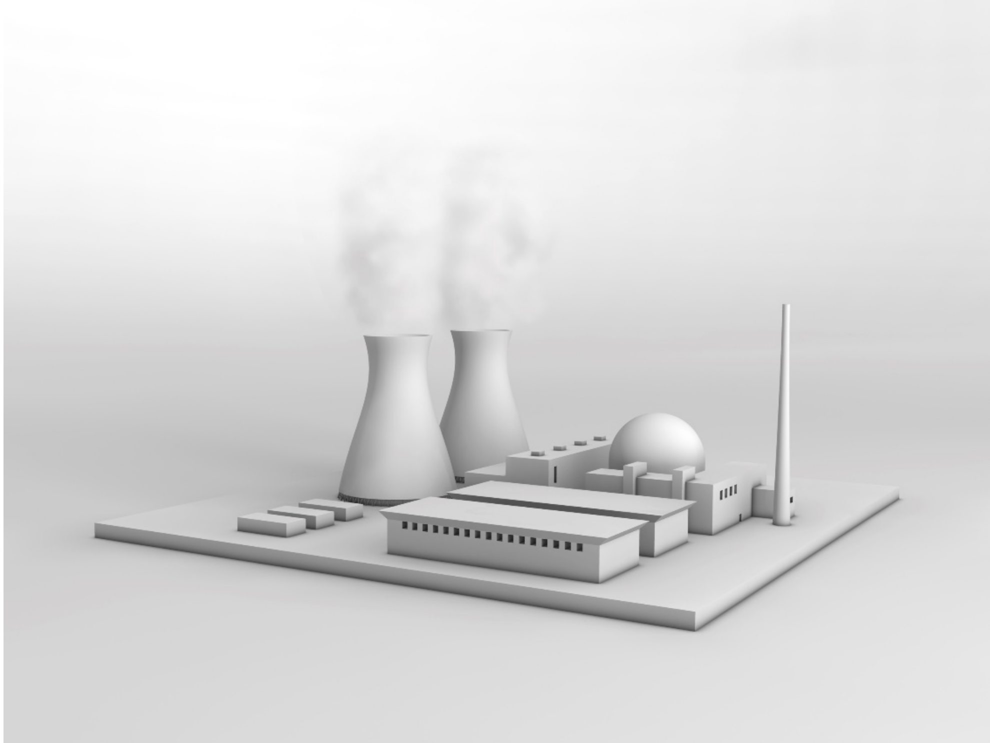
U.S.NRC
United States Nuclear Regulatory Commission
*Protecting People and the Environment*

**TECHNICAL LETTER REPORT**
TLR-RES-DE-2023-006

# Criteria for Determining the Safety of Wireless Technologies at Nuclear Power Plants



**March 2023**

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

**M. Muhlheim, R. Belles, S. Killough, L. Anderson, C. Cooke**
Oak Ridge National Laboratory

**L. Hardin**
U.S. Nuclear Regulatory Commission

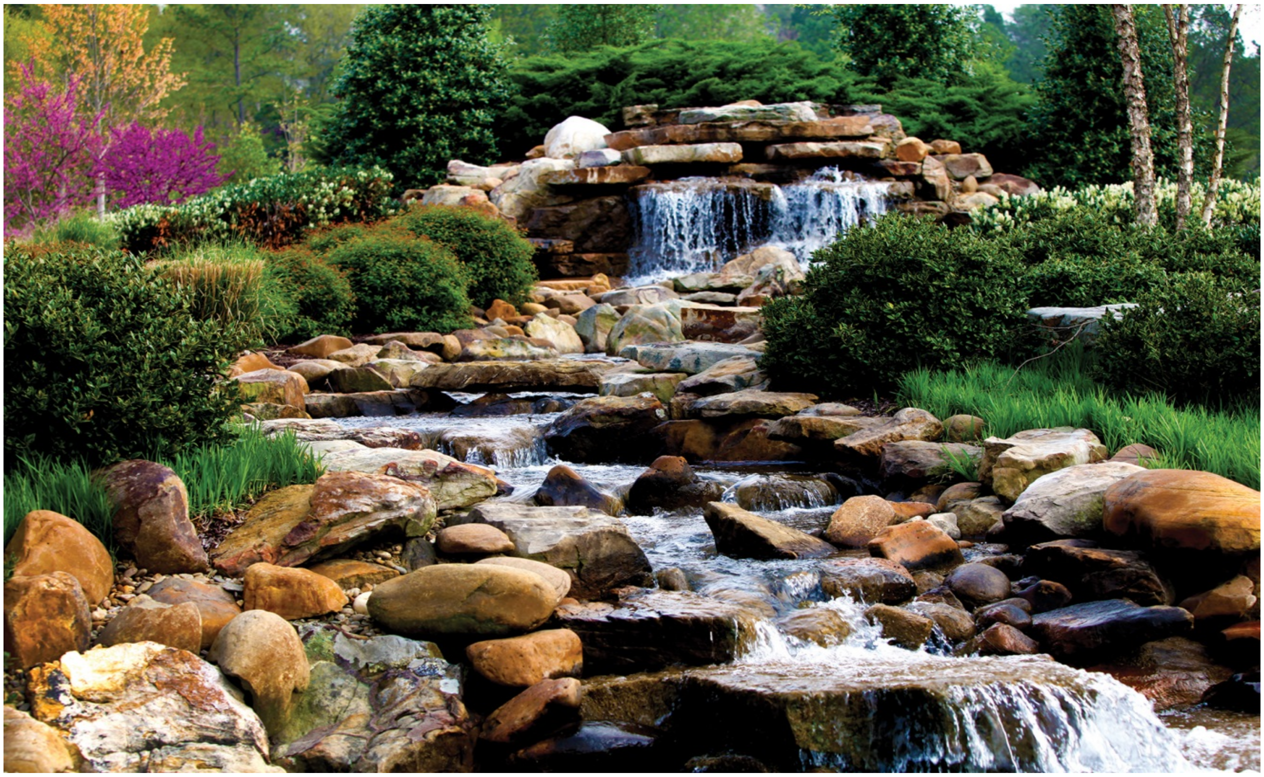
This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

**This report does not contain or imply legally binding requirements. Nor does this report establish or modify any regulatory guidance or positions of the U.S. Nuclear Regulatory Commission and is not binding on the Commission.**

*Page left intentionally blank*

ORNL/SPR-2022/2534

# Criteria for Determining the Safety of Wireless Technologies at Nuclear Power Plants



M. D. Muhlheim
R. J. Belles
S. M. Killough
L. A. Anderson
C. D. Cooke
L. A. Hardin

**March 2023**

L. A. Hardin, Jr., NRC Project Manager

OAK RIDGE
National Laboratory

ORNL IS MANAGED BY UT-BATTELLE LLC FOR THE US DEPARTMENT OF ENERGY

**ORNL/SPR-2022/2534**

Nuclear Energy and Fuel Cycle Division

# CRITERIA FOR DETERMINING THE SAFETY OF WIRELESS TECHNOLOGIES AT NUCLEAR POWER PLANTS

M. D. Muhlheim
R. J. Belles
S. M. Killough
L. A. Anderson
C. D. Cooke
L. A. Hardin

March 2023

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831
managed by
UT-BATTELLE LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

# CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

# ABBREVIATIONS

| | |
|---|---|
| 1G | first generation |
| 2G | second generation |
| 2-RAD | Two-Way Robust Acquisition of Data |
| 3G | third generation |
| 3GPP | 3rd Generation Partnership Project |
| 4G | fourth generation |
| 5G | fifth generation |
| 6G | sixth generation |
| A2LA | American Association for Laboratory Accreditation |
| AAI | automation asset integrity |
| AAMI | Association for the Advancement of Medical Instrumentation |
| AC | alternating current |
| ACLASS | ANSI-ASQ National Accreditation Board |
| ALARA | as low as reasonably achievable |
| AM | amplitude modulation |
| AMS | Analysis and Measurement Services Corporation |
| ANO | Arkansas Nuclear One |
| ANSI | American National Standards Institute |
| AS | Standards Australia |
| ASK | amplitude-shift keying |
| BER | bit error rate |
| BDB | beyond-design-basis |
| BGP | Border Gateway Patrol |
| BIS | Bureau of Indian Standards |
| BS | base station |
| BSI | British Standards Institution |
| C&C | command and control |
| CBRS | Citizens Broadband Radio Service |
| CDA | critical digital asset |
| CDMA | code division multiple access |
| CE | conducted emissions |
| CEN | European Committee for Standardization |
| CENELEC | Comité European de Normalisation Electrotechnique (European Committee for Electrotechnical Standardization) |
| CFR | US Code of Federal Regulations |
| CIGRE | Council on Large Electric Systems |
| CIPCO | Central Iowa Power Cooperative |
| CISPR | Comité International Spécial des Perturbations Radioélectriques |
| CNSC | Canadian Nuclear Safety Commission |
| COTS | commercial-off-the-shelf |
| CS | conducted susceptibility |
| CW | continuous wave |
| DAS | data acquisition system |
| DAS | distributed antenna system |
| dB | decibel-ten times the logarithm to base 10 of a ratio of two powers, or twenty times the logarithm to base 10 of a ratio of two voltages or currents |
| DBE | design basis event |
| dBgA | decibels referenced to one microampere, unit of conducted interference |

| | |
|---|---|
| dBi | decibels relative to an isotropic source |
| dBliV | decibels referenced to one microvolt, unit of conducted interference |
| dBtV/m | decibels referenced to one microvolt per meter, unit of electric field strength |
| dBpT | decibels referenced to one picotesla, unit of magnetic field strength |
| DC | direct current |
| DE | drive end |
| DECT | digital enhanced cordless communications |
| Dimem | Differentiated Services |
| DAkkS | Deutsche Akkreditierungsstelle |
| DoD | US Department of Defense |
| DOE | US Department of Energy |
| DoS | denial-of-service |
| DOT | US Department of Transportation |
| DSRC | dedicated short-range communication |
| DSSS | direct sequence spread spectrum |
| DVR | digital video recorders |
| E3 | electromagnetic environmental effects |
| EASC | Euro Asian Council for Standardization, Metrology and Certification |
| EDGE | enhanced data rates for GSM evolution |
| EIRP | effective isotopically radiated power |
| ELOS | extended line of sight |
| EM | electromagnetic |
| EMC | electromagnetic compatibility |
| EMF | electromagnetic field |
| EMI | electromagnetic interference |
| EMP | electromagnetic pulse |
| EN | European Norm |
| ENSRIC | Energiforsk Nuclear Safety Related I&C Research |
| EPC | evolved packet core |
| EPRI | Electric Power Research Institute |
| EPSS | electronic performance support systems |
| ESD | electrostatic discharge |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| EUT | equipment under test |
| E-UTRAN | Evolved UTRAN |
| eNB | E-UTRAN NodeB |
| EV | electric vehicles |
| EV-DO | Evolutionary – Data Optimized |
| FAA | Federal Aviation Administration |
| FCC | Federal Communications Commission |
| FDD | frequency division duplexing |
| FDMA | frequency division multiple access |
| FHSS | frequency hopping spread-spectrum |
| FM | frequency modulation |
| FMEA | Failure Mode and Effect Analysis |
| FMECA | failure modes effects and criticality analysis |
| FoF | factory of the future |
| FSK | frequency shift keying |
| GA | ground assembly |
| GAA | General Authorized Access |

| | |
|---|---|
| GDC | General Design Criterion |
| GHz | gigahertz |
| GLONASS | global navigation satellite system |
| GMLC | Grid Modernization Laboratory Consortium |
| GOST R | Federal Agency for Technical Regulation and Metrology |
| GPS | global positioning system |
| GSA | Global Mobile Suppliers Association |
| GSM | Global System for Mobile |
| GTEM | Gigahertz Transverse Electromagnetic cell |
| HART | Highway Addressable Remote Transducer Protocol |
| HEMP | high-altitude electromagnetic pulse |
| HMI | human–machine interface |
| HSPA | high speed packet access |
| I&C | instrumentation and control |
| IACS | Industrial Automated Control System |
| IAEA | International Atomic Energy Agency |
| IAF | International Accreditation Forum |
| IAS | International Accreditation Service, Inc. |
| IEC | International Electrotechnical Commission |
| IED | intelligent electronic device |
| IEEE | Institute of Electrical and Electronics Engineers |
| ILS | instrument landing system |
| IMD | intermodulation distortion |
| IMDA | Info-Communications Media Development Authority |
| INMARSAT | international maritime satellite |
| INPO | Institute of Nuclear Power Operations |
| INPP | Ignalina Nuclear Power Plant |
| I/O | input/output |
| IoT | internet of things |
| IP | internet protocol |
| IPv4 | internet protocol version 4 |
| IPv6 | internet protocol version 6, IP next generation, or IPng |
| ISA | International Society for Automation |
| ISG | Interim Staff Guidance |
| ISM | industrial, scientific, and medical |
| ISO | International Organization for Standardization |
| IT | information technology |
| ITU | International Telecommunications Union |
| JAS | Japanese Standards Association |
| JISC | Japanese Industrial Standards Committee |
| JLD | Japan Lessons-Learned Project Directorate |
| kbps | kilobits per second |
| kHz | kilohertz |
| KSA | Korean Standards Association |
| IntServ | Integrated Services |
| LAR | License Amendment Request |
| LAN | local area network |
| LED | light-emitting diode |
| LoRaWAN | Low-power Wide-area Network |
| LOS | line of sight |
| LTE | long-term evolution |

| | |
|---|---|
| LWR | light-water reactor |
| M2M | machine to machine |
| MAC | medium access control |
| MAS | multiple address |
| Mbps | megabits per second |
| MF | medium frequency |
| MHz | megahertz |
| MIC | message integrity check |
| MIL-STD | Military Standard |
| MINER | Mine Improvement and New Emergency Response |
| MIT | Massachusetts Institute of Technology |
| MLA | Multi-Lateral Agreement |
| MME | mobility management entity |
| MMN | medical micropower network |
| MPLS | multi-protocol label switching |
| MWMN | maritime wireless mesh network |
| NEI | Nuclear Energy Institute |
| NFC | near-field communication |
| NIST | National Institute of Standards and Technology |
| NMS | Network Management System |
| NPP | nuclear power plant |
| NR | new radio |
| NRC | US Nuclear Regulatory Commission |
| NTIA | National Telecommunications and Information Administration |
| NVLAP | National Voluntary Laboratory Accreditation Program |
| NZS | Standards New Zealand |
| ODE | opposite drive end |
| OFDM | orthogonal frequency division multiplex technology |
| OHLHS | overhead heavy load handling system |
| OIP | overall integrated plan |
| OIML | International Organization of Legal Metrology |
| OLM | online monitoring |
| OPG | Ontario Power Generation |
| OSC | operations support center |
| OSPF | Open Shortest Path First |
| OT | operational technology |
| PACS | physical access control system |
| PAL | priority access license |
| PC | personal computer |
| PCCV | prestressed concrete containment vessel |
| PDA | personal digital assistants |
| PDN GW | packet data network gateway |
| PED | portable electronic device |
| PHM | prognostics and health management |
| PLC | programmable logic controller |
| PJLA | Perry Johnson Laboratory Accreditation |
| PM | phase modulation |
| PNGS | Pickering Nuclear Generating Station |
| PSEG | Public Service Enterprise Group |
| PSK | phase shift keying |
| PSIMS | physical security information management system |

| | |
|---|---|
| QAM | quadrature amplitude modulation |
| QoS | quality of service |
| RAN | radio access network |
| RAT | radio access technology |
| RE | radiated emissions |
| RF | radiofrequency |
| RFI | radiofrequency interference |
| RFID | radio frequency identification |
| RG | regulatory guide |
| RHR | residual heat removal |
| RS | radiated susceptibility |
| RSSI | received signal strength indicator |
| RSVP | Resource Reservation Protocol |
| RTCA | Radio Technical Commission for Aeronautics |
| RTLS | real-time locating system |
| SAE | Society of Automotive Engineers |
| SAP | Systems, Applications, and Products |
| SATCOM | satellite communications |
| SCADA | supervisory control and data acquisition system |
| SDCWA | San Diego County Water Authority |
| SDGE | San Diego Gas and Electric |
| SER | safety evaluation report |
| SEU | single event upset |
| SFP | spent fuel pool |
| SFPIS | spent fuel pool instrumentation system |
| SGW | serving gateway |
| SHDSL | single-pair high-speed digital subscriber line |
| SHF | super-high frequency |
| SIF | safety instrumented function |
| SINR | signal-to-interference-plus-noise ratio |
| SIS | safety instrumented system |
| SMS | seismic monitoring system |
| SONGS | San Onofre Nuclear Generating Station |
| SR/ITS | safety-related/important-to-safety |
| SRP | Standard Review Plan |
| STA | station |
| STP | South Texas Project |
| STUK | Radiation and Nuclear Safety Authority of Finland |
| SWLAN | secure wireless local area network |
| TTAC | Technical Testing and Analysis Center |
| TCP | transmission control protocol |
| TDMA | time division multiple access |
| TDD | time-division duplex |
| TTE | through-the-earth |
| TOC | tactical operations center |
| TSE | Turkish Standards Institution |
| UDP | user datagram protocol |
| UHF | ultrahigh frequency |
| UMTS | Universal Mobile Telecommunications System |
| U-NII | Unlicensed National Information Infrastructure |
| UPCS | Unlicensed Personal Communications Services |

| | |
|---|---|
| US-APWR | US Advanced Pressurized Water Reactor |
| UWB | ultra-wideband |
| V/m | volts per meter, unit of electric field strength |
| VA | vehicle assembly |
| VDE | Verband der Elektrotechnik, Elektronik und Informationstechnik |
| VHF | very high frequency |
| VoIP | voice over internet protocol |
| VoWLAN | voice over WLAN |
| VSWR | voltage standing wave ratio |
| WAN AP | WSN access point |
| WCS | wireless charging systems |
| WEP | wired equivalent privacy |
| Wi-Fi | wireless fidelity |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WLAN | wireless local area network |
| WMAN | wireless metropolitan area network |
| WNS | wireless network security |
| WPAN | wireless personal area network |
| WPT | wireless power transfer |
| WSN | wireless sensor network |
| W-WAN | wireless wide area network |
| XFC | extreme fast charging |

# EXECUTIVE SUMMARY

This report provides an initial discussion of the potential impact to safety-related/important-to-safety (SR/ITS) systems by the possible expanded use of wireless technologies. One aspect of this discussion is focused on a review of Regulatory Guide (RG) 1.180 Rev. 2 to determine whether any revisions are necessary to reflect the current state of practice in evaluating and protecting instrumentation and control (I&C) systems and components from electromagnetic interference (EMI)[1] or radiofrequency interference (RFI)[2] on safety and nonsafety I&C. Electromagnetic compatibility (EMC)[3] is the ability of a device or system to function satisfactorily in its electromagnetic (EM) environment, which is achieved by limiting the unintentional generation, propagation, and reception of EM energy that may cause unwanted effects such as EMI. The goal of EMC is to ensure the correct operation of different types of equipment in a common EM environment.

To evaluate the potential risk to plant systems, the means by which EMI/RFI from wireless systems can impact these systems is identified herein. The general discussion of these components' degradation and failure modes covers information to be used for the RG review and for test planning.

A broad survey of wireless technologies is also included to support this effort. This base of knowledge is necessary when considering possible EMI/RFI environment changes and subsequent EMC issues for existing plant components resulting from expanded wireless use. This survey was accomplished through a literature review of the technologies and their uses in nuclear and non-nuclear applications. A great deal of valuable information is available on non-nuclear implementations. However, applying this information to nuclear applications can be challenging. Additionally, information on the interaction and failure modes of and between wireless systems and components was also gathered to (1) inform considerations and evaluations on the impact to existing systems, and (2) to provide information for future work.

The review findings and recommendations regarding RG 1.180 Rev 2 follow the wireless technologies survey. The identified issues are intended to inform and establish the initial proof-of-concept tests.

The report then addresses the testing effort to provide initial confirmatory and proof-of-concept results. Because potential test areas are vast, only a small, limited subset of possible tests can be performed at this stage. However, the test plan has been developed as a starting point for follow-on work to further investigate the topic. The primary purpose of the testing discussed here is to show the validity of the concepts discussed and to perform a spot check confirmation of test results vs. analytical analysis results. Finally, the collective information is briefly summarized to restate findings and to more directly present the recommended tasks for future work.

[1] *EMI* is the electromagnetic energy from sources external or internal to electrical or electronic equipment that adversely affects equipment by creating undesirable responses (degraded performance or malfunctions). EMI can affect fields even if their frequencies are not aligned.

[2] *RFI* is emitted by most electronic and electrical devices. The two ways that an electronic or electrical device emits RFI are via *radiated* and *conducted* emissions. In radiated emissions, interference is directly emitted into the environment from the device itself, whereas in conducted emissions, interference is released into an alternating current power line through the power cord of a component or device.

[3] *EMC* addresses the unwanted emissions and the countermeasures that may be taken to reduce unwanted emissions. The three main components of EMC are:

1. *Emission* of electromagnetic energy, whether deliberate or accidental, by some source and its release into the environment.
2. *Susceptibility* of the electronic or electrical equipment to malfunction or break down in the presence of unwanted emissions (i.e., RFI). *Immunity* is the opposite of susceptibility, being the ability of equipment to function correctly in the presence of RFI, with the discipline of "hardening" equipment being known equally as susceptibility or immunity.
3. The *coupling path* is the mechanism by which emitted interference reaches the electronic or electrical device.

EMC problems are generally solved by identifying at least two of the above-mentioned components of EMC and eliminating one of them.

# 1. INTRODUCTION

Numerous US Nuclear Regulatory Commission (NRC) regulations, NRC regulatory guides (RGs), and industry guidance and standards are relevant to current and potential efforts to implement wireless technology at a nuclear power plant (NPP). This report reviews the requirements and guidance for implementing wireless technologies, the available industry evaluations, and the guidance specific to electromagnetic interference (EMI) / radiofrequency interference (RFI), power surges, environmental qualification, and electrostatic discharge that could impact safety-related instrumentation and control (I&C) systems. Although cybersecurity is not a focus of this review, the topic must be addressed when considering expanded implementations of wireless technology into an NPP. For example, wireless technology and cybersecurity are tightly coupled such that if a wireless network was installed in addition to or as a replacement for a wired network in an SR/ITS application, it will require a plant to amend its cybersecurity plan. In many instances, although a wireless network has the same consequences of failure as a wired network, the likelihood of failure and new failure modes (including those related to cybersecurity failures) require an assessment of the new network from all causes. NRC is cognizant of this relationship [1].

Applications for wireless technologies are expanding rapidly, including at NPPs. As the numbers of unique types of wireless networks and the numbers of network devices continue to grow, these networks and devices will increasingly compete for a common frequency band because the available spectrum is not increasing. Additionally, the guidance from many wireless network vendors may not consider the characteristics of the other wireless networks in use. Thus, coexistence and interference are failure modes that must be addressed.

Wireless networks have become more pervasive in many industries, including production and manufacturing, telemedicine, aircraft, airport instrument landing systems (ILSs), and military applications. Wireless networks are gaining in popularity because they eliminate signal wiring costs, they provide the ability to move instruments if needed, and they make it possible to locate instruments in places that would be otherwise impossible. Because of their availability, advantages, and extensive usage in process industries, wireless technologies will continue to migrate into the nuclear arena. Current uses in NPPs include audio communications, data transfer, wireless dosimetry, equipment, and process monitoring, spent fuel pool level indicators, monitoring devices, and heavy equipment operations.

Currently, most NPP wireless systems are targeted for nonsafety-related applications. Overall, the nuclear industry has been very cautious about adopting wireless technologies. The issues of concern include infrastructure, regulatory issues regarding safety and reliability, potential new vectors for plant cybersecurity threats, and the potential for EMI/RFI with existing plant safety systems.

The continued evolution of wireless technology, its increased use, and the cost savings and flexibility it offers reinforce the impetus for the NRC to maintain requirements and guidance on its use in nuclear facilities to reflect current technology.

A major concern in the use of wireless technology in NPPs is the potential impact from EMI/RFI on plant equipment (both safety and nonsafety). Many licensees are introducing wireless networks for nonsafety applications and security functions (e.g., access control) in their NPPs because there are minimal restrictions on its applications and use with no impacts on their cybersecurity plans. NPPs must be able to maintain the same level of safety when wireless technologies are utilized. This includes both when new functionality is added as well as with any replacement of existing capabilities – such as using a wireless network to replace a wired network.

As for the safety aspects of expanded use of wireless technologies, RG 1.180, Rev. 2 was developed to further define and improve the efficiency of equipment emission and susceptibility evaluations to maintain the proper level of protection for SR/ITS systems from all EMI/RFI sources. When applied specifically to wireless technologies, this may lead to excessive conservatism. To more adequately consider factors unique to wireless technology use, such as potential differences in uncertainty between fixed and portable intentional RF sources, as well as complex wireless installations, additional analysis is required.

## 1.1 PHENOMENA OF AN EMI FIELD

Every electronic or electrically powered device radiates some electromagnetic (EM) waves. These EM waves can interfere with nearby radiofrequency (RF)/wireless and hard-wired systems or devices, a condition referred to as EMI. Electromagnetic fields (EMFs) consist of three components:

- the induction field,
- the near field, and
- the far field.

The magnetic induction fields are produced by current-carrying wires. The induction and near fields decay rapidly with distance from the source. Induction tests are performed to determine if the signal lines from the equipment under test (EUT) are immune to power-frequency induction fields.

A control circuit or cable is considered to be in the near field of an EM source when the source to circuit distance is closer than the wavelength ($\lambda$) divided by $2\pi$ (i.e., $\lambda/2\pi$) or roughly 1/6th of the wavelength $\lambda$ of the highest source frequency [2]. With the propagation of EM waves in the *near field* ($r < \lambda/2\pi$), the wave impedance is determined by the characteristics of the source and the distance from the source. In the near field, if the source impedance is high (>377 ohms[4]), the electric and magnetic field strengths attenuate at rates of $1/r^3$ and $1/r^2$, respectively. If the source impedance is low (<377 ohms), the rates of attenuation are reversed: the electric field strength will fall off at a rate of $1/r^2$ and the magnetic field strength at a rate of $1/r^3$.

Measurements in the near field can be made at frequencies above 1600 kHz at a measuring distance of 30 m, frequencies above 4800 kHz at a measuring distance of 10 m, and above 16 MHz at a measuring distance of 3 m [3].

RG 1.180, Rev. 1 addresses the far-field effects of EM waves. Though this discussion was removed in RG 1.180, Rev. 2, the information is still relevant. In the far field, radiation coupling refers to circuits where the source's emissions are seen as a true traveling EM wave. This latter situation involves radio wave transmissions and antenna effects. Thus, at some distance from the source (again, 1/6th of the wavelength $\lambda$ of the highest source frequency), far-field effects dominate; and in free space the EMF behaves as a propagating transverse electromagnetic (TEM) wave. A rate of 1/r is typically used to estimate the attenuation of field strength with distance in the far field.

In a free field, extrapolation of the limits at a particular frequency to distances less than $\lambda/2\pi$ requires extrapolation of the level at that frequency back to the $\lambda/2\pi$ distance using a 1/r extrapolation for the far field attenuation and then further extrapolation from the level at the $\lambda/2\pi$ distance to the final distance

[4] The electromagnetic wave impedance in ohms ($\Omega$) for a plane wave propagating through air (free space) is $120\ \pi$ or 377 $\Omega$.

using a $1/r^3$ or $1/r^2$ relation for the near field attenuation [3]. Extrapolation of the limits at a particular frequency to distances greater than $\lambda/2\pi$ requires that the level at that frequency first be extrapolated to the $\lambda/2\pi$ distance using a $1/r^3$ or $1/r^2$ relation (depending on whether the source is electric or magnetic, respectively) and then further extrapolating the limit from the $\lambda/2\pi$ distance to the final distance using a 1/r relationship

## 1.2 RADIATED/CONDUCTED EMISSIONS/SUSCEPTIBILITY

There are four aspects related to EMI (**Error! Reference source not found.** [5]):

1. **Conducted emissions** are alternating current (AC) signals on electrical wiring caused by circuitry that switches or oscillates. Each device creates EM energy, some of which is conducted onto the power supply cord. Conducted emissions manifest as undesired noise superimposed on the desired signal or power waveform. The goal is to restrict the amount of interference from one device onto another such that the operating device will not be affected by other devices. Standards endorsed by RG 1.180 Rev. 2 that cover conducted emissions (RF) are Military Standard (MIL-STD)-461G, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment" and International Electrotechnical Commission (IEC) 61000-6-4, "Generic Standards – Emissions Standard for Industrial Environments" (low and high frequency). Other standards that cover conducted emissions that are not endorsed by RG1.180 include Comité International Spécial des Perturbations Radioélectriques (CISPR) 11, "Industrial, Scientific, and Medical Equipment – Radio-Frequency Disturbance Characteristics – Limits and Methods of Measurement" and CISPR 32, "Electromagnetic Compatibility of Multimedia Equipment – Emission Requirements", (RF) as well as ANSI C63.27-2017, "American National Standard for Evaluation of Wireless Coexistence". Although 47 US Code of Federal Regulations (CFR) Federal Communications Commission (FCC) 15[5] is a regulation and not a standard (even though it is frequently referred to as a standard), it provides acceptable emission tests.[6] However, IEC 61000-6-4 provides the most recent international guidance for emissions test practices and incorporates by reference the emissions test methods established by CISPR and IEC. RG 1.180 endorses IEC 61000-6-4 and CISPR test 16 for conducted and radiated emission tests. Finally, RG 1.180 allows for FCC certification of Class A or Class B devices under 47 CFR Part 15 [4] to be credited over the frequency ranges covered by certification testing in lieu of additional testing for nonsafety related I&C systems. To take credit for FCC certification for SR/ITS I&C systems, test data and documentation equivalent to the information identified in Regulatory Position C.7 in RG 1.180 Rev. 2 should be maintained and available for review. The American National Standards Institute (ANSI) C63.4 specifies the test setup for conducted emissions tests.

2. **Conducted immunity (susceptibility)**: External low frequency radiated RF fields[7] can couple into equipment via input/output (I/O) or power cables. These conducted electrical disturbances can be caused by electrical fast transients/bursts, surges, disturbances induced by RF fields, ring waves, and low frequency emissions. Conducted susceptibility refers to the ability of a component to properly function in the presence of these disturbances. Standards endorsed by RG 1.180 Rev. 2 that cover conducted susceptibility include MIL-STD-461G, IEC 61000-4-4,

[5] The regulatory responsibility for the radio spectrum is divided between the FCC and the National Telecommunications and Information Administration (NTIA) in the United States Department of Commerce. The NTIA administers spectrum allocation for the federal government's use, and the FCC is responsible for all other enterprises and organizations.

[6] RG 1.180 notes that certification for Class A or Class B devices under 47 CFR Part 15, "Radio Frequency Devices," may be credited over the frequency ranges covered by certification testing in lieu of additional testing for nonsafety-related I&C systems.

[7] An RF field is an AC signal that, when put through an antenna, generates an EMF for wireless broadcasting or communication by sending a current through that antenna.

"Testing and Measurement Techniques – Electrical Fast Transient/Burst Immunity Test" (electrically fast transients/bursts), IEC 61000-4-5, "Testing and Measurement Techniques – Surge Immunity Test" (surges), IEC 61000-4-6, "Testing and Measurement Techniques – Immunity to Conducted Disturbances, Induced by Radio-Frequency Fields" (RF), IEC 61000-4-12, "Testing and Measurement Techniques – Ring Wave Immunity Test" (100 kHz ring wave), IEC 61000-4-13, "Testing and Measurement Techniques – Harmonics and Interharmonics including Mains Signalling at A.C. Power Port, Low Frequency Immunity Tests" (low frequency, 16 Hz to 2.4 kHz), and IEC 61000-4-16, "Testing and Measurement Techniques – Test for Immunity to Conducted, Common Mode Disturbances in the Frequency Range 1 Hz to 150 kHz" (low frequency, 0 Hz to 150 kHz).

3. **Radiated emissions** refers to the unintentional release of EM energy from an electronic device or apparatus. Emissions are inherent to the switching voltages and currents within any digital circuit. Electronic devices with significant amounts of radiated emissions may interfere with the devices' normal operation or the normal operation of other devices in close proximity. Radiated emission find their origin in the flow of RF current on interconnections and cables. Standards endorsed by RG 1.180 Rev. 2 that cover radiated emissions are MIL-STD- 461G and IEC 61000-6-4. Standards for testing radiated emissions include CISPR 11 and 32 and 47 CFR 15 (FCC).

4. **Radiated immunity (susceptibility)** is a measure of how susceptible a device is to emissions originating from other devices in the surrounding area. Radiated immunity ensures that the device can withstand the emissions of surrounding devices. Interference from other devices' emissions can lead to a host of problems. Standards endorsed by RG 1.180 Rev. 2 that cover radiated immunity include MIL-STD-461G, IEC 61000-4-3, "Testing and Measurement Techniques – Radiated, Radio-Frequency, Electromagnetic Field Immunity Test" (EM far field; electric field), IEC 61000-4-8 (magnetic field), IEC 61000-4-9, "Testing and Measurement Techniques – Impulse Magnetic Field Immunity Test" (magnetic field), and IEC 61000-4-10, "Testing and Measurement Techniques – Damped Oscillatory Magnetic Field Immunity Test" (magnetic field).

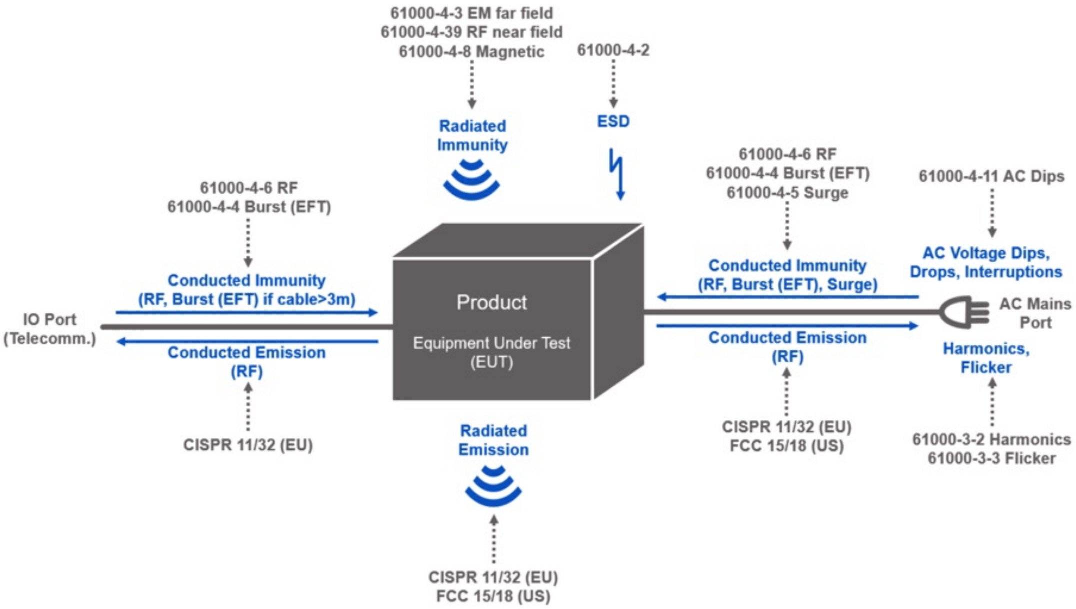


**Figure 1. Types of EMI [5].**

# 2. WIRELESS NETWORKS

Wireless networks include the network system and the elements in that network that make communication possible.

## 2.1 ELEMENTS OF A WIRELESS NETWORK

The essential elements of a wireless communications system are the transmitter, a wireless medium to transmit the signal(s), and the receiver. Antennas are used to transmit and receive the signal(s) and can extend the distance between the transmitter and receiver.

If necessary, the network may use a repeater or nodes to extend the distance from transmitter to receiver. The repeater must also have a receiver and transmitter.

### 2.1.1 Transmitter

A transmitter processes information received from a source, such as a detector (sensor), and then outputs a repeatable, accurate signal. Most transmitters can operate in the presence of certain levels of neutron and gamma radiation. For analog transmitters, such as older hand-held voice radios, a modulation technique is then applied and the information sent out over an RF signal.

For digital transmitters, common in wireless technologies currently in use, the information provided to the transmitter must either be in a digital form or first converted to a digital representation before further processing and transmission over the air. Therefore, if a sensor provides analog information, this data must first be converted to a digital format prior to transmission. Once in a digital format, signal processing is performed involving coding and modulation. Coding[8] and modulation[9] techniques ensure that the desired signal more reliable when exposed to noise (random, unpredictable signals produced by natural processes) and interference (man-made exogenous signals). Coding is a processing operation that makes communication between the transmitter and the receiver more robust. The message is encoded into a sequence of symbols for transmission, which will be decoded back to the original data stream in the receiver. The digital data stream is then translated into a transmittable analog waveform by applying a modulation technique and the information sent out over an RF signal. The ensure compliance with the regulations pertaining to RF emitters, as well as provide the best signal quality for the receiver, the transmitter must ensure that the carrier's transmitted power, frequency, and spectrum bandwidth comply with the specifications established by the appropriate regulatory agencies.

Although not mandatory under the regulations, most transmission standards used in the unlicensed ISM bands[10] divide the total frequency range of the band into several narrower, equally spaced channels

[8] Coding is a processing operation that makes communication between the transmitter and the receiver more robust. The message is encoded into a new sequence of symbols for transmission, and then it is decoded back to the original message in the receiver.

[9] Modulation is the process radios use to transfer information by changing the value of some parameter of the carrier signal. This is also known as *keying* from the early days of wireless telegraphy [9]. The carrier parameter that is varied may be its amplitude (amplitude modulation [AM] or amplitude-shift keying [ASK]), frequency (frequency modulation [FM] or frequency shift keying [FSK]), phase (phase modulation [PM] or phase shift keying [PSK]) or a combination of these, such as quadrature amplitude modulation (QAM), which transfers data by independently changing the amplitude of two carrier waves which are 90° out of phase with each other.

[10] The two specified unlicensed types of bands for the operation of wireless systems are the ISM bands, which include 900 MHz, 2.4 GHz, and 5.8 GHz, and the Unlicensed National Information Infrastructure band, which includes the 5.2 GHz band for broadband access. The FCC issued rules about transmitted power, the use of spread spectrum, and frequency-hopping modulation for wireless devices operating in these frequency bands. Because users in the unlicensed band systems share the same spectrum, there could be interference among all devices operating in those bands.

[6]. For example, devices using 2.4 GHZ frequency bands (e.g., IEEE 802.11 and ISA 100.11a) divide the frequency band into 16 discrete channels (Figure 2). The radio transmitter generates an RF EM wave (the "carrier") centered on one of these channel frequencies, and it superimposes the data signal on the carrier by modulating the input signal.

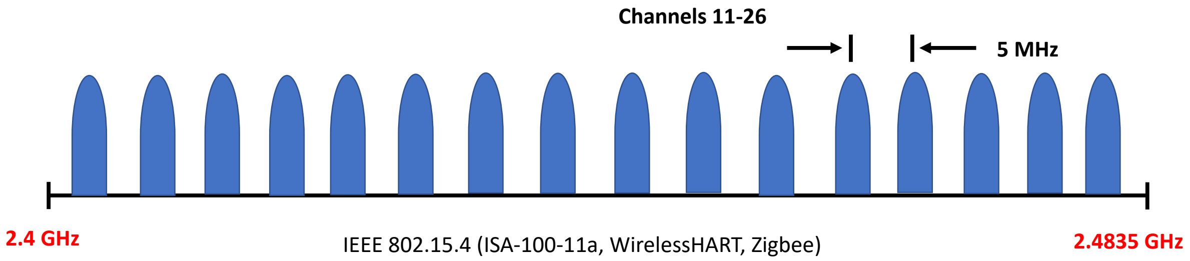


**Figure 2. Frequency channels in the 2.4 GHz range [7, 8].**

Channel width is determined by the amount of information to be transmitted in each time interval and the modulation and filtering design of the wireless device. Higher data rates generally require more channel bandwidth. Regulations set the acceptable channel widths, power levels, and modulation types that may be used in each band. Although regulations do not require ISM band radios to comply with specific frequency plans, the center frequency of the transmitted carriers must be accurate enough to allow transmitters and receivers to link with one another [6].

