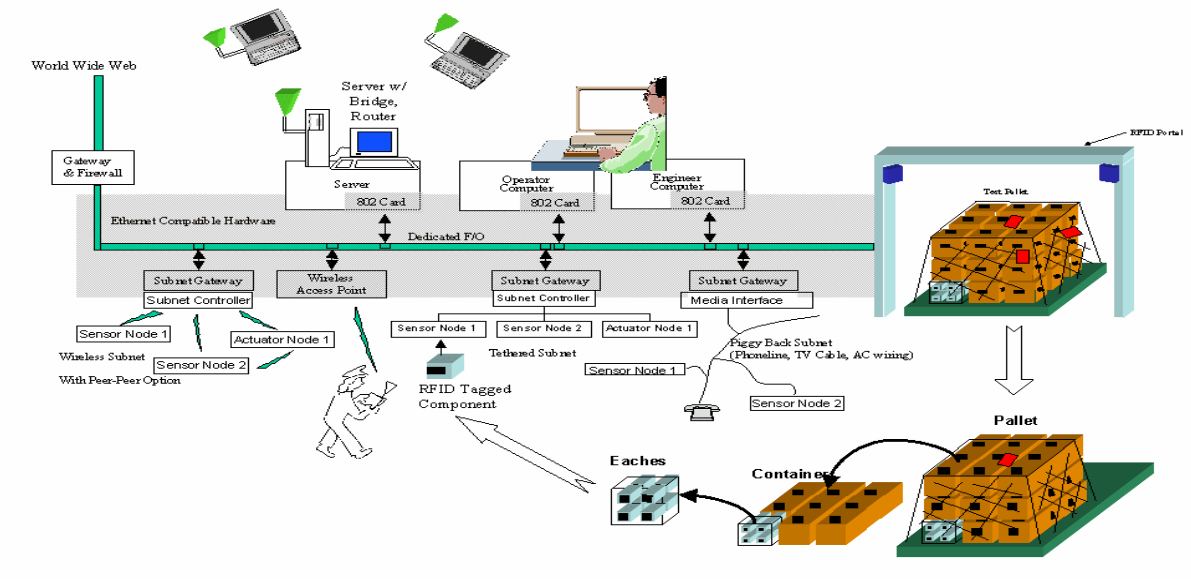

Figure 2.3. Components of a diverse network.

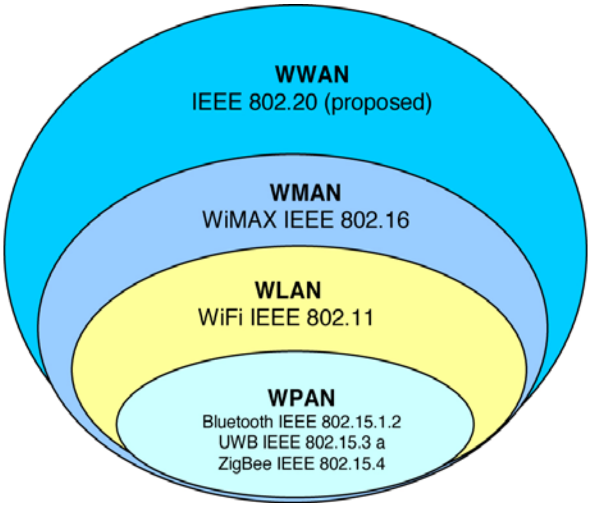

Figure 2.4. Network layouts and applications.

Table 2.1 Overview of wireless standards

Standard	OFDM	FHSS	DSSS	GHz	Size	Range	Maximum Mb/s
802.15		x		2.45	PAN	10s of meters	0.7
802.16b	x			5	MAN	kilometers	54
802.11		x	x	2.45	LAN	100s of meters	1, 2
802.11a	x			5	LAN	100s of meters	54
802.11b		x	x	2.45	LAN	100s of meters	11
802.11g	x		x	2.45	LAN	100s of meters	54

In keeping with the growth of the field, new wireless standards are under development. IEEE 802.15.3 is a wireless PAN standard incorporating ultra-wideband technology for streamlining video over short distances and is also known as the Wireless Media (Wi-Media) standard. The recently formed IEEE 802.20 working group is tasked with developing standards for mobile broadband wireless systems designed to be used in wireless wide area networks (WANs) covering hundreds of kilometers. Emerging developments in wireless standards are discussed in Sect. 3.

2.4.1 Wireless LANs – WiFi

It is becoming harder to find a place where wireless Internet access is unavailable. The surge in laptop computers and personal data assistants (PDAs) has prompted the need for wireless APs to the Internet. The rise of wireless LAN deployments has largely been due to the work of the IEEE 802 subcommittee responsible for the family of 802.11 standards. These standards are typically referred to as the WiFi standards and are supported by the WiFi Alliance (www.wi-fi.org). The motivation for this activity was to develop a "wireless Ethernet" to provide connectivity where wiring was inadequate to support the high data rates of wired Ethernet LANs.

The International Organization for Standardization (ISO) Open Systems Interconnect (OSI) model and its seven layers are shown in Fig. 2.5. The standard OSI model is shown on the left, and the IEEE 802 interpretation of the seven layers is on the right. The original IEEE 802.11 standard was developed to address collision avoidance at the medium access control (MAC) layer so that devices could roam freely throughout a wireless LAN and appear to be stationary to the protocol layers above the MAC. The MAC protocol developed was carrier-sense multiple access with collision avoidance. Modulation and coding functions were part of the physical layer (PHY) and three PHYs were developed (DSSS, FHSS, and infrared), with each capable of operation at 1 and 2 Mb/s. The subcommittee realized that the data rate had to be higher to succeed in the marketplace, and work began to develop new protocols that could support higher data rates. The result was the development of three standards that have found prominence today: IEEE 802.11a[5], IEEE 802.11b[6], and IEEE 802.11g.[7] IEEE 802.11a and IEEE 802.11b are distinct protocols, and IEEE 802.11g is a fusion of the other two.

OSI	IEEE 802
Application	
Presentation	
Session	
Transport	
Network	
Data Link	Logical link control (LLC)
	Medium access control (MAC)
Physical	Physical (PHY)

Figure 2.5 Mapping of ISO OSI to IEEE 802.

<u>IEEE 802.11b</u>

The most prominent of the three IEEE 802.11 protocols is IEEE 802.11b, which has been successfully deployed in business offices, university buildings, and homes around the world. IEEE 802.11b expands on the original IEEE 802.11 data rates and can operate over four different data rates (1 Mb/s, 2 Mb/s, 5.5 Mb/s, and 11 Mb/s). All four data rates can be used in DSSS systems, while only the two slower data rates can be used in FHSS and infrared systems. It should be noted that the FHSS and infrared techniques have not been implemented in any commercially available products. The 1 Mb/s data rate is modulated with differential BPSK (DBPSK), and the 2 Mb/s data rate is modulated with differential QPSK (DQPSK). The modulation technique for the 5 Mb/s and 11 Mb/s data rates is called complementary code keying (CCK) and was implemented to make the data transmission more efficient and robust. The efficiency comes from the increase in data rate within the same signal bandwidth, and the robustness comes from the improved coding ability of having multiple sets of possible transmitted code words. An optional modulation technique for IEEE 802.11b is packet binary convolutional coding (PBCC), a technique developed to carry more data. The operating frequency of IEEE 802.11b devices is in the Industrial, Scientific, and Medical (ISM) band from 2.4 to 2.4835 GHz.

IEEE 802.11a

IEEE 802.11a offers a 5-fold increase in data rate over IEEE 802.11b and can support eight different data rates: 6, 9, 12, 18, 24, 36, 48, and 54 Mb/s. The standard rates are 6, 12, and 24 Mb/s. These rates are realized through the use of 52 different sub-carriers, as required by the OFDM system used by 802.11a. The sub-carriers are modulated using BPSK, QPSK, 16-QAM, or 64-QAM, depending on the desired data rate. To increase its output bit rate, IEEE 802.11a takes advantage of the 5-GHz Unlicensed National Information Infrastructure (UNII) band. Within the 5-GHz UNII band, IEEE 802.11a is subdivided into three different channels of 100 MHz each, resulting in a total of 300 MHz. The three channels for IEEE 802.11a are located in the lower UNII band (5.150 to 5.250 GHz), the middle UNII middle band (5.250 to 5.350 GHz), and the upper UNII band (5.725 to 5.825 GHz). An important reason for distinguishing the three channels over the UNII band is to specify a different transmission output power level for each channel. A maximum of 40 mW is allowed in the lower UNII band. This band is mainly for indoor use, where the lower power can be used because it does not have to span a long distance. The upper UNII band, which allows for a maximum output power of 800 mW, can be used outdoors where distances typically are greater than they would be indoors. The middle UNII band, which allows for a maximum output power of 200 mW, is typically used for in-between distances such as large industrial buildings or to span short distances between indoor and outdoor transceivers. It is not a requirement for IEEE 802.11a compliant devices to be able to transmit and receive in all of the three bands.

IEEE 802.11g

IEEE 802.11g stems from the need for higher data rates in the ISM band. IEEE 802.11g is the most recent standard and products have been appearing in the marketplace for the last couple of years. It is capable of maintaining IEEE 802.11a type data rates up to 54 Mb/s. It is essentially another version of 802.11a simply placed in the ISM band, with a few slight differences. IEEE 802.11a uses 300 MHz of bandwidth in the 5-GHz UNII band, and IEEE 802.11b occupies 300 MHz of bandwidth in the ISM band. It appears to be a feasible task to translate one to the other. The IEEE 802.11g protocol specifically does this by incorporating the same OFDM carrier modulation as IEEE 802.11a and, in turn, obtaining the same data rates. One difference that IEEE 802.11g must account for is that it must also be backward- compatible with 802.11b devices, meaning that it must be able to operate at the same data rates as IEEE 802.11b, using the same modulation schemes. This restriction was put in place so that existing IEEE 802.11b networks, mainly wireless devices placed in laptops and PDAs, would still operate in the new IEEE 802.11g environment. This alleviates the problem of having to switch from one protocol to the other and allows network routers within a building to be switched to IEEE 802.11g, while the devices connected through the wireless network could be operated using either of the two protocols. As time goes by, the old 802.11b devices are expected to be replaced with the newer and faster 802.11g devices.

2.4.2 Wireless PANs

The growth and success of wireless PANs is due to the market availability of small and inexpensive personal devices. These devices include cell phones, PDAs, personal music players, digital cameras, and wireless instrumentation. The leading wireless PAN standards are IEEE 802.15.4[8] (Zigbee) and IEEE 802.15.1[9] (Bluetooth).

Zigbee – IEEE 802.15.4

Zigbee is a collection of major corporations, the most significant being Ember, Freescale, Honeywell, Invensys, Mitsubishi, Motorola, Philips, and Samsung. All are committed to standardizing cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard. This basically means that these companies are looking for a protocol that does not use a large amount of bandwidth and is not very complex, because both of those factors lead to higher costs and higher power consumption. Since its inception, more than a hundred companies have joined the Zigbee Alliance (www.zigbee.org) to support the development of IEEE 802.15.4.

IEEE 802.15.4 targets applications that do not need high data speeds and do not share large amounts of data. In return, Zigbee devices do not consume large amounts of power. To keep power consumption to a minimum, the devices enter a sleep mode when they are not sending data, consuming almost no power. Zigbee devices spend much of the time in sleep mode, only waking to send the value of the current state at a given time. Most Zigbee applications will typically fall within the 10-m range, although in some applications the range can exceed 70 m. For a larger coverage area, a higher transmitted power is required, causing the device to draw more energy from the battery. One technique Zigbee uses to get around the distance dilemma is to relay information between devices until it reaches the desired device.

Zigbee devices incorporate DSSS with O-QPSK modulation to help make them more robust and less susceptible to interference. Zigbee devices operate in the 2.4-GHz band, using the frequencies 2.405 to 2.480 GHz subdivided into 16 different channels, each with an equal spacing of 5 MHz. Allocating the available bandwidth in this fashion allows for a signal quality improvement due to less interference because, while the channel has an available bandwidth of 5 MHz, the signal only occupies a spectrum of 2 MHz. This also allows for the implementation of more channels if the need ever arises. Zigbee devices have a bit rate of 250 kb/s.

Bluetooth – IEEE 802.15.1

IEEE 802.15.1, also known as Bluetooth, is a technology that was developed by the Swedish company L.M. Ericsson for short-range cable replacement.[*] The history of Bluetooth is similar to that of Zigbee. Four years after its inception by Ericsson, a consortium of companies with similar needs got together and decided to generate a new and universal mode for which data transfer could be accomplished without the need for wires and without sacrificing the speed of the transfer. The consortium of companies, including Ericsson, IBM, Intel, Nokia, and Toshiba, formed what is known as the Bluetooth Special Interest Group (www.bluetooth.org). Their goal was a short-range, low-power wireless protocol. These companies wanted to promote products that could interact with products from different companies, hence the need for one basic standard that could be a model for all of the corporations to abide by. The cornerstone for

[*] The name comes from a chapter of Scandinavian history during the 10th century when Denmark was ruled by King Harald Blatand, which when translated into English means Harold Bluetooth. Harald Blatand is known for bringing peace to the area now formed by Norway, Sweden, and Denmark. In much the same way that Blatand united the different cultures during that time, Bluetooth is used to bridge the differences among various devices so that better communication between them is possible.

Bluetooth-compliant devices to date has been their ability to communicate with the personal computer (PC). This ability opens Bluetooth to a vast array of potential customers, since owning a PC has become a staple of both business and personal lifestyles and consumers are demanding that more and more products associated with their computers be wireless. These products include keyboards, mice, printers, and devices that can be used in conjunction with computers, such as PDAs and cell phones.