### 2.1.2 Transmission Medium (Free Space)

Wireless signals can be direct or indirect to the receiver (Figure 3). Transmit times for direct and indirect signals differ and can be recognized by the receiver. Indirect signals can cause coexistence issues for a wireless network. In this project, air is assumed to be the transmission medium that the RF signals will encounter. Due to its low permittivity[11] and permeability[12], it is considered a free space medium.

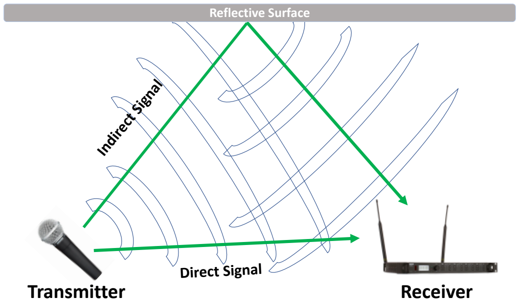


**Figure 3. Wireless signals can be direct or indirect to the receiver.**

[11] The dielectric constant–also called the relative permittivity, indicates how easily a material can become polarized by imposition of an electric field on an insulator. Relative permittivity is the ratio of "the permittivity of a substance to the permittivity of space or vacuum." The relative permittivity of a vacuum is 1 and for dry air is 1.000536.

[12] In electromagnetism, permeability is the measure of magnetization that a material obtains in response to an applied magnetic field. The relative permeability of free space, or vacuum, is 1 and for air is 1.00000037.

### 2.1.3 Receiver

Whereas the transmitter modulates the signal, demodulation is performed by the receiver to strip off the carrier wave and recreate the original message.

The *demodulator* part of the receiver is responsible for determining the performance quality of the radio link. Its prime function is to determine whether the transmitter sent a *one* or a *zero* for every data bit. In the ideal noise-free case, assuming that the full spectrum is transmitted, the demodulated waveform would be made up of perfectly square pulses, so the bit values could be estimated with 100% accuracy. In practice, the filtering applied in the transmitter to force the transmitted signal into compliance with the spectral mask rounds off the square edges of the received data signal. One way to compensate for this effect is to sample the pulses in the middle of the symbol period. In the presence of noise, the waveform is fuzzy to a greater or lesser degree, and the task of making the correct one or zero determination becomes increasingly difficult as the signal power is reduced and/or the noise power is increased [6].

### 2.1.4 Antenna

Each transmitter, node, and receiver may have its own internal or external antenna. Internal antennas can include separate components inside the device case or built on the circuit boards.  External antennas are varied and usually connected to the device through a cable rated for the RF signal and power level.

An antenna's physical characteristics affect its RF radiation patterns. EPRI TR-1003584 [9] shows the radiation and coverage patterns for various antenna types, which are repeated here in Figure 4 through Figure 6. The Electric Power Research Institute (EPRI) also provides a summary of the antenna characteristics that are repeated here in Table 1 [9]. Commonly used antenna types for wireless local area networks (Table 1) include omnidirectional, semidirectional, and directional antennas. These are critical components in a WLAN and directly impact its ability to function efficiently and effectively.

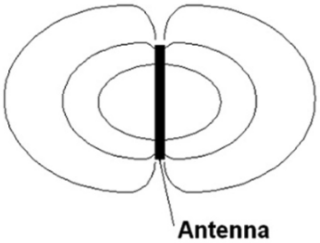


**Figure 4. RF radiation pattern for an omnidirectional antenna.**

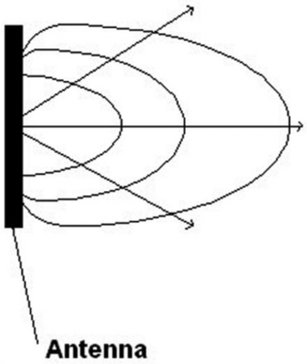


**Figure 5. RF radiation pattern for a semidirectional antenna.**

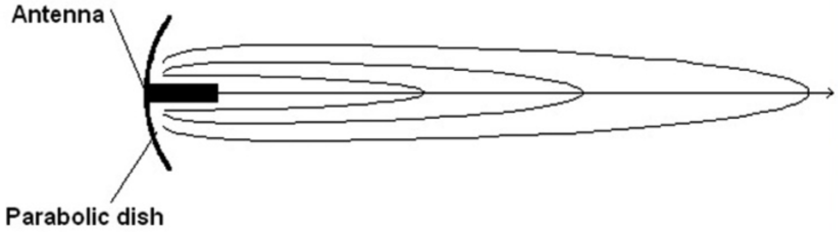


**Figure 6. RF radiation pattern for a highly directional antenna.**

**Table 1. Summary of the three main antenna types**

| Type | Use and application | RF effect |
|---|---|---|
| Omnidirectional | • Dipole antenna, most common for WLAN access points<br>• Also used for point-to-multipoint / hub-and-spoke topology | • RF radiates in all directions in a doughnut-type pattern.<br>• When installed in a multistory building, most of the signal will be concentrated on the same floor, although a significant portion will leak to the floors above and below.<br>• High-gain omnidirectional antennas can offer greater horizontal coverage by limiting coverage leaking. |
| Semidirectional | • Point-to-point, point-to-multipoint, and short- to medium-range applications such as bridging or linking two networks<br>• Also used for indoor coverage applications such as long hallways and narrow facilities | • RF radiation design is a hemispherical or cylindrical coverage pattern. This can improve the reach of the RF signal for short- and medium-range applications.<br>• For certain installations, semidirectional antennas can limit the signal leak to noncoverage areas, potentially increasing security. |
| Highly directional | • Long distance point-to-point applications | • Additional applications include concentrating a signal through building structures (e.g., containment materials).<br>• A signal can be transmitted for miles.<br>• The RF coverage area is typically not suitable for general WLAN users and related client devices. |

A nondirectional antenna, also called an *omnidirectional antenna*, radiates energy more or less uniformly in all directions [10]. This is analogous to how a lighted match or a light bulb radiates light in all directions. The maximum node distance for omnidirectional antennas is 100 m nominal [11].

The range and reliability of a wireless network can be increased using directional antennas [12]. A directional antenna focuses the energy in one direction. Using the light analogy, a directional antenna is similar to a flashlight. A flashlight points most of the light energy in one direction. A flashlight uses a reflector behind the bulb that is shaped to focus the energy on the desired direction. Similarly, reflectors behind an EM energy source create highly directional antennas, as in a satellite dish. The maximum node distance for *directional antennas* is 1 km nominal.

As applications approach maximum distances, latency requirements may become more difficult to achieve with some technologies.

Antennas can be used to transmit and receive information. The *transmit antenna* may be located internally as a printed circuit board trace or a lumped element component on the board, externally on the transmitter housing, or remotely, connected by a coaxial cable. The transmit antenna acts as the coupling mechanism between the transmission line and free space, allowing the carrier wave to radiate outwards from the transmitter location [6]. The antenna determines the polarization of the wave and may also focus and direct it in a desired direction.

At the other end of the link, a fraction of the energy in the original wave is picked up by the *receive antenna*, which, like the transmit antenna, may be located internally as a printed circuit board trace or a as a lumped element component on the board, externally on the receiver housing, or remotely, connected by a coaxial cable. Depending on the specific application and constraints on physical size, the receive antenna design may be directional to maximize the signal power received from a fixed direction, or it may be omnidirectional to allow reception from any direction [6]. In general, larger antennas will be more directional and will capture more energy from the received wave (i.e., have higher gain). In one-way links, in which antenna gain is not constrained by the limits on transmitted effective isotopically radiated power (EIRP), high-gain receive antennas can be used to achieve very long-range reception.

*Antenna gain* is the ratio of the power emitted by a given antenna as measured at a point along the line of maximum power to the power which would be measured at the same point if transmitted by a hypothetical (spherically omnidirectional) isotropic radiator, which radiates uniformly in all directions. Antenna gain is expressed in dBi, or decibels relative to an isotropic source. In free space, the power density in the transmitted beam decreases in inverse proportion to the square of the distance from the transmitter.

#### 2.1.4.1 Antenna Categories

There are two broad categories of antenna systems—discrete antenna (single-point) systems, and distributed antenna (multipoint) systems [10]. Discrete antenna systems are often made of simple pieces of wire. There are two types of discrete antennas—directional and nondirectional [10]. As discussed earlier, a nondirectional antenna is an *omnidirectional antenna*, radiating energy more or less uniformly in all directions. On the other hand, a directional antenna focuses the energy in one direction. Using the light analogy, a directional antenna is similar to a flashlight. A flashlight points most of the light energy in one direction. A flashlight uses a reflector behind the bulb that is shaped to focus the energy on the desired direction. Similarly, reflectors behind an EM energy source create highly directional antennas, as in a satellite dish.

In most discrete antenna systems, the same antenna used to transmit the RF signal from the transmitter also receives the RF signal for the receiver. However, a combined antenna cannot transmit and receive at the same time on the single antenna. To get around this issue, some systems use separate antennas for the transmitting and receiving functions [10].

There are other limits to a discrete antenna. For example, a discrete antenna has a limited and localized physical size. In addition, the dimensions of the antenna are much smaller than the coverage area or coverage range.

The other broad category of antenna systems is the *distributed antenna system* (DAS). Unlike a discrete antenna system, in which the energy is transmitted and received at one location, a DAS distributes the energy over a broad area, and the antenna system can be quite large. For years, DAS has been popular for providing radio coverage in confined spaces such as tunnels. More recently, DAS has been used to provide cellular radio coverage inside large buildings and other hard-to-reach areas such as parking garages. Given this history, DASs are good candidates for applications in underground mining [10].

Most DAS applications create a continuous coverage area by providing many overlapping radiation points or continuous radiation along the length of the system. The leaky feeder system discussed in the next section is an example of a DAS with continuous radiation along the length of the system. However, the use of exclusion zones in an NPP, in which physical distance used to protect a vulnerable system attenuates an RF signal to a sufficiently low level to protect systems, may complicate the adoption and use of DAS implementations.

Additionally, NPPs may use the concept of a physical RF protection zone. Similar to exclusion zones, and perhaps interchangeable in some situations, the RF protection zone also relies on physical distance to attenuate RF signals to the point that they are background level and thus unreadable: a weak signal solution. This is a method to address security concerns – such a preventing unauthorized reception of the signal. As a DAS distributes the energy over a broad area, the antenna system can be quite large, unlike a discrete antenna system in which the energy is transmitted and received at one location. Thus, the protective boundary could be quite significant. Still, the use of advanced signal processing techniques and high gain antennas can allow reception of extremely weak signals at great distances. In general, it has been shown that simply using a physical boundary is inadequate to ensuring wireless security.

An important limitation of a DAS is that parts of the system require power to boost or amplify the signal [10]. As the signal travels along the length of the DAS, energy is lost as a result of the energy radiated along the length. To offset this loss, electrical power is required for the amplifiers within the DAS to boost the signal. This need for available power and the issues related to safely handling this power have presented problems and are limiting factors for certain implementations such as the use of a DAS in an underground coal mine.

Another limitation of DAS is that it receives the signal along its entire length, so it is also receiving noise over its entire length [10]. Noise can reduce the coverage range of a system; therefore, the cumulative noise can limit the size of a DAS.

#### 2.1.4.2 Antenna Siting

The effectiveness of any antenna is directly related to how it is located. The siting process is a very important part of the design and implementation of any wireless system. Even for a device with an internal antenna, where placement of that antenna is set by the manufacturer, the subsequent positioning of the device or for a handheld device, how it is held, can greatly impact how well the intended communication function is performed.

As for external antennas, there are even more aspects to consider. Recommended best practices for installing an antenna include the following [9]:

- Notice the location and composition of building materials, equipment, and other obstructions near the antenna. Reposition antennas and measure results to optimize signal strength and coverage. Do not place antennas near metal objects such as filing cabinets, railings, I-beams, pipes, ceiling trusses, or heating, ventilation and air conditioning (HVAC) ducts.

- Install each antenna more than one-half wavelength above the ground or another horizontal conducting medium such as roofing material.

- When placing multiple antennas on the same mast, separate the antennas by at least one meter to mitigate signal degradation.

- Install antennas in accessible, maintainable areas.

- Check with local building codes and regulatory agencies concerning safety and aesthetic requirements. Consider line-of-sight requirements and related antenna mast aesthetics.

- Be aware that placing access point antennas more than 100 feet above the ground exposes them to greater amounts of interference. Other factors associated with high placement include feed line losses, zoning restrictions, and potential Federal Aviation Administration (FAA) lighting requirements.

- Think 3D by visualizing horizontal and vertical antenna radiation patterns and attempt to contain signals to the desired coverage area.

- Minimize coaxial cabling and consider relocating access points and data cables to minimize dB signal loss and interference.

- Document and diagram antenna configurations.

- Be skeptical of range estimates supplied in vendor data sheets.

- Without field-testing, assume one-half the estimated coverage to allow for error and unforeseen application issues.

### 2.1.5 Other Wireless Network Elements

Other elements of a wireless network, including transceivers, sensor nodes and repeaters, are discussed below.

#### 2.1.5.1 Transceiver

A transceiver is a communications element that combines elements of a transmitter and receiver. Like receivers, transceivers are used to pick up the RF signals, demodulate, decode, and transfer the information to a processing element. Similarly, the transceiver also performs the transmitter functions to include signal processing, coding, and modulation prior to sending the RF to an antenna. Hand-held transceivers include cellular telephones, security guard transceivers, and citizen's band radios.

Portable transceivers represent the greatest radiated continuous wave (CW) electric field threat at a plant [13]. Large transceiver-induced electric field signals were recorded at both Zion and Turkey Point. The data obtained at Zion are likely not being properly interpreted in comparison to the susceptibility test levels specified in MIL-STD-461C [15] or PMC 33.1 [14]. The radiated susceptibility test RS02 in MIL-STD-461C imposes a narrow-band signal measured according to procedure with a narrow-band conventional voltmeter instrument, so comparison to broad-band data is not appropriate [13]. However, MIL-STD-461G notes that the concept of classification of emissions as broadband or narrowband in favor of fixed bandwidths and single limits was changed from previous version of this standard because emission classification was a controversial area often poorly understood and handled inconsistently among different facilities. In addition, the numbering was changed in MIL-STD-461D and reflects that in use today (e.g., RS102).

#### 2.1.5.2 Wireless sensor node

A sensor node typically has several parts: a radio transceiver (communication function) with an internal antenna or connection to an external antenna, a microcontroller (computing function), an electronic circuit for interfacing with the sensors (sensing function), and an energy source, which is usually a battery or an embedded form of energy harvesting, although external power connections are also used.

The sensing unit consists of a sensor that converts the phenomenon measured into an equivalent electrical signal. The output of the sensor goes to the computing section that converts the analog signal to a discrete time signal. The discrete time signal is routed to a processor that provides the output as a digital signal. last section of the sensor node's architecture is responsible for the communication function. Depending on the data rate requirements and the communication range needed, a suitable module (i.e., Bluetooth, ZigBee, etc.) for the wireless communication function can be selected. A power unit can be common to all three sections: sensing, computing, and communication [16].

Information from the sensor nodes and a gateway or hub may also be shared in many network topologies, such as a mesh network.  This sharing allows for a more decentralized and flexible network architecture and can improve overall reliability.

Further development and advancement of wireless sensor nodes will lead to increased sensing, processing, and wireless communication capabilities. In general, wireless sensor nodes can minimize radiation exposure to workers and provide significant increases in the availability of data for monitoring and analyses.  Additionally, self-powered wireless sensor nodes can offer significant expansion in the remote monitoring capabilities at nuclear facilities, providing important data on plant equipment and component status during normal operation, as well as during abnormal operation or station blackouts and for post-accident evaluation.

#### 2.1.5.3 Repeater

A repeater receives a low power signal (due to attenuation or low initial transmission power) and retransmits an amplified version of the signal to extend the range of the transmission [17]. Repeaters can be used to extend the range of the network, and the use of repeaters and multiple antennas can ensure the needed signal strength for reliable communication. Repeater spacing varies with frequency, transmitter output power, antenna gain, antenna height, receiver sensitivity, and other factors [7].

## 2.2 TYPES OF WIRELESS NETWORKS

Wireless communication networks include WLANs, wireless personal area network (WPANs), wireless metropolitan area networks (WMAN), wireless wide-area network (W-WAN), low-power wide-area Network (LoRa-WAN) and satellite. WPAN and WLAN have increased cost/complexity while providing greater data rates. WMAN has increased cost/complexity but does not support higher data rates. At the high end is the W-WAN. Not surprisingly, satellite is the most costly and complex and requires the largest amount of power. Appendix A identifies the most common wireless communication networks, costs, and transmission rates.

Many countries and standards bodies have standards that address the use of wireless systems and networks. International and domestic standards define test setups, testing techniques, test equipment, test environment and other considerations regarding EMC emission testing, immunity testing, and measurement (Appendix B). The classifications and descriptions of different EM environments and compatibility levels are also provided. In some standards, the installation and mitigation guidelines regarding earthing and cabling, mitigation of external EM influences, high-altitude EM pulse (HEMP) protection concepts, and so on, are provided. Although the standards endorsed in RG 1.180 are related to testing associated with EMI/RFI and the exclusion zone distance, these standard bodies and their standards were identified to inform the identification and selection of standards related to wireless networks unrelated to RG 1.180.

## 2.3 WIRELESS COMMUNICATION PROTOCOLS

Wireless protocols enable reliable and efficient communication between devices on a network by defining how the data is transmitted and received. Most of these protocols require some type of wireless network access (e.g., cellular, personal area, local area, wide area, mesh, ad-hoc) based on wireless standards. Appendix C provides an overview of the protocols. The standards that cover the wireless protocols include Wi-Fi (IEEE 802.11a, b, e, g, i, and n), Bluetooth (IEEE 802.15.1), ultra-wideband (UWB) (802.15.3), ZigBee (IEEE 802.15.4), WirelessHART (IEEE 802.15.4), WiMax (IEEE 802.16) and ISA-100.11a. Most of these wireless systems operate in the unlicensed FCC frequency bands (900 MHz, 2.4 GHz, and 5.9 GHz) or in the cellular telephone bands (800 MHz and 1.9 GHz). Long-term evolution (LTE) is also called *3.95G* and has been marketed as 4G LTE and Advanced 4G.

5G is the fifth-generation technology standard for broadband cellular networks, which cellular phone companies began deploying worldwide in 2019, and is the planned successor to the 4G networks. The industry consortium setting standards for 5G, the 3rd Generation Partnership Project (3GPP)[13], defines 5G as any system using 5G NR (5G New Radio) software.

From a review of wireless uses at NPPs, the most common protocols applications are the 802.11 and 802.15.4 IEEE standards.

## 2.4 ADVANTAGES / DISADVANTAGES OF WIRELESS SYSTEMS

Many equipment manufacturers for the nuclear industry offer components that include embedded digital devices with wireless communication capabilities and wireless sensors. For example, wireless self-powered sensor nodes can offer significant expansion in remote monitoring at nuclear facilities and can be used to obtain important data on plant equipment and component status during normal and abnormal operation and for post-accident evaluation [18].

Wireless technology has not traditionally been used in NPPs in SR/ITS applications, mainly because of restrictions in safety and security. One of the major concerns is the impact from EMI/RFI and safety function’s vulnerability to wireless transmissions. If a wireless network is implemented, it would be required to maintain, at a minimum, the same level of safety as a wired system and address security (cybersecurity), EMI/RFI, and coexistence issues.

There are potentially significant cost benefits as a result of using wireless technologies. The wiring that connects an instrument’s output signal to a control or monitoring system often makes up a significant part of the total cost (Figure 7). If sensor signals are processed locally and actionable information is passed wirelessly to a receiver and then to the plant control and/or safety systems, when necessary, then wireless networks can significantly reduce installation and maintenance costs. Furthermore, sensors and transmitters can be installed in remote or inaccessible locations. Because there are thousands of miles of cables in each reactor [19], cable pulling costs of up to $2,000/ft [20, 21] require a significant investment in traditional wired systems. In addition, the organic electrical insulation used on cables is combustible and has a lifetime shorter than that of an NPP, so maintenance efforts must include cable pulling and replacement. Routing cables across plant boundaries can also create fire vulnerabilities, so this is also a

[13] The 3rd Generation Partnership Project (3GPP) is an umbrella term for a number of standards organizations which develop protocols for mobile telecommunications. The seven 3GPP Organizational Partners are from Asia, Europe and North America.

significant incentive to use wireless technology. To licensees, cost (and cost savings) is a major factor in determining how to allocate available funding. The lower costs associated with wireless networks increases a licensee's interest in and likelihood of using such networks; however, regulatory uncertainty in what and where wireless networks may be used may be a limiting factor in their potential use.

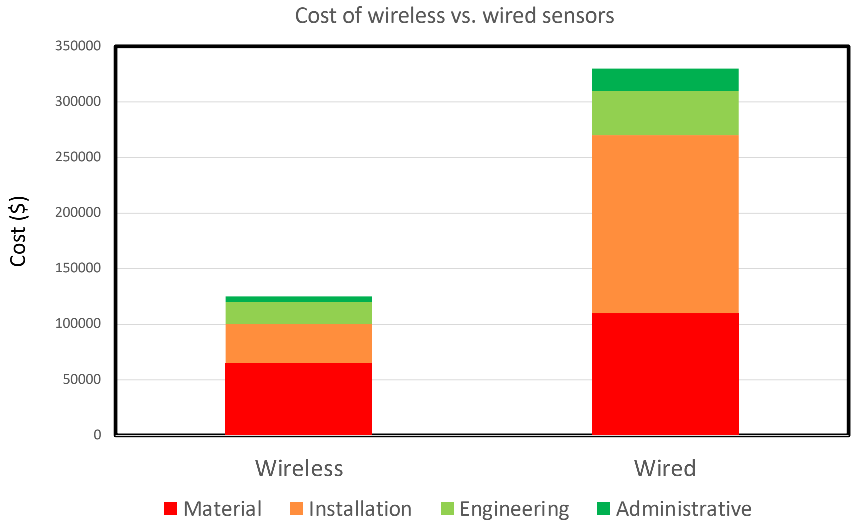


**Figure 7. Cost of wired vs. wireless sensors [22].**

According to the EPRI [23], wireless systems can enhance NPP safety by improving general operational awareness, providing monitoring operations in remote areas, and increasing the mobility and flexibility of plant personnel. Another significant benefit of wireless networks is their potential to lower occupational exposures to plant personnel and to maintain such exposures to levels that are as low as reasonably achievable (ALARA). This is accomplished by tracking personnel and exposure at key locations (such as in the reactor, fuel, turbine, and control buildings) more frequently than has typically been possible in the past.

Wireless systems offer the following advantages when compared to wired systems [7, 24]:

- Less expensive installation costs because there is no need to design or install cables, resulting in lower installation costs, reduced connector failures, lower maintenance costs, and enhanced convenience of use.

- Easier installation because wireless capabilities are usually embedded in devices (i.e., rapid deployment).

- Easier network expansion, modifications, and maintenance.

- Can often be installed by less experienced technicians.

- More portable, so equipment can easily be moved from one spot to another (i.e., increased mobility).

- Easier access in difficult locations.

- Capabilities for automatic connection to an existing wireless network with only the appropriate security features enabled.

Increasing numbers of wireless communications systems have been deployed for monitoring purposes in industrial environments and nuclear facilities. Their use in nonsafety-related applications can inform expansion into SR/ITS systems.

Disadvantages identified by industry include the following [7, 23, 24]:

- EM interception of wireless signals can (1) allow unauthorized access to transmissions within the system's normal transmission range or (2) cause system failures (action/inaction).

- EMI from deliberate or inadvertent external EMI sources can completely block (jam) data transmission, or it can slow transmissions by corrupting the received signal resulting in bit errors and causing the wireless system to retransmit messages.

- RF signal coverage problems from topology constraints can cause weak, faded signals, leading to failed transmissions, loss of critical data, optimization of control and communications, coding, and timing.

- RFI from wireless equipment can affect other equipment or other wireless systems (i.e., interference).

- Information-saturating radio waves can impede transmission (i.e., information is not transmitted via known dedicated cable routes, but information is spread to the whole space and even behind walls).

- Network safety and security issues increase vulnerability to cybersecurity threats, eavesdropping, unauthorized use, and jamming.

- Vulnerability to unauthorized use is increased.

- Wireless systems typically have lower communication speeds.

- Radiation effects can potentially impair wireless devices (note however that radiation affects all electronic equipment—wired and wireless).

- Congestion of unlicensed frequencies can cause delays in data exchanges.

- System design and integration of wireless systems into industrial communications networks are not as well established or tested.

- Concerns exist regarding the fault tolerance, redundancy, retrofitting, and reliable implementations of wireless systems.

- Reliance on battery power can add to the unreliability of the wireless equipment; batteries can run out of energy before expected or can fail without warning.

- Protocol standards for wireless technologies do not always include all the security requirements or complete specifications to ensure total interoperability.

- Different consensus practices and network topologies can result in interference.
- Susceptibility to lightning surges and switching surges [25, 26] increases risk.

## 2.5 FACTORS IN IMPLEMENTING WIRELESS NETWORKS

In general, wireless devices are less susceptible to electromagnetic (EM) events because they do not have long cables attached, unlike wired supervisory control and data acquisition (SCADA) equipment which can have varying levels of susceptibility. Long cable runs over areas between plant buildings, whether buried or above ground, can also exhibit susceptibility to such events. However, wireless networks still have some susceptibility as they have power cables connected as well as antennas that can pick up the EM energy, especially if they are located in an exposed area.

ORNL and EPRI are analyzing cellular LTE vulnerability. More specifically, ORNL is researching this topic as part of the Grid Modernization Laboratory Consortium (GMLC) project, assessing the vulnerability of power generation critical systems. Published work in this area is limited.

Three concerns addressed in Appendix D regarding the implementation of wireless technologies in research reactors and NPPs include EMI/RFI, cybersecurity, and installation issues [27].

## 2.6 DESIGN / INSTALLATION ISSUES

The installation of a wireless network can greatly increase RF emissions, potentially affecting existing devices susceptible to or not immune from those emissions. Installation of additional devices can also introduce new failure modes into the system. Most of these issues are addressed in Appendix D, and they include EMC, improper communication range, environment, multipath propagation packet loss, network latency, network jitter, measurement data quality, fading, burst error, phase shift keying/frequency shift keying corruption, and high voltage standing wave ratio.

Wireless networks can include different elements, can be arranged in different ways, can use different protocols and standards, and can have different failure modes. Each of these factors must be understood to properly assess the robustness of a wireless network. To adequately assess the impact of wireless networks requires that each individual protocol in use be assessed, because each protocol addresses the disadvantages identified above in different ways, possibly affecting normal plant operations.

Wireless sensor networks (WSNs) connect a significant number of devices or sensors wirelessly to the internet of things (IoT), and they also monitor and control systems. A WSN is a network of devices that can communicate the information gathered from a monitored field through wireless links. A WSN is built of wireless sensor nodes. These nodes, discussed earlier, typically have several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors, an energy source, which is usually a battery or an embedded form of energy harvesting and a sensor. Different sensors may be used depending on requirements but are generally a device that responds and detects some type of input from physical or environmental conditions such as pressure, heat, or light. The sensor's output is usually an electrical signal that is delivered to a controller for further processing. WSN data are forwarded through multiple nodes, and with a gateway, the data can be connected to other networks like wireless ethernet or the plant local area network (LAN).

Wireless sensors are becoming very popular in industrial processes for measurement and control, condition monitoring, predictive maintenance, and management of operational transients and accidents. Many sensor manufacturers have teamed with manufacturers of wireless transmitters, receivers, and network equipment to provide industrial facilities with integrated networks of wireless sensors that measure process temperature, pressure, vibration, humidity, and other parameters to improve process safety and efficiency, increase output, and optimize maintenance activities [27].

The host of the WSN obtains the process variable's value and health information from the wireless sensor via a wireless network gateway or access point. Variable health information is used to validate the quality and timeliness of the value. The WSN must include a means to ensure that data are accurate and timely and should be designed to respond appropriately when stale or suspect data are detected.

The use of wireless communications for online monitoring and control also can generate data which can be fed into a system model to provide early warning of impending failure or degradation. According to Rasmussen [28], several requirements must be met for these capabilities to be available:

- Differentiability: Various failure modes or degradation mechanisms for a component or piece of equipment must be differentiable from one another to ensure that the diagnosis is accurate and unambiguous.

- Anomalous: Indications of an anomalous or unusual condition must be identifiable by an online monitoring (OLM) model.

- Repeatability: All occurrences of a given degradation mechanism or failure must consistently produce the same precursor indications.

- Timeliness: Indications must occur and be properly identified with enough lead time to provide some advantage (e.g., event avoidance).

## 2.7 NEW FAILURE MODES

The special nature of wireless network designs compared to hard-wired systems could introduce the potential for unintended behaviors, increased vulnerabilities, and subtle or new failure modes. However, it is expected that the I&C portion of the wireless system will likely behave and fail just like other I&C systems and components [29]. Appendix F provides a list of failure modes for wireless systems.

Increasing the size and complexity of the wireless network will introduce new failure modes compared to single-use setups. Each sensor setup must be able to reliably transmit and receive the data in the presence of other sensor systems from different vendors using the same or different protocols and must operate using the same or different frequencies.

Although both analog and digital equipment are susceptible to EMI, digital equipment responds to EMI differently from analog equipment. The risk of EMI failures could be greater in a wireless network because the network must be able to co-exist in an environment of multiple sensor systems, each of which transmits RF signals and can be a source of EMI/RFI to other components.

Although response time is an issue for both wireless/wired and analog/digital systems, the issues for digital vs. analog are different. The wireless digital network must be configured to fail safely upon loss of the wireless signal. The system timeout must allow enough time to address the redundancy of radio media. The requirements for multiple, simultaneous access to the RF channel from multiple sources can result in slower data transmission. This slower data transmission, which can affect wireless and wired networks, can be caused by slower processing rates, corruption of data due to interference, excessive network traffic to the receiver causing a denial of service to the network, competition of communication protocols that may allow coexistence or that may interfere, and operability issues.

The signal strength from the transmitter or at the receiver may be weak. This can be caused by misaligned systems, too great a distance from the transmitter, interference, or power degradation.

Modulation and coding techniques help the desired signal maintain its integrity or fidelity when exposed to noise (random and unpredictable signals produced by natural processes) and interference (man-made exogenous signals). Besides demodulating and decoding the received signal, the receiver might also amplify and filter it in preparation for delivery to the intended recipient.

A human interface should be able to call up and display data rapidly—generally, a screen of data should be displayed/refreshed in less than two seconds. Wireless networks can be orders of magnitude too slow to satisfy display call-up times, so a data cache is often implemented at the host end of the wireless communication path to satisfy response-time specifications [30].

As a rule, wireless networks experience more issues with packet loss than wired networks. RFI, weaker signals, distance, and physical barriers such as walls can cause wireless networks to drop packets. This problem does also exist in wired networks as faulty cables can impede signal flow.

To summarize, although some of the failure modes provided in Table 2 can occur in wired systems, these failure modes are more pronounced in wireless systems.

**Table 2. Failure modes of concern in wireless networks**

| Failure mode |
|---|
| Failure of multiple sensor/transmitter/receiver combinations |
| Corrupted data caused by interference from collocated transmitters |
| Loss of wireless signal |
| Slower data transmission caused by multiple and simultaneous access needs |
| Weak signal (misaligned system, too great a distance, power degradation, interference) |
| Noise (natural and man-made) |
| Increased packet loss |

## 2.8 CURRENT INTEREST AND OPERATING EXPERIENCE

Traditionally NPPs use wired communications in their I&C systems and operations. When many of the NPPs currently in operation were built, there were no feasible solutions for wireless systems. The nuclear industry has been reluctant to implement wireless technology, and although its use is increasing, the transition is a slow process. As discussed, issues of concern include infrastructure, regulatory issues regarding safety and reliability, introducing new avenues for plant cybersecurity threats, and the potential for EMI/RFI with plant safety systems. Over the years, however, wireless communication technologies have evolved and now offer many solutions for data transfer, audio and visual communication, monitoring and control, and surveillance. Many other industries have demonstrated the benefits of their use [8, 31].

As a result, there is significant interest within the nuclear industry to implement wireless technology in applications that can enhance plant safety or reduce maintenance costs. This can include vibration monitoring used in predictive maintenance or reduced test setup time for specific equipment surveillance activities. Numerous wireless pilot projects are illustrating the possibilities. Still, wireless technology changes very rapidly, which can lead to hesitation to procure equipment that may rapidly become obsolete.

There are many reasons why modern wireless technology implementations can provide more acceptable solutions for use at NPPs. For example, modern systems generally operate at higher frequencies and at significantly lower effective power output levels than ultrahigh frequency (UHF)/very high frequency (VHF) communication systems. This feature of more modern wireless devices, including WLANs, generally requires that the end user be closer to a potentially sensitive device before interference is noted, thus decreasing the potential for impacts to SR/ITS systems. EPRI guidelines for wireless technology in power plants note the following [23]:

> *Wireless technologies have many applications in the power industry, including cellular phone systems, paging systems, two-way radio communication systems, work tracking systems, operator logs, and remote radiation protection monitoring. The potential benefits of implementing wireless technology are substantial and continue to increase as the technology rapidly evolves. . .*
>
> *Wireless technology applications for data/voice/video integration, remote equipment monitoring, outage management, and work process control have the potential to vastly improve plant productivity, reliability, and safety.*

However, the guidelines caution that any significant implementation of wireless technology in an NPP must be weighed carefully.

EPRI guidelines detail a step-by-step approach to implementing wireless technology compliant with current regulations, including under the 10 CFR 50.59 process. The guidelines address specific concerns faced by operators choosing to implement wireless technology: EMI/RFI issues, wireless security, the plant design modification process, network design, vendor selection, and change management.

In its review of wireless systems, EPRI also specifically discussed security threats to a wireless network as a concern. Potential cybersecurity threats identified include sniffing, denial of service, and man-in-the-middle attacks.

### 2.8.1 RFI Events at NPPs

In 2002, EPRI noted [23] that a search for the words "radio" and "trip" in the Institute of Nuclear Power Operations (INPO) operating experience event database identified over 300 records. Of the 300 events documented in INPO's database, more than 20 of events were plant trips that have occurred since 1984. [The INPO database search appears to cover 1984-2000.] Data on the events are not provided in the report however, the report notes that cellular phones interfering with personal electronic dosimeters used to track personnel radiation dose are an example of more modern technology causing RFI interference problems. The report also notes that "While some plant licensees have elected to modify equipment sensitive to RF energy, most have relied upon administrative controls to minimize the potential threat of RF interference with plant equipment by prohibiting or restricting the use of RF devices in areas of the plant that have potentially sensitive instrumentation and controls."

Ten years later, EPRI identified 20 EMI-related interference events that occurred between 2000-2011 and were I&C related [32]. Of these 20, one was caused by welding in a cable room, and 11 were dosimeter-related events – two welding related, eight cell phone related, and one from a microwave oven. Only the remaining eight are relevant to this discussion. Four were caused by keying walkie-talkies, two had unknown sources that could have been EMI, although the source is unknown, and two were caused by short circuits of EMI filters.

The following events that occurred at other NPPs since the publication of IN 83-83 show that flash photography can cause radiated emissions that can disrupt digital equipment in the area:

- In another instance, a maintenance planner was taking photographs inside a fire protection panel [33]. Consequently, the $CO_2$ discharge system started its actuation sequence. Plant personnel and the equipment vendor reported that the EMI initiated by the camera operation caused the system actuation. The vendor noted that the system is only vulnerable to EMI disturbances when the enclosure door is open.

- Flash photography, which was taking place in the control room, caused the inadvertent actuation of the Halon Fire Suppression System [33]. This forced the evacuation of the Control Room. Haddam Neck was defueled and preparing for decommissioning at the time. At the time of the event, an electrician was conducting tests at the fire detection system (FDS) panel and a training department representative was taking pictures of the fire system indicators and controls to develop training aids. The light from the camera flash affected an electronic programmable read-only memory (EPROM) microprocessor located inside the Halon FDS control panel. This camera flash caused the normal one minute delay to be bypassed and resulted in an (almost) immediate actuation of the Halon system. The vendor noted that the system is only vulnerable to EMI disturbances when the enclosure door is open. This event prompted the NRC to issue IN 97-82 [34].

- A maintenance planner was taking flash photography of boiler feed pump signal processor power supplies at the Indian Point NPP [33]. The planner was working 18–24 inches from the equipment. Subsequently, one of the boiler feed pumps rapidly decreased in speed to 2,400 revolutions per minute. Control room alarms were initiated, and the licensed plant operator manually initiated a reactor trip. Plant personnel eventually concluded the root cause of pump runback was the radiated emissions generated from the capacitive discharge of the flash tube on the digital zoom camera close to the pump's signal processor power supply.

- Another plant reported failure of non-class 1E instrument air dryer controls when a photograph was taken of the control panel [33]. Investigation determined light from a digital camera flash caused an unpredicted perturbation of the dryer controls electronic EPROM.

EPROMs are used in many other plant systems and not just in the FDS discussed above. Some examples provided in IN 97-82 include security E-fields, Foxboro Spec 200 controllers, smoke detectors and other fire protection systems, battery chargers and inverters, Terry Turbine controls, and emergency diesel generator controls. Therefore, the possibility exists that ambient light or a source such as a camera flash could cause an erasure of programming, unexpected initiation, or have some other unintended effect on plant systems if the window on the EPROM is not sufficiently shielded.

It appears that after the walkie-talkie events in the early 1980s and the issuance of IN 83-83, the strict controls on the use of RF emitters such as cell phones, walkie-talkies, and welding has been successful in minimizing the number of RFI events. This experience shows that the high-power output from walkie-talkies can cause disruptions in I&C systems and that when cell phones are close to I&C equipment, they can also cause disruptions.

### 2.8.2 RFI Events in Other Industries

Examples of interference events in other industries include interference from 5G, interference among medical devices, and US Navy radar shutting down SCADA systems at nearby industrial facilities. The Maroochy Sire sewage spill was caused by a disgruntled former employee that used a copy of the control system to wirelessly alter system alignments and operations. Another disgruntled employee at a car dealership remotely disabled customers' cars. These events are discussed in Appendix G.

### 2.8.3 Current Applications in NPPs

Current wireless technology at NPPs is primarily used in the following seven applications (Appendix H):

- Voice communications,
- Data communications through laptops and PDAs,
- Wireless dosimetry,
- Camera monitoring,
- Heavy equipment operation,
- Equipment condition monitoring, and
- Process monitoring.

An ISA100 meeting presented the results of a survey that showed the percentage and how wireless technology was used in NPPs (Figure 8) [22]. [It is unknown if equipment monitoring includes process monitoring in Figure 8, but the two processes were separated for our listing of applications.]

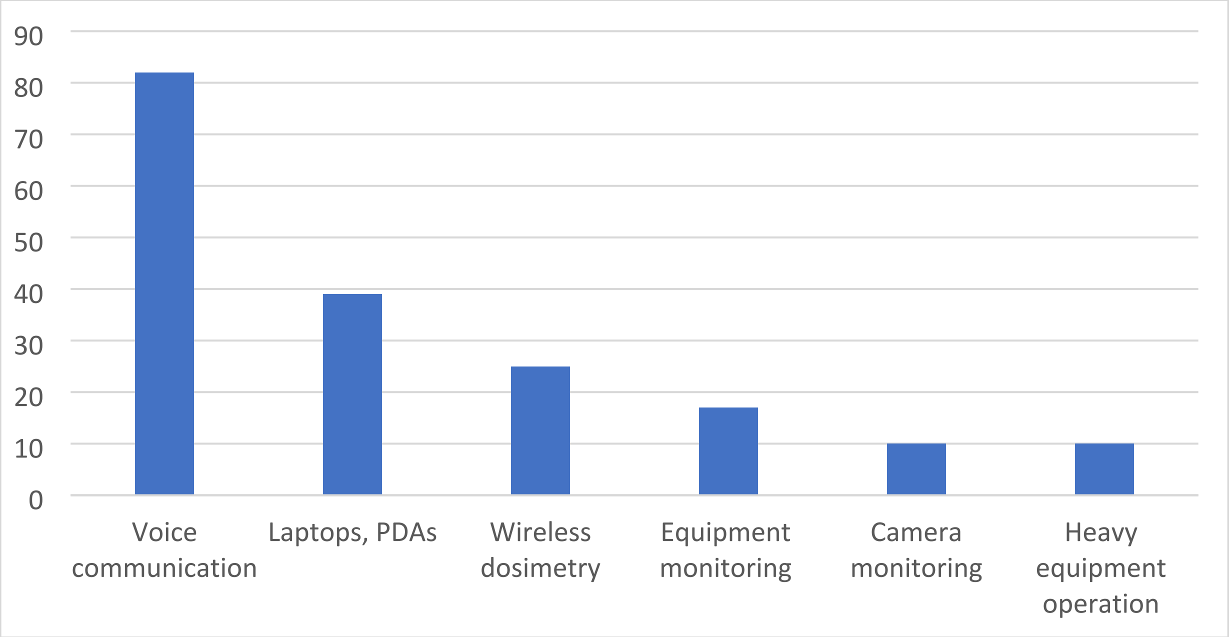


**Figure 8. Uses of wireless technology in nuclear facilities.**

The priority order from nuclear workers in Korea for wireless technology applications showed that voice and data communications are at the top of the list, as are wireless dosimetry, equipment monitoring, and camera monitoring [35]:

- Voice and data communication (30.2%),
- Exposure dose measurement systems (26.8%),
- Component monitoring and instrumentation (24.0%), and
- Wireless cameras (19%)

Most wireless systems in NPPs are targeted for nonsafety-related applications. These applications must be based on existing and emerging wireless standards to ensure interoperability among devices [8]. The type of wireless technology and how it is used can change as the operating modes change from normal operation, outage, service operations before decommissioning, or emergency operations [24].

Specific examples of wireless technologies at NPPs (Appendix H) include its uses at Comanche Peak, Arkansas Nuclear One (ANO), Diablo Canyon, Farley, San Onofre Nuclear Generating Station (SONGS) and South Texas Project (STP). Other examples include the Massachusetts Institute of Technology (MIT) research reactor, and external to the US  the Ignalina Nuclear Power Plant (INPP), and advancements in Canada.

Appendix H also provides further information on some of these applications in non-nuclear industries.

There are numerous wireless devices in a test or trial phase at this writing that could have significant benefit to NPP utilities (also in Appendix H). Successful test conclusions may then lead to a push for more wireless technology to be incorporated in NPPs, creating additional information paths to the operator or to other analytical devices.

The combination of new wireless technology and networks joined with online monitoring could represent a "paradigm shift" in the ability to detect incipient faults more reliably. In a recently completed study, advanced online monitoring was shown more effective in detecting equipment failure modes with the addition of wireless vibration sensors when combined with conventional wired-sensors: 45% of the failure modes versus 11% without the new sensor [21].

Appendix H also discusses some of the wireless applications in the non-nuclear industry.

### 2.8.4 Lessons Learned

The typical NPP environment includes many sources of electrical noise. Examples of EMI/RFI sources include hand-held two-way radios, smartphones, industrial wireless devices, arc welders, switching for large inductive loads, high fault currents, and high-energy fast transients associated with switching at the generator or transmission voltage levels. Lessons learned show the exclusion zone distances can be set using calculated distances or detailed emissions maps. Methods also exist to mitigate vulnerabilities to RF.

In a seminar series on wireless technologies, AMS discussed its development of a cognitive radio system [31] with the ability to generate and output multiple wireless signals (e.g., Wi-Fi, Bluetooth, and cellular communications at varying power levels and frequencies). The system is used to test equipment for EMI/RFI susceptibility in training areas and in actual plant environments.

In another seminar series on wireless technologies, AMS [36] discusses sensitive equipment EMI/RFI exclusion zones, noting that in their experience, these zones are conservative because portable wireless devices do not typically cause interference with plant systems. The AMS process for reducing exclusion distances includes walkdowns to identify equipment that may be susceptible to EMI/RFI and mapping of NPPs to characterize the EMI/RFI environment. AMS also performs in-situ immunity testing to verify that NPP equipment can withstand signals from wireless devices. At a Diablo Canyon NPP project, AMS was able to mitigate all vulnerabilities through the use of metallic fabric shielding.

EPRI guidelines [37] note that EMI/RFI concerns regarding the safe, reliable operation of digital equipment have resulted in requirements for utilities to create detailed emissions maps. EPRI has identified typical emissions sources in NPPs, recommended susceptibility and emissions standards, and detailed design and layout practices for minimizing susceptibility to EMI/RFI.

STUK, the Radiation and Nuclear Safety Authority of Finland [38], recommends that an RF table be created for NPP EMI/RFI specifications and qualification listing all RF emissions allowed on an NPP site, including the highest permissible field intensities. Advisably, the RF table should indicate the maximum permissible transmission power levels for a specific device type, such as mobile phones or handheld devices. Due consideration should be given to EMI/RFI caused by human action, such as interference emissions from the wireless data transmission and telephone systems, as well as the repair, maintenance, and measuring devices used at the NPP.

Exclusion zone distances are set to protect digital equipment that may be sensitive to RF. IAEA Nuclear Energy Series No. NR-T-3.29 [39] notes that an issue with the exclusion zone approach is that the immunity of plant equipment is typically unknown; therefore, the calculated exclusion zone may be overly conservative, or it may be inadequate. Thus, the exclusion zone distances are more related to the uncertainties associated with the device’s susceptibility to RF.

As experience with wireless technologies in NPPs grows, additional insights and lessons learned are to be expected.  The typical NPP environment includes many sources of electrical noise. There are many examples of EMI/RFI sources, including hand-held two-way radios, smartphones, industrial wireless devices, arc welders, switching for large inductive loads, high fault currents, and high-energy fast transients associated with switching at the generator or transmission voltage levels.  Clearly, this is and will remain a complicated topic.

# 3. EVALUATION OF RG 1.180, REV. 2

Applications for wireless technologies are expanding rapidly, and there is significant interest within the nuclear industry to implement wireless technology in applications that can enhance plant safety or reduce maintenance costs. NRC RG 1.180 Rev. 2 is specifically focused on conducted/radiated immunity/emission of EMI and RFI from portable and existing devices within the plant.

In this evaluation, four issues are addressed:

- Is the exclusion zone distance bounding,
- Uncertainty in the exclusion zone distance calculation,
- The possible increase in number of emitters, and
- Evaluation of the wireless protocols.

## 3.1 REQUIREMENTS AND GUIDANCE

10 CFR Part 50 requires that structures, systems, and components important to safety in an NPP must be designed to accommodate the effects of environmental conditions: namely, that they remain functional under postulated design basis events (DBEs). Specific requirements include meeting 10 CFR 50.55a(h); Criterion III, “Design Control,” Criterion XI, “Test Control,” and Criterion XVII, “Quality Assurance Records,” of 10 CFR Part 50, Appendix B; and 10 CFR 50.49. Similarly, 10 CFR Part 52 addresses verification requirements for new reactor designs. 10 CFR 52.47(a) requires that an application for design certification must identify the tests, inspections, analyses, and acceptance criteria (ITAAC) necessary and sufficient to provide reasonable assurance that a plant has been constructed and will operate in conformity with the design certification. ITAAC for 10 CFR Part 53 using a risk-informed assessment, which is under development, is under evaluation.

RG 1.180 Rev. 2 describes methods and procedures that NRC staff considers acceptable for demonstrating compliance with the NRC’s regulations on design, installation, and testing to address the effects of EMI/RFI, power surges, and electrostatic discharge on SR/ITS I&C systems.

The entire wireless communications system must be designed and able to operate reliably, and the design must address the radiated and conducted emissions and the susceptibility of components within the system and those around it. Reasons for this approach are (1) strict regulatory issues concerning safety and reliability, and (2) concerns over new cybersecurity threats being introduced as well as EMI/RFI impacts to other NPP systems.

IEEE Std. 1050-2004, endorsed by RG 1.180 describes the design and installation practices acceptable to NRC staff to limit EMI/RFI and power surge-related effects on safety-related I&C systems employed in NPPs.

Subsection 9.5.2 of the SRP [40] provides review guidance for NPP license applications concerning communications systems. Regarding wireless communications, the guidance requires that the reviewer verify that wireless communications equipment will be compatible with the NPP’s EMI and RFI environment and that design measures have been taken to ensure that there will be no interference between wireless communications systems and other plant equipment. RG 1.180 identifies the EM environment operating envelopes, design, installation, and test practices acceptable to the staff for addressing the effects of EMI, RFI, and power surges on I&C systems and components important to safety. While nonsafety systems are not specifically addressed in RG 1.180, control of EMI/RFI from these systems is necessary to ensure that safety-related I&C systems can continue to perform properly in the NPP environment. When feasible, emissions from nonsafety-related systems should be held to the same levels as the emissions from safety-related systems. More specifically, Subsection 9.5.2 requires "that communications equipment will be compatible with the . . . EMI and . . . RFI environment of the plant and that design measures have been taken such that there will be no interference between wireless communications systems and other plant equipment."

For existing plants, 10 CFR 50.59 requirements encompass the introduction of wireless equipment into an NPP. The licensee must answer "no" to all eight criteria in 10 CFR 50.59(c)(2) for the proposed modification to be made under 10 CFR 50.59. Otherwise, the licensee must make changes to its facility under 10 CFR 50.90 to comply.

The guidance is significant because the existing I&C equipment in NPPs is being replaced with digital I&C systems or advanced analog I&C systems, potentially including wireless applications. Furthermore, this trend is accelerating in the design of advanced reactors as a means to reduce installation costs. The electronic architecture used with these technologies may be more sensitive to the EMI/RFI environment than existing I&C systems.

The guidance in RG 1.180 applies to SR/ITS and nonsafety-related I&C systems whose failure can affect safety functions. The endorsed practices are also acceptable for identifying and evaluating the EMI/RFI effects of nonsafety-related equipment intended for installation near SR/ITS equipment.

## 3.2 BACKGROUND

**RG 1.180, Rev. 0** was issued in January 2000 to provide guidance on controlling electrical noise and the susceptibility of I&C systems to EMI/RFI and power surges. The NRC staff accepted the EPRI TR-102323 in a Safety Evaluation Report (SER) by letter dated April 17, 1996 [41], as one method of addressing issues of EMC for safety-related digital I&C systems in NPPs. The SER accepted the EMI/RFI engineering practices in IEEE Std 1050-1989 and accepted selected test methods in MIL-STD 462, IEEE Std C62.4, and IEC 801, "Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment," as an appropriate means for assessing the EMC of safety-related I&C systems.

**RG 1.180, Rev. 1**, issued in October 2003, provides guidance to licensees and applicants on additional methods acceptable to the NRC staff for complying with the NRC's regulations on design, installation, and testing practices for addressing the effects of EMI/RFI and power surges on safety-related I&C systems. The changes in this revision include endorsing MIL-STD-461E [42] and the IEC 61000 series of EMI/RFI test methods, extending the guidance to cover signal line testing, incorporating frequency ranges where portable communications devices are experiencing increasing use, and relaxing the operating envelopes (test levels) when experience and confirmatory research warrants. Exemptions from specific test criteria are also offered based on technical considerations such as plant conditions and the intended location of the safety-related I&C equipment.

**RG 1.180 Rev. 2** [43], issued in December 2019, recognizes that many standards and guidance documents endorsed in the 2003 revision of RG 1.180 had been updated to incorporate additional guidance and improved methods for evaluating the effects of electrostatic discharge, as well as changes in the operational environment at NPPs arising from the increased use of digital technology, including wireless communication for both personal (laptops, tablets, and smartphones) and industrial (remote I&C) applications. Thus, based on the results of its periodic review, the NRC revised Rev. 1 to address the newer consensus guidance documents.

RG 1.180 Rev. 2 is specifically focused on conducted/radiated emissions of EMI and RFI from devices within the plant. The expanded use of wireless networks will increase radiated emissions in the environment and potentially increase the challenges to the immunity/susceptibility of existing devices.

RG 1.180 and EPRI TR-102323 adhere to the same overall approach and are generally in agreement [44]. The approach relies on the use of exclusion zones to protect plant equipment. Each requirement (1) recommends EMI/RFI-limiting practices based on IEEE Std 1050-1989 [45], (2) endorses emissions[14] and susceptibility (immunity[15]) test criteria and test methods to evaluate safety-related I&C systems, and (3) identifies appropriate operating envelopes for equipment and systems intended for selected locations in NPPs. Each document presents an acceptable means for demonstrating EMC,[16] and all documents are consistent in their respective approaches. The licensee can choose the method best suited to its situation.

The NRC (RG 1.180) and EPRI (EPRI TR-102323) rely on the use of exclusion zones to protect plant equipment. These zones effectively prevent a wireless device from adversely impacting SR/ITS systems. In addition, there is currently no use of wireless applications allowed in safety functions.

In 2015, ORNL determined that the exclusion zone calculations in RG 1.180 still protect the safety equipment, even with the newer technologies [46]. This finding shows that emission from the old technology devices is bounding to what the emissions would be from newer technology devices, and thus the exclusion zone distance in RG 1.180 Rev. 2 is bounding.

In summary, RG 1.180 Rev. 2 endorses the design, installation, and testing practices acceptable to the NRC staff for identifying and addressing the effects of EMI/RFI, power surge, and electrostatic discharge on safety-related I&C systems in an NPP environment. The guidance applies to both safety- and nonsafety-related I&C systems whose failure can affect safety functions. The endorsed practices are also acceptable for identifying and evaluating the EMI/RFI effects of nonsafety-related equipment intended for installation in close proximity to safety-related equipment.

## 3.3 STANDARDS

There are several aspects to consider when identifying and using standards for wireless sensors and networks. First, there are accreditation programs for test facilities that are used to certify compliance with those standards. Next, there are the standards for testing EMI/RFI and achieving certain levels of electromagnetic compatibility.

First, the accreditations for testing facilities can be from (an incomplete list):

- International Accreditation Forum (IAF)
- National Voluntary Laboratory Accreditation Program (NVLAP)
- International Accreditation Service, Inc. (IAS)
- American Association for Laboratory Accreditation (A2LA)

[14] *Emissions* (electromagnetic, from radio noise): phenomenon by which electromagnetic energy emanates from a source.

[15] *Immunity* (to a disturbance): the ability of a device, equipment, or system to perform without degradation in the presence of an electromagnetic disturbance.

[16] *EMC*: the ability of equipment to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment.

- ANSI-ASQ National Accreditation Board (ACLASS)

- Perry Johnson Laboratory Accreditation (PJLA)

The IAF [47] includes 84 signatory accreditation bodies from more than 70 countries that are signatories of the IAF Multi-Lateral Agreement (MLA), which recognizes the equivalence of other member's accreditations. There is a designated IAF member entity in each country that performs accreditation. For example, in the United States, ANSI and IAS are national accreditation bodies while in the Federal Republic of Germany, it is the Deutsche Akkreditierungsstelle (DAkkS). Thus, IAF member accreditations are valid in most countries of the world.

The National Institute of Standards and Technology (NIST) administers the NVLAP. Each laboratory accreditation program includes specific test or calibration standards and related methods and protocols assembled to satisfy the unique needs for accreditation in a field of testing or calibration. The Technical Testing and Analysis Center (TTAC) at ORNL is accredited by the NVLAP to the ANSI/IEEE N42 Homeland Security Standards in the radiological, mechanical, environmental, and electromagnetic areas as well as to IEC radiation protection instrumentation standards. This means that the Anechoic Chamber and the Gigahertz Transverse Electromagnetic (GTEM) cell at the TTAC are accredited to test for RF susceptibility (26 MHz–18GHz), RF emissions (30 MHz–1 GHz) and conducted immunity (150 KHz-80 MHz); and RF emissions (30 MHz–1 GHz) and RF immunity (DC–18 GHz), respectively.

The standards from IEEE, ISA, IEC, and the US Department of Defense (DoD) address the selection and use of wireless devices and wireless networks. (ISA and IEC have standards that address the WirelessHART protocol.) Expanding the use of wireless sensors and networks will introduce new sources of emissions that could impact existing devices that should be protected (immunity).

Several IEC standards address the ability of two or more spectrum-dependent devices or networks to operate without harmful interference (IEC 62988), Wireless Communication Requirements and Spectrum Considerations (IEC 62657), and Coexistence Management (IEC 62657).

A review of standards development organizations and others that develop standards on wireless networks and protocols, both domestic and international, is provided in Appendix B.

### 3.3.1 Standards Endorsed by RG 1.180, Rev. 2

Establishing and continuing an EMC program for safety-related I&C systems in NPPs contributes to the assurance that safety-related structures, systems, and components are designed to accommodate the effects of, and to be compatible with, the environmental conditions associated with NPP service. Application of consensus standard practices regarding the design, testing, and installation of safety-related I&C system modifications or new installations constitutes an important element of such a program.

The changes implemented in Rev. 2 of RG 1.180 include endorsing the current versions of the previously endorsed EMC standards. This RG revision extends the guidance to endorse updates in the test methods, adds a test method for electrostatic discharge (ESD), adjusts frequency ranges when appropriate, and relaxes operating envelopes (test levels) if experience and confirmatory research warrants. Conditions under which specific test criteria may be omitted are also offered based on technical considerations.

The updated standards endorsed in RG 1.180 Rev. 2 are listed in Table 3, and the coverage ranges of the tests are shown in Figure 9.

**Table 3. Standards endorsed by RG 1.180, Rev. 2**

| Standard | Title |
|---|---|
| MIL-STD-461G | Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment |
| IEC 61000-3 | Electromagnetic Compatibility (EMC) - Part 3: Limits |
| IEC 61000-4 | Electromagnetic Compatibility (EMC) - Part 4: Testing and Measurement Techniques |
| IEC 61000-6 | Electromagnetic Compatibility (EMC) - Part 6: Generic Standards |
| IEEE Std. 1050-2004 | IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations |
| IEEE Std. C62.41.1-2002 | IEEE Guide on the Surge Environment in Low-Voltage (1000 V and Less) AC Power Circuits |
| IEEE Std. C62.41.2-2002 | IEEE Recommended Practice on Characterization of Surges in Low-Voltage (1000 V or Less) AC Power Circuits |
| IEEE Std. C62.45-2002 | IEEE Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage (1000 V or Less) AC Power Circuits |

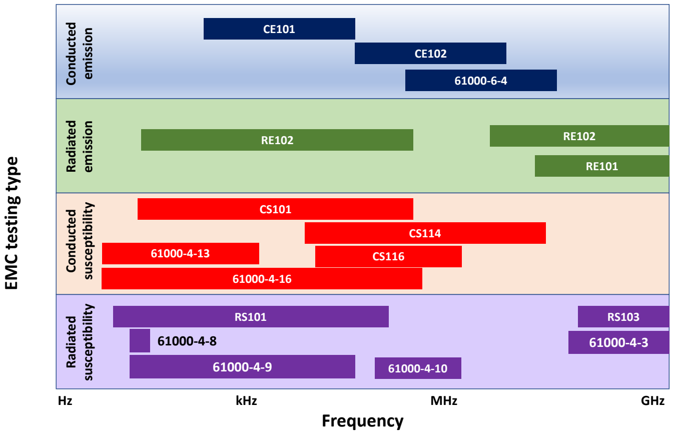


**Figure 9. EMC testing standards endorsed by RG 1.180 and their associated frequency ranges [8].**

MIL-STD-461G provides the latest revision of domestic guidance for emissions test methods, so it represents current US practice.

### 3.3.2 Other Standards

Other standards that are not endorsed by NRC may still provide insights into EMI/RFI issues. These standards are provided for informational purposes in Appendix C.

In general, the most important requirements for a wireless network are [49] reliability, security, robustness, determinism, quality of service (QoS), interoperability, integration with existing systems, scalability, and the availability of support tools for designing the network layout, process information, and monitoring. These other standards address issues such as minimizing possible interference caused by other wireless networks through defined protocols, as well as issues related to mesh network topologies and security. These topics are outside the scope of RG 1.180, Rev 2, and would require coverage in related guidance.

Additional consideration of wireless characteristics beyond EMI/RFI may also need to be considered, such as the failure modes for transmitters. Further consideration regarding such topics as the transmission medium, receiver issues, and antenna design and optimization may also be appropriate, although separate documents or informational papers would likely be needed.

## 3.4 EXCLUSION ZONE

### 3.4.1 Background on Exclusion Zone

RG 1.180 defines an exclusion zone “as the minimum distance permitted between the point of installation and where EMI/RFI emitters are allowed to be activated. The size of the exclusion zones should be location-specific and depend on the effective radiated power and antenna gain of the portable EMI/RFI emitters used within a particular nuclear power plant. The size of exclusion zones should also depend on the allowable electric field emission levels designated for the area in the vicinity of the installed safety-related I&C system.” Portable EMI/RFI emitters include devices such as hand-held transceivers (cellular telephones, broadcast transmitters, security guard transceivers, citizen’s band radios), RF-stabilized arc welders, induction heaters and RF electrostatic drying equipment. These devices produce considerable amounts of RF energy, which generally is not contained and can therefore reach I&C equipment.

Exclusion zones were established in the early 1980s when plant personnel realized that two-way radios would affect sensitive plant equipment. NRC IN 83-83 [50] reports four instances in which portable radio transmitters caused system malfunctions and spurious actuations in NPPs.

1. The first example occurred at Grand Gulf on July 25, 1983, in which shutdown cooling loop B was lost for 30 minutes because of a spurious isolation trip. The isolation was initiated by an residual heat removal (RHR) equipment area high-temperature trip which immediately cleared. The licensee concluded that the most plausible cause was an accidental keying of a walkie-talkie (i.e., a two-way FM radio) in the area of the RHR equipment. The walkie-talkie that was used has a power output of approximately 4 watts in the frequency range of 451–456 MHz. The walkie-talkie was accidently keyed in the upper cable spreading room, which is the location of the RHR equipment area high-temperature trip unit (a Riley temperature switch model PTGF-EG.) This temperature switch is a solid-state device that is connected by 16 American wire gauge copper shielded cable to a thermocouple.

2. The second example of a spurious actuation caused by a walkie-talkie occurred at Sequoyah 1 on May 31, 1979. A health physics technician who was in the in-core instrument room was attempting to communicate with the control room when he keyed his walkie-talkie, resulting in a spurious signal to all four channels of pressurizer pressure, thus initiating a safety injection. The in-core instrument room is located inside containment. The event was duplicated intentionally with the same results.

3. The third example occurred at Three Mile Island on February 19, 1982. Workers were preparing to enter the containment for some cleanup work when the combustible gas monitors they were carrying indicated the presence of hydrogen and low levels of oxygen. The workers became suspicious when the readings varied with the use of their face mask radios. Later, gas sampling outside of containment verified that the face mask radios caused false readings on the combustible gas monitors.

4. The fourth example occurred at the Farley Nuclear Plant in 1975. During initial energization of a 600-V load center, a false operation of the transformer differential relay was observed. The licensee determined that the Differential Relay Type 12 STD 15B5A is radio frequency sensitive and trips with an activated transceiver in proximity of the relay. A test revealed that the activated transceivers—having frequencies between 150 and 470 MHz with power ratings of 5-watt input

> to the final radio frequency amplifier placed within a radius of approximately 5 feet of the relay—caused the differential relay operation. As a further test, the relay was subjected to test currents of 0.5 amp and 5 amp applied to the restraint windings to determine if the relay was less sensitive to radio frequencies under simulated operating conditions. This test also resulted in a false operation of the relay. This GE Type STD differential relay is a solid-state device with certain parts mounted on a printed circuit board which apparently picked up a signal from a transceiver and fed it into the relay amplifier. This would result in the amplified signal passing into the operate section of the relay which caused the false operation.

IN 83-83 states that

> *To date, solid state devices installed in nuclear power plants have been responsible for all of the known cases of radio frequency interference (RFI) generated by portable radio transmitters. Three of the four examples cited in this information notice occurred during preoperational testing or early in plant operation.*
>
> *Many of the older nuclear power plants have so few solid state devices that this explains their apparent invulnerability to RFI generated by portable radio transmitters. As newer plants are built that use more solid state equipment and as older plants retrofit solid state equipment, more cases of RFI by portable radio transmitters are likely to result.*

Some of the areas that could have equipment highly sensitive to EMI/RFI, based on equipment EMI/RFI susceptibility tests or other analyses, could have portions designated as exclusion zones for wireless equipment use. These areas could include the main control room, the control rod drive mechanism cabinet room, and the electric equipment room [35]. In general, areas such as these generally contain highly important SR/ITS systems, with varying levels of EMI/RFI susceptibility, which must be protected from adverse impact.

Proximity effects can easily offset the fact that a radiating source of EMI is otherwise low-power. For example, an 800 MHz cellular phone does not radiate much peak power by itself, but if brought into close proximity to victim circuits such as those within an electronic equipment cabinet with the door open, considerable EMI can be coupled into these circuits. Unlike most two-way radio equipment, cellular telephones radiate even when they are not in actual two-way use by their operator because they must periodically notify the cellular site's computer that they are on and where they are so that incoming calls may be received.

To establish the size of an exclusion zone, an 8 dB difference between the susceptibility operating envelope and the allowed emissions level, as measured in dBμV/m (or similar unit), should be maintained.[17] For the radiated susceptibility operating envelope of 10 V/m (140 dBμV/m),[18] the size of the exclusion zones is set such that the radiated electric fields emanating from EMI/RFI emitters are

[17] When a physical quantity is measured in relation to a reference level, such as power or intensity, it is represented in decibels (dB), a logarithmic unit. dB is not the same as dBm, but it is related. The unit dBm stands for decibels per meter of power, where P is the power in watts. This shows 1 W = 30 dBm.

$$P_{dBm} = 10 \times \log\left(\frac{P_W}{1\,mW}\right) + 30$$

[18] *Radiated field strength* is defined as the intensity of an electric or magnetic field that is radiated from the transmitting antenna. EMC standards represent the radiated field strength in different units such as V/m, A/m, dBμV/m, and dBμA/m. dBμV/m is described as voltage level in decibels referenced to 1 microvolt per meter and is used for electric field intensity measurement. This shows that 140 dBμV/m = 10 V/m.

$$Radiated\ field\ strength\left(\frac{V}{m}\right) = 10^{\left(\frac{\frac{dB\mu V}{m}-120}{20}\right)}$$

limited to 4 V/m (132 dBμV/m) in the vicinity of safety-related I&C systems. The minimum distance of the exclusion zone can be calculated using the free space propagation equation provided in RG 1.180.

The 8 dB margin between the operating limits and the measured/expected values allows for variations in performance between manufactured items and plant emissions data. The margin should be large enough to compensate for (1) any instrumentation inaccuracy, (2) uncertainties in site survey, (3) variations between the measured sites (plants), (4) possible lack of sufficient data, and (5) variations in operating conditions.

As described, this margin accounts for the uncertainty in a stated measurement. Measurement uncertainty can be caused by the lack of an adequate test method, instrumentation uncertainty, or compliance uncertainty. EPRI 1020562 notes that the uncertainty of an RF emission measurement in a well-run laboratory to be around 5 dB [51]. A 5 dB measurement uncertainty indicates that if one laboratory finds a device exactly at the required safety limit, then another laboratory might find the same device at 1.77 over the limit or 0.56 under the limit.

To account for the various potential issues described, this 8 dB margin was determined to provide an acceptable level of protection for the plant's SR/ITS systems from EMI/RFI sources. Thus, this margin is incorporated into RG 1.180 Rev 2. Although this value may result in overly conservative limitations or restrictions in the use of wireless technologies, in the context of RG 1.180 Rev 2, it appropriately serves its purpose. Relaxation of these limits or restrictions requires further analysis to ensure that an acceptable level safety level is maintained.

For enforcement, administrative controls (among other controls) are normally used to prohibit the activation of RF emitters (e.g., walkie-talkies, cell phones, welders) within the exclusion zone of safety-related I&C equipment during operation. However, to ensure effective EMI/RFI protection of sensitive I&C equipment, exclusion zones may need to be applied in combination with other strategies (e.g., RF shielding and barriers).

The most recent guidance on how to establish exclusion zones distances is contained in RG 1.180, Rev. 2 and in EPRI 3002015757 [52], which is Rev. 5 to EPRI TR-102323. Revs. 1–5 to EPRI TR-201323 use the same exclusion zone distance calculation as RG 1.180, Rev. 2.

### 3.4.2 Exclusion Zone Distance

RG 1.180 Rev. 2 and numerous other documents such as EPRI TR-1019186 [8] and NUREG/CR-6431 [53] specify that the minimum distance of an exclusion zone (d) in meters should be calculated as follows:

$$d = \frac{\sqrt{30 P_t G_t}}{E} \, (meters),$$

where

d = the far field distance from the portable transceiver (m),
$P_t$ = for the wireless device, $P_t$ is the average transmitter radiated power of the EMI/RFI emitter (watts),
$G_t$ = the gain of the EMI/RFI emitter antenna (G=1 for an isotropic emitter), and
E = the allowable radiated electric field strength of the EMI/RFI emitter (V/m) at the point of installation.

Note that unintentional transmitters (e.g., welders, motors) will typically have a gain less than or equal to 1 (the gain of an isotropic emitter), and the gain for intentional transmitters (e.g., two-way radios, cell phones) will typically be greater than 1. Typical values for the gain of intentional transmitters might vary from 1.5 for a short dipole antenna to 3 for a monopole antenna, and to 6 for a horn antenna.

As noted above, the NRC staff accepted the EPRI TR-102323 [54] in an SER as one method of addressing issues of EMC for safety-related digital I&C systems in NPPs. EPRI TR-102323 was published in 1994 and was written to reduce conservatism in plant equipment emission and susceptibility testing limits. It identifies emissions sources in NPPs, recommends susceptibility and emissions standards, and details design and layout practices for minimizing susceptibility to EMI.

One of the major changes made from EPRI TR-102323 to Rev. 1 [37] based on comments from the NRC's SER [41] was "an increase of the margin between the allowable plant emissions limit and the susceptibility limit from 6 dB to 8 dB." As previously discussed, EPRI 1020562 notes that the uncertainty of an RF emission measurement in a well-run laboratory should be in the area of 5 dB [51]. Therefore, increasing the susceptibility limit from 6 to 8 dB further considers measurement uncertainty and increases the safety margin [55]. EPRI TR-102323 Rev. 1 also recognized the dangers of relying on EM surveys exclusively because most interference events occur because of infrequent, transient events.

EPRI TR-1000603 [56], which is Rev. 2 of EPRI TR-102323, reduced the 5 V/m defined in Rev. 1 to a 4 V/m maximum emission limit. In addition, a ⅓-meter absolute minimum protection distance was added. The total distance scale was reduced from 10 to 4 meters. In addition, a second scale was added to the vertical axis showing the effective radiated power and the field strength. Although the guidance remains relatively the same, these differences indicate the difficulty of enforcing an exclusion zone over larger areas [57].

EPRI TR-1003697 [13], which is Rev. 3 of EPRI TR-102323, refines the equation of exclusion distance in Rev. 2 by adding an antenna gain factor G. This equation is the same as that provided above for RG 1.180, recognizing that $V_d = E$.

EPRI 3002000528 [58], which is Rev. 4 (2013) to EPRI TR-102323, updates the practices to ensure that EMC updates/validates testing standards and limits, provides guidance that supports the increased use of wireless technologies, and provides a standard EMI procurement testing standard. Rev. 4 (2016) drops the endorsement for the CS114 test to the Army Ground Limit, recommends testing in accordance with IEC 61000-4-6 (Level 3), and provides guidance to test in accordance with the limits appearing in the latest revision of RG 1.180 if using the CS114 test.

EPRI 3002015757 [52], which is Rev. 5 to EPRI TR-102323, defines specifications to obtain additional emissions data to validate these guidelines, develop a basis for equipment emissions testing, bounds highest observed emissions from NPPs, and eliminates the need for individual site surveys. Additional data from seven plants that were obtained in 1993 and 1994 were added. Emissions data collected under NRC RG 1.180 was integrated with EPRI data to define more pragmatic limits to reduce conservatism without compromising nuclear safety. This report also includes practices that promote EMC in the field. Appendices have been developed to provide fixed and portable wireless device emissions control guidance and to provide a generic EMC testing procurement specification based on the current recommendations in the report.

### 3.4.3 Advantages and Limitations of Exclusion Zones

Exclusion zones had significant advantages in existing nuclear plants from the beginning, when there were fewer portable wireless devices. However, exclusion zones have also presented several limitations that will continue to be applicable to digital I&C upgrades in existing plants and rolled over to design in advanced plants unless a different strategy is taken. Some of the advantages of exclusion zones [57] are listed below:

- They are directly controlled by each individual plant.
- They can be customized to the specific needs and conditions in each plant or area of a plant.
- They do not require specialized training or equipment.
- They are not dependent on equipment vendors, outside labs, or other external entities.
- They can focus on specific classes of equipment that are problematic.
- They do not increase the cost of equipment or require specialized equipment installation practices.

The disadvantages of exclusion zones are also significant and well understood by those responsible for implementing and enforcing them. These include the following [57]:

- It can be difficult to implement exclusion zones.
- Enforcement of exclusion zones is increasingly difficult and sometimes errors do occur.
- They are the direct responsibility of each individual plant, costing time and resources.
- Exclusion zones can take on different shapes and areas, even across plants that use similar designs; there are enough variations in exclusion zones across these plants to create difficulties in designing and implementing system-wide policies designed to appropriately limit the use of wireless transmission devices.
- Exclusion zones may conflict with the legitimate need to use wireless-enabled technologies to perform necessary job functions.
- Exclusion zones by themselves do not consider the susceptibility of devices and thus oversimplify the problem, thereby providing a generalized and possibly non-optimal solution.
- Exclusion zones must use general rules that are often overly conservative.
- Exclusion zones often cannot be fully implemented around I&C systems because of physical barriers (e.g., rails, steps, other equipment) that are in the way.
- Exclusion zones can extend into areas that must remain clear as well as walkway areas that must support the heavy traffic of plant personnel.
- Exclusion zones are designed to protect I&C equipment from EM energy emanating from a known inventory of wireless transmission devices (typically portable walkie-talkies). Plants strive to control the use of wireless transmission devices, especially cell phones, owned by contractors and visitors. If these devices are allowed in a plant, then specific exclusion zones alone may not adequately protect I&C equipment.

Advances in technology and experience with transceivers in sensitive areas may allow some relaxation of the exclusion zone distances. Conversely, the addition of wireless networks introducing RF into the environment may identify sensitivities that currently do not exist. That is, performance and design advancements in the I&C components, to include decreased chip die size, can adversely impact the operation of digital systems through such potential occurrences as the increased likelihood of extraneous EM noise being misinterpreted as legitimate logic signals. In addition, variations in wireless technology such as frequency, modulation type, and transmission technology have variable impacts that the current guidance in RG 1.180 Rev. 2 does not consider.

### 3.4.4 Ways to Protect Equipment

In the past, exclusion zones by themselves sometimes failed to provide the required protection. Interference incidents that have occurred demonstrate the failure of the exclusion zone strategy to provide the desired level of EMC protection for I&C systems. There are multiple documented cases of malfunction and upset of I&C systems in existing plants caused by  sources, including by the operation of portable wireless transmission devices (not always a walkie-talkie) too close to a standard system cabinet with its doors closed.

Most equipment in NPPs have never been tested for vulnerability to wireless transmission [59]. Testing has been more focused on general EMI/RFI susceptibility, which is not completely encompassing of aspects of newer wireless technologies. As such, the impact of modern wireless devices on nuclear safety and plant reliability is not completely understood. The IAEA states that the immunity of plant equipment is typically unknown; therefore, the calculated exclusion zone may be overly conservative, or it may be inadequate [39]. However, the 8 dB additional margin specified in RG 1.180 Rev 2 ensures that an adequate level of safety is still maintained. However, existing guidance on the use of exclusion zones to protect plant equipment, may also result in exclusion zones of up to 2.4 m [8 feet] for some tablet devices, thus rendering them ineffective for the mobile workforce.

One way to reduce the exclusion zone distance is to perform in situ immunity testing of plant equipment to objectively and more precisely determine the exclusion distance for a particular piece of plant equipment. Special consideration must be given to planning, performing, and interpreting the test results for in situ immunity testing. Combined with engineering evaluations, these test results can be used as objective evidence for establishing appropriate exclusion distances. However, this approach requires careful consideration of portable devices that can emit signals but are not in fixed locations as well as other surrounding equipment that may have different susceptibility levels.

Fortunately, there are multiple ways to protect equipment from EMI [57]:

1. Keep unwanted energy out of sensitive I&C equipment by separating the emitting equipment from sensitive equipment. This is the exclusion zone strategy.

2. Protect sensitive equipment from the unwanted energy by using additional shielding or filtering either at the system cabinet level or inside the cabinet, but external to sensitive equipment.

3. Design sensitive equipment to be inherently immune to the effects of unwanted energy.

Operating history shows that high energy emissions such as those from walkie-talkies, flash photography, and welding can adversely affect sensitive equipment. Therefore, exclusion zones are often set up in various parts of the plant to safeguard these sensitive instruments from EMI. With that reasoning, wireless modules deployed in an NPP and using lower power signals would be allowed to have a smaller exclusion zone distance. However, there are drawbacks to consider with his approach.  For example. lowering the transmitting power level may also severely restrict the communications range, which has likely already been adversely impacted by the harsh EMI environment and complex, packed space found inside NPP containment areas [60].

A three-step approach can be used when expanding the use of wireless technologies to ensure that no EMI issues occur as a result of the use of these devices [61]:

1. Perform walkdowns and visual evaluations of the installation of the existing plant equipment.

2. Characterize the EM environment within the plant through an EMI/RFI site survey.

3. Perform targeted immunity testing of select plant equipment to provide data-driven exclusion zones.

A site walkdown is performed to evaluate the installation of sensitive/critical equipment throughout the plant for vulnerabilities to EMI from wireless devices. During the walkdown, aspects such as grounding, shielding, use of conduit and cable trays, and exposed signal leads would be inspected, and a list of vulnerable equipment would be identified. Such a list would include equipment with vulnerable installations critical to plant operation or safety with a history of malfunction in the presence of wireless devices or that could cause nuisance alarms for plant operators due to such devices.

After the walkdown, EMI/RFI site surveys of the selected areas would be used to characterize the EM environment and determine what level of emissions currently exist. The EMI/RFI site surveys will aid wireless implementation efforts by identifying the sources of frequencies that may compete with wireless devices, determining if the existing EM environment negates the need for immunity testing, and locating sources of frequencies that may indicate equipment vulnerabilities. Mapping the site and performing the walkdown would also provide information needed to identify equipment with emissions in the frequency band of wireless devices. Those systems, along with other critical plant systems, could then be selected for in situ immunity testing.

The site survey would involve measurement of the radiated emissions present at various locations throughout the plant. The measurements would be performed using applicable guidance in NRC RG 1.180 and/or EPRI TR-102323 [54], Rev. 1 [37], Rev. 2 [56], Rev. 3 [13], Rev. 4 [58], or Rev. 5 [52] and would utilize hardware such as a receiving antenna, a spectrum analyzer, and a computer to analyze and store the site survey data. An example of site survey testing is shown in Figure 10. In the figure, the summation of the emissions from the various sources of EMI/RFI (walkie-talkie, workstation, and power inverter) are collected at the receiving antenna and captured by the spectrum analyzer to produce an overall envelope of the plant's EM environment. The figure illustrates an example of the test results obtained before and after installation of the wireless access point. The dark spike at 2.4 GHz is attributed to the wireless signal transmission. Using the site survey data, a determination can be made regarding the impact of the plant environment on the wireless system, the impact of the wireless device on the plant environment, and identification of equipment that may be susceptible to interference from the wireless transmission.