Bluetooth is a simple cable replacement protocol. Rather than sending data through a wire, the medium that is used is free space, removing the inconvenience of wires running in all directions. Bluetooth has a data rate of 1 Mb/s and uses an FHSS technique. Rather than spreading the entire signal over a portion of the allotted frequency band, Bluetooth keeps the same narrowband signal and simply changes the carrier frequency of the transmitted signal, thus hopping from one frequency range to another. This hopping fashion decreases the likelihood that an interferer will be located on several hop sequences in a row. Bluetooth incorporates a special modulation scheme, Gaussian frequency shift keying (GFSK), and operates in the 2.4-GHz unlicensed ISM frequency band. Bluetooth uses 79 MHz of the 83.5 MHz bandwidth available. This allows for 79 channels that are 1 MHz wide, corresponding to the data rate of 1 Mb/s. The timing within a Bluetooth network is critical because the protocol follows a TDMA access system, and devices are given certain time increments in which to send data.

When two or more Bluetooth devices are trying to communicate with each other, a piconet is created. A piconet consists of a master device and its accompanying slave devices. There is nothing about a device that makes it either a master or a slave. All devices are built equally, and being a master only depends on who initiates the contact. A piconet can contain up to 255 devices, although at a given time only 8 can be active—1 master with 7 slaves. When several piconets are located within the same area, and some devices belong to several piconets, a scatternet evolves. Within a scatternet, masters and slaves can belong to different piconets. A master in one piconet can be a slave in another, and vice versa. A slave in one piconet can be a master in another, but a master of one piconet cannot be a master of a different piconet; otherwise, it would just be considered one big piconet. This is because the timing and hopping sequence is controlled off the master clock.

2.4.3 Wireless MANs

The proliferation of commercial hotspots and obscure wireless LANs based on IEEE 802.11 standards is driving the demand for broadband connectivity back to the Internet. The term “broadband” simply means that the wireless system is capable of delivering significant bandwidth (i.e., having a transmission rate greater than 1.5 Mb/s).[10] The wireless MAN is a fixed wireless access system designed to provide the desired last-mile broadband access. Wireless MANs are advantageous in areas that are hard for wired infrastructure to reach or where high installation costs make it prohibitive. The IEEE 802.16 standards are intended to offer wireless broadband technology for the long-range connection back to the service provider. They are also known as WiMAX standards and are supported by the WiMAX Forum, an industry-led, nonprofit corporation formed to promote the compatibility and interoperability of broadband wireless products (www.wimaxforum.org).

IEEE 802.16 technology provides speeds comparable to wired systems, like cable and digital subscriber line (DSL) links. End users can connect it to their internal wired Ethernet or wireless LANs. The original IEEE 802.16 standard[11] addressed fixed line-of-sight (LOS) point-to-point transmissions in the 10 to 66 GHz frequency band using the CDMA signal format. The standard was amended and IEEE 802.16a[12] addressed fixed non-line-of-sight (NLOS) point-to-multipoint transmissions in the 2 to 11 GHz band using the OFDM signal format. IEEE 802.16a has since been improved a number of times and now includes portable applications and another signal format, orthogonal frequency division multiple access (OFDMA). OFDM supplies each user with its own frequency range (sub-carrier), while OFDMA assigns multiple sub-carriers to different users, allowing greater spectral efficiency. All of the revisions to IEEE

802.16a have been redrafted into IEEE 802.16d.[13] To address mobile applications, the IEEE 802.16 working group developed IEEE 802.16e.[14] This standard covers NLOS point-to-multipoint transmissions in the 2 to 6 GHz band. A summary of the IEEE 802.16 standards is shown in Table 2.2.

Table 2.2 IEEE 802.16 series of standards

Standard	**802.16**	**802.16a / 802.16d**	**802.16e**
Completed	Dec 2001	802.16a: Jan 2003 802.16d: Sep 2004	Dec 2005
Spectrum	10 to 66 GHz	2 to 11 GHz	2 to 6 GHz
Channel conditions	LOS	NLOS	NLOS
Maximum data rate	134 Mb/s (28 MHz channel)	75 Mb/s (20 MHz channel)	75 Mb/s (20 MHz channel)
Modulation	QPSK, 16-QAM, 64-QAM	OFDM, OFDMA, QPSK, 16-QAM, 64-QAM, BPSK	Same as 802.16d
Mobility	Fixed	Fixed and portable	Mobile and roaming
Channel bandwidths	20, 25, and 28 MHz	Scalable 1.5 to 20 MHz	Same as 802.16d
Typical cell radius	1 to 3 miles	3 to 5 miles	1 to 3 miles

(Source: WiMAX.com)

2.5 Related Wireless Activities

In a related wireless activity, there is an IEEE 1451[15] working group developing a wireless interface standard for sensors, IEEE 1451.5. Wireless technology that has the potential to transform operations in industrial environments is RFID tagging, though the standardization process is lagging deployment. RFID devices can be attached to just about anything and can be used for a variety of applications from inventory control to access management.

Intentionally Left Blank

3. EMERGING TECHNOLOGIES

Wireless technology has advanced rapidly in the past few years and the rapid pace is expected to continue. Hence, if the focus of this report were entirely on what is available today, some significant insights might be overlooked. Technological advancements that are likely to show up in the marketplace in the next 5 years are identified and discussed in this section. These technologies very well may make an impact on nuclear facilities in the future.

3.1 Ultra-Wideband Technology for Short Distance Communications

Ultra-wideband (UWB) technology has recently been endorsed by the Federal Communications Commission (FCC) for communications applications. It had previously been restricted to specialty applications, mostly involving ground-penetrating radar and vehicle proximity detection. In particular, UWB has been useful for the precise measurement of distances, determining precise locations, device tracking, and obtaining the images of hidden objects. The recent ruling means that the electromagnetic environment of the future will also have to take into account the potential utility of UWB communication and the possibility of its interference with other systems. IEEE 802.15.3[16] is a recently issued wireless PAN standard taking advantage of the FCC ruling and incorporating UWB technology for streamlining video over short distances. IEEE 802.15.3 is also known as the Wi-Media standard.

In general, UWB systems emit very short pulses of radio frequency (RF) or microwave energy, much like a radar pulse. UWB systems may use time, phase, or amplitude modulation to convey information at high speeds. The modulated UWB signal may be several gigahertz wide and consequently provides significant processing gain. UWB devices must operate in the frequency band 3.1–10.6 GHz and must be designed to ensure that operation occurs indoors or must consist of hand-held devices used in a peer-to-peer mode. The speed of UWB devices can vary, with a high speed of 55 Mb/s. UWB technology is targeted for high throughput applications like multimedia devices.

3.2 Mobile Broadband Wireless Access for Wide Area Communications

The recently formed IEEE 802.20 working group is developing a standard for mobile broadband wireless access.[17] The standard is intended for use in WANs and is expected to be completed by 2006. The purpose of IEEE 802.20 is to develop the specification for an efficient packet-based free-space interface that is optimized for the transport of Internet protocol (IP)-based services. The goal is to enable worldwide deployment of affordable, ubiquitous, always-on, and interoperable multivendor mobile broadband wireless networks. IEEE 802.20 equipment will operate in the licensed bands below 3.5 GHz, with peak data rates per user in excess of 1 Mb/s. IEEE 802.20 supports vehicle speeds of up to 250 km/h in a WAN environment and targets spectral efficiencies, sustained user data rates, and numbers of active users that are significantly higher than existing mobile systems.

3.3 Voice-Over IP and IEEE 802.11e

Voice-over IP across the Internet is drawing much attention with discussion of the convergence of voice and wired data networks. Hospitals and businesses are already deploying voice-over IP to save cost on their telephone bills.[18] A natural extension to voice-over IP in the wired data network, of course, is voice-over IP in the wireless network, providing the added benefit of mobility. However, voice traffic is not very tolerant of delay and is also very intolerant of variations in delay (known as jitter). Therefore, quality of service (QoS) mechanisms are required on any network that hopes to satisfy user demands of voice traffic.

IEEE 802.11e is the IEEE 802.11 standards group's attempt to standardize key QoS characteristics over wireless networks. This standard answers some of the concerns that WiFi vendors have when considering voice-over IP over WiFi networks, such as bandwidth partitioning and jitter. It is expected that the vendors will support the IEEE 802.11e QoS parameters and make them available in their products.

3.4 Multiple Input–Multiple Output Technology

A fourth PHY for 802.11 networks is described in IEEE 802.11n and is expected to result in products that will be available in the marketplace in 2007. The foundation of this standard is multiple input–multiple output (MIMO) technology, and it is expected to maximize real data throughput to 100 Mb/s or more by using multiple antennas coupled with multiple transmitters/receivers. The basis of smart antenna technology is the use of an antenna array system that is aided by a signal processing system using array algorithms to improve wireless system performance. Some basic types of signal processing systems that can be found in smart antenna systems include beamforming, diversity combining, and space-time equalization.

Through beamforming, a high-gain antenna beam can be formed and pointed in the direction of the desired signal. Beamforming systems can be implemented in two ways: fixed beamforming or fully adaptive beamforming. A fixed system uses RF switches and antennas controlled by logic to select a particular beam. In adaptive beamforming, the antenna consists of array elements that are combined in an elaborate cluster of phase shifters and attenuators. The signal processing unit executes array algorithms to determine the gain for each array element, and the resulting adaptive antenna beam can be steered as necessary. With diversity combining, simple algorithms such as maximal ratio combining, equal gain combining, and selection diversity are developed to select an individual antenna from a set of available antennas. This is different from an array because these individual antennas are not combined, as with beamforming. Equalization, or space-time adaptive processing, can be used to remove the effects of frequency distortion and frequency selective fading and provide additional antenna gain. This scheme requires array processing at the transmitter and receiver. Spatial multiplexing of the array can enhance the data rate for a given bandwidth, and space-time coding can be used to combat fading.

MIMO technology can improve performance by using the spectrum efficiently without sacrificing reliability. It uses multiple spatially separated antennas to increase the data rate and improve data traffic. Each antenna carries a separate low-speed data stream, and multiple paths are used to send the streams simultaneously. The MIMO receiver uses mathematical algorithms to unravel and recover the transmitted signals that were combined during the wireless transmission. At the present time, the best ratio of complexity to performance has been achieved with three antennas.[19] Theoretically, there are no limits on the number of antennas that can be used. In the future, multiple antennas are expected to improve transmission and reception without requiring additional spectrum.

3.5 Spectrum and Power Management

IEEE 802.11h[20] has been recommended by the International Telecommunication Union to combat against interference to and from other RF devices. Military radar systems and medical devices are the primary concern. It uses spectrum and power management techniques to reduce the risk of interference. Though this standard is presently targeted at devices deployed in Europe, it hints at the type of control future wireless devices can be expected to possess.

3.6 Protected Access

IEEE 802.11i[21] was developed to ensure security in IEEE 802.11a, b, and g wireless LANs. The standard provides improved encryption algorithms based on the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES). WiFi Protected Access 2 (WPA2) products are based on the IEEE 802.11i standard and are eligible for Federal Information Processing Standard (FIPS) 140-2 compliance. FIPS 140-2 was developed by the National Institute of Standards and Technology (NIST) and describes the federal requirements for information technology (IT) products for sensitive but unclassified use. It includes not only encryption, but also authentication, key management, and physical security (tamper resistance). WPA2 replaces WiFi Protected Access (WPA), a short-lived security attempt based on the RC4 encryption algorithm that did not hold up to the scrutiny of the security community.

3.7 Cognitive Radio

Cognitive radio is a term coined by Joseph Mitola in the late 1990s when he visualized cognition running in the application layer of networks.[22] The cognitive radio is programmed to handle unanticipated radio channels and events. Cognitive radios can sense RF spectrum, geographical surroundings, and the user's needs. They have the capacity to learn in both supervised and unsupervised modes and the ability to adapt within any layer of the communication system to optimize performance, enhance spectrum usage, and further advance wireless ubiquity. Cognitive radios can maintain a high QoS and reduce interference to neighboring radios.

Cognitive radio is based on a software-defined radio platform and includes spectrum analysis and network protocol synthesis capabilities. It gains adaptability through the use of a policy engine and applicable policy databases. Also, intelligent agents can be used to locate and plug in software interfaces where necessary to add important services. At the present time, cognitive radio is still in the laboratory development stage. A few groups, including ORNL, are in the process of building cognitive radios based on genetic algorithms and game theory. The Software Radio Forum is active with discussions on this topic (www.sdrforum.org).

Intentionally Left Blank

4. TECHNOLOGY DIFFERENTIATORS

Deployment of wireless technologies within a nuclear facility should be based on needs that have been balanced with the risks and costs. Designers and decision makers can, and should, step through a decision process to determine the proper technology to deploy and the best system design utilizing that technology. System designers should view systems globally and not treat the wireless portion as a separate system. For example, wireless technologies that connect to another system can often be modified at the connecting interface to increase functionality and security. In deciding what kinds of wireless equipment should be used in a nuclear facility, it is necessary to understand the different technological issues, the different types of implementations, and the pros and cons of each. In many cases, it is necessary to make tradeoff decisions to come up with a system that is balanced overall. Though in a commercial turnkey system the vendor has stepped through the process and made the majority of the decisions, the implementer (and to some degree the user) also needs to understand the issues to deploy and use the system in an effective and efficient manner. The following technology differentiators are among those that should be considered:

- open standards vs proprietary products,
- unlicensed vs licensed frequencies,
- frequency vs propagation,
- network size and throughput vs range,
- focused antenna vs omnidirectional,
- modulation and coding techniques,
- power considerations, and
- network topologies and media access control.

These technology differentiators are useful for evaluating the deployment of existing products into a new nuclear facility system. They are also useful for following and evaluating technologies that are expected to emerge in the future.

4.1 Open Standards vs Proprietary Products

The issue of open standards vs proprietary products may not be entirely obvious. Standards-based products may be more readily available in the marketplace; and after reaching a sizeable market, they are generally easy to acquire and often are inexpensive. However, this same availability may be a possible cause for concern. The standardization of wireless LAN protocols is a case in point. IEEE 802.11b is based on spread-spectrum technology that was originally developed for use in military systems for its low probability of detection. One would therefore think that IEEE 802.11b networks are inherently secure, which is not the case. IEEE 802.11 networks have flaws in their designs that have actually been exploited by hackers. It is even possible that the availability of technical details in published standards has contributed to this exploitation. For example, details about IEEE 802.11 key management in the standards cite how the standardized wireless equivalency privacy (WEP) encryption algorithm splits the per-packet key (also called a seed) into an initialization vector and an encryption key. The initialization vector changes for each new packet, but the encryption key remains the same. This flaw was first published by Lariat[23] and has since been thoroughly exploited.