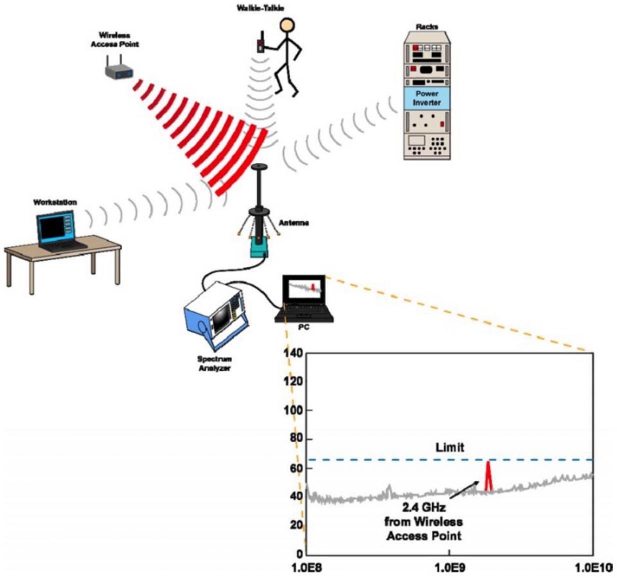


**Figure 10. Example of test setup and results from a spectral emissions site survey [8, 27].**

In-situ immunity testing is used in qualification testing of equipment. RF energy is radiated onto equipment and cables within a facility to objectively measure its response to EMI. Preventative measures such as shielding are established so as not to interfere with any nearby equipment that may also be vulnerable. This targeted immunity testing can be used to objectively determine each system's immunity to wireless devices. With the knowledge of which equipment is susceptible to EMI, the site could implement administrative procedures to limit the potential for EMI for those systems.

## 3.5 AREAS FOR CONSIDERATION

As discussed, a purpose of this effort is to determine if any changes or updates are necessary to RG 1.180 Rev. 2 or if additional guidance is appropriate to properly address advances in wireless technology. In addition, revisions to endorsed standards, and other standards that may be useful in providing guidance for the use of wireless in NPPs based on their use in other industries, should also be addressed. After a review of wireless networks and uses, protocols, testing standards, common EM threats, and a review of RG 1.180 Rev. 2, further insights into the exclusion zone distance, coexistence, testing, spectrum coverage, uncertainty, and cybersecurity can be developed. It should be noted that the guidance for determining the exclusion zone distance meets the objective of protecting devices from EMI/RFI. The RG does not address how to determine the susceptibility of devices to EMI/RFI; however, this is outside the scope of determining if the exclusion zone distance is bounding. RG 1.180 is not the appropriate place to address this because each device will behave differently, and the analyzing the number of possible devices and their uses would be a vast undertaking.

At the time of the original issuance of RG 1.180, wireless systems were limited to operational radios and pagers; however, their application has now been expanded to network-based communications spanning diverse applications, as well as cellular communication devices. The focus of RG 1.180 is primarily to provide guidance on the exclusion zone distance and testing of EMI/RFI for interference of safety-related I&C from portable transceivers and other portable devices. The potential greater use of fixed emitters will significantly alter the EM environment. Many of the standards identified during the review of EMC standards are not endorsed by RG 1.180 but may be considered in a future revision of that RG or if it is determined that a new RG that specifically address wireless communications from a safety and cyber perspective is necessary (Appendix B). These standards are used in different industry sectors and have a broader scope because they address not only EMI/RFI, but also wireless networks. ANSI C63.27 [62] provides methods for evaluating a device's capability to coexist in its intended RF wireless communications environment.

The only potential "gap" identified for RG 1.180 is that it does not address the full spectrum in use today, which can range up to 60 GHz.

Although not explicitly addressed in the RG, uncertainty is covered in the 8 dB margin. This 8 dB margin was increased from 6 dB and is consistent with a 5 dB uncertainty associated with different users, test setups, and environments using the same certified test equipment. Thus, the 8 dB margin is sufficient to protect new and existing systems based on the exclusion zone distance.

Cybersecurity is also not addressed in RG 1.180, and although the consequences of network failures and cybersecurity attacks may be the same, cybersecurity issues are outside the scope and intent of RG 1.180. Thus, cybersecurity issues should continue to be addressed as part of the requirements to meet 10 CFR 73.54. "Protection of Digital Computer and Communication Systems and Networks".

### 3.5.1 Exclusion Zone Distance, Testing and Applicability

As discussed, an *exclusion zone* is defined as the minimum distance permitted between the point of equipment installation and the location where portable EMI/RFI emitters are allowed to be activated. The size of an exclusion zone depends on the effective radiated power and antenna gain of the portable EMI/RFI emitters. It is important to note that the exclusion zone not only considers the distance of a radiated field, but also the distance to components that may be susceptible to EMI/RFI.

The calculation of the exclusion zone is based upon a single component being the emitter or the receiver. It is unknown whether this accurately reflects what the insult to a system would be as the environmental complexity increases.

More precisely, the calculation of the exclusion zone is based upon a single component being the emitter or the receiver in an unobstructed (no reflector or absorber) environment. It is unlikely that this accurately reflects the system that would be present as the environmental complexity increases. But it is a useful simplified tool for bounding evaluations and due to the large added margin, capable of assuring the SR/ITS systems are protected.

The exclusion zone distance is also not only applied for portable EMI/RFI emitters, but also for fixed instrumentation. This is necessary because fixed instrumentation can also emit RF energy and thus be a source of EMI/RFI and may itself subject to EMI/RFI.

Even without these newer devices, present-day observations show that multiple wireless systems already operating in NPP nonsafety systems are using unlicensed FCC frequency bands between 1 and 10 GHz. This suggests that there are now numerous additional sources of EMI between 1 and 10 GHz that should be considered during testing. The frequency ranges and operating envelopes of the RE102 and RS103 tests were adjusted to 10 GHz in Position 6 of the current RG, so coverage for these wireless systems is already in place.

The task remains to ensure that emissions from the wireless systems do not invalidate the current radiated emissions operating envelope. Because of their unlicensed nature, these wireless systems are low powered (usually < 1 W), and an increase in these systems should not pose a significant escalation in the noise levels of the overall EM environment. Without additional plant data, it is logical that the emission levels already incorporated for the RE102 test over this range be maintained. However, periodic measurements should be taken in a sampling of plants to affirm that the operating envelopes are not challenged by new implementations or modifications and thus remain valid. It is also logical that the susceptibility operating envelope (10 V/m) for the frequency range between 1 GHz and GHz be maintained [46].

Additionally, the complex real-world environments found in NPPs can effectively render ineffective simple solutions such as the exclusion zone. For example, cable not only acts as a transmission line for EMI but can also act as a transmitting and receiving antenna – similar to the DAS concept discussed earlier. Thus, a single cable can pick up 100–1000 kHz energy anywhere along its route, deliver it elsewhere, and then reradiate it. It is therefore not surprising that in a room where thousands of cables from all over the plant converge, a noticeable background radiated medium-frequency magnetic field is not only present but is actually stronger than at most other locations in the plant [63].

Then there is the fact that there is no clear connection between increased wireless complexity and the impact on the co-located non-wireless systems represented in the information and tests. Wireless coexistence information and testing indicate concerns over the increased complexity preventing a component from being able to maintain the required wireless functional performance. However, the information does not directly correlate back into the increase in RF environmental complexity. The EMC/EMI/RFI tests used for non-wireless equipment continue to use relatively simplistic parameters. More valuable data would be obtained from direct measurement of a component's immunity to EMI/RFI. This could also lead to a refined or hybrid exclusion zone calculation and process which could separate the exclusion distance equation into two equations—emitters and susceptibility.

In addition, it would be useful to consider the effectiveness and applicability of EMC standards and how that may relate to the exclusion zone calculations and process. For example, start with a component designed to a certain EMC standard and test to failure (degradation). The results should correlate with the standard's information and the test procedures such as IEC 61000. In the same manner, it could also be beneficial to analyze how the exclusion zone correlates distance to a component's immunity to EMI/RFI.

Another item to consider is the use of peak or average power in the exclusion zone calculation. Though there are other aspects to consider, an important factor is the use of average power will determine a smaller exclusion zone value than using the peak value. And there is evidence that this is a more relevant position to take. For example, in the FCC's *2008 Biennial Review Report*, the FCC revised the radiated power rules for other commercial mobile services because it determined that allowing licensees to meet radiated power limits on an *average* rather than a *peak* basis would more accurately predict the interference potential for newer technologies such as orthogonal frequency division multiplex (OFDM) technology.

### 3.5.2 Coexistence and Interference Avoidance

*Coexistence* is the ability for two or more different wireless devices to simultaneously operate without significant degradation or interruption. Because energy from one device will affect another device, the avoidance of all interference is not possible. Interference can be unintentional or intentional. Unintentional interference can occur when manufacturers use overlapping frequencies. One method to keep the impact of interference below levels deemed to be harmful is to strictly adhere to a common standard for each device. Excessive intentional interference could be equivalent in impact to a denial-of-service attack. Section 2.6.2.4 further discusses and identifies additional failure modes related to the coexistence of wireless devices.

*Coexistence analysis* and *interference analysis* are complementary and related concepts [64]. A coexistence analysis starts at the system level and studies the ability of a recipient system to communicate or accomplish its intended useful effect in the presence of interference introduced by a source system. An interference analysis starts with the energy introduced by a source and studies the effect of that energy on recipient systems.

NIST Technical Note 1885 [65] examines interference and coexistence testing issues related to the use of wireless devices in critical infrastructure systems. The technical note discusses the challenges of characterizing complex EM environments, emulating such environments in the laboratory, and designing test methods that adequately evaluates the ability of a device to perform in that environment.

Devices operating at different frequencies are unlikely to interfere with each other because their operating frequencies do not overlap. However, there are multiple protocols and network systems that operate at many different and potentially overlapping frequencies.

For example, the 2–4 G cellular networks are up to 2.6 GHz. The frequency bands for 5 G are in the range of 20–60 GHz. The operating frequency is 2.4–2.48 GHz in the ISM band for Bluetooth. The standard operating frequency for Zigbee is 2.4–2.4835 GHz (worldwide), 902–928 MHz (Americas and Australia) and 868–868.6 MHz (Europe) ISM bands. WirelessHART uses the 2.4 GHz band. WLAN can operate at two frequency bands of 2.4 and 5 GHz. WiMAX uses licensed spectrum bands of 2.3, 2.5, and 3.5 GHz. UWB can range from 3.1 to 10.6 GHz and is typically spread over at least 500 MHz, or 20% of the center frequency. RFID is based on a variety of wireless technologies operating at different frequencies, most commonly at low frequencies of 125 kHz, at high frequencies of 13.56 MHz, and at ultrahigh frequencies (UHFs) of 867 MHz. For active transponders, 2.45 GHz frequency is often used.

Those devices operating within the same frequency band that use the same wireless protocol can minimize interference by selecting separate frequency channels within the allotted frequency range, specifying a certain time for each device to transmit information, and using spread spectrum techniques [8]. The protocols for the standards use discrete channels within the fixed bandwidths to assist with interference avoidance.

Coexistence becomes more complicated when two wireless devices are communicating in the same frequency band but operate under different standards. The increasing use of advanced analog and digital based I&C systems in reactor protection and other safety-related plant systems has led to concerns with respect to the creation of additional noise sources. These additional emissions, both radiated and conducted, in combination with the electrical noise already present in the NPP environment, may increase the potential impact to the existing and new equipment as their susceptibility (immunity, both radiated and conducted immunity) limits are approached.

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. 24 of the 79 Bluetooth channels [IEEE 802.15.2] are susceptible to interference from a single operable 802.11b network [17]. 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. 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, packets must be retransmitted, and the overall usage of the network increases, resulting in an increased probability of more interference.

Wireless networks operating on the same frequency bands can interfere with each other's operations. For example, IEEE 802.11 [66], IEEE 802.15.4 [67] and Bluetooth devices operate in the same 2.4 GHz ISM band. This unlicensed band is used by a variety of devices. At the time of concluding the IAEA's coordinated research project in 2020 [39], NUREG/CR-6939 [68] was the only source of guidance available for the coexistence of wireless networks in NPPs.

IEEE P2425, “Standard for Electromagnetic Compatibility Testing of Electrical and Instrumentation and Control Equipment at Nuclear Power Generating Stations and Other Nuclear Facilities,” is being written by Working Group 2.16 – Electromagnetic Compatibility for Nuclear Power Plant Equipment. It will provide qualification methods and criteria to establish the EMC of equipment in NPPs and other nuclear facilities. EMC qualification identified in this standard involves two elements: (1) testing to assess susceptibility of equipment to interference levels that bound the expected EM environment at the installation site, and (2) testing to assess emissions of equipment to ensure that the contribution to the EM environment does not invalidate bounding interference levels applied for susceptibility testing.

*Coexistence testing* is the determination of how wireless devices can coexist with one another. Coexistence is mainly a concern for devices that operate in the same frequency band (e.g., in the 2.4 GHz ISM band). If two devices have sufficient frequency separation, then there should be no interference. For two wireless devices communicating using the same wireless protocol, this is also not a concern, because the protocol should handle coexistence through interoperability, channel access, and other channel sharing techniques. Some protocols even use these same techniques to coexist with other protocols. When two different wireless protocols occupying the same frequency band operate in proximity to one another, there is the potential for interference. Organizations operating NPPs must employ a spectrum management program to understand the frequency usage in their plants and manage any coexistence concerns.

Lower frequency bands (below 1 GHz) have historically been congested with numerous signals, whereas the higher frequency bands have been less crowded [8]. However, the number of devices using 2.4 GHz (e.g., 802.11 and ISA100.11a) or higher is increasing, which will lead to congestion at higher frequencies and will also result in increased interference. To address this concern, wireless protocols often use multiple channels within their defined frequency bands to transmit information.

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 [17].

There are numerous additional sources of EMI between 1 and 10 GHz. As previously discussed, the frequency ranges and operating envelopes of the RE102 and RS103 tests were adjusted to 10 GHz in Position 6 of RG 1.180 Rev. 2, so coverage for wireless systems is already established. It is important to ensure that emissions from the wireless systems do not invalidate the current radiated emissions operating envelope.

Interference with other systems from an RF source is a separate issue and commonly referred to as RFI. In these situations, RF energy has been known to be absorbed by systems that do not intentionally use RF energy in their normal operations. For example, such RF energy transmitted by wireless data devices could cause erroneous readings on affected instrumentation. A related issue but in the other direction is the possibility that existing systems and equipment could interfere with the wireless system. The shows the importance of EMC on both the wireless system and the existing system.

In addition to free space path loss properties, lower frequency signals also pass through many objects more effectively than those of higher frequencies. As a rule of thumb, for applications above 10 GHz, a clear line-of-sight (LOS) path between the transmitter and receiver is required because of the losses associated with object collisions. Applications below 10 GHz can transmit effectively on a non-LOS basis.

Directional antennas can also be used to provide a more focused signal. In turn, this can overcome interference better than an omnidirectional antenna that transmits and receives equally in all directions.

For usage of emerging wireless technologies such as LTE, Bluetooth, Wi-Fi, or WirelessHART, the wireless signal spans a much greater spectrum instead of a narrow bandwidth [59]. These different modulations and spread spectrum techniques transmit energy over a much greater spectrum and are not as significant in amplitude as in previously used wireless devices such as older analog hand-held radios, which correlates to the field strength emitted from the device. Additionally, today's common wireless devices often spread the energy over a much larger bandwidth as a result of digital modulation techniques such as quadrature amplitude modulation, possible frequency hopping, or windowing attributes such as spread spectrum technologies. With the energy spread over a much wider bandwidth, the amplitude/ is minimized and results in a lesser field strength given off by the wireless device as compared to older wireless transmitting devices. This may also present a problem when evaluating a device's potential to interfere with a SR/ITS system during operation.  A common technique to gather RF emission values is to use a spectrum analyzer's recorded maximum hold value during an emissions measurement. In a case like this, the recorded value is a peak value and thus not necessarily indicative of the overall power that may impact other systems. As recognized by the FCC and discussed previously, the average value is often a better indicator of the potential risk to other components.

It is clear that as the number of RF applications increases, the spectrum will become more crowded. Because RG 1.180 is focused on existing plant setups and not the introduction of wireless networks, the RG and the endorsed standards do not specifically address the associated increase in emissions and the immunity of existing devices. However, instead of increasing the scope of RG 1.180, it is more appropriate to develop additional supplemental guidance to address the coexistence of sensors/networks and their interference avoidance. Like the IEEE 802.x standards, such guidance should consider discussing interference avoidance in the context of the increasing wireless sensors and networks being added.

NIST also addresses coexistence and states that it is addressed in multiple communication standards [65]. The standards cited by NIST as examples include:

- IEEE Std 1900.2-2008 [64] discusses how to analyze and report on the coexistence problem in a communication network.

- IEEE Std 802.15.2-2003(R2009) [69] provides some analysis and best practice suggestions for coexistence between two specific protocols, namely IEEE Std. 802.15.1-2002 [70] for wireless personal area networks (WPAN) and IEEE Std. 802.11b-1999 [15] for wireless local area networks (WLAN).

- IEEE Std 802.19.1-2014 [71] discusses approaches to coexistence in the TV white space spectrum which focus on managing potential coexistence problems in industrial networks.

- IEC 62657-2:2013 [72] discusses approaches to coexistence in the TV white space spectrum which focus on managing potential coexistence problems in industrial networks.

- CTIA - The Wireless Association (CTIA) and Wi-Fi Alliance (WFA), [73] "Test Plan for RF Performance of Wi-Fi Mobile Converged Devices," Version 1.3, June 2009.

NIST notes that when multiple wireless transmitters are in close proximity to each other and to other electronic systems, the possibility of interference and coexistence problems significantly increases, especially when the devices attempt to share the same frequency bands. Furthermore, the advance of communications and wireless technology is moving at a much faster pace than the development of interference and coexistence test standards and measurement metrics.

Possible coexistence solutions range from protocol design to consideration of network topology. However, as is typical in the current state of wireless standards, none of the standards reviewed describe or recommend how to perform a coexistence test.

Other standards and efforts to address this topic are as follows: IEC 62657 Part 2 [72] was developed to address coexistence of industrial wireless networks. The ANSI C63.27 [62] standard defines the coexistence test guidelines for medical equipment. IEEE 802.15.2-2003 (R2009) (inactive) [69] addresses the problem caused by interference because of various competing wireless technologies in the same band and recommends general practices to combat interference problems. Although this standard is inactive, because NPPs and industry still use this standard, it is recognized as guidance for coexistence. The IEEE 802.19 Technical Activity Group (TAG) on IEEE 802 Coexistence, which was formed when the original 802.15.2 standard was published (2003), had already been handling coexistence concerns for IEEE 802 in general for many years [74] since its formation.

ANSI C63.27 specifies methods for assessing the RF wireless coexistence of equipment that incorporates RF communications. One risk control measure to ensure that the technology can be integrated at a level of acceptable risk is through coexistence. This standard specifies key performance indicators (KPIs) that can be used to assess the ability of the EUT to coexist with other equipment in its intended operational environment. This type of testing focuses on devices and systems that intentionally use wireless, and it extends beyond traditional EMC to examine a device’s performance in frequency bands where it uses wireless communication.

IEEE 1900.2-2008 [64] provides technical guidelines for analyzing the potential for coexistence or in contrast interference between radio systems operating in the same frequency band or between different frequency bands. It does not propose judgments on what constitutes interference or on what constitutes harmful interference. It does, however, indicate a number of effects and conditions that should be considered to provide a complete interference and coexistence analysis.

It is important to recognize that the impact of the EM environments and obstacles on the individual EM signal communication channel must be addressed. Lessons learned from the military indicate that without specific design and verification requirements, problems caused by the external EM fields typically are not discovered until the system becomes operational. In the past, the EM environment generated by the system's onboard RF subsystems (electronic warfare, radars, communications, and navigation) produced the controlling environment for many systems. Regarding probability of exposure, these items still play a critical role. However, with external transmitter power levels increasing, external transmitters can drive the overall system environment.

Appendix A of MIL-STD-464D [75] states that “Unless otherwise specified by the procuring activity, all ordnance is to be designed to operate in the joint EM environment detailed in TABLE IX.” TABLE IX specifies both “unrestricted” and “restricted” environments. The unrestricted environment represents the worst-case levels to which the ordnance may be exposed. The restricted environment involves circumstances in which personnel are directly interacting with the ordnance (assembly/disassembly, loading/unloading). For the special case of handling operations, the environment is intentionally restricted to prevent personnel from being exposed to hazardous levels of EM energy or contact currents.

Other factors to consider are that some sources of severe interference are not widely distributed in the general population; however, NPPs may commonly find them introduced. Additionally, some kinds of transmitters are intended to be installed in fixed locations and remain stationary, and others are designed to be portable. The significance of these sources of interference must be evaluated based on their impacts to NPPs. An additional factor is that the methods used to provide RF immunity to the most common sources of RF interference also tend to provide wideband immunity. The result is that I&C systems immune to mobile phones will also have good RF immunity to several other types of potential interference sources and electronic devices, even though they may operate in different frequency bands. This statement, like most generalities, will have exceptions and must be reexamined as new types of RF interferences are evaluated. But it also provides additional support that even as upper frequency limits increase, the existing protocols in place should still provide adequate EMI/RFI protection to the SR/ITS systems.

### 3.5.3 Immunity / Susceptibility

As discussed above, EMC is the ability of a device or system to operate in a manner such that it both functions acceptably within the surrounding EM environment and will not cause detrimental interference to its neighbors [65]. When this concept is applied to most electronic devices, it implies that there is sufficient immunity to the effects of external signals or noise, and that EM emissions are well controlled. This can usually be accomplished by proper circuit design including the addition of filtering and shielding as needed. However, the trend toward lower voltage, more power efficient and densely packed electronics, along with the ever-present desire to reduce costs, can have an impact on the immunity to EMI. The addition of a radio transceiver and antenna can further increase the possibility of interference from internally generated signals, as well as external signals or noise detected by the antenna and coupled into the device. Maintaining EMC has also become more challenging as the density of wireless (radio) communications systems increases and these systems occupy more of the EM spectrum.

ANSI C63.15 recognizes that “Selecting immunity test levels requires estimation of the range of EM environments that a product can experience at some time in use.” These tests, however, are limited in that they are based on a signal from a single emitter and not on more complex environment from multiple emitters in a complex environment that can be expected now and in the future.

An important point is that an EM susceptibility limit should be set to represent the actual EM environment in which the equipment is to be operated. ANSI C63.15 recognizes that “Past experience with specific product immunity cannot be relied upon because the EM environment is changing rapidly, and products are being updated with more sensitive electronics. Selecting immunity test levels requires estimation of the range of EM environments that a product can experience at some time in use.” Additionally, a method to address classes of products of most concern and to monitor trends and market changes in many other classes of devices would help reduce RF emissions and increase immunity or show that existing immunity is sufficient [76].

The following items are essential to immunity assessments [77]:

a. Establishing a known immunity test signal that adequately represents the real-world EM environment (encompassing both radiated and conducted disturbances) at the various locations where electrical and electronic equipment are required to operate reliably.

b. Repeating the immunity signal at different facilities for different types of equipment under test (EUT) or different configurations. Different environments can require different immunity signal types or amplitudes.

c. Exposing the EUT and its associated I/O wiring using efficient, cost-effective methods that do not interfere with other processes or tests running nearby.

d. Monitoring the acceptance criteria (immunity performance criteria) without disturbing the immunity test signal imposed on the EUT.

To identify those types of devices with a significant potential for producing RF interference with I&C systems, one must understand the characteristics that make a class of equipment sensitive to RF transmission. Using audio interference as an example, audio RF interference requires that the following two conditions exist [76]:

1. The receptor device must be exposed to an RF field with sufficient intensity to overcome its RF immunity.

2. The modulation of the RF field must contain substantial baseband audio components. Reduction of the RF power or the content of the audio band modulation will reduce the amount of interference created.

Furthermore, for a particular source of audio RF interference to become common, the following two criteria must also be met:

1. The combination of RF field intensity and modulation must be common enough to have an unacceptable probability of causing an interference problem.

2. There must not be any readily available and easily applied remedies available to the user. If interference is easily recognized as being caused by RF and its consequences are neither serious nor too rapid for human action to adequately address, then it is entirely possible that some mitigation taken by the operator will be entirely acceptable. An example might be a noise coming from a speaker that is eliminated by moving a walkie-talkie off the console and further away from the speaker.

Because relatively few RF devices have these four characteristics, concerns about RF interference can be focused on those wireless devices that, when considered as a class, do have these characteristics and present a serious threat for producing EMI/RFI related malfunctions and failures.

An analysis process similar to that provided above can be developed for I&C systems used in NPPs. The characteristics of a system's susceptibility must be understood in the context of the transmission parameters of potential sources that impact interference and to quantify those modulation characteristics that impact interference. For example, a CW signal can introduce a DC bias resulting in audio distortion or gain change, but generally these are not observed to be real field problems. At much lower power levels, modulated signals with strong content in the audio band result in disruptive audio interference in devices that produce sound. Similarly, pulsed modulations may interfere with digital circuits such as those used in digital I&C equipment in a variety of ways.

To ensure that an adequate level of RF immunity is designed into I&C systems used in NPPs, the design must consider the frequency range, power levels and modulation types to which systems are likely to respond. However, the design must equally identify the severity of the threat so that an inordinate level of RF immunity will not be required, with its attending cost and complexity resulting in overly burdensome specifications for I&C systems [76].

### 3.5.4 Testing

The current exclusion zone calculation in RG 1.180 is intended for use with both fixed and portable devices, although it does address conducted RF. Several questions related to testing should be clarified:

- Are the tests related to portable devices completely appropriate for fixed WSN or WLAN systems?

- Is the 8 dB margin too small, too large, or appropriate for fixed devices?

- Whereas the tests under RG 1.180 allow for combined testing of different frequencies at the same time, does this accurately reflect the power when using technologies such as frequency hopping, code division multiple access (CDMA), etc.? What if a network that is normally used for low traffic is forced into or inadvertently put into a 100% duty cycle and continuously transmits? (Some protocols check for traffic, but all may not.)

- Are devices developed to EMC standards sufficiently protected, and are their emissions sufficiently quantified such that appropriate protective measures for existing systems can be easily determined and taken while also maintaining functional wireless performance (per IEEE C63.27) in both simple and complex environments? The question likely has a simple answer in a relatively simple environment with conservative exclusion zone determinations. The answer becomes less tangible in a complex environment with objectively based, risk-informed calculations.

- Current testing is for single devices, with the caveat of other devices not causing failure. As more devices are added, the environment complexity increases. Do current tests account for the increased environment complexity with a larger number of emitters, antenna locations, different protocols, and so on? Are the insults to the EUT as expected—bound by the current test procedures (frequency and power level basically)—or does the complex environment change the end result?

- Testing may be to the full power level at a certain frequency and be used to determine the exclusion zone. However, if using average power, how does that impact the results? How does a more complex environment translate into the RF insult to the EUT—is it straightforward? Do the exclusion zone calculations accurately reflect what the EUT actually sees? Do multiple but different emitters have an additive effect or a destructive effect? Are the calculations giving a result more or less restrictive than they should be?

- Also, per IEEE C63.27 or similar, EMC testing for wireless coexistence of the WSN should be analyzed. While maintaining functional wireless performance of the wireless systems, how does that correlate to the issues for the other existing non-wireless systems (to include SR/ITS and/or nonsafety I&C systems)?

- It should be possible to test wireless systems to include sensors, as well as non-wireless equipment such as SR/ITS analogues, and to see failures at a certain point. Tests should be repeated for various levels of environment complexity. What differences are found at the more simplistic configurations vs. more complex environments?

- Testing using a constant wattage signal or a simplistic modulation technique is not necessarily representative of the environment that will be present when using currently available wireless systems. How does this impact the required exclusion zone and the overall EMC determination?

Guidance on emissions testing is provided in

- MIL-STD-461 & MIL-STD-462
- IEC-801 Series
- ANSI/IEEE C63.12 and C62.45

Simulations should also be considered as a means to show acceptance for wireless devices both portable and nonportable, in the NPP as well as evaluating the appropriateness of the exclusion zone distances as an alternative or adjunct to in-situ emission testing.

### 3.5.5 Spectrum Coverage

Spectrum coverage may be a RG issue to be addressed in the near future. The current standards endorsed by RG 1.180 Rev. 2 and the evaluated frequency spectrums cover up to the 40 GHz upper bound of the wireless networks expected to be implemented in NPPs. However, this does not even cover the upper bound of existing technologies. For example, 5G has a spectrum of up to 60 GHz. The operational frequency band for WiMAX is 10–60 GHz. The FCC now regulates frequencies all the way up to 300 GHz, and radio transmitters and receivers operating at frequencies higher than 60 GHz are readily available. IEEE 802.11d, 802.11aj, 802.153c, and 802.16 all address spectrums up to 60 GHz.

And the spectrum situation remains in flux. The FCC recently took action to reallocate a portion of the 3.7–4.2 GHz frequency band, making the frequency spectrum from 3.7–3.98 GHz available for flexible use, including 5G applications. The aviation industry noted in the FCC rulemaking process that deployment of 5G networks in this frequency band may introduce harmful RF interference to radar altimeters currently operating in the globally allocated 4.2–4.4 GHz aeronautical band. Some of the tests endorsed by RG 1.180 cover this frequency band, so any risks introduced by the use of 5G should be of interest for potential gaps in testing of radiated emission and conducted susceptibility tests.

These issues are not the sole concern of the nuclear industry though. It is informative to note the following analysis.  In its assessment of interference from 5G, RTCA used technical information supplied by the mobile wireless industry and radar altimeter manufacturers to provide a quantitative evaluation of radar altimeter performance regarding RF interference from expected 5G emissions in the 3.7–3.98 GHz band, as well as a detailed assessment of the risk of such interference occurring and impacting aviation safety [78]. The results presented by the RTCA in its whitepaper reveal a major risk that 5G telecommunications systems in the 3.7–3.98 GHz band will cause harmful interference to radar altimeters on all types of civil aircraft. Their conclusion is that the safe interference limits are exceeded, as well as the breadth of the impacts to aviation safety. The risk of harmful interference to radar altimeters cannot be adequately mitigated by the aviation industry acting alone.

Overall, the conducted/radiated emissions/immunity evaluations in RG 1.180, without further detailed comparison and review, appear to remain sufficient for most applications. One notable exception is cellular. Still, as discussed previously, there are positive indications that the immunity exhibited by these components confers wideband immunity which may well encompass the higher frequency range. But the fact remains that with the rapidly expanding use of wireless technology and the many different choices, gaps in the current revision of the RG do exist with varying levels of importance that will need to be addressed.

### 3.5.6 Uncertainty

In actuality, uncertainty may be the most critical part of this analysis. Knowing how much we don’t know can help us maintain the risk at an acceptable level.  As defined, measurement uncertainty is the best estimated quantity by which a measured value differs from the true value of a parameter under evaluation. Determining the operational characteristics of the device with respect to EMC compliance requires both emission and immunity measurements. IEEE/ANSI C63.23-2012 [79] describes uncertainty contributors for the conducted and radiated emission EMC test methods, and it illustrates EMC measurement instrumentation uncertainty estimations using example numeric values.

RG 1.180 Rev. 2 and the standards endorsed by RG 1.180 Rev. 2 do not specifically address uncertainty of the radiated and conducted emissions and immunity from those emissions. However, one of the major changes made from EPRI TR-102323, Rev. 0 to Rev. 1 [37] and accepted by the NRC staff as one method of addressing issues of EMC for safety-related digital I&C systems in NPPs [41] was "an increase of the margin between the allowable plant emissions limit and the susceptibility limit from 6 to 8 dB." Increasing the susceptibility limit from 6 to 8 dB accounts for measurement uncertainty [80].

### 3.5.7 Cybersecurity

Cybersecurity is the protection of data and systems from unauthorized access or attack, and it applies to both wired and wireless systems. The purpose of cybersecurity assessments is to detect and then eliminate or mitigate vulnerabilities in the digital system that could be exploited either from outside or inside the digital system protected area.

All the vulnerabilities that exist in a conventional wired network apply to wireless technologies. Malicious entities may gain unauthorized access to an agency's computer network through wireless connections, bypassing any firewall protections.

RG 1.180 Rev. 2 and the standards endorsed by it do not address cybersecurity of wireless networks. However, cybersecurity is addressed elsewhere such as in RG 5.71, Revision 1 "Cybersecurity Programs for Nuclear Power Reactors" [81] and should be considered as outside the scope of RG 1.180.

# 4. TESTING

## 4.1 ANALYSIS OF EXCLUSION ZONE FORMULA

The exclusion zone formula is based on the far field effects from a portable transceiver.

### 4.1.1 Introduction

RG 1.180 Rev. 2 states that "the minimum distance of an exclusion zone (d) in meters should be calculated as follows:

$$d = \frac{\sqrt{30 P_t G_t}}{E} \ (meters)$$

where

d = the far field distance from the portable transceiver (m),
$P_t$ = the effective radiated power of the EMI/RFI emitter (watts),
$G_t$ = the gain of the EMI/RFI emitter antenna (G=1 is the worst case), and
E = the allowable radiated electric field strength of the EMI/RFI emitter (V/m) at the point of installation."

The purpose of this section is to analyze this equation and comment on the assumptions upon which it is based. It is not to be construed as an endorsement of a radiated susceptibility level for I&C systems; nor is it to be interpreted as a validation of the RF propagation model assumed in the formula for use in any environment.

### 4.1.2 Derivation

The following derivation illustrates some of the simplifications applied to the basic signal propagation formula to develop the RG 1.180 calculation and discusses some limitations as well as unique characteristics of different waveforms. However, it is not a complete and exhaustive analysis.

From the Friis transmission equation [82],

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 ,$$

where

$P_t$ = average transmitter power (watts)
$P_r$ = average received power (watts)
$G_t$, $G_r$ = transmitter and receiver gain, respectively (unitless)
$\lambda = c/f$ = signal wavelength (meters)
$c$ = speed of light (meters per second)
$f$ = signal carrier frequency (hertz), and
$d$ = distance between transmitter and receiver (meters).

Solving for $d$,

$$d = \sqrt{\frac{P_t G_t G_r \lambda^2}{P_r (4\pi)^2}}.$$

The receive antenna can be modeled as an “equivalent aperture” with a surface area $A_e$ (meters squared) given by

$$A_e = \frac{G_r \lambda^2}{4\pi} \quad \Rightarrow \quad G_r = \frac{A_e 4\pi}{\lambda^2};$$

thus,

$$d = \sqrt{\frac{P_t G_t \lambda^2}{P_r (4\pi)^2} \frac{A_e 4\pi}{\lambda^2}} = \sqrt{\frac{P_t G_t A_e}{P_r 4\pi}}.$$

The average received power is approximately equal to the product of the receive aperture size $A_e$ times the time averaged Poynting vector magnitude $S_{ave}$, which is given by

$$S_{ave} = \frac{E_{rms}^2}{Z_0},$$

where $E_{rms}$ is the RMS electric field amplitude (volts/meter), and $Z_0 \approx 120\pi$ is the characteristic impedance of free space (ohms). Thus,

$$P_r \approx S_{ave} A_e = \frac{E_{rms}^2}{Z_0} A_e,$$

and

$$d = \sqrt{\frac{P_t G_t A_e 120\pi}{E_{rms}^2 A_e 4\pi}} = \frac{\sqrt{30 P_t G_t}}{E_{rms}},$$

which superficially matches the formula for the exclusion zone in RG 1.180.

The report [1] states that $P_t$ is “effective radiated power.” To be strictly correct, $P_t$ is simply the transmitter power, not the effective radiated power, which is a term of art with a different meaning.

### 4.1.3 Assumptions

The first assumption in this formula is that propagation is taking place in free space, which the Earth’s atmosphere closely approximates. However, this also implies that there is no multipath propagation [3]: that is, no signals are bouncing off of walls, floors, ceilings, and so on.

The free-space exclusion zone calculation appears to be expressed in terms of average power of the transmitter and RMS electric field amplitudes. However, if the waveform of the radio has a high crest factor, where the crest factor $K$ is defined as

$$K = \frac{E_{peak}}{E_{rms}},$$

then the peak electric field magnitude will be much higher than the formula predicts. If it is assumed that failure events usually occur as a result of high amplitude transient voltages induced in I&C circuits, then the assertion could be made that the exclusion zone distance should be calculated based on the peak amplitude rather than the RMS amplitude.

Applying this correction factor yields

$$d = K\frac{\sqrt{30P_tG_t}}{E_{peak}} .$$

For a frequency-modulated (FM) waveform, commonly used in portable analog voice radios, the crest factor is $K_{FM} = \sqrt{2} \approx 1.4$. Modern Wi-Fi physical layer protocols from 802.11g and beyond use OFDM waveforms [83]. An OFDM signal with $N$ subcarriers can have a crest factor as high as $K_{OFDM} = \sqrt{N}$. For 802.11g [84], $N = 52$, leading to a crest factor as high as $K = \sqrt{52} \approx 7.2$. Later Wi-Fi standards increase the data rate in part by increasing the number of subcarriers; 802.11ax, for example, can have as many as $2 \times 996 = 1992$ subcarriers allocated in a single resource unit [85], leading to a crest factor as high as $K = \sqrt{1992} \approx 44.6$. If the prior exclusion zone calculations assumed that interference was caused by an FM voice radio, then the exclusion zone distance should be increased by a factor $\gamma$, given by

$$\gamma = \frac{K_{waveform}}{K_{FM}} ,$$

where $K_{waveform}$ is the crest factor of the new wireless system under consideration for use in a plant environment. For the 802.11g example, the exclusion zone distance should be increased by a factor of $\gamma \approx \frac{7.2}{1.4} \approx 5.1$ relative to what the prior exclusion zone formula predicts. Once again, this is because modern waveforms are "peakier" in the time domain, which is the characteristic that the crest factor measures.

In practice, the crest factors for these OFDM waveforms will be much less than these values as a result of at least two factors:

- For the peak amplitude to be reached, all the subcarriers must be aligned in phase at the same time, which is an event that decreases in probability with an increasing number of subcarriers, and

- The limits of power amplifier technology effectively impose an upper bound on the crest factor that can be generated by the transmitter because of the peaks of the waveform getting "clipped.".

Effectively, while the peak electric field magnitude may be much higher for a modern waveform, the likelihood of this occurring, as well as the very short duration of any such high peak, mitigates the risk to the affected system. An adequate level of assurance is maintained that with the added 8 dB margin, the calculated exclusion zone distance provides sufficient protection. In addition, the FCC's determination to use average rather than peak values, discussed in a previous section, also support this finding. Therefore, the use of average power in the exclusion zone calculation is appropriate. This is an area which could be investigated further though, particularly to inform any efforts such as possibly providing relief to the 8 dB margin for the exclusion zone calculation.

### 4.1.4 Finding

This section derives the exclusion zone distance formula [1] and discusses some of its assumptions and limitations. It notes that changing waveform characteristics of modern communication protocols are not adequately captured in this equation, suggesting a possible modification that can accommodate the effect of the waveform crest factor. Further analytical and experimental study is recommended to validate these assumptions before being utilized by any standards body, government, or non-government organization.

## 4.2 TEST PERFORMANCE

The testing included exploratory evaluations of exclusion zones for broadband vs. narrow band signals. The purpose of this testing is to perform a preliminary analysis of the exclusion zone equation as given in RG 1.180, Rev. 2. There are concerns that this equation is overly conservative when applied to more modern wireless communication technologies. The equation is an integral part of the current method to protect SR/ITS from the impact from any wireless systems. However, it could present a challenge to any efforts to expand the use of wireless technologies in NPPs. Although the test results completed as part of this study cannot comprehensively address the concerns, they can inform future efforts and further research.