Other factors that have contributed to the exploitation of IEEE 802.11 are readily available hardware and close proximity to signals. In a typical metropolitan environment, hackers can sit across the street with an inexpensive network interface card and a homemade (e.g., a Pringles^{TM} can) antenna and hack a network. This has opened up an entirely new hacking community, one with a large "workforce" that includes many teenagers. Information on the results of hacking efforts has been widely shared and perfected to the point that the hacking can even be automated and accomplished while driving an automobile down the street, leading to the creation of the term "war driving." The outcome is that marketing tradeoffs supporting ubiquitous deployment, low cost, high throughput, and ease of use have caused implementation weaknesses that are causing users to unjustly label all wireless technology as "risky."

Proprietary products, on the other hand, are not likely to be as available for would-be hackers to study for vulnerabilities; nor are hardware components that can be used in hacking activities as likely to be available (at least not on a massive scale). Hackers would require inside access to either the vendor of the products or the facility using the products, or both. This does not imply that proprietary products are always designed to be more secure or are immune to design flaws that make them vulnerable. This is clearly not the case because proprietary products have been hacked, and "security by obscurity" is no security at all. Perhaps the issue can be summarized as the relationship between the size of the potential hacking community and the ease of access to the technical details and to hardware. In addition, a key component may be whether the threat is teenagers with too much time on their hands or a determined adversary.

It should be pointed out that it does not matter whether the standard is set by a standardization body, such as IEEE, or is a de facto standard determined by market share, such as is the case with Microsoft products. The fact that Microsoft Windows is a proprietary product has not protected it from the hacking community. One could argue that the large hacking community that subjects open-standard systems to exploitation results in better products in the long run. As designers develop systems intended to operate in the open-standards environment, they should be aware of the threat and strive to develop hack-proof systems at the outset.

Proprietary products are generally much more expensive because of the lack of direct competition and the fact that the large community base does not exist to drive costs down. In addition, once a decision to deploy a proprietary system is made, that decision can become a long-term commitment because upgrades and improvements must be compatible, which means a return order for the chosen vendor. As already stated, there may also be a false sense of security in using uniquely deployed proprietary products. The development of flawed systems is not tied to a standards process, and it is possible that a proprietary system that is poorly designed will be deployed without the large hacking community to pick apart its flaws. Suppliers of proprietary products, by their nature, do not publicize flaws in their designs or security incidences, except perhaps to their own customer base. Their customers, likewise, have no incentive to publicize their own vulnerabilities. Therefore, the same pressures that might cause people to panic over standards-based systems and over-report, might cause problems with proprietary systems to be under-reported. Those systems, therefore, appear superior. It should be noted that the IEEE 802.11 standards are constantly being upgraded to try to alleviate any potential security threats.

4.2 Licensed vs Unlicensed Frequencies

There have been a large number of new wireless products and standards recently that focus on use of the ISM frequency bands. These bands are convenient because they do not require licensing by the FCC. This simple fact has a tendency to boost the marketability of products and make them attractive to individuals and organizations. This has had a significant impact on reducing the prices of these products; and reduced prices have led to an increase in use, which in turn has led to new and improved products. The lack of a user license does not eliminate the need for FCC type-acceptance nor imply a lack of rules and guidelines pertaining to spectrum use and emissions. Power levels, modulation types, and bandwidth limits are all

tightly controlled by the FCC. However, individual users do not need to be concerned with these issues when purchasing a commercial product; the vendor ensures they are properly addressed.
The downside to ISM bands is the fact that they are contention-use bands, where each user is competing for the same frequencies as his neighbors. Also, should there be an existing licensed use of these frequencies that is non-ISM, the ISM use must yield to the other use without causing interference. An example of this is satellite downlinks; an ISM application that interferes with licensed satellite use must be discontinued. Another downside to ISM band use is that there are strict limitations on modulation and power levels for ISM systems; by default, the range of devices using ISM bands is limited. It is also important to note that in most countries around the globe, use of unlicensed devices is permitted in portions of the 2.4 GHz ISM band. This fact has led to international marketing of products in this band and ultimately to their wide use and acceptance.

Licensed frequencies, on the other hand, allow guaranteed use of the frequency for a specific location, power level, and antenna gain. Licensed frequencies must hold to very stringent requirements on frequencies, modulation, and power levels, although in some cases these are quite generous. Some frequencies have been auctioned off by the FCC; therefore, their use comes at some cost to the user. To date, these auctions have focused on common carrier systems (systems where service is sold to end users for a fee, such as cell phone service).

Because licensed bands are not a free-for-all similar to ISM bands, and licensed users in the United States are protected by the FCC, one might assume that interference in these bands is nonexistent. This, of course, is not the case. Though the FCC is empowered to take action against interferers and levy stiff fines, there is no guarantee that it will. In some ways, licensed bands could be compared to speed limits—having them does not guarantee they will not be broken, though it does provide the option of prosecution.

4.3 Frequency vs Propagation

The issues of radio wave propagation are complex.[24–26] Nonetheless, it is important to have at least a feel for the magnitude of the issues as they pertain to nuclear facilities. Even though this discussion will be kept as simple as possible, using two-dimensional models, it is important to remember that radio waves are three dimensional and change constantly with time.

In a radio link, the mechanisms behind electromagnetic wave propagation can generally be attributed to reflection (which for the sake of our discussion will include refraction), diffraction, absorption and scattering. Reflection occurs when an electromagnetic wave impinges upon an object that has very large dimensions compared with the wavelength of the propagating wave. Reflections occur from the surface of the earth, buildings, walls, and other objects in the propagation path. The reflected wave can be characterized by the angle of incidence and polarization of the wave, along with the electrical properties of the media and reflecting surface. Figure 4.1(a) provides an overview of a wave reflected off the ground. A LOS path is shown for a wave propagating between a transmitter (Tx) and a receiver (Rx). E_i and E_r are the incident and reflected electric fields, respectively, while θ_I is the angle of incidence and θ_r is the angle of reflection. Refraction is the portion of the wave that is not reflected but passed through the reflecting surface.

Diffraction occurs when the radio path between the transmitter and receiver is obstructed by a surface that has sharp edges. Knife edge diffraction is the case commonly used for illustrating the phenomenon of diffraction and is depicted in Fig. 4.1(b). The result is perceived as a bending of the signal path, which contributes to NLOS transmission.

Scattering occurs when the objects that the wave encounters are small compared with the wavelength. Scattering may cause the wave energy to spread and distort the signal. Street signs, foliage, lamp posts, or small objects in the propagation path all cause scattering because the surfaces of these objects may look small or rough compared with the wavelength. Relative surface roughness can be assessed by a critical height factor used to determine whether the surface looks rough to the wave. The critical height (h_c) of surface protrusions is defined as

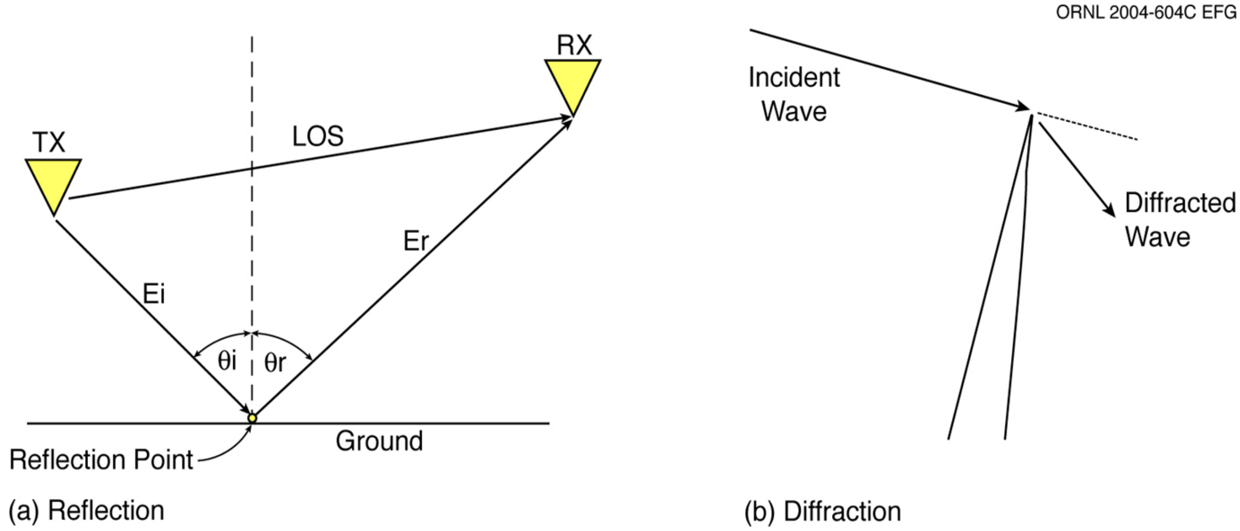

Figure 4.1. Reflection and diffraction.

$$h_c = \frac{\lambda}{8\cos\theta_i}, \qquad \text{(Eq. 4-1)}$$

where λ is the wavelength and θ_i is the incident angle of the wave on the surface. Peak-to-peak height (h) is defined as the minimum to maximum surface protrusion. A surface is considered rough if $h > h_c$, i.e., higher than the critical height.

In considering propagation in the radio link, LOS is an important concept to understand. LOS in radio propagation is usually defined by being obstruction-free within the first Fresnel zone. Fresnel zones represent successive concentric regions between the transmitter and the receiver where secondary waves are nλ/2 times greater than the LOS path. The Fresnel zones will have path lengths of λ/2, λ, 3λ/2, etc., corresponding to n=1, 2, 3, etc. The first Fresnel zone encloses all radio paths for which the additional path length does not exceed λ/2. Figure 4.2 shows the LOS within the first Fresnel zone radio link.

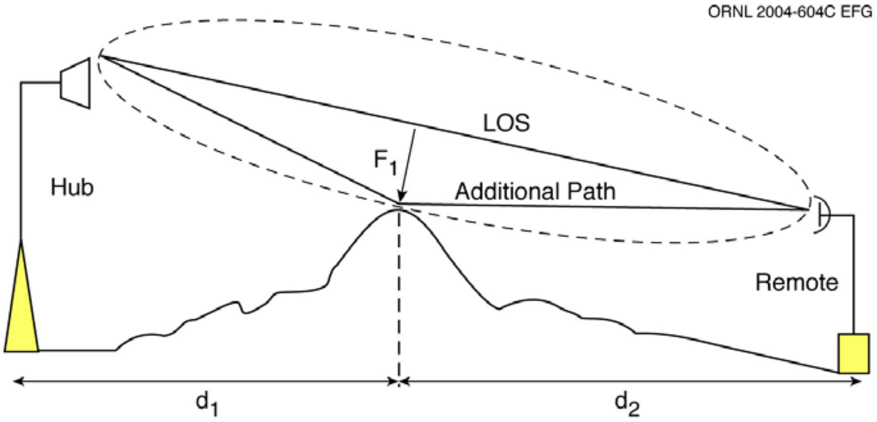

Figure 4.2. The first Fresnel zone.

The first-order Fresnel zone radius can be expressed as

$$F_1 = 17.3\sqrt{\frac{d_1 d_2}{f(d_1 + d_2)}}\ , \qquad \text{(Eq. 4-2)}$$

where F_1 is the ellipse radius (in meters) of the three-dimensional first Fresnel zone, *f* is frequency (in GHz), and d_1 and d_2 are distances (in kilometers) from the transmitter and receiver to the obstructive object. Other Fresnel zones can be computed from the first Fresnel zone using

$$F_n = F_1\sqrt{n}\ , \qquad \text{(Eq. 4-3)}$$

where *n* is the number of the Fresnel zone of interest. Reflections coincident with odd-numbered Fresnel zones result in a received signal that is out of phase with the original. Reflections coincident with even-numbered Fresnel zones result in a received signal that is in phase with the original.

In areas where LOS does not exist, radio paths are called shadowed (or obstructed). Shadowing is caused by vegetation, buildings, or other objects blocking the path between the transmitter and the receiver. Shadowing may cause radio waves going from the transmitter site to the receiver site to bounce (reflect) off multiple surfaces and arrive at the intended receiver at delayed times. The result is known as "multipath." Multipath can also occur with LOS if objects that are nearby and not in the direct path produce reflections that are also captured by the receiver.

Multipath is another frequency versus propagation issue. When higher frequencies see more reflecting surfaces than lower frequencies, multipath becomes a bigger issue for higher frequencies. Multipath causes delayed versions of the desired signal to arrive at the receiver dispersed in time. When the delayed signal arrives at a delayed time less than the chip time (the period of a code clock), it appears as noise and causes degradation. When it arrives at a delayed time greater than the chip time, it can actually help by giving the receiver an alternate signal should the first arrive with insufficient signal strength.

At lower frequencies, diffraction aids in transmission of the radio signal into shadowed areas. However, at higher frequencies, the area of shadow with the diffracted signal is so small that it becomes useless. Current commercial practices call for LOS for higher frequencies and define 10 GHz as the nominal breakpoint for NLOS communications. For frequencies lower than 10 GHz, NLOS is possible. However, for frequencies above 10 GHz, LOS is required. If a suitable LOS path cannot be found, the deployment for high-frequency radio links is problematic. To overcome this problem, some researchers have suggested that reflectors be placed in the propagation path so a reflected signal can be used in lieu of LOS.[27, 28]

To avoid propagation problems in planning wireless communication systems for nuclear facilities, computer simulations can be used to determine the best placement for transmitters and receivers. These simulations are available for both indoor and outdoor environments and should be considered. Software products such as Wireless Insite^{TM} by Remcom (www.remcom.com) and SitePlanner^{TM} by Wireless Valley (www.wirelessvalley.com) allow engineers to do this kind of simulation relatively efficiently.