### 4.2.1 Introduction

RF emissions may cause adverse effects to safety systems, particularly in nuclear power plants. One approach to mitigate these effects is to establish a safe distance between the wireless device and the safety system, which is calculated using the exclusion zone formula. However, the exclusion zone formula is a simplified equation, derived to provide a means to quickly establish stand-off distances for any emitter – whether its emission is from an actual transmitter or from an inadvertent source such as a welder. Thus, there are limitations in its application, particularly with the emergence of more complex waveforms in modern wireless technologies. Again, the purpose of these tests is to begin to evaluate the validity of the exclusion zone formula for use with modern wireless technologies and to make an initial determination as to if it should be refined.

### 4.2.2 Evaluation of the Exclusion Zone

Although discussed in depth previously in this report, it is useful to again consider the purpose, derivation and application of the exclusion zone formula. This formula provides a guideline for establishing a safe distance between a wireless device and a safety system to minimize the potential for adverse effects on the safety system from the wireless device's RF emissions. The formula is a simplified form derived from more complex equations. These initial equations consider several variables, such as the frequency of the RF emission, whereas the exclusion zone equation only considers the power of the emission, antenna gain, and threshold electric field level at which the safety system may be impacted. The equation also only considers one emitter in free space. However, even though this equation is a simplified derivative formula, it does provide adequate protection to SR/ITS systems. To further increase the safety margin, an additional 8 dB value is added to increase separation distance required, which is reflected in the 4 V/m discussed below.

The exclusion zone formula used in this project and repeated here for convenience is

$$d = \frac{\sqrt{30 P_t G_t}}{E} \, (meters),$$

where

d = the far field distance from the portable transceiver (m),
$P_t$ = for the wireless device, $P_t$ is the average transmitter radiated power of the EMI/RFI emitter (watts),
$G_t$ = the gain of the EMI/RFI emitter antenna (G=1 for an isotropic emitter), and
E = the allowable radiated electric field strength of the EMI/RFI emitter (V/m) at the point of installation.

In this analysis, the $G_t$ is assumed to be 1 and *E* of concern is 4 V/m. *d* is in meters. The gain is set to one for these analyses to simplify the process. Any recorded values from the tests will integrate the antenna gain into the values. In addition, the 4 V/m E field is based on the recommended susceptibility as referred to in RG 1.180 Rev 2 for SR/ITS with the addition of an 8 dB margin for increased safety.

However, because the exclusion zone formula is simplified, it has limitations, particularly when used with newer wireless technologies that use more complex waveforms. The formula was originally designed to protect safety systems from such devices as basic analog voice radios or inadvertent emitters such as welders. For newer wireless technologies such as those used in Wi-Fi or cellular devices, the equation may not be entirely applicable. However, as it currently exists, the equation does provide an adequate level of separation between SR/ITS systems and wireless devices.

Additionally, the values used for $P_t$ may not be representative of actual situations, because the actual power level is situationally dependent. Possible issues with the exclusion zone formula include the use of device certified values for $P_t$, which may not be the actual $P_t$ at which the device will be operating. In actual use, the power level will often be much lower. Furthermore, the power level can be locked to a lower level for the specific device. In these cases, the calculated distance may thus be overly conservative.

A preliminary evaluation was conducted to determine the appropriateness of the exclusion zone formula for these uses and to determine whether it needs refinement for modern wireless technologies. The testing plan involves multiple steps. The first step is to use an analog radio to emit RF signals and measure the electric field strength at various distances from the radio to evaluate the formula in its current use. This is a confirmatory test. Subsequent testing evaluated other device types using modern wireless technologies to determine and evaluate the calculate distances vs. the actual values recorded.

The tests were performed using certified maximum power levels, as well as measured power levels in more realistic operation modes. The 4 V/m E field value serves as a proxy for an actual SR/ITS system. Whereas future studies to consider the actual susceptibility of the equipment to the *E* field and the actual means of insult from the RFI may show a possible path to reduce the separation distance by a more accurate susceptibility limit, this is beyond the scope of this work.

In addition, there is a debate as to what value should be used for $P_t$ in this analysis. More modern waveforms have the potential for a high, very fast peak signal that can exceed the certified maximum power level. However, this pulse would be extremely short in duration. It is not expected that this fast pulse would create any significant impact on any nearby SR/ITS systems to any greater extent than the average power value. In addition, tests used for the SR/ITS systems, such as MIL-STD-416G, RS103, utilize a test signal with a power value much more similar to the average power value seen in the modern wireless waveforms. If a high peak occurs from such a modulation technique as OFDM (as used in some 802.11 devices), then the pulse, limited by device clipping/FCC limits and the very short duration of such a peak, would affect the average power very minimally. In addition, there is minimal expectation that this peak would have an impact on any of the SR/ITS systems. Furthermore, tests that would address the impact to an SR/ITS system from a peak (MIL-STD-416G, RS105) utilize much higher power levels than the peak being discussed here would achieve. Therefore, based on the established susceptibility testing and the additional information, the average power that would be recorded during these tests is sufficient.

In summary, the exclusion zone formula provides a guideline for establishing a safe distance between a wireless device and a safety system, but it has limitations and refinements for modern wireless technologies. The objective of this testing is to evaluate the validity of the exclusion zone formula, and further research may be necessary to develop more accurate and applicable guidelines for calculating safe distances between wireless devices and safety systems. However, it should again be noted that there is no indication that the current formula is deficient in providing a safe separation distance.

### 4.2.3 Process

Two types of tests were conducted as part of the evaluation of the exclusion zone formula. The first set of tests was performed in an open environment to compare actual measured values from emitters versus the values predicted by the exclusion zone equation. The tests consisted of taking various measurements at increasing distances relative to the maximum allowable field strength. The second set of tests was conducted in an anechoic chamber to eliminate external RF interference and to more accurately capture the emission characteristics of each device. It is important to note that these tests were designed to perform a quick analysis to inform future work and were not intended to be comprehensive. Limitations were known and expected.

Three representative wireless devices were chosen for the testing: a walkie-talkie, a Wi-Fi client, and a cellular phone. Information from the FCC certification and registration database was used to provide data on antenna gain and position, frequencies, power limits, and other characteristics of use when testing the devices.

### 4.2.4 Results

A subset of test data was analyzed and compared to the values predicted by the exclusion zone formula. The open environment tests were chosen for the initial evaluation as they represent the case of most uncertainty. As shown below, for the modern wireless technologies (Wi-Fi (2.45 GHz at 100 mW) and cellular (800 MHz and 100 mW)), the measured field strength values were less than the values calculated using the equation zone formula in almost all cases. In one measurement of the Wi-Fi device, the measured and calculated values were equal.

As expected, there was less deviation between the analog communication device (walkie-talkie) and the formula results. 4 of the 10 measured values were actually higher than the calculated values. However, the overall composite percent difference was still positive. In addition, this is bounded by the 8 dB added margin for the exclusion zone calculation.

Thus, it is evident that the exclusion zone equation performs as it should to protect the SR/ITS systems from an EMI/RFI source. In many cases, the calculated value may be more conservative than required. This is in line with anecdotal evidence and information from other sources available to ORNL, as well as information available to the NRC.

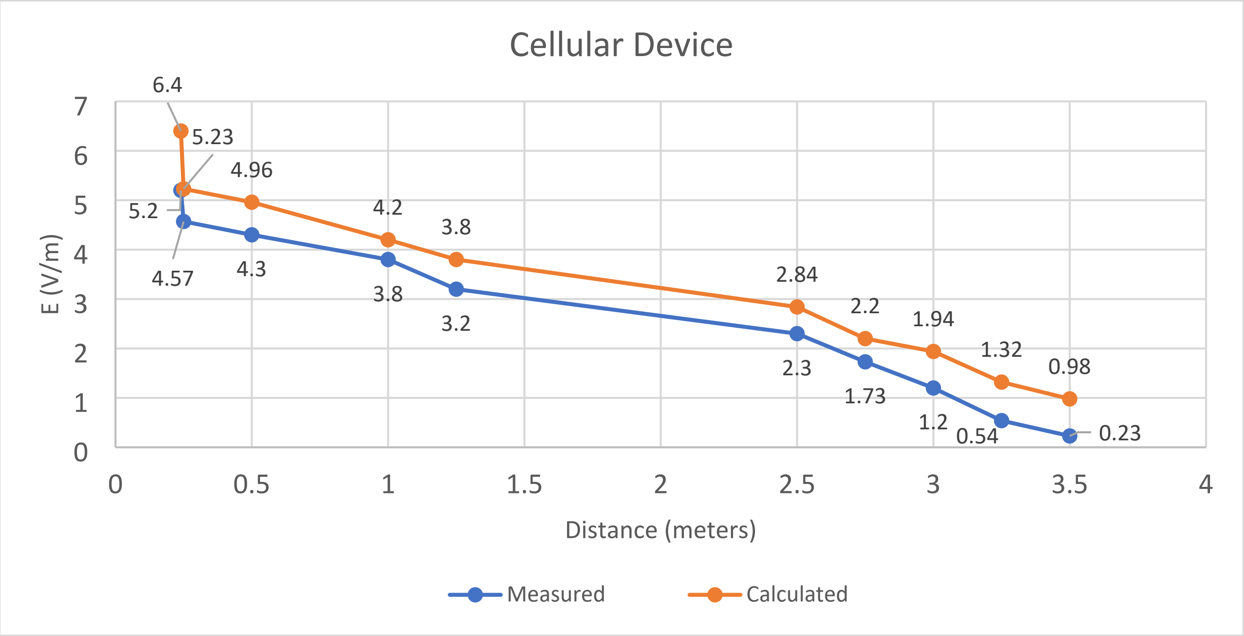


**Figure 11. Cellular device–measured E field vs. calculated E field.**

The data shown in Figure 11 is for a 100 mW cellular device with the 863 MHz signal (i.e., wavelength of 0.347 m). The 4 V/m limit occurs in the far field with the decay of 1/r. The 4 V/m limit occurs at 0.8 m and 1.1 m for the measured and calculated values, respectively.

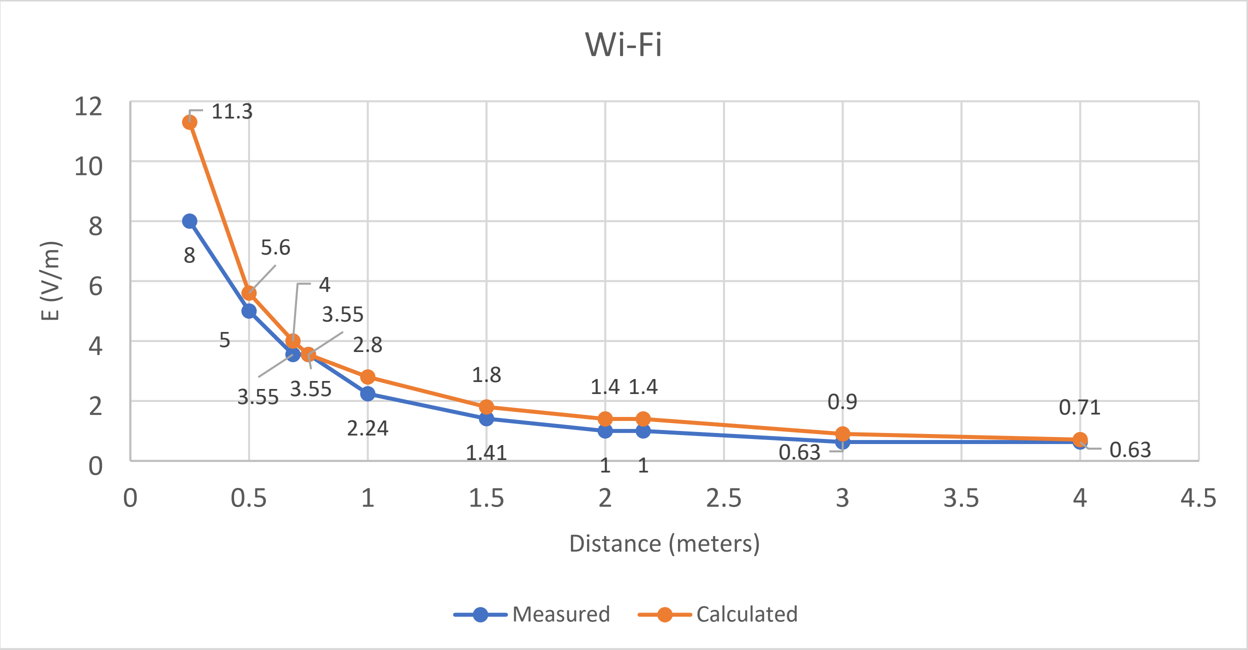


**Figure 12. Wi-Fi device–measured E field vs. calculated E field.**

The data shown in Figure 12 is for a 100 mW Wi-Fi device with a 2.45 GHz signal (i.e., wavelength of 0.122 m). The 4 V/m limit occurs in the far field with the decay of 1/r. The 4 V/m limit occurs at 0.63 m and 0.685 m for the measured and calculated values, respectively.

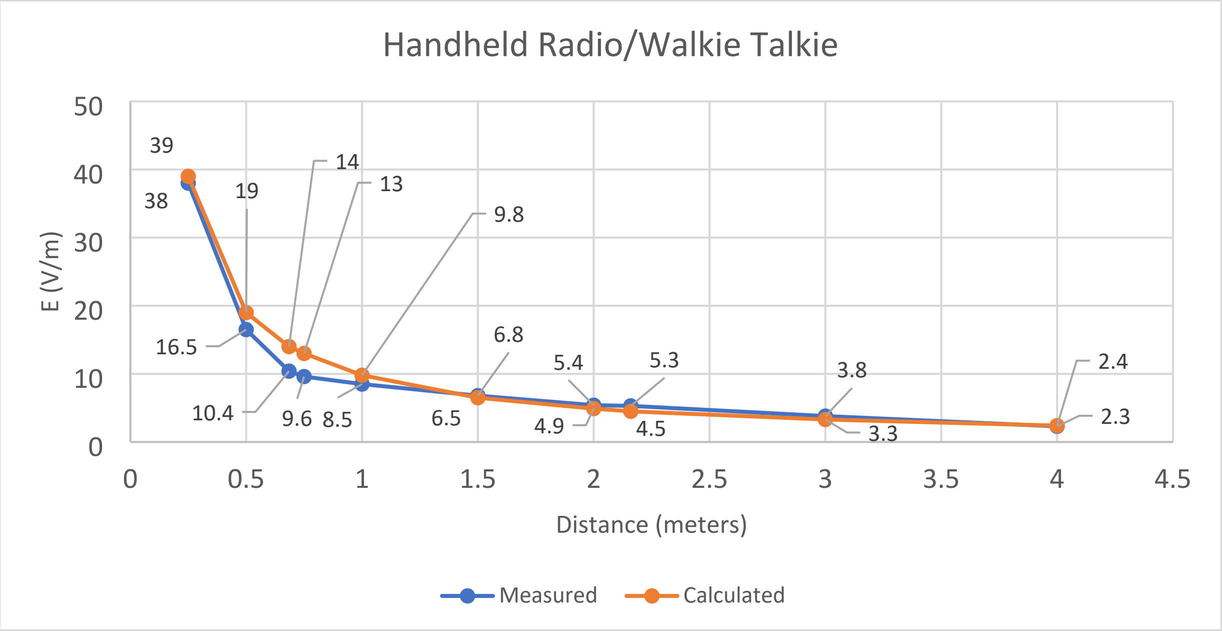


**Figure 13. Handheld radio/walkie talkie–measured E field vs. calculated E field.**

The data shown in Figure 13 is for a 2 W handheld radio with a 415 MHz signal (i.e., wavelength of 0.722 m). The 4 V/m limit occurs in the far field with the decay of 1/r. The 4 V/m limit occurs at 2.7 m and 2.5 m for the measured and calculated values for a 2 W transmitter, respectively.

**Table 4. Comparison of percent differences for measured E field vs. calculated E field values**

| Device | Max percent difference – measured value less than calculated | Max percent difference – calculated value less than measured | Composite percent difference |
|---|---|---|---|
| Cellular | 144% | 0% | 66% |
| Wi-Fi | 43% | 0% | 25% |
| Handheld radio/walkie talkie | 35% | -15% | 6.5% |

Only a subset of the recorded data was used for this initial analysis, but the entire set of test data will be used for further analysis, to include verification/validation of predictive techniques such as simulations and modeling. However, these analyses are not expected to contradict the findings from these initial tests, but rather to inform additional research.

### 4.2.5 Discussions and Implications

The testing results have shown that the exclusion zone formula in RG 1.180, Rev 2, may provide overly conservative results in many cases, particularly for modern wireless technologies. Because the purpose of the formula is to ensure a sufficient safe separation distance between EMI/RFI and SR/ITS systems, the results demonstrate that the formula achieves its intended goal. However, for increased implementation of wireless technologies in NPPs, a more accurate distance calculation may be appropriate.

# 5. CONCLUSIONS

All RG 1.180 versions discuss the use of exclusion zones to protect I&C equipment and systems. The minimum distance of the exclusion zone can be calculated using the free space propagation equation provided in RG 1.180. Exclusion zones are used to prohibit the activation of portable EMI/RFI emitters (e.g., welders and handheld communication devices) inside these areas where safety-related I&C systems have been installed. The same process can also be used to determine areas where fixed systems cannot be deployed.

The results of this review agree with previous studies showing that the exclusion zone distance provided in RG 1.180 protects I&C devices from EMI/RFI. Many other entities, such as EPRI, IAEA, and other countries, use this same method for determination of the exclusion zone distance. It may be conservative, but as a bounding case, it meets the objective. Thus, from a safety perspective, no revision is recommended for RG 1.180, Rev. 2.

RG 1.180 Rev. 2 is focused on conducted/radiated immunity/emission of EMI and RFI from portable devices on existing systems within the plant. Minimal discussion is included in the RG regarding fixed sources and primarily just to encompass all sources under the 8 dB margin of protection. However, there is evidence that due to the reduced uncertainty inherent to a fixed emitter (such as precise location, non-mobile, etc.) a relaxation of the margin may be appropriate for these devices. Still, until more data becomes available, the exclusion zone should not be reduced. Additionally, the susceptibility/immunity issue creates the greatest uncertainty in the exclusion zone calculations. The exclusion zone could potentially be reduced though if a plant couples the established exclusion zone with other efforts to increase immunity.

As the number of wireless applications increases, the spectrum has and will continue to become more crowded. The current tests and guidance at present do not cover the entire frequency range of new devices. Because RG 1.180 endorses the MIL and CISPR standards, changes to the standards would originate from those organizations instead of from NRC. Any device that transmits at a frequency higher than those in the MIL and CISPR standards would require enhanced reviews.

The 8 dB margin in RG 1.180 Rev 2 seems appropriate. Tests using calibrated testing equipment can differ by up to a 5 dB. Other uncertainties associated with testing, environment, and devices could increase the uncertainties up to the 8 dB margin. Increasing the uncertainty margin associated with the exclusion zone simply because more devices are using wireless technology is arguably an overly conservative approach and likely wasteful of spectrum or unnecessarily burdensome on system designs.

Cybersecurity threats are addressed in guidance such as RG 5.71, Rev. 1 [81]. At present, licensees must meet NRC cybersecurity requirements and their cybersecurity plans include requirements that restrict the use of wireless technologies for CDAs associated with SR/ITS functions. As the incident at Maroochy Water Services in Australia demonstrates, adequate wireless system security controls are imperative. Although the failure modes for wireless systems and CDAs may be the same, and the concerns are the same, addressing cybersecurity concerns does not fit in the scope of RG 1.180.

Although many NPPs are using wireless networks, at present, they are all in nonsafety-related applications. Applications at NPPs are based primarily on IEEE and WirelessHART standards. With increased use, it is only a matter of time until licensees begin to explore the use of wireless technologies in SR/ITS applications. In fact, one licensee has expressed interest in expanding its use in safety-related applications; this would be the first implementation of wireless technology on safety-related equipment in the nuclear industry. This could be considered outside the scope of RG 1.180. In addition, coexistence issues should be addressed elsewhere rather than in RG. 1.180.

Finally, licensees always have the option of proposing alternative methods to ensure protection of the safety systems. For example, site surveys and simulations of the environment could inform the development of appropriate limitations on wireless uses in conjunction with the option to use the exclusion zone distance. Overall, these options can all be used separately or together with in situ emission testing to evaluate proposed wireless implementations, both portable or fixed, and to confirm that acceptable levels will exist in the environment to adequately protect the safety systems.

This report reviews issues regarding the potential expanded implementation of wireless technologies at NPPs. A summary of available knowledge on the current state of wireless technology is presented. The exclusion zone calculation and its uses are considered, and possible methods to augment its application are examined. An overall finding is made that RG 1.180 Rev 2's use of this equation is bounding and adequately ensures that EMI/RFI emitters (to include wireless devices) will not adversely impact SR/ITS systems. Additionally, this report recommends that any enhancements or adjustments for the specific use of wireless technology implementations should be addressed outside of RG 1.180.

# 6. REFERENCES

1. Leroy Hardin and Erick Martinez Rodriguez, “Safety and Security Considerations for the Use of Wireless Technologies in NPPs,” *ANS Winter Meeting 2022*, Phoenix, AZ, November 13–17, 2022.
2. R. D. Meininger, W. H. Lewis, and J. W. Shank, *Handbook for Electromagnetic Compatibility of Digital Equipment in Power Plants Volume 2: Implementation Guide for EMI Control*, EPRI TR-102400 Vol. 2, Electric Power Research Institute, Palo Alto, California, October 1994.
3. ANSI C63.12-2015, American National Standard Recommended Practice for Electromagnetic Compatibility Limits and Test Levels, American National Standards Institute, Approved 18 June 2015.
4. 47 CFR Part 15, “Radio Frequency Devices.”
5. Academy of EMC, *EMC Standards*. https://www.academyofemc.com/emc-standards.
6. ISA-TR100.00.01-2006, *The Automation Engineer’s Guide to Wireless Technology Part 1 – The Physics of Radio, a Tutorial*, International Society of Automation, Approved 29 December 2006.
7. EPRI TR-1011751, *Assessment of Wireless Technologies in Substation Functions, Part II: Substation Monitoring and Management Technologies*, Electric Power Research Institute, Palo Alto, California, March 2006.
8. EPRI TR-1019186, *Implementation Guideline for Wireless Networks and Wireless Equipment Condition Monitoring*, Electric Power Research Institute, Palo Alto, California, December 2009.
9. EPRI TR-1003584, Final Report, *Guidelines for Wireless Technology in Power Plants, Volume 1: Benefits and Considerations*, Electric Power Research Institute, Palo Alto, California, December 2006.
10. The National Institute for Occupational Safety and Health (NIOSH), *Basic Tutorial on Wireless Communication and Electronic Tracking: Technology Overview*, Center for Disease Control and Prevention, accessed May 4, 2022. https://www.cdc.gov/niosh/mining/content/emergencymanagementandresponse/commtracking/commtrackingtutorial1.html
11. ISA-TR100.00.03-2011, *Wireless User Requirements for Factory Automation*, International Society of Automation, International Society of Automation, Approved 26 May 2011.
12. EPRI TR-110125, *Assessment of Emerging Technologies for Wireless Communications*, Electric Power Research Institute, Palo Alto, California, July 1998.
13. EPRI 1003697, *Guidelines for Electromagnetic Interference Testing of Power Plant Equipment, Revision 3 to TR-102323*, Electric Power Research Institute, Palo Alto, California, November 2004.
14. Process Measurement Control, Inc., PMC Document 33.1, *Electromagnetic Susceptibility of Process Control Instrumentation*, Scientific Apparatus Makers Association (SAMA), 1978.
15. MIL-STD-461C, Electromagnetic Emission and Susceptibility Requirements For The Control Of Electromagnetic Interference, Department of Defense, Washington, D.C., 4 August 1986.
16. Chaitanya Vijaykumar Mahamuni, “Sensor Node Failure Affecting Coverage of WSNs: An Overview,” October 2020.
17. B.J. Kaldenbach, et al., *Assessment of Wireless Technologies and Their Application at Nuclear Facilities*, US Nuclear Regulatory Commission, NUREG/CR-6882, US Nuclear Regulatory Commission, July 2006 (ML062140045).
18. Yanliang Zhang and Vivek Agarwal, “Thermoelectric Generator for Efficient Power Harvesting for Self-powered Sensor Nodes,” *Advanced Sensors and Instrumentation*, Issue 5, September 2016.
19. L. S. Fifield, “State of Electrical Cable Aging in U.S. Nuclear Power Plants,” *Transactions of the American Nuclear Society*, Vol. 118, Philadelphia, Pennsylvania, June 17–21, 2018.
20. D. D. Dudenhoeffer et. al., *Technology Roadmap on Instrumentation, Control, and Human-Machine Interface to Support DOE Advanced Nuclear Energy Programs*, INL/EXT-06-11862, March 2007.

21. EPRI 1010468, *Automation in Power Plants and Wireless Technology Assessments*, Electric Power Research Institute, Palo Alto, California, December 2005.
22. Peter L. Fuhr, "Secure wireless sensor networks for the monitoring and control of nuclear power plants," book chapter in *Wireless for Nuclear Power Plants in Handbook of Industrial Wireless Sensor Networks*, Woodhead Publishing/Elsevier, Oxford, United Kingdom July 2014.
23. EPRI 1007448, *Guidelines for Wireless Technology in Power Plants, Volume 2: Implementation and Regulatory Issues*, Electric Power Research Institute, Palo Alto, California, December 2002.
24. Arto Laikari, *Wireless in nuclear feasibility study*, VTT Technical Research Centre of Finland Ltd, 8.3.2018.
25. IEEE Std C62.41.1-2002, *IEEE Guide on the Surge Environment in Low-Voltage (1000 V and Less) AC Power Circuits*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 11 April 2003.
26. IEEE Std C62.41.2-2002, *IEEE Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and Less) AC Power Circuits*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 11 April 2003.
27. H. M. Hashemian, C. J. Kiger, G. W. Morton & B. D. Shumaker (2011) "Wireless Sensor Applications in Nuclear Power Plants," *Nuclear Technology*, 173:1, 8-16, DOI: 10.13182/NT11-1.
28. Brandon Rasmussen, "On-Line Monitoring System Diagnostics," Joint NRC/DOE Workshop on U.S. Nuclear Power Plant Life Extension Research and Development ("Life Beyond 60"), February 19-21, 2008 (ADAMS Accession No. ML080601302).
29. U.S. NRC, *Final Safety Evaluation by the Office of Nuclear Reactor Regulation, Topical Report WCAP-17867-P, Revision 1, Westinghouse SSPS Board Replacement Licensing Summary Report*, Pressurized Water Reactor Owners Group, September 19, 2014 (ADAMS Accession No. ML14260A143).
30. ISA-TR84.00.08-2017, *Guidance for Application of Wireless Sensor Technology to Non-SIS Independent Protection Layers,* International Society of Automation, Approved 24 April 2017.
31. A. Laikari, J. Flak, A. Koskinen & J. Häkli, *Wireless In Nuclear; Feasibility Study*, Energiforsk, Report 2018:513, July 2018.
32. EPRI 1022984, *Assessment of Electromagnetic Interference Events in Nuclear Power Plants*, Electric Power Research Institute, Palo Alto, California, 2011.
33. EPRI 1018702, R. Torok, Project Manager, *Indian Point-2 Flash Photography Event, An Independent Assessment by the EPRI Electromagnetic & Radio Frequency Interference Working Group*, Electric Power Research Institute, Palo Alto, California, March 2009.
34. Information Notice No. 97-82: Inadvertent Control Room Halon Actuation due to a Camera Flash, US Nuclear Regulatory Commission, November 28, 1997.
35. Do Young Ko and Soo Ill Lee, "Applicable approach of the wireless technology for Korean nuclear power plants," *Nuclear Engineering and Design* 265 (2013) 519– 525.
36. Arto Laikari, *Wireless In Nuclear Applications Seminar Report*, ENERGIFORSK Nuclear Safety Related I&C, ENSRIC Report 2018:514, 2018.
37. EPRI TR-102323, Rev 1, *Guidelines for Electromagnetic Interference Testing in Power Plants*, Electric Power Research Institute, Palo Alto, CA, 1996.
38. STUK, *Safety Design of a Nuclear Power Plant*, STUK Radiation and Nuclear Safety Authority, GUIDE YVL B.1, June 2019.
39. IAEA Nuclear Energy Series No. NR-T-3.29, *Application of Wireless Technologies In Nuclear Power Plant Instrumentation And Control Systems*, International Atomic Energy Agency, Vienna, 2020.
40. NUREG-0800, Subsection 9.5.2, Revision 3, "Communications Systems," US Nuclear Regulatory Commission, March 2007.
41. Letter from Bruce Boger, Director Division of Reactor Controls and Human Factors, Office of NRR, to Mr. Carl Yoder, EPRI EMI Working Group Chairman, "Review of EPRI Utility Working

Group Topical Report TR-102323, Guidelines for Electromagnetic Interference Testing in Power Plants," US Nuclear Regulatory Commission, April 17, 1996.

42. MIL-STD-461E, *Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,* Department of Defense, Washington, D.C., 20 August 1999.
43. RG 1.180, Rev. 2, *Guidelines For Evaluating Electromagnetic and Radio-Frequency Interference In Safety-Related Instrumentation And Control Systems*, US Nuclear Regulatory Commission, December 2019.
44. C. Antonescu and P. D. Ewing, *EMI/RFI and Power Surge Withstand Guidance for the U.S. Nuclear Regulatory Commission*. https://technicalreports.ornl.gov/cppr/y2001/pres/111829.pdf
45. IEEE Std 1050-1989, *IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, Approved February 2,1989.
46. Richard T. Wood and Paul D. Ewing, *Task 4 – EMI/RFI Issues Potentially Impacting Electromagnetic Compatibility of I&C Systems (NRCHQ6014D0015)*, ORNL/LTR-2015/254, Oak Ridge National Laboratory, Oak Ridge, TN, May 2015.
47. International Accreditation Forum Secretariat, " IAF MLA Committee Members," 11 August 2023. https://iaf.nu/wp-content/uploads/2021/12/MLA-Member-List.pdf
48. MIL-STD-461G, *Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,* Department of Defense, Washington, D.C., 11 December 2015.
49. Márcio S. Costa and Jorge L. M. Amaral, *Analysis of Wireless Industrial Automation Standards: ISA-100.11a and WirelessHART*, https://blog.isa.org/analysis-wireless-industrial-automation-standards-isa-100-11a-wirelesshart
50. *Information Notice No. 83-83: Use of Portable Radio Transmitters Inside Nuclear Power Plants*, US Nuclear Regulatory Commission, December 19, 1983.
51. EPRI 1020562, *Program on Technology Innovation: Impact of Wireless Power Transfer Technology Initial Market Assessment of Evolving Technologies, Final Report*, Electric Power Research Institute, Palo Alto, California, December 2009.
52. EPRI 3002015757, *Guidelines for Electromagnetic Compatibility Testing of Power Plant Equipment: Revision 5 to TR-102323*, Electric Power Research Institute, Palo Alto, California, Dec 16, 2019.
53. P. D. Ewing and R. T. Wood, *Recommended Electromagnetic Operating Envelopes for Safety-Related I&C* ***S****ystems in Nuclear Power Plants*, NUREG/CR-6431, US Nuclear Regulatory Commission, January 2000 (ML003706139).
54. EPRI TR-102323, *Guidelines for Electromagnetic Interference Testing in Power Plants*, Electric Power Research Institute, Palo Alto, CA, 1994.
55. Song-Hae Ye, Yong-Sik Kim, Ho-Sun Lyou, Min-Suk Kim, and Joon Lyou, "The applications of wireless technology for operating Nuclear Power Plants," *2014 14th International Conference on Control, Automation and Systems (ICCAS 2014)*, 22-25 Oct. 2014.
56. EPRI TR-1000603 [Revision 2 to EPRI TR-102323], *Guidelines for Electromagnetic Interference Testing in Power Plants*, Electric Power Research Institute, Palo Alto, CA, 2000.
57. Philip F. Keebler, "Eliminating the Need for Exclusion Zones in Nuclear Power Plants," *IN Compliance*, June 1, 2011. https://incompliancemag.com/article/eliminating-the-need-for-exclusion-zones-in-nuclear-power-plants/
58. EPRI 3002000528, *Guidelines for Electromagnetic Compatibility Testing of Power Plant Equipment: Revision 4 to TR-102323*, Electric Power Research Institute, Palo Alto, California, Dec 08, 2013.
59. Chris L. Lowe, Chad J. Kiger, David N. Jackson, David M. Young, "Implementation of Wireless Technologies in Nuclear Power Plants' Electromagnetic Environment Using Cognitive Radio System," *NPIC&HMIT 2017*, San Francisco, CA, June 11-15, 2017.
60. Ataul Bariand & Jin Jiang (2014) "Deployment Strategies for Wireless Sensor Networks in Nuclear Power Plants," *Nuclear Technology*, 187:1, 82-95, DOI: 10.13182/NT13-1

61. Chad Kiger, *Overview of Wireless Technology Implementation," Scientech User Group Meeting*, August 10, 2015. https://www.cw-connect.com/sites/default/files/2020-01/Overview_of_Wireless_Technology_Implementation_2015.pdf
62. American National Standards Institute, *American National Standard for Evaluation of Wireless Coexistence*, ANSI C63.27-2017, IEEE, Piscataway, NJ (2017).
63. S. W. Kercel, M. R. Moore, E. D. Blakeman, P. D. Ewing, and R. T. Wood, "Survey of Ambient Electromagnetic and Radio-Frequency Interference Levels in Nuclear Power Plants," NUREG/CR-6436, US Nuclear Regulatory Commission, November 1996.
64. IEEE Std 1900.2-2000 [Inactive], *IEEE Recommended Practice for the Analysis of In-Band and Adjacent Band Interference and Coexistence Between Radio Systems*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 29 July 2008.
65. Galen Koepke, William Young, John Ladbury, and Jason Coder, *Complexities of Testing Interference and Coexistence of Wireless Systems in Critical Infrastructure*, NIST Technical Note 1885, U.S. Department of Commerce, National Institute of Standards and Technology, July 2015.
66. IEEE Std 802.11-2020, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, Approved 3 December 2020.
67. IEEE Std 802.15.4-2020, *IEEE Standard for Low-Rate Wireless Networks*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, Approved on 6 May 2020.
68. M. Howlader, C.J. Kiger, and P.D. Ewing, *Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment*, NUREG/CR-6939, ORNL/TM-2006/86, US Nuclear Regulatory Commission, July 2007 (ML072210179).
69. IEEE Std 802.15.2-2003(R2009), *IEEE Recommended Practice for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, Reaffirmed 13 May 2009 (WITHDRAWN).
70. IEEE 15.1-2005, Part 15.1: *Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 14 June 2005.
71. IEEE Std 802.19.1-2018, *IEEE Standard for Information technology--Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 19: TV White Space Coexistence Methods*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 02 November 2018.
72. IEC 62657-2017, Industrial communication networks - Wireless communication networks - Part 2: Coexistence management, International Electrotechnical Commission, Geneva, 2017.
73. CTIA - The Wireless Association (CTIA) and Wi-Fi Alliance (WFA), "Test Plan for RF Performance of Wi-Fi Mobile Converged Devices," Version 1.3, June 2009.
74. Email from Christy A. Bahn, Senior Program Manager, Operational Program Management, IEEE Standards Association (IEEE SA) to Michael Muhlheim, RE: IEEE 802.15.2, March 8, 2023.
75. MIL-STD-464D, *Electromagnetic Environmental Effects Requirements For Systems*, Department of Defense, Washington, D.C., 24 December 2020.
76. Philip Keebler and Stephen Berger, "Managing the Use of Wireless Devices in Nuclear Power Plants," *InCompliance Magazine*, November 1, 2011. https://incompliancemag.com/article/managing-the-use-of-wireless-devices-in-nuclear-power-plants/
77. ANSI C63.15-2017, "*American National Standard—Recommended Practice for the Immunity Measurement of Electrical and Electronic Equipment*," The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 13 July 2017.

78. RTCA Paper No. 274-20/PMC-2073, *Assessment of C-Band Mobile Telecommunications Interference Impact on Low Range Radar Altimeter Operations*, RTCA, Inc., Washington, DC, October 7, 2020.
79. ANSI C.63.23-2012 (Reaffirmed 2020), *American National Standard Guide for Electromagnetic Compatibility—Computations and Treatment of Measurement Uncertainty*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 2013.
80. Song-Hae Ye, Yong-Sik Kim, Ho-Sun Lyou, Min-Suk Kim, and Joon Lyou, "The applications of wireless technology for operating Nuclear Power Plants*," 2014 14th International Conference on Control, Automation and Systems (ICCAS 2014)*, 22-25 Oct. 2014.
81. Regulatory Guide 5.71, Revision 1, *Cybersecurity Programs For Nuclear Power Reactors*, US Nuclear Regulatory Commission, February 2023. (NRC ADAMS Accession No. ML22258A204)
82. W. L. Stutzman and G. A. Thiele, *Antenna Theory and Design*, 3rd Ed., Wiley, 2013.
83. A. Goldsmith, *Wireless Communications*, Cambridge University Press, Aug 8, 2005.
84. IEEE 802.11g, Part 11: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 2003.
85. IEEE 802.11ax, Part 11: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 2021.

# APPENDIX A. TYPES OF WIRELESS NETWORKS

An overview of the cost/complexity vs. the data rates of some of the most common standards for wireless networks is shown in Figure A.1. Low-rate wireless personal area networks (LR-WPANs) are at the lower end of cost/complexity. WPAN and WLAN have increased cost/complexity while providing greater data rates. The wireless metropolitan area network (WMAN) has increased cost/complexity but does not support higher data rates. At the high end is the wireless wide area network (W-WAN). Not surprisingly, satellite is the most costly and complex and requires the largest amount of power. The communication protocols used in those networks could be Wi-Fi (wireless fidelity), Bluetooth, 5G, Zigbee, and so on (Appendix C).

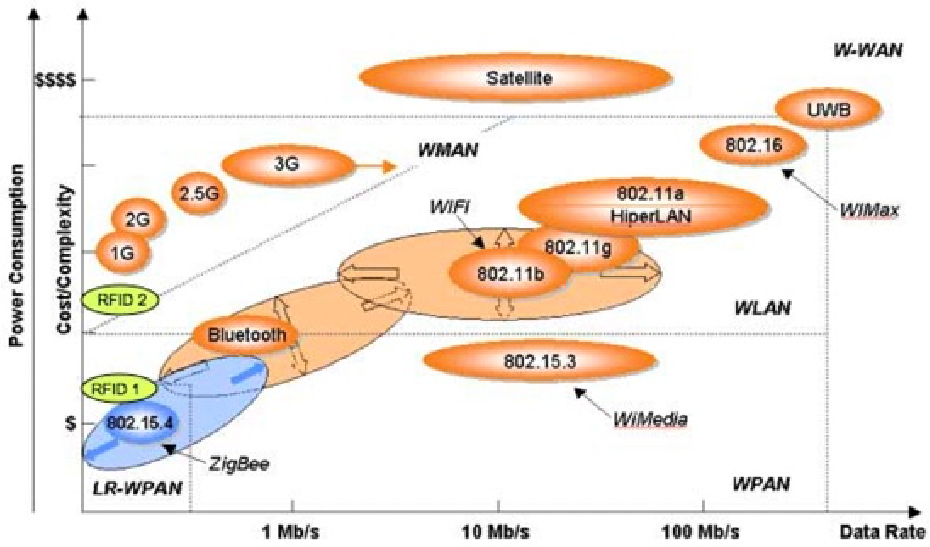


**Figure A.1. Overview of cost/complexity vs. data rates of many wireless technologies [A.1].**

Several standards describe the general requirements for I&C systems in NPPs; however, they are outside the scope of this review but are included because they are in use at those NPPs with wireless capabilities.

## A.1 WLAN

WLAN is a wireless network providing communication between computers, smartphones, tablets, and so on, within a limited area such as an office building or industrial plant. WLAN transmits information over radio waves. Data are sent in packets that contain layers with labels and instructions. The unique media access control addresses are assigned to endpoints, enabling routing to intended locations.

IEEE 802.11 is the dominant WLAN standard, but others have also been defined. WLAN transmits data in the 5 GHz band and operates at data rates of approximately 23.5 Mbps [A.2].

Wi-Fi is the universal standard for connecting laptops and mobile devices in a home or office. It is commonly deployed alongside of ethernet, and both wireless and wired devices can exchange data with each other for backup and file sharing.

The benefits of WLAN are its standardization and interoperability that even work for older computer-based control systems. It is also easily deployable/integrated into the overall system. Disadvantages include its limited range and its greater surface for cyberattacks compared to that of hard-wired systems.

### A.2 WPAN

Wireless personal area networks (WPANs) are small-scale wireless networks that require little or no infrastructure. A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables. Its range is from a few centimeters to a few meters. A WPAN can be implemented using technologies including infrared, Bluetooth, and ZigBee (low data rates up to 250 kbps).

Typical applications are connections between computers, smartphones, and peripherals such as remote controllers, wireless printer connections, wireless computer keyboards, wireless mouse devices, speakers, headsets, and wearable devices [A.3].

Examples of WPAN standards include the following [A.2]:

- IEEE 802.15.1 (Bluetooth). This WPAN standard is designed for wireless networking between small portable devices. The original Bluetooth operated at 2.4 GHz and has a maximum data rate of approximately 720 kilobits per second (Kbps); Bluetooth 2.0 can reach 3 Mbps.

- IEEE 802.15.3 (High-Rate Ultrawideband; WiMedia, Wireless USB). This is a low-cost, low power consumption WPAN standard that uses a wide range of GHz frequencies to avoid interference with other wireless transmissions. It can achieve data rates of up to 480 Mbps over short ranges and can support the full range of WPAN applications.

- IEEE 802.15.4 (Low-Rate Ultrawideband; ZigBee). This is a simple protocol for lightweight WPANs. It is most commonly used for monitoring and control products, such as climate control systems and building lighting.

### A.3 WMAN

Wireless metropolitan area networks (WMAN) are networks that provide wireless broadband access over longer distances than WLAN can provide, ranging up to several miles. This type of network is also known as the Worldwide Interoperability for Microwave Access WiMAX). WiMAX licensed bands include 2.3, 2.5, and 3.5 GHz [A.3]. For example, IEEE 802.16e (better known as WiMAX) is a WMAN standard that transmits in the 10 to 66 GHz band range. An IEEE 802.16a addendum allows for large data transmissions with minimal interference. WiMAX provides throughput of up to 75 Mbps, with a range of up to 30 miles for fixed line-of-site communication. However, there is generally a tradeoff; 75 Mbps throughput is possible at half a mile, but at 30 miles the throughput is much lower [A.2].

### A.4 W-WAN

A wide-area network, or WAN, is a telecommunications network that connects various local area networks to each other, cloud servers, and elsewhere thereby allowing users to share access to applications, services, and other centrally located resources.

A wireless WAN (W-WAN) often differs from wireless local area network (WLAN) by using mobile telecommunication cellular network technologies such as 2G, 3G, 4G LTE, and 5G to transfer data. W-WAN connectivity allows a user to connect from anywhere within the regional boundaries of cellular service.

W-WAN, which is at the high end of the wireless networks, is the result of such mergers allowing worldwide coverage by interconnecting WLANs and WMANs through routers, repeaters, and even satellites to form geographical areas in the range of 15 km. Wireless connectivity to WANs is achieved using the Mobil-Fi protocol, which is based on the IEEE 802.20 standard. This wireless technology extends high-speed wireless access to mobile users with a relatively fast data rate of 1 Mbit/s. Not surprisingly, satellite is the most costly and complex and requires the largest amount of power.

### A.5 LoRaWAN

While the other WANs have been around longer and are frequently updated, the LoRa modulation technique was invented in 2010 by Cycleo and was acquired in 2012 by Semtech. LoRaWAN is a technology standard developed and supported by the LoRa Alliance, which consists of international telecommunications companies and manufacturers, as well as integrators. LoRaWAN (Low-power Wide-area Network) specification is open-source; it has been supported and maintained by the LoRa Alliance since 2015. LoRaWAN networks are wireless and have a wide coverage radius. The LoRa Alliance reports that the main advantage of such networks is low power consumption, and the amount of data transfer in such networks is measured in bytes, but this is enough to transmit the necessary telemetry from the end device to the dispatcher server. Basically, devices with LPWAN connection are typical microcontrollers with minimal power consumption and a wireless network interface. These devices usually communicate with their gateway (base station), which has an IP address for accessing the internet. Key elements of a LoRaWAN network are the devices that send and receive messages in the LoRA wireless network, the Gateway that works as a relay that sends all messages from the end devices and transmits them to the network server and back, the network server that manages and maintains the LoRA network, and the application server that sends the messages to the client's final application.

LPWANs can accommodate data packets sizes from 10 bytes to 1 kB at uplink speeds up to 200 kbps; long-range connectivity varies from 2 to 1,000 km depending on the network technology. Most LPWAN technologies have a star topology, which means that each device connects directly to a central access point.

### A.6 REFERENCES

A.1 EPRI TR-1011751, *Assessment of Wireless Technologies in Substation Functions, Part II: Substation Monitoring and Management Technologies*, Electric Power Research Institute, Palo Alto, California, March 2006.

A.2 Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-97, U.S. Department of Commerce, National Institute of Standards and Technology, February 2007.

A.3 A. Laikari, J. Flak, A. Koskinen & J. Häkli, *Wireless In Nuclear; Feasibility Study*, Energiforsk, Report 2018:513, July 2018.

# APPENDIX B. INTERNATIONAL AND DOMESTIC STANDARDS

International and domestic standards define test setups, testing techniques, test equipment, test environment and other considerations regarding EMC emission testing, immunity testing, and measurement. The classifications and descriptions of different EM environments and compatibility levels are also provided. In some standards, the installation and mitigation guidelines regarding earthing and cabling, mitigation of external EM influences, HEMP protection concepts, and so on, are provided.

The following subsections provide details on the EMC standards, some of which are for testing, and some of which provide a system-based view. These standards were not reviewed, but they are discussed here for informational purposes.

## B.1 INTERNATIONAL STANDARDS

There are about 50 technical committees and subcommittees preparing and publishing EMC product standards. Standards in EMC are either defined and developed by international and national or regional organizations and committees on behalf of administrative bodies (like the EU delegates who draft EMC Standards to the European Committee for Electrotechnical Standardization [CENELEC]), or the administrative and/or regulatory bodies draft the EMC standards and regulations themselves. Table B.1 lists the international and national (regional) organizations and committees that develop and/or define the applicable EMC standards [B.1]:

**Table B.1. International and National Organizations That Develop EMC Standards.**

| | |
|---|---|
| **IEC** | International Electrotechnical Commission (IEC) |
| **IEEE** | Institute of Electrical and Electronic Engineers (IEEE) |
| **ISO** | International Organization for Standardization (ISO) |
| **ITU-T** | ITU Telecommunication Standardization Sector (ITU-T) |
| **CIGRE** | International Council on Large Electric Systems (CIGRE) |
| **Eurelectric** | The Union of the Electricity Industry (Eurelectric) |
| **OIML** | International Organization of Legal Metrology (OIML) |
| **Australia / New Zealand** | Standards Australia (AS)<br>Standards New Zealand (NZS) |
| **Canada** | Canadian Standards Association (CSA) |
| **China** | Standardization Administration of China (SAC, representing China in National in ISO and IEC committees)<br>SAC/TC79: National Radio Interference Standardization Technical Committee (the corresponding Chinese committee to IEC/CISPR)<br>SAC/TC246: National Electromagnetic Compatibility Standardization Technical Committee (the corresponding Chinese committee to IEC/TC77) |
| **Europe (EU)** | Comité Européen de Normalisation Electrotechniques (CENELEC)<br>European Telecommunications Standards Institute (ETSI)<br>European Committee for Standardization (CEN) |
| **Germany** | Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) |
| **India** | Bureau of Indian Standards (BIS) |
| **Japan** | Japanese Industrial Standards Committee (JISC)<br>Japanese Standards Association (JAS) |
| **Korea** | Korean Standards Association (KSA) |

**Table 4. International and National Organizations That Develop EMC Standards (continued).**

| | |
|---|---|
| **RTCA** | Radio Technical Commission for Aeronautics (RTCA) |
| **Russia** | Federal Agency for Technical Regulation and Metrology (GOST R) |
| **Russia, Azerbaijan, Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Turkmenistan, Uzbekistan, Ukraine** | Euro Asian Council for Standardization, Metrology and Certification (EASC) |
| **Singapore** | Info-Communications Media Development Authority (IMDA) |
| **Turkey** | Turkish Standards Institution (TSE) |
| **United Kingdom (UK)** | British Standards Institution (BSI) |
| **United States (USA)** | Association for the Advancement of Medical Instrumentation (AAMI)<br>American National Standards Institute (ANSI)<br>US Department of Defense (DoD)<br>Federal Communications Commission (FCC)<br>Radio Technical Commission for Aeronautics (RTCA)<br>Society of Automotive Engineers (SAE) |

Many of the standards and organizations have adopted the IEC and CISPR standards. For example, Standards Australia (AS) and Standards New Zealand (NZS) have adopted many of the IEC and CISPR standards for EMC. CSA has adopted the IEC standards that are renamed *CSA-IEC*. The European Union (EU) EMC standards are closely related to the international EMC standards, and they start with the letters *EN,* or *European Norm*. EN standards are developed by CENELEC, CEN, and ETSI and are generally harmonized with the international IEC/CISPR standards. The main organizations and associations governing wireless technology that are working to develop standards at the time of this report include [B.2, B.3, B.4] CISPR, IEC, IEEE, and RTCA.

A comparison between the endorsed IEC standards and the IEEE standards was not performed in this review.

### B.1.1 CISPR

The Comité International Spécial des Perturbations Radioélectriques (CISPR; English: International Special Committee on Radio Interference) was founded in 1934 to set standards for controlling EMI in electrical and electronic devices and is a part of the IEC. The IEC 61000-6-4 tests address measurement of emissions for electrical and electronic equipment intended for use in industrial environments in the frequency range from 150 kHz to 6 GHz. IEC 61000-6-4 incorporates the test methods of CISPR 16 by reference and is endorsed for use by RG 1.180. Table B.2 provides a list of the most commonly applied CISPR standards.

**Table B.2. CISPR EMC Standards.**

| Number | Title | Endorsed by RG 1.180 | Test type |
|---|---|---|---|
| CISPR 11 | Industrial, scientific and medical equipment - Radio-frequency disturbance characteristics - Limits and methods of measurement | No | Conducted, Radiated |
| CISPR 12 | Vehicles, boats and internal combustion engines - Radio disturbance characteristics - Limits and methods of measurement for the protection of off-board receivers | No | |
| CISPR 13 (withdrawn) | Sound and television broadcast receivers and associated equipment - Radio disturbance characteristics - Limits and methods of measurement | No | |
| CISPR 14 | Electromagnetic compatibility - Requirements for household appliances, electric tools and similar apparatus - Part 1: Emission | No | Emission |
| CISPR 15 | Limits and methods of measurement of radio disturbance characteristics of electrical lighting and similar equipment | No | |
| CISPR-16-1-1 | Specification for radio disturbance and immunity measuring apparatus and methods – Part 1-1: Radio disturbance and immunity measuring apparatus – Measuring apparatus | No | |
| CISPR-16-2-1 | Specification for radio disturbance and immunity measuring apparatus and methods – Part 2-1: Methods of measurement of disturbances and immunity – Conducted disturbance measurements | Yes | Conducted, Radiated |
| CISPR-16-2-3 | Specification for radio disturbance and immunity measuring apparatus and methods – Part 2-3: Methods of measurement of disturbances and immunity – Radiated disturbance measurements | Yes | Conducted, Radiated |
| CISPR 22 | Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement | No | |
| CISPR 32 | Electromagnetic compatibility of multimedia equipment - Emission requirements | No | Conducted, Radiated |

### B.1.2 IEC

Before international standards for the application of wireless technologies in NPPs were available, IEC published IEC Technical Report 62918 [B.5] for NPPs on the selection and use of wireless devices to be integrated into systems important to safety. IEC later published the standard IEC 62988 [B.6] to address the selection and use of wireless devices in NPPs. More IEC standards have been developed for the use of wireless technologies in industrial environments that may be informative for wireless applications in NPPs [B.7, B.8].

IEC 62591 [B.9], the WirelessHART system engineering guideline, applies to end user adoption of WirelessHART self-organizing mesh networks to automate process manufacturing projects of any size.

An automated coexistence management concept to use the spectrum efficiently is specified in IEC 62657-1 [B.7]. More information on these types of issues may be found in IEC 62657-2 [B.8].

Table B.3 provides a summary of the IEC wireless standards.

**Table B.3. IEC wireless standards**

| IEC wireless standard | Name/application |
|---|---|
| IEC TR 62918 | Use and Selection of Wireless Devices |
| IEC 62988:2018 | Selection and Use of Wireless Devices |
| IEC 62657-1:2017 | Wireless Communication Requirements and Spectrum Considerations |
| IEC 62657-2017 | Coexistence Management |
| IEC 62591:2016 | WirelessHART |

RG 1.180 Rev. 2 endorses many of the IEC 61000 series of EMI/RFI test methods, extending the guidance to cover signal line testing, incorporating frequency ranges where portable communications devices are experiencing increasing use, and relaxing the operating envelopes (test levels) when experience and confirmatory research warrants.

The IEC 61000-6-4 test method for EMI/RFI emissions as endorsed by RG 1.180 Rev. 2 is as follows:

- Conducted emissions, low frequency, 30 Hz to 10 kHz
- CISPR 16—Conducted emissions, high frequency, 150 kHz to 30 MHz
- Radiated emissions, magnetic field, 30 Hz to 100 kHz
- CISPR 16—Radiated emissions, electric field, 30 MHz to 6 GHz

IEC 61000-6-4 incorporates the test methods of CISPR 16 by reference. IEC standards of interest are listed in Table B.4.

**Table B.4. IEC EMC standards**

| Number | Title | Endorsed by RG 1.180 | Test type |
|---|---|---|---|
| IEC 61000-3-2 | Methods for harmonic current emissions | No | Emission |
| IEC 61000-3-3 | Methods for voltage fluctuation and flicker | No | Emission |
| IEC 61000-4-2 | Electrostatic Discharge Immunity test | No | Conducted |
| IEC 61000-4-3 | Radiated susceptibility, electric field, 26 MHz to 6 GHz | Yes | Conducted |
| IEC 61000-4-4 | Conducted susceptibility, electrically fast transients/bursts | Yes | Conducted |
| IEC 61000-4-5 | Conducted susceptibility, surges | Yes | Conducted |
| IEC 61000-4-6 | Conducted susceptibility, disturbances induced by RF fields, 150 kHz to 80 MHz | Yes | Conducted |
| IEC 61000-4-8 | Radiated susceptibility, magnetic field, 60 Hz | Yes | Conducted |
| IEC 61000-4-9 | Radiated susceptibility, magnetic field, 60 Hz to 50 kHz | Yes | Conducted |
| IEC 61000-4-10 | Radiated susceptibility, magnetic field, 100 kHz and 1 MHz | Yes | Conducted |
| IEC 61000-4-11 | Voltage dips, short interruptions and voltage variations immunity test | No | Conducted |
| IEC 61000-4-12 | Conducted susceptibility, 100 kHz ring wave | Yes | Conducted |
| IEC 61000-4-13 | Conducted susceptibility, low frequency, 16 Hz to 2.4 kHz | Yes | Conducted |
| IEC 61000-4-16 | Conducted susceptibility, low frequency, 0 Hz to 150 kHz | Yes | Conducted |
| IEC 61000-4-39 | Radiated close proximity fields test methods | No | Conducted |
| IEC 61000-6-1 | Residential test levels | No | Conducted |
| IEC 61000-6-2 | Industrial test levels | No | Conducted |
| IEC 61000-6-3 | Residential limits | No | Emission |
| IEC 61000-6-4 | Industrial limits | No | Emission |

### B.1.3 IEEE

The methods of testing for the United States are mostly specified by the IEEE. Important EMC standards endorsed by RG 1.180 Rev. 2 include the following:

- IEEE 1050-2004, *IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations*

- IEEE Std. C62.41.1-2002, *IEEE Guide on the Surge Environment in Low-Voltage (1000 V and Less) AC Power Circuits*

- IEEE Std. C62.41.2-2002, *IEEE Recommended Practice on Characterization of Surges in Low-Voltage (1000 V or Less) AC Power Circuits*

- IEEE Std. C62.45-2002,*IEEE Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage (1000 V or Less) AC Power Circuits*

Other IEEE standards of interest of interest for evaluating the EM environment include the following:

- ANSI C63.2-2016, *American National Standard for Specifications of Electromagnetic Interference and Field Strength Measuring Instrumentation in the Frequency Range 9 kHz to 40 GHz*

- ANSI C63.4a-2017, *American National Standard for Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9 kHz to 40 GHz*

- ANSI C63.5- 2017/Cor 1-2019, *American National Standard for Electromagnetic Compatibility—Radiated Emission Measurements in Electromagnetic Interference (EMI) Control—Calibration and Qualification of Antennas (9 kHz to 40 GHz)*

- ANSI C63.10-2020, *American National Standard of Procedures for Compliance Testing of Unlicensed Wireless Devices*

- ANSI C63.15-2017, *American National Standard Recommended Practice for the Immunity Measurement of Electrical and Electronic Equipment*

- ANSI C63.25.1, *American National Standard Validation Methods for Radiated Emission Test Sites, 1 GHz to 18 GHz*

- ANSI C63.27-2017, *American National Standard for Evaluation of Wireless Coexistence*

- IEEE 1900.2-2008, *IEEE Recommended Practice for the Analysis of In-Band and Adjacent Band Interference and Coexistence Between Radio Systems*

The use of proper measurement instrumentation is critical to obtaining accurate, reproducible results. Various measuring accessories that may be needed are selected according to the particular measurements to be performed. The reproducibility of measurements of radiated interference from one test site to another has not been completely satisfactory. In 1982, a concerted effort was organized in Subcommittee No. 1 of American National Standards Committee C63 to determine how the technique could be improved. Evidence showed that the variability was caused in part by the following inadequate processes:

- Control of site reference ground plane conductivity, flatness, site enclosures, effects of surrounding objects, and certain other site construction features

- Accounting for antenna factors, associated cabling, and balun and device under test characteristics

- Consideration of mutual coupling effects between the device under test and the receiving antenna and their images in the reference ground plane

ANSI C63.4-2014 states that both spectrum analyzers and receivers may be used to make emission measurements. This document is intended to standardize the methods, instrumentation, and facilities used to characterize device emissions with respect to voluntary or regulatory compliance requirements designed to protect authorized communication services. This standard is intended to be used for making emission measurements of unintentional radiators (including digital devices and receivers) and for making emission measurements of the digital device portions contained in or used in intentional radiators. The methods described in this standard may not be adequate or applicable for measurement of emissions from incidental radiators, avionics, or ISM equipment. The companion document, ANSI C63.10, specifies methods of measurement for certain devices other than ISM that purposefully radiate RF energy, such as intentional radiators. However, the methods stipulated in ANSI C63.10 might not be applicable for licensed transmitters. ANSI C63.4a-2017 is an amendment to ANSI C63.4-2012 that mainly updates the test site validation procedures in Annex D in ANSI C63.4-2014 and corrects equations in several annexes.

ANSI C63.10-2020 provides procedures for testing the compliance of a wide variety of unlicensed wireless devices (transmitters) including remote control and security unlicensed wireless devices, frequency hopping and direct sequence spread spectrum (DSSS) devices, antitheft devices, cordless telephones, medical unlicensed wireless devices, Unlicensed National Information Infrastructure (U-NII) devices, intrusion detectors, unlicensed wireless devices operating on frequencies below 30 MHz, automatic vehicle identification systems, and other unlicensed wireless devices authorized by a radio regulatory authority. Excluded by this standard are test procedures for unlicensed wireless devices already covered in other published standards (e.g., Unlicensed Personal Communication Services [UPCS] devices). Procedures for testing some of these devices were previously provided in ANSI C63.4-2014, but they will be removed in a future revision of that standard. The procedures for testing the compliance of a wide variety of unlicensed wireless transmitters are covered in this standard,

ANSI C63.27 specifies methods for assessing the RF wireless coexistence of equipment that incorporates RF communications. One risk control measure to ensure that the technology can be integrated at a level of acceptable risk is through coexistence. This standard specifies key performance indicators (KPIs) that can be used to assess the ability of the equipment under test (EUT) to coexist with other equipment in its intended operational environment. This type of testing focuses on devices and systems that intentionally use wireless, and it extends beyond traditional EMC to examine a device’s performance in frequency bands where it uses wireless communication.

IEEE standards of interest to using wireless networks in an NPP are listed in Table B.5.

**Table B.5. IEEE EMC standards**

| Standard | Title | Endorsed by RG 1.180 | Type test |
|---|---|---|---|
| IEEE 1050-2004 | IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations | Yes | EMI/RFI limiting practices |
| IEEE Std. C62.41.1-2002 | IEEE Guide on the Surge Environment in Low-Voltage (1000 V and Less) AC Power Circuits | Yes | SWC testing |
| IEEE Std. C62.41.2-2002 | IEEE Recommended Practice on Characterization of Surges in Low-Voltage (1000 V or Less) AC Power Circuits | Yes | SWC testing |
| IEEE Std. C62.45-2002 | IEEE Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage (1000 V or Less) AC Power Circuits | Yes | SWC testing |
| ANSI C63.2-1996 | American National Standard for Electromagnetic Noise and Field Strength Instrumentation, 10 Hz to 40 GHz - Specifications | No | |
| ANSI C63.4-2014 | American National Standard for Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9 kHz to 40 GHz | No | Emissions |
| ANSI C63.4a-2017 | American National Standard for Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9 kHz to 40 GHz, Amendment 1: Test Site Validation | No | Emissions |
| ANSI C63.5-2006 | American National Standard for Calibration of Antennas Used for Radiated Emission Measurements in Electro Magnetic Interference | No | |
| ANSI C63.7-2005 | American National Standard Guide for Construction of Open-Area Test Sites for Performing Radiated Emission Measurements | No | |
| ANSI C63.9-2008 | American National Standard for RF Immunity of Audio Office Equipment to General Use Transmitting Devices with Transmitter Power Levels up to 8 Watts | No | |
| ANSI C63.10-2020 | American National Standard of Procedures for Compliance Testing of Unlicensed Wireless Devices | No | Conducted, Radiated |
| ANSI C63.11-2000 | American National Standard for Limits and Methods of Measurement of Radio Disturbance Characteristics of Industrial, Scientific, and Medical (ISM) Radio-Frequency Equipment | No | |
| ANSI C63.12-1999 | American National Standard Recommended Practice for Electromagnetic Compatibility Limits | No | |
| ANSI C63.13-1991 | American National Standard Guide on the Application and Evaluation of EMI Power-Line Filters for Commercial Use | No | |

**Table B.5. IEEE EMC Standards (continued).**

| Standard | Title | Endorsed by RG 1.180 | Type test |
|---|---|---|---|
| ANSI C63.14-2014 | American National Standard Dictionary of EMC including Electromagnetic Environmental Effects (E3) | No | |
| ANSI C63.15-2010 | American National Standard Recommended Practice for the Immunity Measurement of Electrical and Electronic Equipment | No | |
| ANSI C63.16-1993 | American National Standard Guide for Electrostatic Discharge Test Methodologies and Criteria for Electronic Equipment | No | |
| ANSI C63.17-2013 | American National Standard Methods of Measurement of the Electromagnetic and Operational Compatibility of Unlicensed Personal Communications Services (UPCS) Devices | No | |
| ANSI C63.22-2004 | American National Standard Guide for Automated Electromagnetic Interference Measurements | No | |
| ANSI C63.23-2012 | American National Standard Guide for Electromagnetic Compatibility—Computations and Treatment of Measurement Uncertainty | No | |
| ANSI C63.27-2017 | American National Standard for Evaluation of Wireless Coexistence | No | Conducted, Radiated |
| IEEE 1900.2 | IEEE Recommended Practice for the Analysis of In-Band and Adjacent Band Interference and Coexistence Between Radio Systems | No | |

Specific test procedures for verifying the compliance of unlicensed personal communications services (UPCS) devices (including wideband voice and data devices) are established, including applicable regulatory requirements regarding radio-frequency emission levels and spectrum access procedures.

### B.1.4 Radio Technical Commission for Aeronautics (RTCA)

RTCA is a membership organization encompassing companies and governments across the globe representing all facets of the air transportation industry. RTCA provides a venue for the development of consensus-driven performance standards and guidance materials that serve as a partial basis for certification of critical systems and equipment used in the conduct of air transportation. Adherence to these standards serves as ones means of compliance with related FAA regulations.

DO-160 [B.10] contains environmental conditions and test procedures for airborne equipment and is the minimum standard for the environmental testing of commercial avionics hardware. The following sections of DO-160 are related to EMC:

- 15 - Magnetic Effect (effect of on-board equipment to compass)
- 16 - Power Input (conducted emissions and susceptibility)

- 17 - Voltage Spike (susceptibility of equipment at alternating current [AC] or direct current [DC] power leads)

- 18 - Audio Frequency Conducted Susceptibility - Power Inputs

- 19 - Induced Signal Susceptibility (susceptibility of equipment on induced voltages)

- 20 - Radio Frequency Susceptibility (radiated and conducted)

- 21 - Emission of Radio Frequency Energy (radiated and conducted)

- 22 - Lightning Induced Transient Susceptibility (indirect lightning effects)

- 23 - Lightning Direct Effects (limited to equipment mounted on the exterior aircraft)

- 25 - Electrostatic Discharge (for equipment accessible during operation and service)

DO-230G [B.11] provides guidance on acquiring and designing security systems, testing and evaluating system performance, and operational requirements for airport security access control systems. Where applicable, Special Committee (SC) 224 for the standard has made these references in the interest of providing a complete picture of the possible direction of a standard and/or technology. RTCA SC 224 recommends that readers of this guidance document solicit the latest information on any referenced technology, processes, and procedures before moving forward with planned implementation of an airport security access control system. Finally, the document provides information on technology trends in physical access control systems (PACSs), access card technology, video, wireless and physical security information management systems (PSIMs) deemed current at the time of publication but that may be obsolete or overcome by other emerging technology.

DO-233 [B.12] addresses the potential interference to installed aircraft electrical and electronic systems from portable electronic devices (PEDs) carried aboard by passengers. It defines the potential interference phenomena; outlines the risk potential from interference events; provides test methods to determine if a potential for interference exists for certain PEDs, aircraft and combinations thereof; and addresses acceptable levels of interference. The report also recommends modification of FAA Regulation 91.21, continued PEDs testing to identify and better define the possibility of interference to aircraft electronic systems, increased public awareness of the potential for interference from PEDs, and the development and use of devices to detect spurious PED emissions. RTCA standards of interest to using wireless networks in an NPP are listed in Table B.6.

**Table B.6. RTCA EMC standards**

| Standard | Title | Endorsed by RG 1.180 | Type test |
|---|---|---|---|
| DO-160G | Environmental Conditions and Test Procedures for Airborne Equipment | No | Conducted, radiated |
| DO-230G | Standards for Airport Security Access Control Systems | No | Security access control systems |
| DO-233 | Portable Electronic Devices Carried Onboard Aircraft | No | |

## B.2 DOMESTIC STANDARDS

The domestic standards of interest for evaluating EMC are from the DoD (MIL), FCC, and NIST. The standards cover conducted/radiated emissions and immunity/susceptibility to those emissions, similar to those standards endorsed in RG 1.180. The frequency ranges are also similar.

The list of domestic standards appears to cover the same topics as those endorsed by RG 1.180 Rev. 2, except that IEEE has a standard for the treatment of uncertainty (IEEE/ANSI C63.23-2012). An interesting standard is the automated EMI measurements in IEEE/ANSI C63.22-2004. This is interesting because this guide describes, in general terms, the use of automatic test equipment and the automation of measurements of electromagnetic emissions.

### B.2.1 US Military

RG 1.180 Rev. 2 endorses MIL-STD-461G [B.13] for EMI/RFI test methods, extending the guidance to cover signal line testing, incorporating frequency ranges where portable communications devices are experiencing increasing use, and relaxing the operating envelopes (test levels) when experience and confirmatory research warrants. MIL-STD-461G contains test methods that can be applied to address EMI/RFI susceptibility for a selection of environments. Other documents and reviews may cite MIL-STD-462 [B.14], although this standard was cancelled and future users should refer to MIL-STD-461E (now MIL-STD-461G).

MIL-STD-461G provides the latest revision of domestic guidance for emissions test methods, so it represents current US practice. RG 1.180, Rev. 2 endorses MIL-STD-461G.

MIL-STD-461 provides a basis for evaluating the EM characteristics of equipment and subsystems by setting operational acceptance criteria. The requirements of MIL-STD-461 are typically applicable only as specified in the contracting agreement between a private enterprise and the federal government.

The applicability of the MIL-STD-461G test requirements depends on the class designation assigned to the equipment or subsystem under review. This standard notes that it is best suited for items with the following features: electronic enclosures no larger than an equipment rack, electrical interconnections that are discrete wiring harnesses between enclosures, and electrical power input derived from prime power sources. MIL-STD-461 should not be directly applied to items such as modules located inside electronic enclosures or entire platforms. The principles in MIL-STD-461 may be useful as a basis for developing suitable requirements for those applications.

DoD standards of interest for using wireless networks in an NPP are listed in Table B.7.

**Table B.7. US military EMC standards**

| Standard | Title | Endorsed by RG 1.180 | Type test |
|---|---|---|---|
| MIL-STD-461G | Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment | Yes | EMI/RFI emissions and susceptibility |
| MIL-STD 462D<br>Superseded by -461G | Measurement of Electromagnetic Interference Characteristics | No | |
| MIL-STD-464D | Electromagnetic Environmental Effects Requirements for Systems | No | |

MIL-STD-461G contains test practices that can be applied to characterize EMI/RFI conducted and radiated emissions (CE and RE):

- CE101—Conducted emissions, low frequency. 30 Hz to 10 kHz
- CE102—Conducted emissions, high frequency. 10 kHz to 10 MHz
- CE106. Antenna port. 10 kHz to 40 GHz
- RE101—Radiated emissions, magnetic field. 30 Hz to 100 kHz
- RE102—Radiated emissions, electric field. (2 MHz to 10 GHz is used in RG 1.180, Rev.2)
- RE103. Antenna spurious and harmonic outputs. 10 kHz to 40 GHz

Specific test methods from MIL-STD-461G and IEC 61000-4 acceptable to the NRC staff for performing conducted and radiated *susceptibility* (CS and RS) *testing* of safety-related I&C systems intended for installation in NPPs include:

- CS101—Conducted susceptibility, low frequency, 30 Hz to 150 kHz
- CS103. Antenna port, intermodulation. 15 kHz to 10 GHz
- CS104. Antenna port, rejection of undesired signals. 30 Hz to 20 GHz
- CS105. Antenna port, cross-modulation. 30 Hz to 20 GHz
- CS109. Structure current. 60 Hz to 100 kHz
- CS114—Conducted susceptibility, high frequency, 10 kHz to 30 MHz
- CS115—Conducted susceptibility, bulk cable injection, impulse excitation
- CS116—Conducted susceptibility, damped sinusoidal transients,10 kHz to 100 MHz
- CS117. Lightning induced transients, cables and power leads.
- CS118. Personnel borne electrostatic discharge. 8 kV contact discharge
- RS101—Radiated susceptibility, magnetic field, 30 Hz to 100 kHz
- RS103—Radiated susceptibility, electric field, 30 MHz to 10 GHz
- RS105. Transient electromagnetic field

These test methods may be applied in the indicated combinations subject to the clarifications and conditions specified in the standard. Acceptable limits are given for each test in the form of identified operating envelopes.

### B.2.2 FCC

CFR Title 47 (Telecommunications), Chapter I (Federal Communication Commission) address EMC regulations in the United States.

Many countries and customs unions are adopting the EMC standards and regulations from the FCC and IEC/CISPR. The major differences between FCC regulations and IEC/CISPR standards are:

- **Rules vs. Standards.** The FCC publishes legally binding rules and regulations (47 CFR) which contain concrete emission limits, or in the case of FCC MP-5-1986, even test methods for FCC Part 18 (ISM equipment). IEC and CISPR publish EMC standards which by their nature are not legally binding. Standards in the United States and abroad can become legally binding if a country or customs union (e.g., EU) decides to adopt the standards into national (legally binding) standards.

- **Immunity.** At this writing, the FCC regulations do not specify a level of EM immunity/susceptibility. However, several IEC immunity standards are defined.

- **Conducted Emission** (FCC Part 15 / unintentional radiators[19]). The conducted emission limits for FCC Part 15 for equipment that is designed to be connected to the public utility (AC) power line, (47 CFR 15.107) are identical to the CISPR 32 limits (commission amending of FCC in 2002).

- **Radiated Emission** (FCC Part 15 / unintentional radiators). The FCC released a document that describes the applicability of CISPR standards for FCC 15 subpart B (unintentional radiators) approval.

FCC regulations related to the use of wireless networks in an NPP are listed in Table B.8.

**Table B.8. FCC EMC standards**

| Standard | Title | Endorsed by RG 1.180 | Type |
|---|---|---|---|
| FCC MP-5-1986 | Methods of Measurement of Radio Noise Emissions from Industrial, Scientific and Medical (ISM) Equipment) | No | Radiated |
| 47 CFR (FCC) Part 15 | Radio Frequency Devices | Yes* | Conducted, Radiated |
| 47 CFR (FCC) Part 18 | Industrial, Scientific, and Medical Equipment | No | Conducted, Radiated |

* Certification for Class A or Class B devices under 47 CFR Part 15, "Radio Frequency Devices," may be credited over the frequency ranges covered by certification testing in lieu of additional testing for nonsafety-related I&C systems.

Unlike EU regulations, US regulations (FCC, Title 47, Chapter I) specify the limits in the law; for example, for the conducted limits of unintentional radiators 47 CFR 15.107. However, in EU laws and directives, test limits are specified in the EMC standards issued by the IEC/CISPR organizations.

### B.2.3 NIST

NIST, founded in 1901, is now part of the US Department of Commerce and is one of the nation's oldest physical science laboratories.

**NIST SP 800-48** [B.15] provides recommendations for WNS, especially for IEEE 802.11a/b/g and Bluetooth devices.

**NIST SP 800-97** [B.16] provides recommendations for wireless network security (WNS), especially for IEEE 802.11i.

**NIST Technical Note 1885** [B.17] examines interference and coexistence testing issues related to the use of wireless devices in critical infrastructure systems. The technical note discusses the challenges of characterizing complex EM environments, emulating such environments in the laboratory, and designing test methods that adequately evaluate a device's ability to perform in that environment. NIST guidance documents of interest for using wireless networks in an NPP are listed in Table B.9.

[19] An unintentional radiator as defined by Part 15 is a "device that intentionally generates radio frequency energy for use within the device, or that sends radio frequency signals by conduction to associated equipment via connecting wiring, but which is not intended to emit RF energy by radiation or induction."

**Table B.9. NIST EMC standards**

| Standard | Title | Endorsed by RG 1.180 | Type |
|---|---|---|---|
| NIST SP 800-48, Rev. 1 | Wireless Network Security for IEEE 802.11a/b/g and Bluetooth | No | Wireless security |
| NIST SP 800-97 | Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i | No | Wireless security |
| NIST Technical Note 1885 | Complexities of Testing Interference and Coexistence of Wireless Systems in Critical Infrastructure | No | Interference and coexistence |

## B.3 REFERENCES

B.1 Academy of EMC, *EMC Standards*. https://www.academyofemc.com/emc-standards

B.2 EPRI TR-1019186, Final Report, *Implementation Guideline for Wireless Networks and Wireless Equipment Conditioning Monitoring*, Electric Power Research Institute, Palo Alto, California, December 2009.

B.3 IAEA Nuclear Energy Series No. NR-T-3.29, *Application of Wireless Technologies In Nuclear Power Plant Instrumentation and Control Systems*, International Atomic Energy Agency, Vienna, November 2010.

B.4 J. Dion, M. K. Howlander, and P. D. Ewing, *Wireless Network Security in Nuclear Facilities*, NPIC&HMIT 2010, Las Vegas, Nevada, November 7-11, 2010 (NRC Adams Accession No. ML103210371).

B.5 IEC 62918:2014, *Nuclear Power Plants: Instrumentation and Control Important to Safety — Use and Selection of Wireless Devices to be Integrated in Systems Important to Safety*, International Electrotechnical Commission, Geneva, 2014.

B.6 IEC 62988:2018, *Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Selection and Use of Wireless Devices*, International Electrotechnical Commission, Geneva, 2018.

B.7 IEC 62657-1:2017, *Industrial Communication Networks — Wireless Communication Networks — Part 1: Wireless Communication Requirements and Spectrum Considerations*, International Electrotechnical Commission, Geneva, 2017.

B.8 IEC 62657-2017, *Industrial Communication Networks — Wireless Communication Networks — Part 2: Coexistence Management*, International Electrotechnical Commission, Geneva, 2017.

B.9 IEC 62591:2016, *Industrial Networks — Wireless Communication Network and Communication Profiles — WirelessHART*, International Electrotechnical Commission, Geneva, 2016.

B.10 DO-160F, *Environmental Conditions and Test Procedures for Airborne Equipment*, RTCA Inc., Washington, D.C., December 6, 2007.

B.11 DO-230G, *Standards for Airport Security Access Control Systems*, RTCA Inc., Washington, D.C., June 21, 2016.

B.12 DO-233, *Portable Electronic Devices Carried Onboard Aircraft*, RTCA Inc., Washington, D.C., August 20, 1996.

B.13 MIL-STD-461G, *Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,* Department of Defense, Washington, D.C., 11 December 2015.

B.14 MIL-STD 462D, *Measurement of Electromagnetic Interference Characteristics,* Department of Defense, Washington, D.C., 11 January 1993.

B.15 K. Scarfone, D. Dicoi, M. Sexton, and C. Tibbs, *Wireless Network Security for IEEE 802.11a/b/g and Bluetooth*, NIST SP 800-48 (rev. 1), U.S. Department of Commerce, National Institute of Standards and Technology, August 2007.

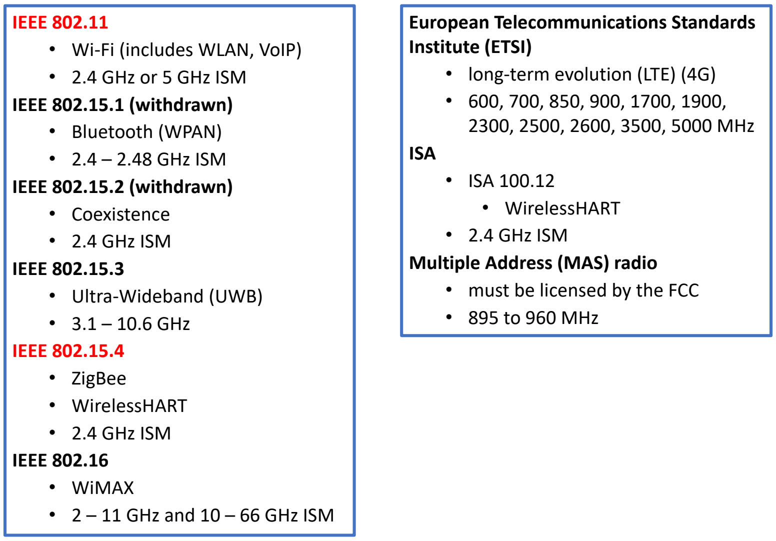
B.16 S. Frankel, B. Eydt, L. Owens, and K. Scarfone, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, NIST SP 800-97, U.S. Department of Commerce, National Institute of Standards and Technology, February 2007.