4.4 Network Size and Throughput vs Range

Four critical performance parameters can be used to characterize communication network performance from the user's perspective: throughput, latency, reliability, and security. Throughput measures the amount of user information that can be sent through the communication network continuously and is typically expressed as kb/s or Mb/s. It can be expressed as a maximum, minimum, and/or nominal value for the network. Throughput should be specified from the end user perspective and not from the raw bit rate perspective. The protocol overhead should be accounted for in this parameter. Any repeated transmissions due to errors must be accounted for as well. A critical design parameter is trading off the BER and forward error correction (FEC) with throughput, because uncorrected errors in a packet will trigger retransmission of the entire packet and thus impact realizable throughput.

Latency is a measure of the time that elapses from the issuance of the request until the requested operation is performed. It can be expressed as a minimum, maximum, and/or nominal value. The units are usually seconds or microseconds. For example, a command to close a breaker sent to the field from an arbitrary remote site requires a finite amount of time before the breaker actually closes. Note that the communication required for confirmation of the action is included in the measure of the latency; and in the example cited, the latency includes not only the communication system latency but also the control system latency.

Reliability is a measure of the mean-time-between-failure (MTBF) for the communication network. This is the time (seconds or years) that can be expected between communication failures. A failure is defined as a communication sent that fails to arrive or fails to arrive within specified latency, throughput, or security constraints. MTBF takes into account any failures caused by hardware or software malfunction, unavailability due to downtime for maintenance (e.g., battery replacement), or downtime required to reconfigure the communication network as new nodes are added or removed. It is simply a measure of the likelihood or MTBF that, if a command is issued to open a breaker at some arbitrary time, the breaker will actually respond within the timeframe allotted for the action.

Security measures the ability to protect against unauthorized access while providing authorized access without significant impact. This can be time based, probability based, or cost based. Measuring the cost of security is more than just the cost of procuring and installing the hardware and software. A critical cost parameter is the cost impact of the operation of the security system. The ideal security system would prevent all unauthorized access and permit all authorized access without any cost impact.

The basic measures of performance of a data communication system, from a communication systems engineer's perspective, also include BER. For a given design, it generally takes a certain level of energy to distinguish each data bit from the noise around it. It follows, then, that system design considerations for the length of the bit (data speed), the power output, the design of the antenna, the modulation technique, the length of the link, etc., all have impact on the range vs throughput metric.

Perhaps it is obvious that a physically large network (in terms of distance between nodes) requires higher power levels and/or more sensitive receivers and/or high-gain antennas. Hence, for a given receiver sensitivity, an increase in output power will allow an extended range. Likewise, an increase in antenna gain allows an extended range. Also, for a fixed power level, an increase in receiver sensitivity will allow an increase in range, assuming that the background noise level is acceptably low.

The free-space path loss between the transmitter and receiver, assuming there are no obstructions, can be expressed as a dimensionless parameter:

$$P_L = 20 \log \frac{\lambda}{4\pi\, d} \,, \qquad \text{(Eq. 4-4)}$$

where P_L is the path loss (in dB), λ is the wavelength (in meters), and d is the range (in meters). Since $\lambda/4\pi d<1$, P_L is a negative number because it is a logarithmic value. Thus, the longer the range is, the larger the attenuation. Path loss is also a consideration when selecting a transmission protocol for a particular application. The various protocols each have maximum ranges over which reliable transmission is not assured without appropriate compensatory measures (e.g., repeaters). Tables 2.1 and 2.2 showed the effective ranges of several transmission protocols. However, for nuclear facilities, the relationship between path loss and range defined by Eq. 4-4 does not consider other potential sources of interference and attenuation, such as motor control centers, switchgear, reactor containment buildings, etc., that would need to be analyzed prior to final implementation of a wireless system.

Figure 4.3 shows some typical ranges vs throughput for wireless LAN cards. Note that the FHSS unit and the unit from Siemens have fixed data-rate range combinations. In comparing these units, it is also informative to make note of the power consumption. All of the power consumption values listed apply during transmission. A typical node of this type can deliver 1 Mb/s over a range of 300 ft for a power consumption of about 1 to 2 W.

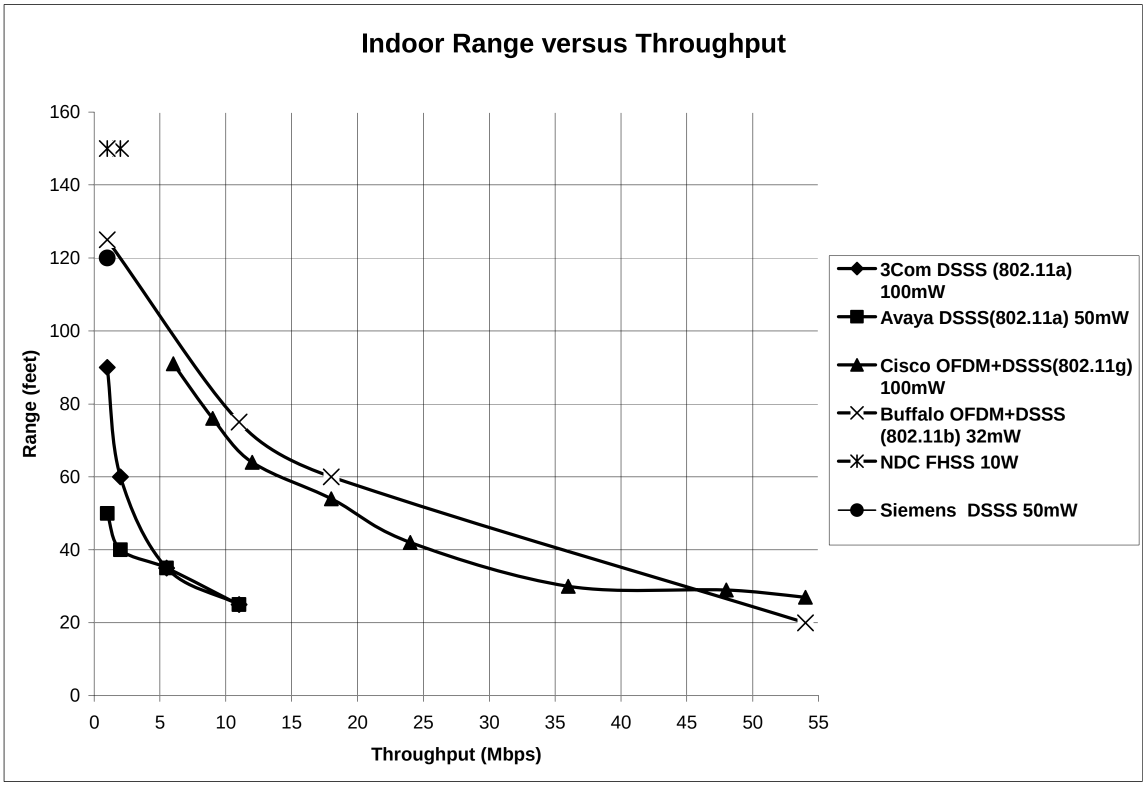

Figure 4.3. Graph of throughput vs range for different output powers.

Though the relationship between power and range is relatively clear, what is probably not as obvious is the effect of network protocols on network size and range. This discussion, of course, assumes that the network consists of more than two fixed-point nodes. For a multinode network to be effective, each node on the network must be able to use the wireless channel without interfering with other nodes. This is generally governed by the media access method. As the network grows in size, so does the probability that nodes on the network will be unable to maintain clear contact with all other nodes on the same network. In an IEEE 802.11 wireless LAN, an AP is typically used to reduce this problem. However, the media access method must resolve the issue of multiple nodes trying to communicate with the AP. These are nodes that communicate with the AP but not with each other because of distance and obstructions. They are known as “hidden nodes.” Two specific methods for dealing with this problem in the IEEE 802.11 standards are use of the network assignment variable (NAV) in distributed coordination function (DCF) mode or use of the point coordination function (PCF) mode. PCF is simply described as a central node controlling access to the channel by polling individual nodes in turn. NAV is essentially the use of a request to send/clear to send (RTS/CTS) method. This issue is important because in many IEEE 802.11 implementations, use of these methods, and adjustments to their parameters, are optional. For example, it is possible for some nodes on a network to adjust their RTS/CTS thresholds to improve their performance when the network is busy. However, this comes at the expense of other nodes on the network.

4.5 Focused vs Omnidirectional Antenna

A discussion of antenna pattern and therefore gain should follow the previous discussion of network size and range. A high-gain antenna at the receiver can significantly boost the received signal strength. A high-gain antenna on the transmitter can also result in a directed antenna pattern that must be aimed to line up the transmitter with the intended receiver. Directional high-gain antennas are very useful in a point-to-point stationary network where they do not move and are required only to communicate with one other node. However, in a multinode mobile network, the use of high-gain antennas is offset by the need for antenna pointing technology. As discussed in Sect. 3.4, research in smart antennas that follow the mobile node indicates that this technology is feasible.

In those cases where the use of directional antennas is possible, it should be considered. Use of directional antennas can reduce the amount of signal transmitted to areas outside the confines of the facility perimeter, where it would be available for interception by someone with bad intentions.

4.6 Modulation and Coding Techniques

How a signal is coded, modulated, and propagated determines (1) how efficiently it uses available bandwidth, (2) how it will tolerate noise and adjacent signals, and (3) in some systems, how many users can share the same bandwidth at the same time. In an industrial environment, it is important that the signal be tolerant of noise, yet not transmit more energy than necessary to avoid interfering with sensitive instruments.

A discussion of four types of modulation techniques was presented in Section 2.2: linear, constant envelope, combined linear and constant envelope, and spread spectrum. Linear techniques vary the amplitude of the transmitted signal linearly with the modulating signal. Constant envelope modulation techniques keep the amplitude of the carrier constant despite variations in the modulating signal. Combined linear and constant envelope techniques generate multiple carrier signals by varying both the envelope and phase. Many of the modulation techniques used in wireless systems are listed in Table 4.1.

Coding is used to either increase the amount of information that can be transmitted on the channel or increase the ability to accurately receive the information in the presence of errors. Numerous coding schemes are available, and they are applied to the baseband signal before modulation takes place.

Table 4.1 List of modulation types

Symbol	Modulation scheme
BPSK	Binary phase shift keying
CCK	Complementary code keying
DBPSK	Differential binary phase shift keying
DQPSK	Differential quadrature phase shift keying
DSSS	Direct sequence spread spectrum
FHSS	Frequency hopping spread spectrum
GFSK	Gaussian frequency shift keying
n-QAM	Quadrature amplitude modulation
O-QPSK	Offset quadrature phase shift keying
PBCC	Packet binary convolutional coding
QPSK	Quadrature phase shift keying

The selection of an appropriate spectrum spreading technology has a significant bearing on the planning of a wireless network. The spread-spectrum technique (DSSS, FHSS, or OFDM) serves the purpose of spreading the energy from the data transmission across the spectrum in the unlicensed frequency bands, so as not to cause interference with other devices or systems in the vicinity. DSSS and FHSS are spread-spectrum modulation techniques. DSSS spreads the transmitted signal by multiplying its data pulses with a PN sequence, while FHSS involves hopping a series of modulated data bursts over a sequence of carrier frequencies. On the other hand, OFDM is not strictly a modulation technique (because modulation is added to each of its carriers), and it is not strictly a spectrum-spreading technique (because it is a combination of narrowband channels). However, it is used to spread the data transmission and is part of the PHY for several wireless systems.

As shown in Fig. 4.4, DSSS (on the left) produces a more noise-like spectrum, while FHSS (on the right) produces narrow-band peaks. The picture on the right can also be used to illustrate the spectrum of OFDM. Note that seeing all of the narrow-band peaks of FHSS on one screen is a function of the spectrum analyzer display persistence, and only one peak is actually present at a given moment. However, for an OFDM signal, all peaks are present at the same time. OFDM uses a group of closely spaced (minimally spaced, orthogonal) carrier frequencies, each of which carries 1/*n* (where *n* is the number of carrier frequencies) of the total bits in a message, to simultaneously transmit multiple signals in parallel. The number of carrier frequencies will vary with the desired data rate. In FHSS, the carrier hops to each of these frequencies one at a time; in OFDM, all carriers are used simultaneously. The better OFDM systems adapt to the channel by avoiding the specific frequencies that exhibit a high BER.

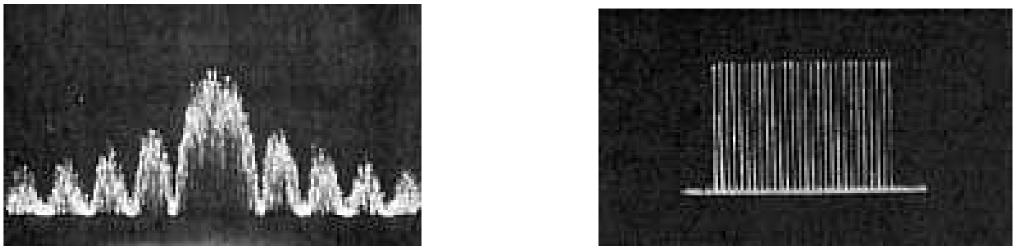

Figure 4.4. Spectrum analyzer outputs for DSSS and FHSS.

Because OFDM uses essentially all of the available frequencies (with minimum spacing) for all transmissions, it appears to have the best spectral efficiency (i.e., bits/s/Hz) of the three methods, particularly compared with typical implementations of FHSS and DSSS. This is particularly true in the case of adaptively modulated OFDM formats, like those employed in IEEE 802.11a protocols. Here, each OFDM carrier may be individually modulated via BPSK or *n*-QAM constellations (usually with *n* = 4, 16, 64, or 256), thus yielding even higher spectral efficiency figures when the link has a high signal-to-noise ratio. In general, DSSS has the second-best spectral efficiency, and FHSS is third. Another overall selection consideration is that under current ISM regulations, the FCC does not permit OFDM in the 915-MHz band; however, a possible change in this aspect of the ISM-band rules is presently under consideration.