B.17 Galen Koepke, William Young, John Ladbury, and Jason Coder, *Complexities of Testing Interference and Coexistence of Wireless Systems in Critical Infrastructure*, NIST Technical Note 1885, U.S. Department of Commerce, National Institute of Standards and Technology, July 2015.

# APPENDIX C. WIRELESS COMMUNICATION PROTOCOLS

As part of their policy to complement international standards, the NRC and has endorsed in part several IEC 61000-x standards in RG 1.180 Rev. 2 and has also endorsed two CISPR standards, primarily through the endorsement of IEC 61000-6-4. Furthermore, RG 1.180 endorses several IEEE standards related to surge testing. RG 1.180 Rev. 2 recognizes that MIL-STD-461G provides the most recent revision of domestic guidance for emissions test methods and that it represents current US practice. RG 1.180 also notes that certification for Class A or Class B devices under 47 CFR Part 15, "Radio Frequency Devices," may be credited over the frequency ranges covered by certification testing in lieu of additional testing for nonsafety-related I&C systems. Many other standards organizations and standards address wireless networks and devices. A review of these organizations, both domestic and international, is provided in Appendix B.

WSNs can be built using several radio technologies and communication protocols. Wireless protocols are provided to move the information. Protocols can employ point-to-point networking. However, modern protocols employ mesh networking, in which all sensor network nodes can relay messages. Mesh networking adds robustness to a wireless network by providing multiple paths for the information. For example, a faulty node can automatically be bypassed. Mesh networking also provides better coverage for the WSN in demanding environments. Some of the most common sensor network radio protocols are shown in Figure C.1 and discussed below [C.1].



**IEEE 802.11**
- Wi-Fi (includes WLAN, VoIP)
- 2.4 GHz or 5 GHz ISM

**IEEE 802.15.1 (withdrawn)**
- Bluetooth (WPAN)
- 2.4 – 2.48 GHz ISM

**IEEE 802.15.2 (withdrawn)**
- Coexistence
- 2.4 GHz ISM

**IEEE 802.15.3**
- Ultra-Wideband (UWB)
- 3.1 – 10.6 GHz

**IEEE 802.15.4**
- ZigBee
- WirelessHART
- 2.4 GHz ISM

**IEEE 802.16**
- WiMAX
- 2 – 11 GHz and 10 – 66 GHz ISM

**European Telecommunications Standards Institute (ETSI)**
- long-term evolution (LTE) (4G)
- 600, 700, 850, 900, 1700, 1900, 2300, 2500, 2600, 3500, 5000 MHz

**ISA**
- ISA 100.12
  - WirelessHART
- 2.4 GHz ISM

**Multiple Address (MAS) radio**
- must be licensed by the FCC
- 895 to 960 MHz

**Figure C.1. Frequency bands for popular wireless networks.**

Wireless systems are being deployed in increasing numbers in nuclear facilities for nonsafety-related applications, including some I&C types such as field bus data, distributed control systems, voice and visual communications, plant process monitoring, computer access points, mobile work orders, mobile drawings and procedures, and personal radiation detection devices [C.2]. Most of these applications require some type of wireless network access (e.g., cellular, personal area, local area, wide area, mesh, ad-hoc) based on wireless standards. These networks include Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15.1), ZigBee (IEEE 802.15.4), WirelessHART, and ISA-100.11a. Some process control vendors are developing proprietary wireless systems to support their specific needs (e.g., OneWireless by Honeywell, Smart Wireless by Emerson, and ION by Aprion). Most of these wireless systems operate in the unlicensed FCC frequency bands (900 MHz, 2.4 GHz, and 5.9 GHz) or in the cellular telephone bands (800 MHz and 1.9 GHz).

FCC MP-5-1986 specifies methods for measuring radio noise emissions from ISM equipment. Wireless standards define the transmission speed, the spectrum of operation, and the type of modulation used in an application. These characteristics help determine the type of application for which the standard can be used and the cost [C.3].

Wi-Fi is perhaps the most widely known standard. It is used by wireless devices to communicate with a router connected through a wired link to the internet [C.4]. Six IEEE standards, not including revisions, govern Wi-Fi—802.11a, 802.11b, 802.11e, 802.11g, 802.11i, and 802.11n. Other IEEE standards govern Bluetooth (802.15.1), UWB (802.15.3), Zigbee (802.15.4), and WiMAX (802.16). Table C.1 presents a sampling of the IEEE wireless standards in use at NPPs.

**Table C.1. IEEE wireless standards**

| IEEE standard | Name | Operational frequency | Data rate (Mbps) | Range |
|---|---|---|---|---|
| 802.11-2020 | Wi-Fi | 2.4 and 5.7 GHz | 11–248 | 120–250 m |
| 802.15.1-2005<br>(Inactive 7-5-2018) | Bluetooth | 2.4 GHz | 1 | 0.5–100 m |
| 802.15.2-2003<br>(Inactive 7-5-2018) | Coexistence | MHz to GHz | — | — |
| 802.15.3-2016 | UWB | 5 GHz | 100 | 16 km |
| 802.15.4-2020 | Zigbee | 2.4 GHz | 0.25 | 10–70 m |
| 802.16-2017 | WiMAX | 2-11 GHz, 10-66 GHz | 75 | 80 km |

Based on a review of wireless uses at NPPs, the most common protocols applications are the 802.11 and 802.15.4 IEEE standards. Field network devices commonly used for network access, internet communication, and wireless sensors for which battery life is not an issue typically use the 802.11 communications standard. It can be a challenge to provide reliable power to the wireless sensors. Power supplied by batteries increases a sensor's operating cost because personnel must occasionally replace the battery. This additional cost is offset by the significantly increased flexibility of battery-powered sensors; they can be relocated or moved between plant components to adapt to changing equipment or environmental conditions. Low-power battery-operated wireless sensors that measure elements such as pressure, level, flow, temperature, vibration, steam trap monitors, and valve position indication use the 802.15.4 standard [C.5].

Coexistence is the ability of multiple systems to perform their tasks in a given environment in which they may or may not be using a similar set of rules [C.6]. The IEEE 802.15.2 standard provides coexistence specifications for local area networks operating predominantly in the unlicensed spectrum. Because NPPs and industry still use this standard, it is recognized as providing guidance for coexistence. IEEE 802.19 addresses coexistence concerns for IEEE 802 in general.

Not only is the use of wireless growing dramatically, but also, the resulting spectrum crowding is requiring reexamination of how a spectrum is regulated and its coexistence with other spectrum users. There is an increasing trend toward more flexible spectrum regulations, allowing devices to dynamically share frequency bands. It is now common for devices to be capable of communicating on multiple frequency bands using multiple RF protocols. With software-defined radio, a device's capabilities may be changed by a remote software update. The result is that a single device may—from an RF interference viewpoint—serve as many devices, using different frequency bands and protocols at different times. A single device may be capable of operating on the cellular networks using CDMA, Global System for Mobile (GSM), Universal Mobile Telecommunications System (UMTS) or LTE protocols on LANs using any of several ISM frequency bands and 802.11 protocols, or by using Bluetooth, digital enhanced cordless telecommunications (DECT), or a number of other protocols and bands. Having access to multiple radio access technologies (RATs) is a great benefit, but it presents a real challenge for EMC management.

A review by Phillip Keebler and Stephen Berger [C.7] shows the most popular equipment categories in each band from 1990–2010. Their review presents a variety of equipment types using each of the ISM bands, with the 900 MHZ and 5.8 GHz bands ranging in the hundreds of grants per year, and the 2.4 GHz bands ranging in the thousands of grants/year. Under FCC rules, any device may use the ISM bands as long as it complies with the service rules for that specific band. Figure C.1 shows the frequency bands for the popular network protocols. WirelessHART and ISA-100.11a are two of the most used standards available that are focused on applications of wireless networks in process automation [C.8].

Generally, coexistence mechanisms may be categorized as *collaborative* or *noncollaborative*. Collaborative mechanisms exchange information between two different systems, whereas noncollaborative mechanisms do not. IEEE 802.15.2 provides more information on coexistence mechanisms, along with various techniques to support coexistence between IEEE 802.11 and IEEE 802.15.1 devices [C.4, C.6]. Because NPPs and industry still use this standard, it is recognized as providing guidance for coexistence. IEEE 802.19 addresses coexistence concerns for IEEE 802 in general.

Wireless networks operating on the same frequency bands can interfere with each other's operations. For example, IEEE 802.11 (WLAN), IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (Zigbee) devices operate in the same 2.4 GHz ISM band. Three different aspects of interference must be considered when evaluating wireless technologies [C.9]:

1. Interference of wireless devices with existing plant equipment

2. Interference of wireless devices with one another (coexistence)

3. Interference (intentional or unintentional) of other equipment with wireless devices (intentional interference would include jamming devices.)

Radio spectrum management is also important for ensuring the coexistence of various wireless technologies.

## C.1 WI-FI

Wi-Fi is probably the most familiar wireless networking technology. It is commonly used within a business to provide wireless connectivity among organizational or visitor laptops by a WLAN. The WLAN may exist behind a firewall or to a separate intranet, but Wi-Fi is generally intended to connect the various computers and other devices to the IoT [C.10].

Wi-Fi uses the unlicensed ISM band at 2.4 or 5 GHz. This is the same frequency band used by cordless phones, microwave ovens, and Bluetooth devices. Wi-Fi can theoretically work at distances up to 1,000 feet (~300 meters); however, a more optimum range is about 300 feet (~90 meters) [C.5].

**802.11a.** This standard governs Wi-Fi use in the unlicensed ISM spectrum in the 5 GHz range. Devices using this standard are not compatible with 802.11b. For a variety of reasons, including the presence of more channels in the 5 GHz range, 802.11a offers theoretical data rates up to about 54 Mbps [C.3].

**802.11ac**. IEEE 802.11ac (adopted in 2014) has a maximum link rate of 6933 Mbps. The more recent revisions are even faster.

**802.11ax**. This version of the standard was developed to address the problem of crowded spectrum usage. The goal being a greater throughput density of the whole network per a physical area by improving spatial reuse [C.11].

**802.11b.** Most WLAN devices are built using the 802.11b standard. This standard governs Wi-Fi use in the unlicensed ISM spectrum in the 2.4 GHz range. This is the same frequency band used by cordless phones, microwave ovens, and Bluetooth WPAN devices. Theoretically, 802.11b devices can work at distances up to about 1,000 feet (304.8 meters), but in practice, 802.11b devices work at distances up to about 91.4 m (300 ft) at a data rate of 11 Mbps. Because the spectrum is shared with other users, the data rates decline as more users log on. Security within 802.11 is provided by the wired equivalent privacy (WEP) protocol, which has been shown to be easily cracked by hackers, so in all but the simplest environments, additional security measures should be added to networks based on Wi-Fi technology [C.3].

**802.11e.** This specification was created to improve and manage quality-of-service issues. This is critical for organizations that want to use WLAN technology for voice over internet protocol (VoIP), remote video systems, video conferencing, and streaming media. Such systems require more quality-of-service enhancements for critical environments than are currently practical with other Wi-Fi protocols because of their relative intolerance of dropped or missed data [C.3].

**802.11g.** This standard is considered the next generation for WLAN services. It provides roughly the same data rates as 802.11a devices and is backward compatible with 802.11b devices [C.2].

**802.11i.** This standard provides stronger encryption for data over the air by using a nonproprietary 128-bit encryption solution called *enhanced security network*, which supports the Advanced Encryption Standard algorithm [C.3].

NIST SP 800-97 [C.12] provides recommendations for WNS, especially for IEEE 802.11i.

**802.11n.** This standard provides specifications to improve data reliability for WLAN devices and to extend their range. Data throughput is forecast to be 5 times that of 802.11g at 248 Mbps [C.5].

## C.2 BLUETOOTH

The Bluetooth standard, 802.15.1 addresses Bluetooth technology, which is a short-range radio standard and communications wireless technology that allows fixed and mobile devices to transmit and receive data such as linking devices to a smart phone (WPAN). The standard governs a low-power, low-cost alternative to Wi-Fi. Bluetooth can provide 1 Mbps data rates for coverage from a few meters to a hundred meters, depending on the transmitted power level [C.4].

Because computers are used extensively in all facets of research and in industrial process applications for monitoring and control purposes, Bluetooth has potential for data transfer applications in such settings. However, Bluetooth technology applications in industrial settings are limited to performing administrative tasks rather than playing a key role in establishing digital communication networks for use in I&C applications [C.1, C.13].

NIST SP 800-48 [C.14] provides recommendations for WNS, especially for IEEE 802.11a/b/g and Bluetooth devices.

The Bluetooth operating frequency is 2.4–2.48 GHz in the unlicensed ISM band, and the operating range depends on the power class:

- Class 1: 100 mW, ~100 m.
- Class 2: 2.5 mW, ~10 m.
- Class 3: 1 mW, ~1 m.
- Class 4: 0.5 mW, ~0.5 m

Bluetooth communications use a packet-based protocol with a master/slave architecture in which one master may communicate with up to seven slaves [C.1]. Bluetooth technology is implemented in a low-cost chip that can be plugged into any device that is capable of supporting wireless communications and transmitting data at a rate of 1 Mbps [C.13]. Today, low-energy Bluetooth can transmit at rates up to 24 Mbps. However, the Bluetooth standard IEEE 802.15.1-2005 became inactive on July 5, 2018.

## C.3 ZIGBEE

ZigBee is the commercial name for a wireless technology for low powered, low data rate communications. Unlike communication protocols such as Wi-Fi and Bluetooth, which are designed for human interaction, ZigBee is intended for machine-to-machine (M2M) data communications in business, residential, and potentially industrial settings. The ZigBee protocol is optimized for M2M communications and may be suited for several NPP applications. ZigBee operates in the unlicensed ISM band [C.15].

The Zigbee standard, 802.15.4, Zigbee, provides specifications for a high-level communication protocol designed to use small, low-power digital radios for M2M communications. Zigbee is intended for battery-powered applications such as remote sensors with low data rates and low power consumption that allows individual devices to run for a year or more, with a single alkaline battery transmitting over an area of 10 to 70 m (~30 to 230 ft). The technology was developed to be simpler and cheaper than other WPAN protocols such as Bluetooth. Zigbee operates in the unlicensed 2.4 GHz ISM spectrum with a data rate of 0.25 Mbps. It appears to be well suited for several power utility applications [C.4, C.5, C.15].

Zigbee is a mesh networking technology that provides redundant communication. The maximum transmission rate is 250 Kbit/s, and a single Zigbee network can have 65,535 nodes [C.10]. One of Zigbee’s limiting factors is transmission coverage, which is limited to approximately 10 m. The coverage can be extended by relaying information between several devices [C.16].

ZigBee products can minimize power consumption by entering a sleep mode when the device is not active. In sleep mode, power consumption is low, but the device can be awakened at any time. There is typically a 15 ms delay for a device to wake up and an additional 15 ms delay for the active slave to access the channel [C.16].

ZigBee-enabled devices are available for home automation, commercial office applications, and the industrial sector, including sensors for monitoring motion, temperature, tank level, radiation, and pressure. In an NPP, ZigBee devices can be applied to monitor the status of various plant parameters and to provide appropriate warnings [C.16].

## C.4 WirelessHART

WirelessHART is based on the Highway Addressable Remote Transducer (HART) protocol, and it uses the 2.4 GHz band. WirelessHART was developed for wireless communication for industrial process control. WirelessHART forms a flat mesh network in which every participating station acts simultaneously as a signal source and a repeater for other stations. This means that a field device does not have to communicate directly with the gateway; it only needs a neighbor device to transmit its data. The neighbor device is responsible for sending data to another field device until it arrives at the gateway. The mechanism extends the network range and creates redundant communication paths, thus increasing network reliability [C.1, C.8].

HART is a bidirectional communication protocol between intelligent field instruments and host systems supporting wired and wireless devices and is based on the IEEE 802.15.4 standard in the 2.4 GHz ISM band [C.5].

WirelessHART was the first standard (IEC 62591) developed for wireless communication for process control. It adds wireless communication capability to the HART protocol, and it is compatible with existing HART devices. Each HART field device may act as a router of other device's data packets. The mechanism extends the wireless network range and also creates redundant communication paths, which increases the network reliability [C.8].

The HART communication foundation offered unrestricted access to its WirelessHART standard to the ISA (ISA100.12). IEC 62657-1:2017 provides the IEC standard for WirelessHART protocol. This provides access to HART-compatible control systems.

The main purpose of the ISA100 committee is to provide a family of standards for industrial wireless networks to address the needs of the whole plant, to include process control, personnel and asset tracking and identification convergence of networks, and long-distance applications [C.8]. ISA100 factory automation networks are formed from nodes that implement the functions of automation.

ISA100.11a is the standard the specifies a mesh network designed to provide secure wireless communication to process control [C.8]. ISA100.11a is designed to meet wireless industrial plant needs, including process automation and factory automation. It supports peer-to-peer communications to ensure device interoperability [C.5].

**ISA100.12** provides specifications to converge ISA100.11a and WirelessHART applications into a single worldwide standard.

**ISA100.14** provides specifications to improve the reliability and security of wireless networks. This includes configuration and simplification in a plant environment.

**ISA100.15** provides specifications for industrial backhaul of wireless systems into an industrial setting. It addresses issues such as security, flow control, network management, and fault tolerance.

Table C.2 provides a summary of the ISA100 wireless standards [C.5].

**Table C.2. ISA100 wireless standards**

| ISA Wireless standard | Name/application |
|---|---|
| ISA100.11a | Process Applications |
| ISA100.12 | WirelessHART and ISA100.11a Converged Network Applications |
| ISA100.14 | Trustworthy Wireless |
| ISA100.15 | Wireless Backhaul/Backbone Network |
| ISA100.21 | People and Asset Tracking and Identification |

ISA-TR100.20.01-2017 [C.17] is a technical report that provides an overview, principles, concepts of common network management, as well as terminology related to and the expected benefits from adopting a CNM standard.

ISA-TR100.00.03-2011 [C.6] is a technical report that presents descriptive user and market-related requirements of wireless communication in factory automation applications. The architecture shall support coexistence, and this ISA TR identifies the applicable IEEE, ISA, IEC, or Zigbee standards for different technologies and frequencies.

## C.5 ULTRA-WIDEBAND (UWB)

With UWB technology, short signal pulses are sent over a broad frequency spectrum, typically spreading over at least 500 MHz or 20% of the center frequency. Use of such a wide frequency band leads to low-power spectral density, and thus negligible interference with other types of radio systems. UWB provides the high bandwidth needed for very high data throughput, exploiting short-range communications and robustness against multipath fading. Possible applications include communications and sensor systems, ground- and wall-probing radars (through-wall imaging), medical imaging, precision location within buildings, surveillance systems, and automotive (anti-collision) radar systems [C.1].

UWB can operate in the frequency range of 3.1 to 10.6 GHz at a range of up to 10 miles without licensing requirements. One of the main advantages of the UWB transmitting signal is that it is less likely to cause interference with the conventional narrow band radio signals because of its high bandwidth and short-range coverage [C.16].

802.15.3 UWB is the standard that provides for devices that require high data rates at ranges of up to 16 km (10 miles). The specification was initially used by the military for radar applications [C.5]. UWB devices operate in the frequency range of 3.1 to 10.6 GHz without licensing requirement and transmits information by spreading it over a bandwidth exceeding 500 MHz [C.16].

## C.6 WIMAX

The 802.16 WiMAX standard provides specifications for high-speed internet access at ranges of up to 80 km (50 miles). WiMAX operates in the unlicensed ISM bands of 2–11 and 10–66 GHz. The specification integrates well with 802.11 but is now used largely outside the United States. Inside the United States, this specification has been largely replaced by the LTE standard, which is based on GSM and EDGE technology for 4G cellular [C.5].

## C.7 LTE (4G)

In LTE architecture, core network includes mobility management entity (MME), serving gateway (SGW), and packet data network gateway (PDN GW), whereas Evolved UTRAN (E-UTRAN) has E-UTRAN

NodeB (eNB) [C.18]. LTE has increased data rates, improved spectrum efficiency, and packet-optimized system over 4G. The LTE air interface physical layer offers data transport services to higher layers. The access to these services is with a transport channel via the medium access control (MAC) sublayer. The evolved architecture for LTE comprises E-UTRAN on the access side and EPC (evolved packet core) on the core side [C.19].

LTE is a registered trademark owned by ETSI for the wireless data communications technology and a development of the GSM / UMTS standards. LTE is based on the GSM/EDGE and UMTS / High Speed Packet Access (HSPA) standards.

The 3rd Generation Partnership Project (3GPP)[20] developed the LTE standard to be as flexible as possible to support the plethora of deployment options that exist all over the world. According to September 2013 figures from the Global Mobile Suppliers Association (GSA), there were 213 commercial LTE networks, including 21 LTE time-division duplex (TDD) networks, with 10 of these networks deployed by operators who also operate an LTE frequency division duplexing (FDD) network [C.20]. LTE is deployed in ~20 different frequency bands, including 5 of the 6 channel bandwidth options.

LTE is also called *3.95G* and has been marketed as 4G LTE and Advanced 4G. EDGE is also standardized by the 3GPP as part of the GSM family. The LTE standard covers a range of many different bands, each of which is designated by both a frequency and a bandwidth number. In North America, the frequencies of LTE are 600, 700, 850, 1700, 1900, 2300, 2500, 2600, 3500, 5000 MHz, and the channel bandwidths are 2, 4, 5, 7, 12, 13, 14, 17, 25, 26, 29, 30, 38, 40, 41, 42, 43, 46, 48, 66, 71 MHz. Wireless networks may also use 5G.

In the United States, the newly assigned 900 MHz spectrum leased to utilities allows for low-band coverage of the power infrastructure, whereas the Citizens Broadband Radio Service (CBRS) Priority Access License (PAL) and General Authorized Access (GAA) spectrum introduce the capacity for grid monitoring of sensors and controllers in the grid [C.21]. These and similar agreements for access to low band/mid band spectrum have enabled 3GPP-based wireless cellular technology to drive consolidation of diverse mesh networks.

Protocol specifications for LTE include the following [C.22]:

- 3GPP TS 36.201 - E-UTRA; LTE physical layer; general description
- 3GPP TS 36.211 - E-UTRA; physical channels and modulation
- 3GPP TS 36.212 - E-UTRA; multiplexing and channel coding
- 3GPP TS 36.213 - E-UTRA; physical layer procedures
- 3GPP TS 36.214 - E-UTRA; physical layer; measurements

Testing on altimeters was based on the following:

- 3GPP TS 38.101-1 V16.4.0, “5G; NR; User Equipment (UE) Radio Transmission and Reception; Part 1: Range 1 Standalone,” July 2020.

[20] 3GPP is a consortium with seven national or regional telecommunication standards organizations as primary members (organizational partners) and a variety of other organizations as associate members (market representation partners). The organizational partners are as follows:

- Association of Radio Industries and Businesses, Japan
- Alliance for Telecommunications Industry Solutions, USA
- China Communications Standards Association, China
- European Telecommunications Standards Institute, Europe
- Telecommunications Standards Development Society, India
- Telecommunications Technology Association, South Korea
- Telecommunication Technology Committee, Japan

- 3GPP TS 38.141-1 V16.4.0, “5G; NR; Base Station (BS) Conformance Testing; Part 1: Conducted Conformance Testing,” July 2020.

## C.8 MULTIPLE ADDRESS (MAS) RADIO

A basic MAS radio link consists of a master radio transmitter/receiver unit and multiple remote radio transmitter/receiver units operating in spread spectrum, so MAS will hop frequencies within a given frequency band. A master unit can access multiple units via a pair of transmit/receive frequencies. MAS RF pairs operate between 895 to 960 MHz by LOS between the master-slave pair. The data rate is up to 4.8 kbps. The master unit is set up to always be ready to transmit and receive to minimize transmitter keying. Each remote unit is set up in the listening mode until queried and is then ready to transmit. Each remote unit has a unique address, so no two units will try to answer the query at the same time. The frequency pair used by MAS must be licensed by the FCC. The same frequency pair can be reused elsewhere in a plant or industrial setting if it does not cause any interference [C.6, C.10].

## C.9 REFERENCES

C.1 A. Laikari, J. Flak, A. Koskinen & J. Häkli, *Wireless In Nuclear; Feasibility Study*, Energiforsk, Report 2018:513, July 2018.

C.2 Richard T. Wood and Paul D. Ewing, *Task 4 – EMI/RFI Issues Potentially Impacting Electromagnetic Compatibility of I&C Systems (NRCHQ6014D0015)*, ORNL/LTR-2015/254, Oak Ridge National Laboratory, Oak Ridge, TN, May 2015.

C.3 EPRI 1010468, Technical Update, *Automation in Power Plants and Wireless Technology Assessments*, Electric Power Research Institute, Palo Alto, California, December 2005.

C.4 M. Howlader, C.J. Kiger, and P.D. Ewing, *Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment*, NUREG/CR-6939, ORNL/TM-2006/86, US Nuclear Regulatory Commission, July 2007 (NRC ADAMS Accession No. ML072210179).

C.5 EPRI TR-1019186, Final Report, *Implementation Guideline for Wireless Networks and Wireless Equipment Conditioning Monitoring*, Electric Power Research Institute, Palo Alto, California, December 2009.

C.6 ISA-TR100.00.03-2011, Technical Report, *Wireless User Requirements for Factory Automation*, International Society of Automation, May 2011.

C.7 Philip Keebler and Stephen Berger, “Managing the Use of Wireless Devices in Nuclear Power Plants,” *InCompliance Magazine*, November 1, 2011. https://incompliancemag.com/article/managing-the-use-of-wireless-devices-in-nuclear-power-plants/

C.8 M. S. Costa and J. L. M. Amaral, *Analysis of Wireless Industrial Automation Standards: ISA-100.11a and WirelessHART*, accessed January 28, 2022, https://blog.isa.org/analysis-wireless-industrial-automation-standards-isa-100-11a-wirelesshart.

C.9 IAEA Nuclear Energy Series No. NR-T-3.29, *Application of Wireless Technologies in Nuclear Power Plant Instrumentation and Control Systems*, International Atomic Energy Agency, Vienna, November 2010.

C.10 EPRI TR-1018454, Final Report, *Demonstration of Wireless Technology Security in Substation Network Architecture*, Electric Power Research Institute, Palo Alto, California, February 2009.

C.11 Goodwins, Rupert (3 October 2018). "Next-generation 802.11ax Wi-Fi: Dense, fast, delayed". *www.zdnet.com.*

C.12 S. Frankel, B. Eydt, L. Owens, and K. Scarfone, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, NIST SP 800-97, U.S. Department of Commerce, National Institute of Standards and Technology, February 2007.

C.13 K. Korsah, et al., *Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update*, NUREG/CR-6992, US Nuclear Regulatory Commission, October 2009 (ML092950511).

C.14 K. Scarfone, D. Dicoi, M. Sexton, and C. Tibbs, *Wireless Network Security for IEEE 802.11a/b/g and Bluetooth*, NIST SP 800-48 (rev. 1), U.S. Department of Commerce, National Institute of Standards and Technology, August 2007.

C.15 EPRI TR- 1013864, Final Report, *Assessment of Wireless Technologies for Advanced Automation*, Electric Power Research Institute, Palo Alto, California, December 2007.

C.16 EPRI, *IntelliGridArchitecture*, Accessed January 21, 2022, http://xanthus-consulting.com/IntelliGrid_Architecture/New_Technologies/Tech_Multiple_Address_(MAS)_Radio.htm.

C.17 ISA-TR100.20.01-2017, *Common Network Management: Concepts and Terminology*, International Society of Automation, Approved 10 March 2017.

C.18 "LTE Protocols & Specifications," *4G 5G world*. *http://www.4g5gworld.com/lte-protocols-specifications*

C.19 "Long Term Evolution (LTE)," *4G 5G world*. *http://4g5gworld.com/wiki/long-term-evolution-lteIU*

C.20 *The LTE Standard*, Signals Research Group, April 2014.

C.21 Gautam Talagery, *Wireless: The smart network for the smart grid and grid modernization*, Ericsson, September 03, 2021. https://www.ericsson.com/en/blog/2021/9/the-smart-network-for-the-smart-grid-modernization

C.22 "Air Interface Physical Layer," *4G 5G world*. http://www.4g5gworld.com/specification/air-interface-physical-layer

# APPENDIX D. CONCERNS FOR IMPLEMENTING WIRELESS NETWORKS

Although detrimental impacts from EMI/RFI on wireless networks may seem more likely than such impacts on cable networks, long cable runs over areas between plant buildings, whether buried or above ground, can also pose problems. In general, in this context wireless devices may be less susceptible to electromagnetic (EM) events such as an electromagnetic pulse (EMP) because they do not have long cables attached, unlike wired SCADA equipment. However, the equipment could have power cables connected, as well as antennas that pick up EM energy, especially if located in an exposed area.

ORNL and EPRI are analyzing cellular LTE vulnerability. More specifically, ORNL is researching this topic as part of the Grid Modernization Laboratory Consortium (GMLC) project, assessing the vulnerability of power generation critical systems. Published work in this area is limited.

Three major concerns regarding the implementation of wireless technologies in research reactors and NPPs include EMI/RFI, cybersecurity, and installation issues [D.1].

Many of the failure modes are the same for wireless networks and hard-wired systems (Appendix E). Some of the risks seen in wireless systems are similar to those of wired systems. However, some risks to wireless networks are new: the failures may transpire in different ways, and the wireless networks may be more susceptible to those failures.

## D.1 EMC

EMC[21] is the ability of a device or system to function satisfactorily in its EM environment, which is achieved by limiting the unintentional generation, propagation, and reception of EM energy that may cause unwanted effects such as EMI. The goal of EMC is to ensure the correct operation of different types of equipment in a common EM environment.

EMC and EMI are tightly connected to spectrum management. Radio spectrum management is important for ensuring the coexisting of various wireless technologies, when they have been accepted to be used in the plant, as mixing several wireless technologies without planning can result in interference problems. This can be especially more apparent in the older NPPs where the old I&C systems were not designed or planned to be used with wireless communication systems. In the new NPPs wireless design can be taken into account in the design phase.

Ideally, electrical equipment does not radiate much energy and is not susceptible to outside interference. However, new and existing equipment can fail when subjected to EMI/RFI radiated from existing plant equipment. EMC standards define the permissible EM interaction between every system and its immediate environment. All electronic systems must be EMC-compatible to all other systems in the

[21] *EMC* addresses the unwanted emissions and the countermeasures that may be taken to reduce unwanted emissions. The three main components of EMC are:

1. *Emission* of electromagnetic energy, whether deliberate or accidental, by some source and its release into the environment.
2. *Susceptibility* of the electronic or electrical equipment to malfunction or break down in the presence of unwanted emissions (i.e., RFI). *Immunity* is the opposite of susceptibility, being the ability of equipment to function correctly in the presence of RFI, with the discipline of "hardening" equipment being known equally as susceptibility or immunity.
3. The *coupling path* is the mechanism by which emitted interference reaches the electronic or electrical device.

EMC problems are generally solved by identifying at least two of the above-mentioned components of EMC and eliminating one of them.

affected environment. This system compatibility must be proven by tests to be certified by the applicable EMC standard.

EMC engineering uses analytical methods, design practices, test procedures, and solution hardware and components to enable the system to function without errors in its target EM environment and to prevent it from inflicting errors to any adjacent system. This approach also enables the system to meet EMC control specifications limits.

EMC engineering includes the analysis of unwanted emissions and determination of the countermeasures to be taken to reduce unwanted emissions. EMC engineering includes three main classes of issue:

- *Emission* of EM energy, whether deliberate or accidental, by some source and its release into the environment.

- *Susceptibility* of the electronic or electrical equipment to malfunction or break down in the presence of unwanted emissions (i.e., RFI). *Immunity* is the opposite of susceptibility, being the ability of equipment to function correctly in the presence of RFI, with the discipline of *hardening* equipment known to be equally as susceptible or immune.

- The *coupling* path: the mechanism by which emitted interference reaches the electronic or electrical device.

Interference mitigation, and hence EMC, may be achieved by addressing the emission, susceptibility, or coupling path individually or collectively (i.e., quieting the sources of interference, inhibiting coupling paths and/or hardening the potential victims (i.e., electronic or electrical equipment). In existing plants, EMC is a concern because the existing equipment was installed prior to most EMC standards. This concern is partially because of plant experiences regarding security personnel's walkie-talkie radios inadvertently affecting plant systems. Most equipment in NPPs has never been tested for vulnerability to wireless transmission [D.2]. As such, the impact of modern wireless devices on nuclear safety and plant reliability is not understood.

## D.2 EMI/RFI

The introduction of new or additional equipment could increase the EMI/RFI issues that could potentially impact the EMC of I&C systems. EMI/RFI concerns have led to reluctance to implement widespread use of wireless technologies in NPPs. EMI/RFI may cause interference with the existing sensitive plant equipment. When security personnel's walkie-talkie radios were shown to affect plant systems, exclusion zones for wireless devices were established around certain sensitive or critical equipment. Wireless sensor technologies typically operate with power levels on the order of 100 mW; the radios typically used by plant security personnel can transmit at a much higher power level of several watts. The transmission frequency also impacts the amount of interference with plant equipment that can be experienced. The frequency of operation for walkie-talkie radios is in the megahertz region, and modern sensor technologies operate in the gigahertz range of frequencies. In general, these characteristics of modern wireless devices (lower power and higher frequency) significantly decrease the chances of interference with nuclear power reactor equipment [D.3].

NPPs have numerous sources of EMI/RFI, such as inverters, motors, and relays. Plant devices connected to AC or DC power are also susceptible to EMI that is conducted through power cables. The increased use of digital technology raises the concern for EMC: the faster microprocessor clock rates and lower logic voltage levels can increase the potential for disruption by EMI/RFI [D.4]. Similarly, the introduction of wireless technology will likely increase EM emissions. Therefore, before any new digital system, including a wireless system, is implemented, an emissions site survey should be performed to confirm the EMC of the systems and/or devices in the plant environment.

## D.3 CYBERSECURITY

Cybersecurity is not a focus of this review, but the topic must be addressed for the implementation of wireless technology into an NPP. Wireless technology and cybersecurity are tightly coupled as a wireless network that is installed or replacing a wired network for use in an SR/ITS application would require a plant to amend its cybersecurity plan. In many instances, although a wireless network has the same consequences of failure as a wired network, the likelihood of failure and new failure modes (including those related to cybersecurity failures) require an assessment of the new network from all causes.

NRC documents that address cybersecurity are listed in Table D.1.

**Table D.1. NRC documents on cybersecurity**

| Document | Title |
|---|---|
| 10 CFR 73.54 | Protection of Digital Computer and Communication Systems and Networks |
| NRC Order EA-02-026 | Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants |
| NRC Order EA-03-086 | Design Basis Threat for Radiological Sabotage |
| NUREG/CR-6847 | Cyber Security Self-Assessment Method for US Nuclear Power Plants |
| RG 5.71, Rev. 1 | Cyber Security Programs for Nuclear Facilities |
| RG 1.152, Rev. 3 | Criteria for Use of Computers in Safety Systems of Nuclear Power Plants |
| RG 5.83 | Cyber Security Event Notifications |
| NUREG/CR-6852 | An Examination of Cyber Security at Several US Nuclear Power Plants |
| SRP BTP 7-14, Rev. 6 | Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems |
| SRP 13.6.6, Rev. 0 | Cyber Security Plan |

## D.4 REFERENCES

D.1 H. M. Hashemian, C. J. Kiger, G. W. Morton & B. D. Shumaker (2011) “Wireless Sensor Applications in Nuclear Power Plants,” *Nuclear Technology*, 173:1, 8-16, DOI: 10.13182/NT11-1.

D.2 Chris L. Lowe, Chad J. Kiger, David N. Jackson, David M. Young, *Implementation of Wireless Technologies in Nuclear Power Plants’ Electromagnetic Environment Using Cognitive Radio System*, NPIC&HMIT 2017, San Francisco, CA, June 11–15, 2017.

D.3 EPRI 1007448, *Guidelines for Wireless Technology in Power Plants, Volume 2: Implementation and Regulatory Issues*, Electric Power Research Institute, Palo Alto, California, 2002.

D.4 EPRI 1019186, *Implementation Guideline for Wireless Networks and Wireless Equipment Condition Monitoring*, Electric Power Research Institute, Palo Alto, California, December 2009.

# APPENDIX E. DESIGN / INSTALLATION ISSUES

The installation of a wireless network can greatly increase RF emissions, potentially affecting existing devices susceptible to those emissions or not immune from those emissions. Thus, the installation of additional devices can introduce new failure modes into the system. Most of these failure modes are recognized. Some of these issues are addressed in Appendix B, including coexistence, improper communication range, environment, multipath propagation packet loss, network latency, network jitter, measurement data quality, fading, burst error, phase shift keying/frequency shift keying corruption, and high voltage standing wave ratio.

## E.1 COEXISTENCE

The use of such wireless technology must be evaluated for any possible adverse impact it may have on other plant equipment likely to be in use at the same time. Consider the example of the wireless spent fuel pool (SFP) instrumentation[E.1]. The impact from other plant equipment must also be considered.

Coexistence relates to the ability of the wireless device to function properly when installed in proximity to other wireless equipment operating in the same frequency band. To ensure coexistence, it is important to select equipment that has been tested and certified to be compliant with all relevant spectrum utilization requirements.

*Noise immunity* refers to the ability of the wireless device to function properly while being subjected to EMI and RFI in its installed environment. To ensure adequate noise immunity, it is important to select equipment that has been tested and certified to be compliant with relevant EMC requirements. To further ensure adequate coexistence and noise immunity, it is recommended that equipment utilized has been shown to perform adequately in similar operating environments.

Noise and interference in radio systems can be broadly defined as “unwanted disturbances superimposed upon a useful signal that tend to obscure its information content” [E.2]. The term “noise” is generally used to denote disturbances which result from basic physical properties of the devices used in building the radio equipment. Interference can be a problem, even when received signal levels are high, but noise is usually only a concern when signal levels are low.

Radio transmission reliability is a compromise. A user should expect that between 1 and 10% of individual transmissions will be corrupted or lost as a normal condition. Error rates much higher than 10% may require corrective action because higher rates can be a source of higher than reasonable radio traffic, higher than desired latency, and higher than desirable battery power consumption. In other words, high error rates can be a problem, even though fault tolerance techniques ensure adequate packet delivery and availability.

## E.2 IMPROPER COMMUNICATION RANGE

One of the most important considerations in establishing a highly reliable sensor network is communication range. For best results, assume a conservative range from device to device and from devices to wireless infrastructure. Range determination should consider factors such as the density of the surrounding infrastructure. WSNs should be designed with a communication range that provides the required signal strength to ensure reliable communications as the environment changes.

Some manufacturers offer software tools to aid in the layout and analysis of wireless field networks. These tools can be used to ensure that a proposed network achieves the desired performance with sufficient margin to deliver high data reliability. Some tools allow a proposed network to be stress tested by reducing the effective range of devices in the network.

## E.3 ENVIRONMENT

Both magnitude and duration of exposure to environmental variables should be considered when assessing equipment performance during and after environmental exposure. Equipment is not typically qualified for specific locations, but instead it is qualified for values that bound the effects in the area where it is located. Ideally, the effects of environmental conditions on the instrument readings should be estimated by allowing for the local environmental conditions, which can deviate from global conditions. Instrumentation that is qualified under global conditions may not function properly under local conditions. The expected failure modes and resultant instrument indications (e.g., off-scale high, off-scale low, or floating) for instrumentation failures in severe accident conditions beyond the design basis must be identified [E.3]. This will be important for wireless networks because they will likely be used in harsh environments.

## E.4 MULTIPATH PROPAGATION

Multipath propagation is the phenomenon that results in radio signals reaching the receiving antenna by two or more paths. When the same signal is received over more than one path, it can create interference and can cause phase shifting of the signal. Copies of a signal that have taken a different path may arrive at the receiver at slightly different times, a phenomenon known as *time dispersion*. Destructive interference causes fading, and this may cause a radio signal to become too weak in certain areas to be received adequately.