Another way to describe spread-spectrum systems is “processing gain.” As stated, there are benefits in spreading the desired signal throughout the available spectrum. One of those benefits is immunity to noise (and interfering signals); the level of immunity is defined as processing gain. In DSSS systems, the processing gain can be expressed as

$$G_p = R_c/R \,, \qquad \text{(Eq. 4-5)}$$

where R is the bit rate, R_c is the chip rate, and a chip is the information transmitted during one clock interval. This can be expressed in decibels (dB) by using

$$G_{p(dB)} = 10 \log (R_c/R) \;. \qquad \text{(Eq. 4-6)}$$

For IEEE 802.11b DSSS systems, the signal is spread by using 11 chips per bit. The resulting processing gain is approximately 10 dB. Processing gain of an FHSS system depends on whether the system is a slow frequency hopping (SFH) or fast frequency hopping (FFH) system. An SFH system transmits multiple bits per chip (hop) and therefore does not provide any processing gain. The FFH system transmits several chips (hops) per bit and provides processing gain. Because OFDM does not spread the signal, there is no processing gain.

4.7 Power Considerations

Power consumption and type of input power are major concerns for mobile wireless networking systems; especially those that are to be used in remote locations and over extended periods of time. It should be clear that the RF output power level is proportional to the input power. Earlier, the connection was made between output power, range, and data rate. Therefore, range and data rate are limited by the input power.

Engineers have been trying to find ways to extend range, data rate, and battery life since mobile radio systems have been in use. Current technology has made great progress in this regard. However, the issue is still very much a concern. A comparison of the commercial offerings of IEEE 802.11 and IEEE 802.15.4 will be helpful. IEEE 802.11 provides a longer range and higher data rate but is generally intended to be used in devices that are attended or where line power is available. In fact, one way to increase the longevity of a laptop battery significantly is to disable the wireless interfaces when they are not in use. Also, the use of power over Ethernet became popular with the increase in IEEE 802.11 APs. This allows the use of APs in hard-to-reach places without requiring that a separate power line be run to those locations.

In contrast, IEEE 802.15.4 devices are intended to be used over the long term, unattended, and in remote locations. Coincident with these expectations, however, these devices are designed to have limited range (unless a mesh network is used) and data rate. Products are advertised to require a battery change only every 2 years. However, these devices are intended to spend most of their time in a dormant stage (sleeping) with their radio units turned off.

4.8 Network Topologies and Media Access Control

The basic topology of a network is one of the early design considerations that must be addressed. In a wired network, this includes options such as star, ring, bus, or mesh topologies. At the physical layer, these options essentially describe how the wires connect the nodes to each other. The majority of LAN deployments currently in industry are star networks in which each node connects directly to a network switch or hub.

In a single-channel wireless network—essentially all of which are shared bus topologies from a PHY layer perspective, since they share the same channel—topology issues focus on media access technologies. Access to the “bus” can be controlled in a contention-based manner (i.e., if the channel is idle, the user is allowed to transmit) as in carrier sense multiple access (CSMA) or scheduled as in a TDMA system. Access can also be controlled with polling, a token (i.e., a device’s right to access) being passed around, or a CDMA approach that allows users to transmit simultaneously. Multiple channels can be used, creating a FDMA network—two wireless networks that can be configured at the PHY layer to something other than a shared bus topology. The topology of the network and higher layers of the OSI model need not coincide directly with the PHY topology.

In addition to scheduling or contending for time on the channel, basic topology issues include whether or not repeaters are used. An IEEE 802.11 network that does not use repeaters or interconnection to a wired network is known as an “ad hoc network.” Range in an ad hoc network is typically limited to LOS between any two nodes in the network that must communicate. By definition, ad hoc means self-configured; i.e., no hardware links and no static entry routing tables.

In the mesh topology, as shown in Figure 2.2, each node operates in an ad hoc mode but also acts as a router and forwards traffic from its neighbors through the network. This approach extends the range of the network so that each node can exchange traffic with any other node, as long as there is a complete path between the two. This type of network is sometimes called a peer-to-peer network in industry.

Because the most popular wireless network nodes adhere to the IEEE 802.11 family of standards, it is worthwhile to discuss briefly the techniques that are covered by the standards. IEEE 802.11b, for example, specifies CSMA with collision avoidance (CSMA-CA) as its primary access control method. CSMA-CA is referred to as a *distributed coordination function* because control of the network is distributed to all nodes in the network. The specification also covers options for polling, which is a *point coordination function* because a single node coordinates access to the channel.

IEEE 802.11 also specifies ad hoc, basic service set, and extended service set networks. Basic and extended service-set networks are also referred to as infrastructure networks, and they utilize APs to connect the wireless users with the wired infrastructure. APs in an extended service set are interconnected via the wired distribution network.

5. RECENT WIRELESS DEPLOYMENTS IN NUCLEAR FACILITIES

5.1 General Application Areas in Current Nuclear Facilities

Because of the prevalence that wireless systems have gained in the marketplace in recent years, there have been some deployments in nuclear facilities. However, no applications were found where wireless systems are being used in safety-related systems.

Wireless systems for non-safety applications in nuclear facilities have been identified in the following areas:

- Communication infrastructure for mobile computing, consisting of redundant fiber optic backbone connecting wireless APs deployed throughout the facility.
- Installation of electronic personal teledosimetry system. These help to manage the personnel radiation dose as low as reasonably achievable (ALARA). A wireless teledosimetry system allows real-time radiation data and can be used as an integral part of a nuclear facility's ALARA program.
- Installation of a wireless barcode scanning system that is part of a warehouse materials management system.
- Installation of wireless sensors and data transmission equipment to implement condition-based maintenance (CBM) without installing costly, cable-intensive sensors. CBM programs employ equipment condition data to predict impending faults and failures, enabling the facility staff to schedule maintenance before failure occurs.
- Development of a prototype smart sensor for diagnostic and prognostic health assessment for a centrifugal charging pump gearbox.
- Wireless access to information via wireless LANs for retrieval of manuals, drawings, and procedures by personnel in the field.
- Real-time wireless communication between work-order software and scheduling software.
- RFID for tracking parts into and out of inventory.

The next few sections discuss specific applications in specific facilities within the nuclear industry. Instead of calling out facility names directly, alphabetic designations have been used.

5.2 Wireless LAN Implementation

Perhaps one of the more notable applications of wireless within a nuclear facility is Facility A's deployment of IEEE 802.11b wireless LAN technology throughout the facility. The system consists of a redundant fiber optic backbone connecting wireless APs deployed throughout the facility. The system conforms to IEEE 802.11b and enables voice communication using voice-over IP telephony. A voice-over IP gateway provides for LAN connectivity to the site telephone system. The infrastructure also enables LAN connectivity for data applications. A proof-of-principle pilot and comprehensive site coverage survey was successfully completed in 2002.

The most significant design aspect of the network includes an accommodation of all major voice, data, and video applications in-facility, including

1. Two-way radios (eight channels),
2. Telephony (wired and unwired),
3. On-line equipment monitoring,
4. Intranet and Internet connectivity (wired and wireless),
5. Remote video monitoring and control (wired),
6. Special application video monitoring (wireless),
7. Flexibility to migrate with advances in technology, and
8. Flexibility assured through network redundancy and backup power sources.

Facility A accomplished the deployment of the system during scheduled outages and completed the installation in 2005. The system consists of 400 APs, which are interconnected with a stand-alone fiber optic backbone network (Fig. 5.1). The system does connect to the corporate computing network via security gateway devices approved by the utility.

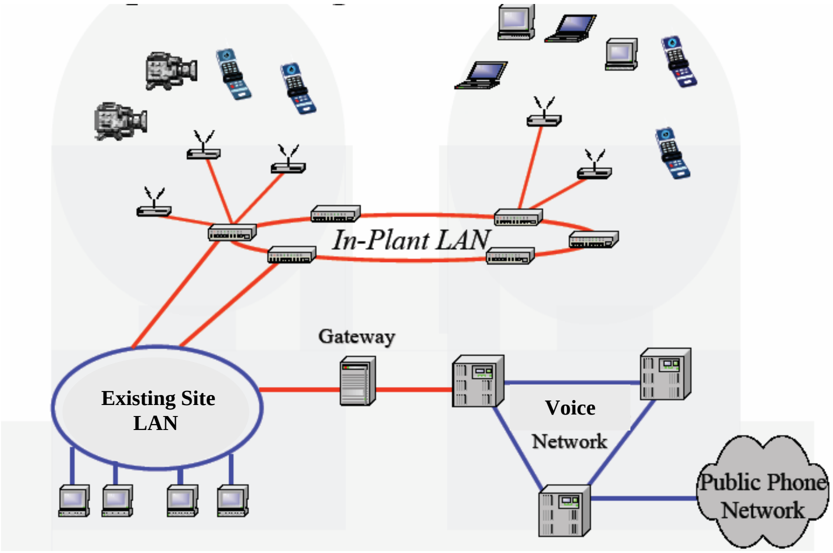

Figure 5.1 Conceptual diagram of communications at Facility A. (reproduced with permission)

This wireless LAN is intended for use with mobile computing devices, portable voice devices, some video applications, and online equipment monitoring. The wireless network is not connected to safety-related systems and will not be used to drive an operator to make a decision. It is a supplemental system. Applications already in use include the following:

- Mobile voice-over IP,
- Mobile communications,
- Monitoring of wireless temperature and vibration data, and
- Wireless discharge motor monitoring (indicates incipient degradation of motor wires by monitoring discharge).

Networking capability inside containment includes voice communications (wired and wireless), LAN connectivity (wired and wireless), and video (40 wired cameras remotely controlled). In the process of developing this wireless LAN, the facility conducted interference tests. It was found that the IEEE 802.11b devices were much less likely to interfere with existing operational instruments than the current land mobile radio (LMR) system. In fact, because of the interference from LMRs, radio-free zones have been declared throughout the facility. It is expected that these radio-free zones will become less restrictive for wireless LAN devices than for LMR devices in the future. Testing with a single wireless LAN transmitter by facility personnel has proved it to operate without causing a deflection on even the most sensitive devices (Barton and Rosemount transmitters), as long as the protective covers for those devices remain in place. Removing the covers can result in upsets caused by electromagnetic interference. Interference issues are discussed in more detail in Sect. 6.

Licensee testing has also shown the IEEE 802.11b devices to be free of interference from the nuclear facility, even with both reactor units operating at full power. In fact, IEEE 802.11b wireless sensor devices are now being deployed for vibration and temperature measurements on rotating equipment as part of a demonstration project in cooperation with EPRI. In this case, wireless devices are being used to provide readings daily, when they would normally be available only monthly when a worker reads the meters. This project has the potential to predict failures in time to make repairs before a failure occurs.

The Facility A deployment of the wireless LAN technology is of great interest for the topic of this report. Not only does its network deployment relate to many of the application areas discussed, but it also reports success. One interesting point of the system must be highlighted here: the entire system is based on IEEE 802.11b technology. Also of interest is the fact that use of any additional wireless technology (e.g., Bluetooth, Zigbee) has not been allowed in the facility because of coexistence concerns (they use the same spectrum).

5.3 Wireless Barcode Scanning System

Facility B currently has two different wireless systems deployed—a materials management system and a personal teledosimetry system. A wireless barcode scanning system that is part of a warehouse materials management system has been installed. The system has the potential to improve warehouse operations and efficiency by allowing warehouse operators to remove items from stock electronically and remotely. The system is integrated with the materials management module of the facility’s SAP^{TM} enterprise software. Though it operated as designed and has the potential to improve operational efficiency, the barcode system has not been popular with the user community and will be decommissioned soon.

5.4 Teledosimetry System

A teledosimetry system was installed as part of Facility C’s safety culture of keeping the personnel radiation dose ALARA. The wireless teledosimetry system allows access to real-time data on radiation exposure and can be used as an integral part of a nuclear organization’s ALARA program. It is used during refueling outages to monitor workers’ possible exposure to radiation.

5.5 Enhancing Condition-Based Maintenance with Wireless Sensors

Most, if not all, utilities have implemented CBM programs to cut spending on maintenance, while reducing the risk of equipment failure that could cause unplanned downtime. These programs employ equipment condition data to predict impending faults and failures, enabling the facility staff to schedule maintenance before failures occur. However, wiring costs and the cost of maintaining the physical cable connections between equipment monitoring devices may prevent a CBM program from being implemented for a significant percentage of installed equipment. One solution to this problem is the integration of wireless communication with on-line equipment monitoring technology.

Facility D has installed wireless vibration and temperature sensors (using an Aeptec/3eTi^{TM} wireless sensor array) on the motors of air exhaust fans with turbine-style blades to monitor incipient failures. These turbine exhaust fans are located within cylindrical ducts and are inaccessible to technicians during facility operation. Wires connect all sensors to a signal transceiver that transmits data via an IEEE 802.11 signal to a LAN AP located over 300 ft (91.4 m) from the fan motor in a support building. When the AP receives the signal, it pushes data onto the LAN via an Ethernet connection, making the data available to motor-condition-assessment software. In addition, a motor testing system located in the facility's load center will, through the installation of an additional wireless transceiver, be made available to the predictive maintenance group through the facility's LAN.

5.6 Centrifugal Charging Pump Gearbox Smart Sensor

EPRI has developed and installed a centrifugal charging pump (CCP) gearbox smart sensor at Facility E. The objective of this work is to improve availability while reducing maintenance costs and downtime. It employs smart sensor and wireless technology for diagnostic and prognostic health assessment for the type of CCP gearbox employed at the facility. The system consists of a wireless embedded sensor and a custom client-side application running on a wireless laptop. The sensor acquires and processes data from two vibration channels. The application running on the laptop fuses data gathered from the smart sensor to estimate current health and predict remaining useful life. The output from the smart sensor includes condition vectors, as well as health and prognostic vectors. These vectors provide information about the condition of the gearbox and its ability to perform its function for a given mission duration, such as the remainder of the fuel cycle.

In evaluating what test frequency and protocol should be used, both IEEE 802.11b and a 900-MHz wireless system were reviewed. IEEE 802.11b was chosen for several reasons, including (1) reservations raised by the facility IT staff that the signals might affect control equipment and (2) the commitment to ensuring minimum signal escapes for possible hacker interception (even though the signals did not serve any control functions). Bluetooth was also reviewed but was not chosen because life projection information and data sampling rates were needed. Figure 5.2 shows the CCP and depicts the gearbox smart sensor monitoring system. Figure 5.3 shows the processing flow involved.

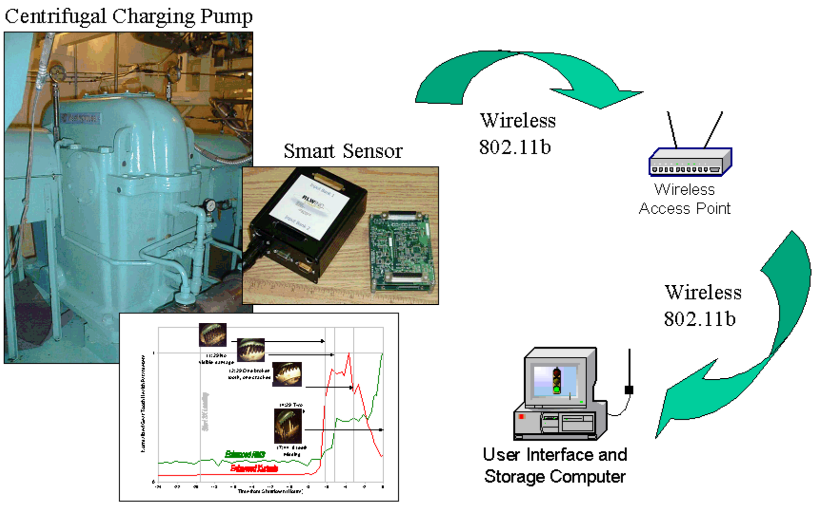

Figure 5.2. CCP gearbox smart sensor and monitoring system at Facility E. (reproduced with permission).

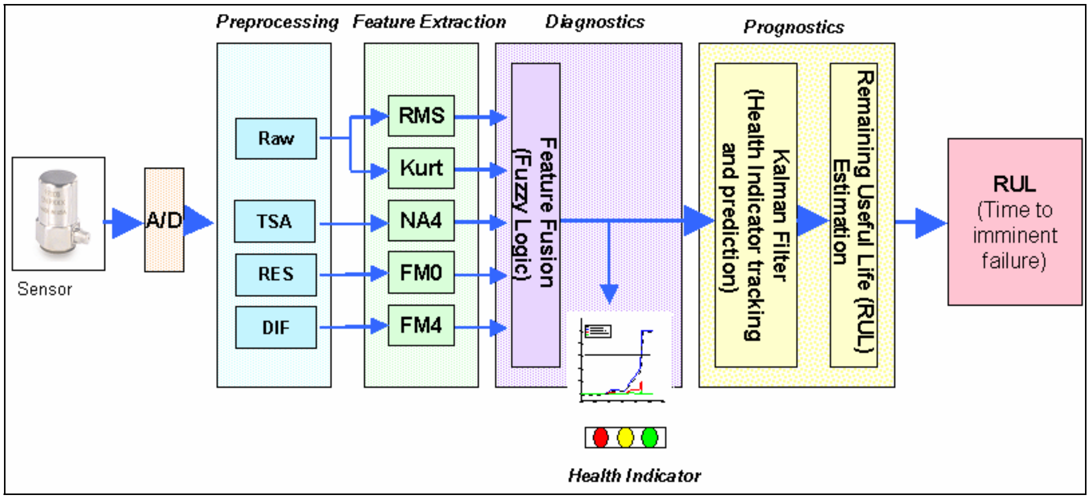
Preprocessing
Feature Extraction
Diagnostics
Prognostics
Sensor
A/D
Raw
TSA
RES
DIF
RMS
Kurt
NA4
FM0
FM4
Feature Fusion (Fuzzy Logic)
Kalman Filter (Health Indicator tracking and prediction)
Remaining Useful Life (RUL) Estimation
RUL (Time to imminent failure)
Health Indicator

Figure 5.3. Processing flow for the CCP smart sensor at Facility E. (reproduced with permission).

5.7 Electronic Performance Support System

The Electronic Performance Support System (EPSS) project was initiated by EPRI and a member utility to bring the benefits of electronic processing and documentation—electronic procedures, document control, data conversion, data storage, workflow tracking, logic algorithms and calculations, error checking, and error reduction—to mobile workers and to the processes that occur both before and after their work is completed. EPSS is a wireless computer-based system that provides performance support relative to the current computer-based system.

As originally envisioned in 2002, EPSS was developed in three phases. Phase 1 was a pilot project at Facility F. This phase was a proof-of-concept phase, as well as a method to gather the necessary implementation estimates for Phases 2 and 3. Phase 2 would consist of a full implementation of the EPSS at the nuclear facility. Phase 3 would be the full implementation of the EPSS at all of the utility's nuclear facilities.

5.8 Smart Wireless Transmitters

Some nuclear facilities have upgraded their non-safety instrumentation and control (I&C) systems to include smart transmitters (***not*** smart **wireless** transmitters). These include smart pressure, temperature, and flow transmitters. The term "smart" implies that the transmitter has an embedded microprocessor and is capable of transmitting variables (e.g., alarm state, limit switch position, transmitter health) to a remote station, such as a system hand-held by a technician. The smart capability of the transmitter also allows it to be reconfigured, self-checked (both remotely), and/or recalibrated in-line using a remote hand-held calibrator or station.

Many smart transmitters have fieldbus capability, a standardized digital communication protocol that provides a two-way communication link among smart field devices and automation systems. It serves as the LAN for instruments used in process automation and has a built-in capability to distribute control application across the network.

Although smart transmitters are in use in non-safety-related applications, the ORNL study did not uncover any use of wireless smart transmitters. The situation in the non-nuclear industry is different. For the latter, several companies make wireless conversions for flow, level, pressure, and temperature transmitters. Some of these are IEEE 802.11 Ethernet-compliant. The closest equivalent wireless technology in the nuclear industry that was identified in this study was the installation of smart sensors on the CCP gearbox for the acquisition of vibration and temperature data at Facility E. However, it is clear that wireless technology is making inroads into the nuclear facility environment, and it is likely only a matter of time before wireless smart transmitters will also be employed in non-safety-related nuclear applications.

6. INTERFERENCE AND COEXISTENCE ISSUES

As stated in previous sections, good spectrum management is important for the overall successful deployment of wireless technologies. Frequency spectrum is a precious and limited natural resource. Humans cannot create any more than what is already available in nature. We can, however, create technologies to use it more efficiently and use portions of it that were previously unavailable.

The issue of limited spectrum is coming to the forefront with the increased use of ISM bands. These bands are particularly relevant to this report because many of the technologies discussed are based on these bands, in particular the 2.4-GHz band. Use of low-power data devices in the ISM bands has been approved based on noninterference with existing systems and contention-based access. This stipulation implies two things: (1) systems that were already in existence or are licensed for these bands have priority, and (2) users of unlicensed systems must compete with each other for available bandwidth.

A separate issue is interference with other systems. RF energy has been known to be absorbed by systems that do not intentionally use RF energy in their normal operations. As an extreme example, hand-held radios, like those used by emergency responders, are known to trip circuit breakers and adversely impact electronic equipment. For this reason, nuclear facilities have established exclusion zones where use of these devices is forbidden. On a smaller scale, there is concern that RF energy transmitted by wireless data devices, such as those discussed in this report, will impact instrumentation and cause erroneous readings. Another related issue is the possibility that systems and equipment in a nuclear facility could interfere with the wireless system. The importance of electromagnetic compatibility in implementing wireless networks is illustrated by the following examples.

6.1 Coexistence between Bluetooth and IEEE 802.11b

The potential for interference between IEEE 802.11b and Bluetooth networks is very real, and each can interfere with the other. This interference is most likely to cause problems when IEEE 802.11b and Bluetooth devices are located next to each other, which is the case in an office where one individual is attempting to use more than one of these technologies. Bluetooth was still in the standardization phase when the first IEEE 802.11b wireless networking products became available on the market; and during the recent years, IEEE 802.11b has enjoyed enormous success. According to the Wireless Ethernet Compatibility Alliance (WECA) an industry trade group that performs compatibility certification for IEEE 802.11b devices, there are now more than 200 member companies and more than 2000 WECA-certified products.[29] WECA counts only those products that have earned WECA's WiFi certification, so there actually are even more IEEE 802.11b products on the market, including products for home, offices, and public spaces.

Many companies have adopted IEEE 802.11b as their standard networking method for notebook and portable computers. When the first Bluetooth products arrived on the market in 2001, many corporate IT managers feared that Bluetooth devices might bring down their IEEE 802.11b networks. In fact, some corporate IT directors have issued an outright ban on Bluetooth devices, at least until the interference issues are resolved. Such a ban may be extreme, though. While the potential exists for interference, "things don't come crashing down," according to John Drury, a WiFi manager for 3Com™. The severity of the interference depends on the proximity of the Bluetooth and IEEE 802.11b devices. With more than 6 ft of separation between devices, there is no interference. As you move the devices closer together, "there's a smooth, graceful degradation" in performance, according to Drury. "It's not a doomsday scenario."[30]

The potential for interference increases as more products are deployed. For example, many notebook computers now come with both technologies built in. Also, it is not uncommon for the user of a notebook computer associated with an IEEE 802.11b wireless LAN to also use a cell phone that may be Bluetooth-enabled.

It can be seen from IEEE 802.15.2 that 24 of the 79 Bluetooth channels are susceptible to interference from a single operable 802.11b network.[31] Assuming each of the 79 channels is used equally, this represents 30 percent of the spectrum. This interference shows up as an increase in latency and would be most notable in real-time voice applications. The converse of this is the Bluetooth signal interfering with IEEE 802.11, causing reduced data rates (and therefore increased latency). As error rates increase, data rates drop and packets must be retransmitted; so the overall usage of the network increases, which results in an increased probability of more interference. IEEE 802.15.2 defines coexistence mechanisms from both collaborative and non-collaborative perspectives. This is a new standard, and there will likely be a delay before products are available for deployment.

Bluetooth interference with IEEE 802.11g networks is similar, although there are differences in modulation type between IEEE 802.11b and IEEE 802.11g. Standard IEEE 802.11g does not use a true spread-spectrum modulation technique. Instead, it takes the channel used in IEEE 802.11b and divides it into 52 equal sub-carriers that are 312.5 kHz wide. These sub-carriers are selected to be orthogonal to one another so they can be spaced closely together. Four of the sub-carriers are dedicated to provide pilot signals, which are used for phase and amplitude references when demodulating the remaining sub-carriers. The IEEE 802.11g signal is most sensitive to interference at the frequencies of these sub-carriers, especially the ones that fall at ± 2 MHz from the center frequency. At the IEEE 802.11g center frequency, a Bluetooth signal that is 11 dB below the 802.11g signal will cause a BER of 0.001. At 2 MHz from the IEEE 802.11g center frequency, a Bluetooth signal that is 22.5 dB below the IEEE 802.11g signal will cause the same BER, leading to poor performance by IEEE 802.11g devices.[32]

Recent developments such as adaptive frequency hopping, MAC scheduling, packet encapsulation rules, or overlap avoidance are addressing the coexistence problems between Bluetooth and WiFi.[33, 34] The effectiveness of these techniques is still under study. The bottom line on IEEE 802.11 and Bluetooth interference is that it is a big enough issue to require action by the standards bodies. And because the ISM band is a non-licensed band, one can expect new technologies to emerge over time that require further consideration of interference.

6.2 Microwave Ovens and ISM Devices

In addition to licensed uses and ISM devices, microwave ovens operate in the 2.4-GHz band. Many studies have shown that because of the disproportionately large power output of microwave ovens compared with low-power IEEE 802.11b and Bluetooth devices, these devices may be impaired. Microwave ovens are not used strictly to heat food. In some facilities, industrial microwave ovens are used for drying. Also, controls on RF leakage for microwave ovens are based on biological effects, not RF interference.

An experimental channel sounding study done by Murakami[35] has provided evidence that the operation of microwave ovens may cause serious interference at the 2.4-GHz band. These researchers characterized the 2.4-GHz band propagation channel. Bluetooth and IEEE 802.11b devices will suffer dropped packets requiring retransmission when a microwave is operating in the vicinity.[36] Some IEEE 802.11b vendors have included a specific microwave oven parameter on their user interface that specifically avoids use of the part of the band used by microwave ovens.

6.3 Zigbee's Coexistence with IEEE 802.11 and Bluetooth

Much analytical and theoretical discussion related to the existence of Zigbee in 2.4-GHz band operation has emerged. In Howitt and Gutierrez's theoretical model,[37] they claim that unless an IEEE 802.11b station is located near an IEEE 802.15.4 cluster with a high aggregate activity level, an IEEE 802.15.4 network will have little to no impact on the IEEE 802.11b network's performance.

Regarding the interference issue related to the coexistence of Zigbee and Bluetooth, no experimental studies were found. However, Neelakanta and Dighe[38] in their analytical study suggest that regardless of the distinct modulation approaches that are used in these two kinds of technologies, mutual interference can occur. The RF link's performance can be impaired as a result of packet losses. ORNL staff are developing coexistence models for Zigbee, Bluetooth, and IEEE 802.11, and the results are expected to be reported in a future NUREG/CR. Experimental or measurement studies are also needed to further illustrate the issues related to the coexistence of Zigbee, Bluetooth, and IEEE 802.11.

Intentionally Left Blank

7. DEPLOYMENT IMPLEMENTATION CONSIDERATIONS

A wireless system should not be deployed in any environment until all potential issues have been considered and a plan established to resolve the issues that are relevant to the particular environment of interest. Many of these issues are covered in detail throughout this document and summarized here at the system level. Though mentioned in this chapter, security issues are covered in more detail in the next chapter.

7.1 Wireless LAN

Wireless LANs provide a convenient way to connect computing devices to each other and/or to a facilities network. The fact that this technology involves computing devices (e.g., laptop computers, palm computers, desktop computers) presents unique implementation issues. The proliferation of mobile computing devices throughout industry makes them accessible not only to facilities with a need to communicate remotely but also to persons with intent to do harm. This, coupled with the fact that RF signals do not obey physical boundaries, makes this technology susceptible to hacking and other abuse. These issues must be considered in detail as decisions to deploy this technology are being made.

At the time of this writing, the security of wireless LAN technology is being hotly debated in industry. Vulnerabilities in the standards have been identified.[23] Facilities with wireless LANs that propagate a usable signal to public areas such as parking lots, streets, and parks have been particularly hard hit. In fact a new breed of hacker, the “war driver,” has emerged. These war drivers identify insecure networks and pass this information along via the Internet, so others in the community can acquire free Internet access, among other things (www.wardriving.com).

This discussion brings home an issue about the level of trust one can have in a wireless LAN. The sensitivity of data being passed on the wireless LAN and the sensitivity of information residing on wireless LAN nodes (even if it is not transmitted) must be considered carefully. A node on a wireless LAN may be susceptible to hacking from other nodes on the wireless LAN, whether or not they are authorized. Its susceptibility depends on the presence and effectiveness of the employed authentication measures. This issue is common to both stand-alone ad hoc networks and networks connected to a network infrastructure. However, implementation issues differ between the stand-alone and interconnected wireless LANs; therefore, they are covered separately later. Careful administration of the individual client computers on a wireless LAN is critical to prevent their being exploited. This should include the deployment of personal firewall protections on each node.

Even given the shortcomings of IEEE 802.11 standard protections discussed in Section 4.1, it is foolish to deploy a wireless LAN without implementing those protections, because the wireless LAN is completely open to abuse if the protective features are left turned off or left at factory default settings. Specifically, the protections referred to here are WEP and the service set identifier (SSID). Even though WEP has been proved to be lacking as far as security is concerned,[23] enabling it at least makes access more difficult for potential hackers. In fact, a person must purposefully hack the network if WEP is enabled; this alone is important should legal action be necessary.

The SSID is used to name the wireless LAN. This SSID can be broadcast to make connections easier for users, although this is not a good idea. The SSID should be set to something different from the default setting. SSID defaults are widely known and published on war-driving web sites. Some in the wireless LAN security business recommend that the SSID be changed to something that does not identify the true use of the network. Even if the SSID is set to non-broadcast mode, it is transmitted in each control frame and is never encrypted; therefore, using a label that suggests that there might be information of interest to hackers is not a good idea. The SSID and WEP encryption key will need to be shared with the authorized users on the network and should be administratively protected.

WEP, the original IEEE 802.11 security protocol, is vulnerable to cryptographic attacks that reveal the shared key used to encrypt and authenticate data. IEEE 802.11i provides improved authentication, authorization, and encryption capabilities. The standard was approved in June 2004 and defines new encryption key protocols, including TKIP and the AES protocol. These will enable wireless LANs to benefit from stronger forms of encryption.

In general, already existing WiFi-certified products should be upgradeable to TKIP. Those that cannot be upgraded will still interoperate with products that use TKIP, but only using WEP for security. Although TKIP offers considerably improved security compared with WEP, the AES algorithm is considered more robust. However, the AES algorithm requires updated hardware, so older IEEE 802.11 hardware will not be upgradeable in many cases. The AES specification is primarily intended for newer hardware. Devices using the AES algorithm would still be able to interoperate with the older devices, but they would use the weaker security technologies. NIST has designated AES as the security standard for wireless networks that carry government information. It is reasonable to suggest that nuclear facility wireless LAN implementations should use hardware that is compatible with the AES security algorithm.

7.2 Wireless PAN

The primary purpose of the PAN is to interconnect devices associated within a small area for use by an individual. Many times these are stand-alone devices, for example, a wireless earphone/microphone for use with a cell phone. However, devices such as a palm computing device that is connected to a desktop computer with a PAN pose a security risk to the desktop computer and any network to which it is connected. These networks are typically very limited in output power and range. Therefore, the issues with RF interference and signal interception are minimized. However, one should not ignore the potential security issues with the wireless PAN. Perhaps it is only a matter of time before the security problems of IEEE 802.11 networks cross over to the wireless PAN. In fact, vulnerabilities of Bluetooth have already been highlighted in a report by @stake.[39]

7.3 Ad hoc Network

The ad hoc network, as defined by IEEE 802.11, is a network of wireless LAN nodes that does not utilize APs or a distribution network. This is essentially a stand-alone wireless LAN consisting of interrelated nodes that must communicate among themselves. This type of wireless LAN does not place a facilities network at risk because the two are not connected. However, as previously pointed out, nodes on the ad hoc wireless LAN are susceptible to hacks over the RF channel and should be protected accordingly.

7.4 Network Infrastructure

An infrastructure wireless LAN utilizes APs and is connected to a distribution network. The distribution network can be as simple as a connection between a couple of APs, or it can be the facilities-wired LAN. It is important to note that the wireless LAN places the distribution network at risk if the connection is made without proper isolation and protection of the distribution network with a device such as a firewall. Therefore, APs should not be placed on a facilities LAN without ensuring that proper protection is in place. It is recommended that APs be placed on the outside of a facilities network perimeter, either physically or virtually. Network vendors offer devices that are intended to be placed between the APs and the facilities network. These devices can enforce rule sets that can make the wireless LAN look like it is outside the facilities network perimeter. In addition, these devices can provide log file information on the traffic coming from the wireless LAN.

7.5 Mobile Device Risk

Wireless LAN nodes have a tendency to migrate between the wireless LAN and the facilities-wired LAN. Therefore, even if the wireless LAN is placed outside the facilities network perimeter, if a node on the wireless LAN falls victim to a Trojan virus, it can compromise that network once it is connected by hardwire to the facilities LAN. Of course, this is the case for all mobile devices used outside a facility; if connected to an untrusted network, they are at risk of being infected by a Trojan virus and spreading the virus (or being exploited) once they are reconnected to the facilities network. It is important that devices that are attached to untrusted networks be protected by products such as personal firewalls and virus scanning software. This concern can be expanded to include storage media that can be used to spread viruses and worms. Memory sticks are of particular concern because they are active devices and can auto-execute code when first plugged in. These issues are independent of the use of wireless LANs and are included here for completeness.

7.6 Sensors

An effort is currently under way within the commercial industry to establish standards addressing the implementation of wireless sensor networks. It is often desirable to place sensors in remote locations in an industrial facility, such as a nuclear facility, and transmit data over a wireless link. Connecting these sensors to the control network or control panel via wireless links is attractive from a cost and ease-of-deployment perspective. In some ways, a wireless sensor is a separate wireless system that needs to be considered separately from other wireless systems. Hence, there is a movement in industry to define a new set of standards for sensors. These are the IEEE 1451 series of standards; in particular, IEEE 1451.5 is a standard for wireless physical layer connectivity. IEEE 1451.5 is expected to support IEEE 802.11b, IEEE 802.15.4, and IEEE 802.15.2.

7.7 RFID

RFID tagging is a technology that could soon find its way into a nuclear facility. RFID tags themselves can be either active or passive. They absorb energy from an interrogator and respond with a specific set of data. A complete RFID system that might be deployed at a nuclear facility would include the tags, as well as the interrogation equipment. Frequency ranges used by RFID systems include those used by IEEE 802.11b and Bluetooth technologies (2.4 GHz to 2.5 GHz), as well as lower frequencies (30 to 500 KHz and 850 to 950 MHz). Again, it is emphasized that successful use of wireless technologies requires proper coordination and planning of all systems utilizing the spectrum.

Intentionally Left Blank

8. WIRELESS SECURITY CONSIDERATIONS

It is not the intent of this section to provide a comprehensive discussion on wireless or cyber security issues. A follow-on project is anticipated that will provide a more encompassing treatment of the security of wireless technology, as well as address guidance on cyber security issues.

The intent of this section is to expose the reader to the fact that there are security issues associated with the use of wireless technology, and then discuss methods of improving the security of wireless communication. Security is a major issue for nuclear facilities—second only to safety. The issue of wireless communication security is fraught with real problems, as well as perceived problems. The real problem is that wireless communication (as opposed to wired communication) is not confined to a conductive path that can be easily seen or easily controlled. Therefore, the signals can be intercepted at locations that may not be obvious if they propagate with sufficient signal strength. Also, they can interfere with other electronic equipment, as discussed in Sect. 6. While wired communication can be "tapped," it is typically perceived as being easier to control access to signals transmitted on wires than to signals that are transmitted wirelessly. Section 8.1 provides a brief overview of general wireless security issues. Section 8.2 provides some concluding remarks on general methods to improve security. It should be emphasized that these remarks should not be taken in isolation. To date, there are two important documents that address cyber security in nuclear facilities. These are NUREG/CR-6847, *Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants*, and NEI 04-04, *Cyber Security Program for Power Reactors*. The discussion on security measures provided herein should be viewed in conjunction with these two documents.

8.1 General Wireless Security Issues

8.1.1 Denial of Service Attack

A typical network connection is initiated in the following manner:

a) A user (or more precisely, an application software) sends a message asking the server to authenticate it;
b) The server returns the authentication approval to the user; and
c) The user acknowledges this approval and then is allowed onto the server.

The idea behind a denial of service attack is for the user to send several authentication requests to the server, filling it up. The trick is that all requests have false return addresses, so the server can't find the attacker when it tries to send the authentication approval. Eventually, after waiting a while (sometimes as much as a minute) the server closes the connection. After the connection is closed, the attacker sends a new batch of forged requests, and the process begins again. This process ties up the service indefinitely.

8.1.2 WEP Encryption

It is very important to secure the wireless communication of data to prevent easy interception, and WEP is a security protocol for wireless networks in this regard. However, WEP was an early attempt to secure wireless networks, and there are freely available open source tools that can easily break WEP encryption. Currently available tools include WepAttack, Wepcrack, and Weptools. Fortunately, better security is also now available, such as the Data Encryption Standard (DES), virtual private networks (VPN), and WPA.

Perhaps one thing that might be said in WEP's favor is that even though it has been proven to be lacking as far as security is concerned,[23] enabling it at least makes access more difficult for potential hackers. In fact, a person must purposefully hack the network if WEP is enabled; this alone is important should legal action be necessary.

8.1.3 Wireless Telephony

Wireless telephones introduce vulnerabilities that are different from those of their wired counterparts. For example, an analog wireless telephone can be heard by anyone with a scanner. Transmission of digital wireless telephone information is scrambled. However, transmissions can be intercepted using the right equipment. Additionally, in the case of cell phones, the phone's identification numbers can be cloned by an attacker. This permits the attacker to use the cloned cell phone as the original cell phone.

8.1.4 Network Discovery Tools

Network discovery tools are used for management of LANs and WANs. However, such tools in the wrong hands can also be used for network penetration. The discovery of a wireless LAN might be used as a "back door" into a network to stage an attack. Technologies such as Insightix's DID passive operating system fingerprint tool can look inside a transmission and, with very few packets, can obtain information about components on a network.

Tools for Bluetooth network discovery, such as Bluesniff and Redfang, are easily available. Redfang enables an attacker to discover devices that one would not normally know to exist. It is designed to attack one of the several optional layers of security built into Bluetooth: a stealth mode in which a device ignores broadcast queries, rendering it invisible to any other devices that don't know its specific six-byte address. Redfang uncovers such hidden devices by sending queries over a large range of addresses and listening for replies. By narrowing the search range to the address space of a single chip vendor, an attacker can complete a scan in a relatively short time.

8.1.5 Unsecured Access Points

Unsecured APs can provide easy access to wireless attackers using readily available tools. One example is when the slammer worm penetrated an unsecured operations network, then worked its way through a T1 line bridging that network and a business network. The T1 line was one of multiple ingresses into the business network that completely bypassed it's firewall**.** This case illustrates the issue that a cyber security breach can compromise ancillary systems where an unsecured AP is allowed between operations and business networks (or any other networks).

8.2 Overview of Security Measures

The foregoing brief discussion on wireless security issues is intended to only suggest that completely securing a wireless communication system is a challenging task. In general, a layered defense approach to security is recommended. No one security measure makes a network impenetrable, and the most important security feature in any implementation is an effective policy. Combinations of the following measures should be employed in wireless networks where possible: (1) password protection, (2) encryption, (3) administrative controls, (4) network diversity/segmentation, (5) AP management (roaming), and (6) signal strength management. The subsequent discussion on these measures is not intended to be comprehensive, as another NRC project is planned for addressing cyber security issues. They are merely discussed in enough depth to highlight the security considerations useful in implementing wireless systems. The discussion on the security measures should be taken in conjunction with recommendations provided in NUREG/CR-6847, and NEI 04-04.

8.2.1 Password Protection

Password protection is a basic feature of all good networks. The system administrator must carefully maintain legitimate access to the facility's networks via password distribution. This access control, of course, includes redistribution of new passwords on a periodic basis, as well as maintaining an up-to-date database of valid users.

8.2.2 Encryption

Any IT system that carries sensitive information must employ appropriate levels of encryption. If the information is business-sensitive, then it is up to the owner to decide which levels of encryption to implement. If the information is classified by a government agency, then that agency's guidelines must be followed.

Encryption is an especially sensitive issue for wireless networks because RF signals do not obey physical or administrative boundaries. It should always be assumed that any information that traverses a wireless network will be subject to eavesdropping. To make this concern more severe, the encryption technique specified in the early IEEE 802.11 standards is weak and susceptible to compromise.[23] The encryption used in more recent IEEE 802.11i compliant devices is considered adequate for sensitive but unclassified information.[40]

8.2.3 Administrative Controls

The term "administrative controls" typically refers to policies instituted to control types of equipment and categories of personnel that are allowed into certain areas. For instance, only the system administrator and designees may have access to the computer room that houses the system servers. Another example would include preventing the use of wireless devices within a given region or room in the facility.

8.2.4 Network Diversity/Hierarchy

For security extensibility, it is a good practice to deploy networks that are segregated and hierarchical. That is, information of like sensitivity should be placed on segments of the network that are protected from segments of the network containing less sensitive information. This may also be referred to as compartmentalization or enclaves. The least sensitive information should be placed closest to the network perimeter. Information and devices outside the network perimeter should be considered untrusted. Wireless devices should be treated very much like untrusted devices. Protection methods between these segments should include traffic monitoring. Establishing this mindset will help prevent the placing of inappropriate information on the wireless networks. It will also help in placing the wireless network in a position in the overall network architecture where it can be properly watched and protected. It is wise to place some sort of firewall device between the wireless network segments and the wired network.

8.2.5 Access Point Control (Roaming Access)

Currently and in the future, the number of personal wireless communication devices that connect wirelessly to communication infrastructures (e.g., Internet and cell phone systems) will grow numerically. In turn, they will likely shrink in physical size and cost less. Therefore, it will become increasingly difficult to control a person's access to wireless networks. As dependency on wireless technology increases, so will the "need" for mobility and roaming. In the case of IEEE 802.11 networks, it is possible to control roaming usage by limiting types of traffic or specific individuals allowed to roam between particular APs.

8.2.6 Signal Strength Management

Another layer of defense is to control the strength and directivity of radio signals that reach the public-access boundary of the facility. Such controls might include the use of directional antennas, power-controlled circuits, or special radio modulation methods, such as DSSS. To accomplish this, propagation analysis should be conducted and verified with field strength testing.

In addition to an initial setup and test, routine spectrum sweeps should be conducted to verify that new unauthorized wireless networks or devices have not been deployed. It is generally agreed that the biggest risk wireless LANs place on a facility's network is the unauthorized AP. Generally, unauthorized APs are placed in a network by people who are looking for convenience and who typically pay no attention to security risks. Routinely patrolling for these unauthorized wireless devices is the best way to ensure they are not in use.

9. SUMMARY

Wireless technology implementation considerations are provided in this section that are applicable in the nuclear environment. Throughout the course of this study, it has become clear that the wireless technology field is rapidly changing and the trend is toward ubiquitous computing and communication. Because the technology is rapidly changing, definitive guidance is difficult to delineate. However, we have undertaken to provide suggested guidance here because of the favorable reception of the technology into non-nuclear industrial applications and the fact that wireless systems are already being deployed for non-safety-related functions in nuclear facilities.

Stringent safety considerations in the nuclear environment will warrant stringent wireless-related security measures. In particular, (1) sensor data must be guarded against unauthorized snooping; (2) unauthorized sensors must be prevented from inserting data into the system; (3) the facility network must be guarded against infiltration through sensor networks; and (4) the facility network must be guarded against spoofing devices. To defend against hacking, wireless networks will need a robust and layered protection mechanism. Current guidance reports on cyber security of nuclear facilities include NEI-04-04, *Cyber Security Program for Power Reactors*, and NUREG/CR-6847, *Cyber Security Self Assessment Method for U.S. Nuclear Power Plants*. The issues and considerations provided in this current report should be viewed in conjunction with NEI-04-04 and NUREG/CR-6847.

Wireless-based systems have the potential for interference with facility systems. To put the probability of interference in perspective, it is important to realize that spread-spectrum technologies reduce the strength of transmissions, increase the quality of the signal, and transmit at lower power levels. Thus, the introduction of spread-spectrum wireless systems will likely have minimal impact on other facility equipment. Regarding the interference issue related to the coexistence of Zigbee, Bluetooth, and IEEE 802.11 devices, the potential for problems is still not fully researched. ORNL staff is conducting experimental studies to confirm the coexistence issues, as well as developing coexistence simulation models. The results are expected to be reported in a future NUREG/CR report.

The locations of wireless transmitters must be given adequate thought and planning. The desired coverage area needs to be defined and a site analysis developed. If possible, a propagation analysis should be conducted; at a minimum, field tests should be conducted once the RF equipment is identified.

User acceptance by facility personnel is a consideration that is often overlooked when implementing wireless systems. Most implementations will be centered around cost savings, efficiency, and remote operations, and the importance of these should not be underestimated. However, safety and security must always be considered with wireless applications at nuclear facilities and should be addressed early in the process. The users need to embrace the technology, yet remain receptive to the safety implications. User awareness of safety and security concerns is essential, as both will be important to the implementation of wireless systems.

A QoS parameter that is important to wireless networks is the ability to predict and/or guarantee performance. In the case of nuclear facilities, the probability that a message will get through, the probability that it will get through in a certain amount of time, and/or the probability that the system will know when a message did not get through are paramount. In safety-related systems, performance should be the most important parameter. Because absolute control of the transmission medium (the spectrum) is not possible, wireless systems by their very nature are not deterministic. Measures will have to be applied to increase the *probability*. The system must take into account the probabilities of success at each intervening node between the originator of the message and the final user. Prudent use of redundancy should be considered when deploying wireless systems.

The issues presented throughout this report have been summarized in Table 9.1, along with potential solutions. It is expected that the expansion of wireless technology will plateau some day, but it probably will not be soon. So, for now, it will be very important to follow the advancements in the technology in preparation for their probable insertion into nuclear facilities.

This report is intended to assist NRC staff in the interim. It documents the state of the technology from the perspective of possible use in nuclear facilities and the wireless standards presently in use, as well as new standards under development. The report identifies present applications of wireless systems in nuclear facilities and describes deployment issues that could impact regulatory policy. It also discusses the safety implications of implementing wireless systems and the lessons learned from recent deployments, and provides:

- An introduction to wireless systems for NRC staff;
- Background technical information on wireless technology and potential deployment issues for its implementation into nuclear facilities;
- Assistance in assessing wireless systems proposed for nuclear facilities that may come up for review by NRC; and
- A knowledge base for operating simulation tools that can assess the performance of wireless devices in nuclear facilities.

Table 9.1. Issues and possible resolutions

Issue	Resolutions
Wireless system interference on facility equipment	• Characterize the susceptibility of facility systems to RF interference • Use spread spectrum modulation techniques • Control output power • Test before deployment
Wireless system interference on safety-related systems	• Characterize the susceptibility of facility systems to RF interference • Use spread spectrum modulation techniques • Control output power • Test before deployment • Implement administrative controls
Facility equipment interference on wireless systems	• Characterize the susceptibility of facility systems to RF interference • Conduct field tests • Use spread spectrum modulation techniques
Wireless system interference on other wireless systems	• Characterize the susceptibility of facility systems to RF interference • Control output power • Coordinate frequency usage • Implement administrative controls • Test before deployment
Reliability of wireless systems	• Deployment practices ensure path redundancy • Deployment practices ensure device redundancy • Use positive acknowledgments
Extreme environmental impact on wireless systems (including ionizing radiation)	• Use physical controls on equipment (sealed enclosures, etc.) • Use industrialized hardware • Use radiation shielding
Security of wireless systems — Security of data	• Use FIPS 140-2 encryption, authentication, validation, etc.
Security of wireless systems — System vulnerability	• Use spread spectrum modulation techniques • Use FIPS 140-2 • Segregate by compartmentalization
Security of facility networks from wireless systems	• Segregate by compartmentalization • Use firewall protections

Intentionally Left Blank

10. REFERENCES

1. T. Rappaport, *Wireless Communications: Principles & Practices*, Prentice Hall, Inc., Upper Saddle River, New Jersey, 1996.
2. R. Dixon, *Spread Spectrum Systems with Commercial Applications*, John Wiley & Sons, Inc., New York, New York, 1994.
3. R. Ziemer and R. Peterson, *Digital Communications and Spread Spectrum Systems*, Macmillan Publishing Company, New York, New York, 1985.
4. F. Doula, Ed., *Handbook of RF and Wireless Technologies*, Elsevier, Inc., Burlington, Massachusetts, 2004.
5. IEEE Std 802.11a, *Supplement to IEEE Standard for Information Technology— Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Physical Layer in the 5 GHz Band*, Institute of Electrical and Electronics Engineers, 1999.
6. IEEE Std 802.11b, *Supplement to IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Physical Layer Extension in the 2.4 GHz Band*, Institute of Electrical and Electronics Engineers, 1999.
7. IEEE Std 802.11g, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Institute of Electrical and Electronics Engineers, 2003.
8. IEEE Std 802.15.4, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements. Part 15.4: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, Institute of Electrical and Electronics Engineers, 2003.
9. IEEE Std 802.15.1, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements. Part 15.1: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, Institute of Electrical and Electronics Engineers, 2002.
10. Cooklev, T., *Wireless Communications Standards, A Study of IEEE 802.11^{TM}, 802.15^{TM} and 802.16^{TM}*, IEEE Press, New York, New York, 2004, p. 225.
11. IEEE Std 802.16, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, Institute of Electrical and Electronics Engineers, 2001.
12. IEEE Std 802.16a, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems–Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz*, Institute of Electrical and Electronics Engineers, 2003.
13. IEEE Std 802.16-REVd (802.16-2004), *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, Institute of Electrical and Electronics Engineers, 2004.
14. IEEE Std 802.16e, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed Broadband Wireless Access System–Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands*, Institute of Electrical and Electronics Engineers, 2005.

15. IEEE 1451, *Smart Transducer Interface for Sensors and Actuators*, Institute of Electrical and Electronic Engineers, 2003.
16. IEEE Std 802.15.3, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements. Part 15.3: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs)*, Institute of Electrical and Electronics Engineers, 2003.
17. IEEE Std 802.20 Home Page. <http://grouper.ieee.org/groups/802/20/>.
18. S. Breidnbach, *Network World*, May 3, 2004, p. 44.
19. C. Temme, *Network World*, July 26, 2004, p. 33.
20. IEEE 802.11h, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe*, Institute of Electrical and Electronics Engineers, 2003.
21. IEEE 802.11i, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control Security Enhancements*, Institute of Electrical and Electronics Engineers, 2004.
22. J. Mitola. and G. Q. Maguire, *Cognitive Radio: Making Software Radios More Personal*, IEEE Personal Communications, August 1999, pp. 13–18.
23. E. Amir and H. Balakrishnan, *An Evaluation of the Metricom Ricochet Wireless Network,* May 7, 1996, <http://www.lariat.org/Berkeley/paper.html>.
24. J. Lavergnat and M. Sylvain, *Radio Wave Propagation :Principles and Techniques,* John Wiley & Sons, Ltd, West Sussex, England, 1997.
25. H. Bertoni, *Radio Propagation for Modern Wireless Systems,* Prentice Hall, Inc., Upper Saddle River, New Jersey, 1999.
26. E. Johnson, R. Desourdis, et al., *Advanced High-Frequency Radio Communications,* Artech House, Inc., Norwood, Massachusetts, 1997.
27. Hayn, A., Rose, R., and Jakoby, R., *Multipath Propagation and LOS Interference Studies for LMDS Architecture*, Eleventh International Conference on Antennas and Propagation (IEE Conf. Pub. No. 480), Vol. 2, 2001, pp. 686–90.
28. Seidel, S. Y. and Arnold, H. W., *Propagation Measurements at 28 GHz to Investigate the Performance of Local Multipoint Distribution Service (LMDS)*, IEEE Global Telecommunications Conference, Vol. 1, 1995, pp. 754–7.
29. WiFi Alliance Certified Product Listing Home Page, <http://www.wi-fi.org/OpenSection/Certified_Products.asp?TID=2>.
30. *Peaceful Coexistence*, ExtremeTech Home Page, <http://www.extremetech.com/article2/0,1558,1157712,00.asp>.
31. IEEE 802.15.2, *Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bonds*, Institute of Electrical and Electronic Engineers, August 2003.
32. S. Selby, "Co-existence Warrants a Second Glance," *Wireless Systems Design*, October 2003, <http://www.wsdmag.com/Articles/Index.cfm?ArticleID=19205&Extension=pdf>.
33. N. Golmie, N. Chevrollier, and O. Rebala, *Bluetooth and WLAN Coexistence: Challenges and Solutions,* <http://w3.antd.nist.gov/pubs/golmie_CompCommMagazine03.pdf>.
34. C. F. Chiasserini and R. R. Rao, *Coexistence Mechanisms for Interference Mitigation in the 2.4-GHz ISM Band*, Wireless Communications, *IEEE Trans*., **2**(5), September 2003, pp. 964–975.
35. T. Murakami, Y. Matsumoto, and Y. Yamanaka, "Propagation Characteristics of the Microwave Oven Noise Interfering with Wireless Systems in the 2.4 GHz Band," pp. 2726–2729 in *The 14th*

IEEE 2003 International Symposium on Personal Indoor and Mobile Radio Communication Proceedings.

36. T. W. Rondeau, M. F. D'Souza, and D. G. Sweeney, *Residential Microwave Oven Interference on Bluetooth Data Performance, Consumer Electronics*, IEEE Transactions, **50**(3), pp. 856–863, August 2004,.
37. I. Howitt and J. A. Gutierrez, IEEE 802.15.4, "Low Rate—Wireless Personal Area Network Coexistence Issues," *Wireless Communications and Networking*, 2003, WCNC 2003, 2003 IEEE, **3**, March 16–20, 2003, pp. 1481–1486.
38. P. S. Neelakanta and H. Dighe, "Robust Factory Wireless Communications: A Performance Appraisal of the Bluetooth and the ZigBee ZigBee Collocated on an Industrial Floor," Industrial Electronics Society, The 29th Annual Conference of the IEEE, **3**, November 2–6, 2003 pp. 2381–2386.
39. O. Whitehouse, *War Nibbling: Bluetooth Insecurity*, @stake Research Report, October 2003. <http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf>.
40. FIPS Pub 140-2 *Security Requirements for Cryptographic Modules*, May 25, 2001.