## E.5 PACKET LOSS

In any network environment, data are sent and received across the network in small units called *packets*. Packet loss occurs when one or more of these packets is interrupted or corrupted in its transmission/reception and does not reach the destination with enough of the packet decodable. Packet loss is commonly caused by network congestion, hardware issues, software bugs, an overtaxed device, or a security breach, as detailed below.

- Network congestion causes packet loss.

- Power losses from network hardware problems from firewalls, routers, and network switches considerably weaken network signals.

- Software bugs, either in installed software or from updates, disrupt network performance and prevent delivery of packets.

- Overtaxed devices cause data packets to be unread (i.e., the network was not designed to handle the amount of data packets received).

- Security breach results in data packets being dropped.

## E.6 NETWORK LATENCY

*Network latency* is the term used to describe delays in communication over a network. In networking, *latency* refers to the amount of time it takes for a packet of data to be captured, transmitted, processed through multiple devices, and then received at its destination and decoded. Causes of high network latency include a large distance between the transmitter and the receiver, large load content, a receiver low on memory, effects of security devices and firewalls, insufficient bandwidth, signal conversion from A-to-D or D-to-A, and interference with other wireless devices.

Because of the relatively slow transport of data, wireless network transport time typically make up most of the overall system data latency [E.4]. Wireless network gateways typically calculate data latency for a particular data packet by comparing the packet's time stamp (the time the measurement was acquired) to the current system time when the data were received.

## E.7 NETWORK JITTER

*Jitter* is a variance in latency, or the time delay between when a signal is transmitted and when it is received; *jitter* is described as the disruption in the normal sequence of sending data packets. All networks experience some amount of latency, especially wide area networks. Causes of jitter include network congestion (insufficient bandwidth) or low quality wireless network connection. Jitter may also be the result of not prioritizing packet data transmitted/received.

Network jitter causes data transmission to be delayed and leads to poor processor performance. High jitter is a problem for real-time applications.

## E.8 MEASUREMENT DATA QUALITY

*Measurement data quality* is typically provided by wireless sensors as an indication of the trustworthiness of the measurement data [E.4]. For example, if the input of a pressure sensor is saturated, then the actual pressure may be much greater than the value reported. In this example, the pressure sensor would typically report a data quality of *uncertain*, along with an indication that the input is *saturated high*. Wireless sensors and networks should include a means to validate measurement data quality, as well as a means to propagate data quality metrics for each measurement value to the gateway and then to the host application.

## E.9 FADING

*Fading* is the time variation of received signal power caused by changes in transmission medium or paths. Large-scale fading occurs when an obstacle comes in between transmitter and receiver. This interference type causes significant amount of signal strength reduction. This is because the EM wave is shadowed or blocked by the obstacle. It is related to large fluctuations of the signal over distance.

Large-scale fading can occur when the transmitted signal attenuates over distance as the signal is being spread over an increasing area from the transmit end towards the receive end (i.e., path loss). Large-scale fading can also occur when obstacles are over the path between the transmitter and receiver (i.e., shadowing effect). Small-scale fading includes (1) multipath delay spread in which all the frequency components of the received signal fluctuate in the same proportions simultaneously and (2) Doppler spread, which depends on the mobile speed of the receiver with respect to the transmitter.

## E.10 BURST ERROR

A *burst error* occurs when two or more bits in the data unit have changed from 0 to 1, or vice-versa. Note that burst error does not necessary mean that an error occurs in consecutive bits. The length of the burst error is measured from the first to the last corrupted bit (Figure E.1). Some bits in between may not be corrupted.

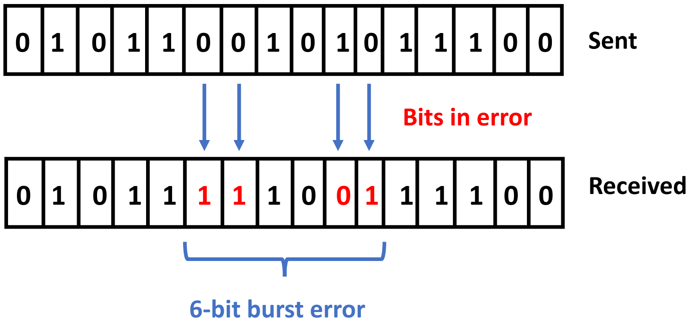


**Figure E.1. Example of a 6-bit burst error.**

Burst errors are most likely to occur in serial transmission and could be design related. The duration of the noise is typically longer than the duration of a single bit, which means that the noise affects data; it affects a set of bits. The number of bits affected depends on the data rate and duration of noise.

## E.11 PHASE SHIFT KEYING/FREQUENCY SHIFT KEYING CORRUPTS SIGNAL

Information in digital form is referred to as *keying*, a word inherited from hand-keyed Morse code, an early form of digital modulation. Radios transfer information by changing the value of some parameter of the carrier signal. This process is generally known as *modulation*, but the term *keying* from the early days of wireless telegraphy is also used. *Phase shift keying* is a type of modulation that 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 would represent 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.

A signal could be corrupted during this phase shift. The first part, shift keying, occurs because during the course of transmission of digital data, the values of the quantity used for coding the data (e.g. amplitude, frequency, phase) shift between two or more discrete switching (= keying) values.

## E.12 HIGH VOLTAGE STANDING WAVE RATIO

For a radio (transmitter or receiver) to deliver power to an antenna, the impedance of the radio and transmission line must be well matched to the antenna’s impedance. The parameter voltage standing wave ratio (VSWR) is a measure that numerically describes how well the antenna’s impedance matches the radio or transmission line to which it is connected. VSWR is sometimes called *SWR* to avoid using the term *voltage* and to instead use the concept of power waves. For an ideal system, voltage does not vary, so its VSWR is 1.0. When reflections occur, voltages vary, so the VSWR is higher. Increased VSWR correlates with reduced transmission line (and therefore overall transmitter) efficiency.

## E.13 REFERENCES

E.1 NEI 12-02 [Revision 1], *Industry Guidance for Compliance with NRC Order EA-12-051, “To Modify Licenses with Regard to Reliable Spent Fuel Pool Instrumentation”*, August 2012.

E.2 ISA-TR100.00.01-2006, *The Automation Engineer’s Guide to Wireless Technology Part 1 – The Physics of Radio, a Tutorial*, International Society of Automation, Approved 29 December 2006.

E.3 IAEA Nuclear Energy Series No. NP-T-3.16, *Accident Monitoring Systems for Nuclear Power Plants*, International Atomic Energy Agency, Vienna, 2015.

E.4 ISA-TR84.00.08-2017, *Guidance for Application of Wireless Sensor Technology to Non-SIS Independent Protection Layers*, International Society of Automation, International Society of Automation, Approved 24 April 2017.

# APPENDIX F. FAILURE MODES

Many important applications served by wireless networks are characterized by being mission critical, meaning that the failure of the wireless network could have serious implications. Thus, it is imperative that the wireless network functions properly throughout its intended mission time. This poses stringent reliability requirements on the wireless network that must be addressed in the design and deployment phase [F.1]. It is also important to understand that failure or interference in a wireless network can cause failure of other I&C equipment.

The most important requirements for I&C systems and components are [F.2] reliability, security, robustness, determinism, QoS, interoperability, integration with existing systems, networks with a large number of devices (scalability), and support tools for designing the network layout, process information, and monitoring. Thus, in addition to evaluating the current state of EMI/RFI issues identified in RG 1.180 Rev. 2, this report also evaluates factors that affect the overall reliability of wireless communication systems and how their operability/inoperability can affect other systems. EMI/RFI, the focus of RG 1.180, can cause latency issues, slow response times, and other failures, including failures of other I&C components and systems. Understanding the reliability of the wireless network requires an understanding of all the failure modes.

RG 1.180 address the generation of RF signals and a component's ability to withstand those signals. However, understanding the *reliability* of a wireless network requires a more complete knowledge of the failure modes. Although the failure modes of a wireless network are the same as those for an I&C system, there are failure modes specific to the wireless network that are not applicable to a wired network, and even for those failure modes that are the same, the causes or propagations of the failures are different. The failure modes of a wireless system must consider [F.3, F.5] the following factors:

1. The impact of the plant environment on the wireless system
2. The impact of the wireless device on the plant environment
3. The identification of equipment that may be susceptible to interference from the wireless transmission

The most common failures of wireless networks are communication errors and hardware/software failures [F.5]. Wireless communication errors are mainly the result of radio fading, signal attenuation, radio interference, and background noise. Sensors are easily disturbed by environmental factors, network problems, and node failures. The data collected by sensors are not completely reliable [F.6], so analysis of the sensor nodes' data reliability and adaptability under disturbance conditions is crucial.

Radio interference or jamming attacks can seriously interfere with the normal operation of wireless networks and can affect their performance. Radio interference is one of the main factors that can affect the routing decisions and employed routing protocols in wireless networks. The ability to detect radio interference attacks is important because it is the main basis for building a secure and dependable wireless network [F.7]. Several parameters are monitored to detect jamming, such as signal strength, carrier sensing time and packet delivery ratio. Proven countermeasures against jamming include spread spectrum and frequency hopping techniques.

Wide spectrum communication (e.g., UWB), frequency hopping technologies, and/or directional antennas can be used as a measure against jamming [F.9]. Directional antennas may be used to minimize the potential for EMI/RFI or eavesdropping [F.7].

EMI/RFI-induced failure modes are identified separately in the list of failure modes of wireless networks. In addition to installation issues, new failure modes that are introduced in wireless networks are also addressed for each part of the wireless network.

The use of such wireless technology must also be evaluated for any possible adverse impact they may have on other plant equipment likely to be in use while the wireless instrumentation is functioning. Licensees should also consider the ability of a wireless communication link to perform in the environment (e.g., high humidity, radiation) where it may be required to function. Wireless technologies must meet the same requirements as wired technologies.

A failure mode can be thought of as loss of a particular equipment function. Automation equipment can be used to execute different types of functions in various applications, so the impact of a particular failure mode is unique to the application. Regarding the equipment and its safety instrumented function (SIF), these failure modes may be considered safe if they cause the process to be placed in a safe state, or they may be considered dangerous if they fail to operate when there is a process demand. Whether a specific failure mode is safe or dangerous is highly dependent upon the process and the safety instrumented system (SIS) design.

Radio transmitters are a part of the overall plant emissions profile that are *not* always included in the facility map [F.9]. For example, a transmitter can be used to measure flow during a process in which high and/or low flow can cause hazardous conditions. If the failure results in a high output, then the low trip will fail, and if it results in a low output, then the high trip will fail: the failure is dangerous in either direction. Conversely, if the failure results in a high output on a high trip or low output on a low trip, then the failure is safe. Even with a switch contact, the terms *safe* and *dangerous* take on different meanings for energize-to-trip and deenergize-to-trip. If ventilation fan output or flow from fire water pumps are required during a demand, then the fan or pump motors must remain energized to perform the safety function. In such a design, loss of the electrical supply to the motor would be dangerous. Once the impact of each failure mode has been determined for a specific application, improvements to both safety and reliability can be gained if diagnostics coupled with appropriate architectures are properly employed. The use of diagnostics helps reduce the number of undetected failures that can occur by alerting the operating and maintenance personnel that repairs are needed. It should be recognized that diagnostics are themselves acting as protection for the equipment and may also be prone to undetected failures. This propensity is dependent upon the particular diagnostic. Any time that diagnostics are being used to enhance SIS performance, they must be addressed and considered in the overall automation asset integrity (AAI) program.

## F.1 FAILURE MODES OF WIRELESS NETWORKS

As more parts of the control subsystems become wireless, it may become more difficult to provide a safety claim. Communication failures are more prevalent in wireless systems than in wired controllers. Failsafe strategies can reduce the impact of communication failure by using a local sequencer and self-supervising capabilities for state transition, along with fault detection and limiters for control variables. Specific control and coding can overcome communication failures. A generic list of failure modes for wireless networks was developed based on a review of the architectures and failure modes of wireless networks in numerous applications. Applications reviewed to identify architectures and failure modes include electrical substations, telemedicine, unmanned aircraft, radar and RF systems for aeronautical uses, microphones, industry, fast charging systems, automation, and uses in NPPs.

Failure modes were identified for each element of the wireless network and are provided in Table F.1. These failure modes were evaluated at a higher level and not at the subcomponent level (e.g., an integrated circuit chip could cause failure because of single event upsets [SEUs]). Repeater failure modes can be determined by reviewing transmitter and receiver failure modes.

**Table F.1. Identification of failure modes for each element of a wireless network**

| Failure mode | Transmitter | Transmission medium (air) | Receiver | Antenna |
|---|---|---|---|---|
| Buffer overflow | ✓ |  | ✓ |  |
| Burst error (noise) | ✓ |  | ✓ |  |
| Clock drift |  |  | ✓ |  |
| Communication network damage |  |  | ✓ |  |
| Connector to antenna fails because of oxidation | ✓ |  | ✓ | ✓ |
| Connector to I&C system has lost all contact |  |  | ✓ |  |
| Data not updated | ✓ |  | ✓ |  |
| Decrease in efficiency (i.e., air gap increases and EMF emissions increase) | ✓ |  | ✓ |  |
| Denial of service |  |  | ✓ | ✓ |
| Different messages sent to different nodes (i.e., not all messages correct) | ✓ |  |  |  |
| Electrical interference | ✓ |  | ✓ |  |
| EMI |  |  | ✓ |  |
| Erroneous signal sent to node or receiver | ✓ |  | ✓ |  |
| Excessive CPU utilization | ✓ |  | ✓ |  |
| Excessive data loss (i.e., packet loss) | ✓ |  | ✓ |  |
| Fading |  | ✓ |  |  |
| Fail high | ✓ |  | ✓ |  |
| Fail low | ✓ |  | ✓ |  |
| Failure in electrical system | ✓ |  | ✓ |  |
| Frequency coordination | ✓ |  | ✓ |  |
| Frozen output (dangerous undetected) | ✓ |  |  |  |
| Hardware degradation of demodulator |  |  | ✓ |  |
| High voltage standing wave ratio causing inaccurate measurements | ✓ |  |  |  |
| Improper installation | ✓ |  | ✓ | ✓ |
| Interference | ✓ |  | ✓ |  |
| Intermittent faults / outage (i.e., loose connector) | ✓ |  | ✓ | ✓ |
| Intermodulation distortion | ✓ |  | ✓ |  |
| Jitter (low quality network, insufficient bandwidth) | ✓ |  | ✓ |  |
| Large fault currents produce instantaneous tripping | ✓ |  | ✓ |  |
| Latency (time delay, insufficient bandwidth) | ✓ | ✓ | ✓ |  |
| Leakage current | ✓ |  |  |  |
| Loss of connectivity / signal (i.e., no output) | ✓ | ✓ | ✓ |  |
| Low signal strength |  |  | ✓ |  |

**Table F.1. Identification of failure modes for each element of a wireless network (continued).**

| Failure Mode | Transmitter | Transmission medium (air) | Receiver | Antenna |
|---|---|---|---|---|
| Malfunction/failure | ✓ | | ✓ | |
| Malicious modification of data (i.e., tampering) | | | | |
| Misalignment of antenna | ✓ | | ✓ | ✓ |
| Misapplication (sensor mismatch) | ✓ | | | |
| Mismatched signals between sensor, transmitter, node, receiver | ✓ | | ✓ | |
| Multipath echoes | | ✓ | | |
| Multipath interference | | ✓ | | |
| Multipath propagation | ✓ | | ✓ | |
| No message is delivered to any receiver | ✓ | | | |
| No message is delivered to any receiving node | ✓ | | | |
| No message received by destination nodes | ✓ | | | |
| Open circuit of wireless to microcontroller interface | ✓ | | ✓ | |
| Operating frequency not appropriate | ✓ | | ✓ | |
| Out of range (i.e., no signal received by node or receiver) | ✓ | | ✓ | |
| Phase shift keying/Frequency shift keying corrupts signal | ✓ | | ✓ | |
| Physical damage to antenna causing failure | ✓ | | ✓ | ✓ |
| Power supply failure (weak or dead battery) | ✓ | | ✓ | |
| Radio interference | | ✓ | | |
| Re-transmission rate | | | | |
| Replay attack (i.e., a valid data transmission is maliciously or fraudulently repeated or delayed) | ✓ | | ✓ | |
| Shock and vibration | ✓ | | ✓ | |
| Single erroneous message is delivered to all receiving nodes | ✓ | | | |
| Slow response time | ✓ | | ✓ | |
| Spoofing attack (i.e., a device successfully masquerades as another) | ✓ | | ✓ | |
| Sybil/Black hole/Wormhole/Selective-forwarding attack (e.g., malicious modification of routing information such that packets may be lost or transit through a malicious device) | ✓ | | ✓ | |
| Synchronization problem | | | ✓ | |
| Temperature and temperature cycling causing fatigue | ✓ | | ✓ | |
| The messages, even faulty, are all identical | ✓ | | ✓ | |
| Unauthorized users can get into the system | ✓ | | ✓ | |
| Unstable signal | ✓ | | ✓ | |
| Water/water ingress | ✓ | | ✓ | ✓ |
| Waveguide damage to antenna | ✓ | | ✓ | ✓ |
| Weak signal | ✓ | ✓ | | |
| Wet surface of antenna | ✓ | | ✓ | ✓ |
| Wind loading on antenna | ✓ | | ✓ | ✓ |

Battery and battery life are frequently listed as disadvantages of wireless networks and are recognized failure modes of transmitters and receivers. Because of this, much research has been performed on batteries and battery life. The types of energy sources may be grouped into five categories:

- Mains
- Limited battery (e.g., button cell)
- Moderate battery (e.g., lead acid)
- Rechargeable battery
- Environmental or energy-scavenging

Wireless sensors with low power consumption and infrequent data transmission are typically battery powered and achieve long battery life through duty cycled operation, resulting in a typical battery life in the range of 5–10 years. A sensor with high power consumption and frequent data transmission may require battery replacement or recharging much more frequently, such as weekly. Alternately, sensors may still be connected to a local power source.

The reason for incorporating energy scavenging is to eliminate the lifetime limitation of fixed storage batteries [F.10]. For example, some devices such as the Rosemount, Inc. THUM Adapter, which allows wireless access to HART measurement and diagnostic information, powers itself by scavenging power. The need to extend battery life makes energy-efficient messaging extremely important. The use of battery power or energy scavenging/harvesting techniques for connected field devices requires additional considerations in communication layer design, compared to the approach taken for wired devices [F.11]. Not only does every communicating layer need to consider device resource availability, but also it needs to consider energy consumption minimization to extend battery life or to operate within the scavenging/harvesting budget.

Another possible way to replace batteries is through wireless power transfer (WPT) [F.12]. Large and continually operating industries such as electric power plants are interested in evaluating WPT as a power source alternative for sensors and transducers.

Because energy is consumed by message processing, as well as by the fundamental control operation of the device, it is necessary to balance communications efficiency with the use of proven, well-accepted architectural principles of information separation, as well as message processing efficiency.

## F.2 SOURCES FOR IDENTIFICATION OF FAILURE MODES

Architectures and failure modes from different applications in different industries were reviewed to identify the elements of a wireless system and the failure modes of those elements. These systems have been in operation for many years, and their failure modes should be well known. Industries include the military, aircraft landing systems, unmanned aircraft, wireless audio, telemedicine networks, and electrical fast charging systems.

### F.2.1 NIST

Risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity, and some are new. “Perhaps the most significant source of risks in wireless networks is that the technology’s underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot” [F.14].

The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

Specific threats and vulnerabilities to wireless networks and handheld devices include the following [F.14]:

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an agency's computer network through wireless connections, bypassing any firewall protections.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- DoS attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and subsequently be introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other agencies or organizations for the purposes of launching attacks and concealing their activities.
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.
- Malicious entities may use third-party, untrusted wireless network services to gain access to an agencies or other organization's network resources.
- Internal attacks may be possible via ad hoc transmissions.

A list of failure modes created based on the review of NIST documents is provided in Table F.2.

**Table F.2. Failure modes identified by NIST**

| Failure mode |
|---|
| Internal attacks |
| Unauthorized users can get into the system, gain control |
| Security breaches |
| Denial of service |
| Degraded network performance |
| Corrupted data |
| Internal attack |

### F.2.2 Substations

The different types of wireless systems—such as Wi-Fi, Bluetooth, WiMAX, ZigBee, 3G cellphone systems, and spread spectrum radio—will have different performance impacts of high EMI and large steel structures. These performance impacts would include statistics on delays in data transmissions, communication errors, communication failures, loading of communications bandwidth, and security breaches, including integrity and denial of service attacks [F.16].

However, wireless systems have several disadvantages. Reliability of wireless transmissions and vulnerability to security threats are perceived to be the primary reasons for questioning or limiting the use of wireless technologies in utility operations. These threats include [F.16] the following:

- EM interception of wireless signals can permit unauthorized entities to eavesdrop on transmissions within the normal transmission range of the wireless system
- EMI from deliberate or inadvertent external EMI sources can completely block (jam) transmissions of data, or can slow down these transmissions by causing the wireless systems to re-transmit messages
- Weak, faded signals can cause the failure of transmissions
- RFI from wireless equipment can affect other equipment
- Congestion of unlicensed frequencies can cause delays in data exchanges
- System design and integration of wireless systems into industrial communications networks are not as well developed or tested as for wired systems
- Reliance on battery power can add to the unreliability of the wireless equipment; batteries can run out of energy before they are supposed to, or can fail without warning
- Protocol standards for wireless technologies do not always contain all of the security requirements or completeness of specifications to ensure total interoperability

Translating these weakness and vulnerabilities into failure modes for each wireless section is presented in the Table F.3.

**Table F.3. Failure modes of wireless networks in substations**

| Failure mode |
|---|
| EMI/RFI |
| Weak, faded signal |
| Delays in data exchange (congestion of frequencies) |
| Loss of battery power |
| Delays in data transmission |
| Communication error |
| Communication failure |
| Loading of communications bandwidth |
| Security breach |
| Denial of service |

### F.2.3 Military Radar System

The paper by Wileman and Perinpanayagam reviews fault causes within a military radar system using a failure modes effects and criticality analysis (FMECA), and it provides a framework for applying prognostics to monitor the health of the system [F.17]. A review of the reliability and degradation mechanisms in RF devices is also presented. Although the document focuses on failure mechanisms such as corrosion, the failure modes relevant to this review were collected and are presented in Table F.4.

**Table F.4. Failure modes of wireless networks in a military radar system**

| Wireless section | Failure mode |
|---|---|
| Fixed antennas, including arrays | Mismatching antennas, arrays<br>Waveguide damage to antenna |
| Main equipment RF Power transmitters, including HT transformer | Voltage standing wave ratio<br>Power dissipation<br>Leakage current |

### F.2.4 Military Applications

Wireless technology in military applications in the area of ad hoc and sensor networks introduces many new challenges [F.17]. Ad hoc and sensor networks operate in environments where the restrictions on nodes with respect to their computation and communication capabilities vary greatly.

The easiest assumption about faults is that they exhibit fail-stop behavior, which implies that the faulty processor ceases operation and alerts other processors of this fault. However, a more comprehensive identification of faults is shown below [F.17]:

- Crash fault (i.e., the processor is down)
- Omission faults where values are not delivered or sent (i.e., communication problem)
- Timing fault (e.g., outputs are produced in an untimely fashion)
- Transient faults imply temporary faults (e.g., glitches, with fault free behavior thereafter)
- Intermittent faults are transient faults that occur frequently

If the wireless network relies on nodes this paper provides fault types in the five-fault hybrid fault model:

1. Benign: a benign fault is self-evident to all nodes.

2. Transmissive symmetric: a single erroneous message is delivered to all receiving nodes. The messages, even faulty, are all identical.

3. Omissive symmetric: no message is delivered to any receiving node. As before, all nodes are affected the same, but the omissive behavior causes the destination nodes to likely take different action, as if the message had been received.

4. Transmissive asymmetric: this fault can exhibit any form of arbitrary asymmetric behavior and is capable of delivering different erroneous messages to different receivers.

5. Strictly omissive asymmetric: a correct message is delivered to some nodes and no message is received by other nodes. Here, the omissions have the capability of affecting the system in an asymmetric way because those nodes that have not received the message will most likely react differently (e.g., selecting a default action) than those that have received the message.

One interesting observation is that in wireless systems, there is only limited opportunity for asymmetric faults. Specifically, transmissive asymmetric faults are in general not possible within one broadcast domain because all nodes within the range of the sender receive the same information. However, asymmetric faults are possible when messages traverse over disjoint paths. These weakness and vulnerabilities are translated into failure modes for each wireless section, as presented in Table F.5.

**Table F.5. Failure modes of wireless networks in military applications**

| Failure modes |
|---|
| Crash fault (i.e., the processor is down) |
| Omission faults where values are not delivered or sent (i.e., communication problem) |
| Timing fault (e.g., outputs are produced in an untimely fashion) |
| Transient faults imply temporary faults (e.g., glitches, with fault free behavior thereafter) |
| Intermittent faults are transient faults that occur frequently |
| erroneous message is delivered to all receiving nodes |
| no message is delivered to any receiving node |
| different erroneous messages sent to different receivers |
| a correct message is delivered to some nodes and no message is received by other nodes |

### F.2.5 Instrument Landing System (ILS)

The ILS at an airport transmits signals that provide landing guidance for approaching aircraft. The ILS is comprised of the localizer and the glideslope systems [F.18]. The localizer contains two identical transmitter systems, either of which can be designated as *main*, whereas the other is *standby*. Both transmitters are connected to the changeover and test assembly, which channels signals from the operating transmitter to the antennas via the distribution circuits. During ordinary operations, the main transmitter provides the radiated signal while the standby transmitter is off.

Both glideslope systems are similar to the localizer in the use of a main and a standby transmitter, changeover and test panel, integral monitoring, recombination circuits, redundant monitor channels and a control unit. However, glideslope systems use a near-field monitor instead of the far-field monitor used with the localizer. A near-field monitor alarm is delayed by two seconds before the glideslope is shut down. Other monitoring is essentially the same for the glideslope as for the localizer. The transfer and shutdown operation of the control unit is also essentially the same as that of the localizer control unit.

The remote control/monitor panel receives and displays status information from the localizer and glideslope and allows remote control of transmitter selection. A separate control indicator module is used for each localizer and each glides lope system installed.

The ILS, which is related to wireless systems for NPPs, consists of a transmitter, antenna, wireless signal (moderator), and receiver. The remote control/monitor panel that displays the information to users is outside the scope of this review.

Failure modes for these ILS systems are mostly the same as those identified by other wireless systems (Table F.6). Any alarm circuitry in the transmitter can cause a failure of the transmitter, which shows that any added features to the transmitter (or receiver) can cause its failure. Failure of the signal modulation is specifically called out, but it is included in this collection of failure modes as a failure to transmit the data over radio waves.

**Table F.6. Failure modes identified by NIST**

| Item name | Failure mode |
|---|---|
| Transmitter | Generation of an erroneous transfer signal<br>Generation of an erroneous shutdown signal due to alarm processing circuitry<br>Inability to process a transfer signal<br>Inability to process a shutdown signal<br>Inability to process any or all power/environmental alarms<br>Generation of an erroneous control signal that shuts down the main transmitting unit<br>Generation of a continuous inhibit to the monitor channels<br>Inability to process a main inhibit to the monitor channels<br>Loss of +12 volts in control unit power supply<br>Loss of all modulation<br>Loss of RF carrier |
| Modulation | Loss or degradation of RF/VHF carrier<br>Loss of all modulation |
| Monitors | Loss of monitoring ability producing alarms<br>Loss of monitoring ability producing no alarms |
| Receiver/Detectors | Total loss of signal<br>Distortion of signal<br>Total loss of signal<br>Incorrect signal<br>Major distortion of signal<br>Distribution circuits<br>A loss, degradation, or incorrect phasing of any signal feedings to any one of the three antennas<br>Power failure |
| Course antenna array | Failure causing loss or incorrect signal<br>Failure causing a loss (or incorrect) signal<br>Loss of alignment of the antenna<br>The failure modes are identified for the transmitter, receiver, modulation, and antenna array. |

### F.2.6 Unmanned Aircraft

A failure mode and effect analysis (FMEA) for Class I unmanned aircraft is conducted to show that a single failure of one component does not lead to a failure of the complete system (single failure–tolerant system). A table in Appendix F of AON 67 [F.19] lists all the primary common failure causes (single point failure). A compilation of failure modes identified from the review of wireless unmanned aircraft systems is provided in Table F.7.

**Table F.7. Failure modes of a wireless unmanned aircraft system**

| Failure mode | Effect |
|---|---|
| **Failure of the transmitter**<br>e.g., power supply transmitter, antenna intermitted, failure in electrical system | Connection between transmitter and receiver is jammed, pilot is not able to interfere with the flight path |
| **Failure of the receiver**<br>e.g., problem with electrical system, antenna intermitted | Receiver cannot process the control signals |
| **Interrupted datalink**<br>e.g., radio interference, out of range, EMI | Flawless control of the unmanned aircraft no longer possible |
| **Engine failure**<br>e.g., malfunction of an engine, loss of propeller, loss of rotor | Uncontrolled loss of altitude and airspeed, limited maneuverability |
| **Shortcut**<br>e.g., in the camera gimbal, sensors, operation in rain/humidity | Derogation in the power supply of essential flight control systems |
| **Failure of the board power system**<br>e.g., Faulty cables of the power system, failure of battery | Receiver/ Servos are no longer provided with electrical power |
| **Malfunction/failure of the flight controller**<br>e.g., malfunction of the electrical flight controller | Automatic flight control system limited or not available |
| **Malfunction/failure of Global Navigation Satellite System**<br>e.g., malfunction of satellite receiver | Loss of automatic angular positioning |
| **Malfunction/failure of the telemetry system**<br>e.g., Malfunction of sensors, failure in the data transmission | Loss of telemetry data that areessential for the safe operation(voltage of bus system) |
| **Thermal overload of the battery**<br>e.g., internal failure of LiPo accumulators, overload through high current/unbalance | Decrease of battery capacity,thermal overload of surroundings in the aircraft |

### F.2.7 Wireless Audio

Shure Incorporated provides numerous wireless products including microphones, wireless systems, headphones, and audio electronics. Fear of signal dropouts or system failures is a common reason for not making the switch to wireless. Shure documents the following most common reasons for wireless failure [F.20]:

- Reason #1: dead or weak batteries (wireless battery terminals on the transmitter may not be making a secure contact to the battery terminals)

- Reason #2: mismatched frequencies between the wireless transmitter and the receiver

- Reason #3: failure of an audio interconnect cable (e.g., short)

- Reason #4: operating frequency is not appropriate for the location (e.g., frequency may not be an open frequency)

- Reason #5: local interference from other electronic devices or wireless systems
- Reason #6: improper installation of the wireless receiver or its antennas
- Reason #7: failure of the receiver's external power supply

A compilation of failure modes identified from the review of wireless audio systems is provided in Table F.8.

**Table F.8. Failure modes of a wireless audio system**

| Failure mode |
|---|
| Battery failure |
| Mismatched signals between sensor, transmitter, node, receiver |
| Interconnect cable failure |
| Improper operating frequency |
| Interference from other devices or wireless systems |
| Improper installation of wireless receiver or antennas |
| Failure of power supply |

### F.2.8 Wireless Microphones

Wireless microphones (transmitters) are prone to interference, noise, dropouts, and many other RF problems. The importance of frequency coordination cannot be understated because the wireless landscape continues to evolve, with more and more devices competing for less available spectrum [F.21].

Multipath interference is when portions of RF energy arrive at the receiver's antenna at slightly different times (Figure F.1). Radio waves always travel as straight lines, so they must bounce to get around a corner. As a transmitted wave spreads, it encounters surfaces that reflect or absorb different parts of the wave. As these waves bounce off and around surfaces, they arrive at the receiver at slightly different times and thus out of phase—creating dropouts and dead spots. Also, the polarity of the wave flips 180 degrees every time it reflects off a surface. When these signals mix in an antenna, they almost always cause signal cancellation and therefore dropouts.

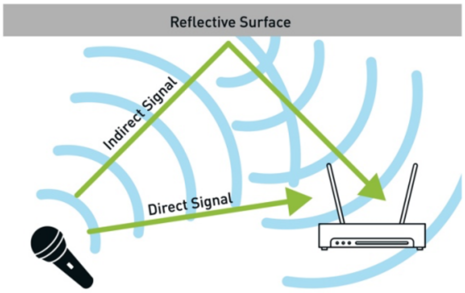


**Figure F.1. Wireless signals can be direct or indirect to the receiver.**

**Multipath interference.** The diversity microphone receiver was designed to reduce interference caused by multipaths by using two antennas with different perspectives instead of one and by employing a switching function that discriminates between the relative strengths of the two signals. The odds that a null develops at both antennas are much lower than with a single antenna. However, the design of the diversity receiver can solve one problem while introducing another: a poor signal will often cause the system to rapidly switch back and forth between antennas, leading to quick dropouts and "swooshing" sounds caused by the switching noise.

Noise floor and interference is the result of the noise floor of a radio receiver, which is the level of background noise present before any wanted signals are received. An RF system requires a sufficient signal-to-noise ratio (or carrier-to-noise ratio) to stay above this ever-present ambient noise floor. In general, the closer the wireless receivers (or remote antennas) are to the wireless transmitters, the better. This provides the transmitter and receiver a shorter distance and stronger signal, which presents a higher signal over the noise floor, which usually does not change at the receiver.

Intermodulation distortion (IMD) can cause ghost signals. Frequency coordination is essential in wireless systems to avoid not only third-party transmitters, but also the harmful effects of IMD. IMD is the result of two or more signals passing through a nonlinear device such as a diode or an amplifier. IMD manifests as ghost signals from wireless transmitters or handheld transmitters. These appear at predictable frequencies in the RF spectrum. If these ghost signals are too close to one of the frequencies used by the transmitter, then distortion can result.

A compilation of failure modes identified from the review of wireless microphones is provided in Table F.9.

**Table F.9. Failure modes of wireless microphones**

| Failure mode |
|---|
| Multipath interference |
| Floor noise (background noise) level is too high |
| Distorted signal |

### F.2.9 Wireless Media

Network foundations are sometimes called the *lower layers*, which start at the physical medium using copper, optical fiber, or wireless techniques [F.22]. Physical layer techniques and failure modes provide for the attachment of a single device to the medium, whereas data-link layer methods which involve interactions of multiple devices with a shared medium.

Communication to the wireless media can be through simple transmit-only devices that report only identity and location (e.g., RF and infrared identification devices, or tags); through somewhat more complex two-way devices such as control buttons that turn power on and off; or through intelligent devices such as telephones, portable computers, and the wide range of devices that blend voice, video, and data. Failure modes of wireless media (i.e., no physical medium is required for transmission) are presented in Table F.10.

**Table F.10. Media failure modes**

| Scope | Failure mode |
|---|---|
| Medium itself, multiple local hosts | Intermittent faults (improper grounding) |
| Medium itself, connection to WAN POP | Loss of WAN connectivity |
| Intermittent signal to wireless media | Weak signal (lack of access ports, outside service area) |
| Duplicate frames from wireless media | Multipath echoes (bad multipath resolution, service area too large) |

Connector and patch-cord problems are most common with the physical layer connection. Although the physical layer is outside the scope of this review, failure modes of the physical medium are provided in Table F.11.

**Table F.11. Failures of connection to the physical medium**

| Scope | Failure mode |
|---|---|
| Single device connection to medium | Dead (lost contact, access device has failed) |
| | Intermittent (loose connector, cracked wire, bad grounding, cable bent) |

### F.2.10 Telemedicine Network

The telemedicine network was reviewed because of its reliance on wireless technology and its need for a reliable network. Telemedicine network infrastructure provides a crucial communication link between medical service providers and patients and cannot be limited by geographical locations. The network backbone forms a core component of any wireless telemedicine system and is often the bridge between the healthcare service provider and the end user [F.23]. Failure of the radio link can lead to service interruption that may result in loss of critical time for emergency treatment.

Prognostics and health management (PHM) for the network backbone may have different requirements: the network backbone can be either a direct LOS radio link or a multi-hop network of vast coverage. For networks in which a point-to-point link is insufficient, hub placement is also an important consideration to ensure maximum network reliability. A compilation of failure modes for a wireless telemedicine network based on a review of the article by Fong et al. [F.23] are listed in Table F.12.

**Table F.12. Failure modes for a wireless telemedicine network**

| Network component | Failure mode |
|---|---|
| Demodulator (receiver) | • Phase shift<br>• High frequency noise<br>• Demodulator hardware degradation/failure<br>• Synchronization problem<br>• Clock drift<br>• low or weak signal strength |
| Antenna | • Wind loading<br>• Physical damage<br>• Wet surface<br>• Connector oxidation<br>• Misalignment |
| Channel (air interface and feed lines) | • Burst error<br>• Excessive data loss (i.e., Packet loss)<br>• Latency (time delay, insufficient bandwidth)<br>• Jitter (low quality network, insufficient bandwidth)<br>• fading<br>• Interference and noise<br>• Intermittent outage<br>• Temporary path obstruction by objects moved into path of signal<br>• link failure resulting in outage between transmitter and receiver |

| | |
|---|---|
| | • abrupt drop in the received signal power<br>• performance degradation due to attenuation<br>• low transmission power |
| Network management system (NMS)<br>(for fault identification and isolation that incorporate error detection and correction circuits, self-checking, and self-verification) | • Lengthy response time<br>• Excessive CPU utilization<br>• Efficiency decrease<br>• Data congestion<br>• Power failure |
| Routing (congestion) Control | • Excessive re-transmission<br>• Packet loss<br>• Buffer overflow<br>• Increased or overuse of network<br>• congestive collapse (cell delay/loss) |

### F.2.11 Fast Charging Networks

A report by Gurpinar and others [F.24] focuses on the assessment and FMEA of various concept architectures as static charger, and extreme fast charger for high-power wireless and wired EV charging systems. The report is divided into two main sections: wireless charging systems (WCSs) and extreme fast charging (XFC) for EVs.

The fundamental concept of wireless charging of EVs is based on the transfer of power from the source (e.g., grid) to the load (e.g., battery) via HF air core transformers. The ground side (transmitter) coil is stationary, and the vehicle side (receiver) coil is located on the vehicle. Wireless charging eliminates cable connection between the primary side charging unit and secondary side vehicle unit, so no plugging and unplugging of a connector/cable occurs to charge the vehicle.

Wireless communication from the vehicle assembly (VA) side to the ground assembly (GA) side, and vice versa, forms an integral part in closed-loop control architecture for WPT charging systems. The most commonly used wireless communication tools are classified as follows:

a. Bluetooth: range is limited to 33 ft (approximately 10 m). The communication frequency is at 2.45 GHz.

b. Wi-Fi: range is limited to 150 ft (approximately 50 m). The communication frequency is at 2.4 GHz.

c. Dedicated short-range communication (DSRC): Range is around 1 km. The communication frequency is 5.9 GHz. Most DSRC radios are equipped with wireless, LAN, 3G/4G/LTE, GPS/navigation, Bluetooth, and so on, with many added functionalities.

Regardless of the wireless communication used, the minimum delay in communication is about 100 ms. This delay is only between the wireless units and is further increased by the serial controlled area network and ethernet interfaces. This delay severely limits the maximum achievable bandwidth of closed loop control architectures for WPT systems.

A compilation of failure modes for a wireless charging system is provided in Table F.13.

**Table F.13. Failure modes of a wireless charging system**

| Component | Failure mode |
|---|---|
| Wireless charging pad | Electrical open/short circuit failures |
| | Mechanical failure |
| | Increased EMF emissions |
| Receiver | Loss of load |
| Transmitter | Reduced output power or no power flow |

## F.3 REFERENCES

F.1 Dina Deif and Yasser Gadallah, "A comprehensive wireless sensor network reliability metric for critical Internet of Things applications," *EURASIP Journal on Wireless Communications and Networking* (2017) 2017:145. DOI 10.1186/s13638-017-0930-3

F.2 Márcio S. Costa and Jorge L. M. Amaral, *Analysis of Wireless Industrial Automation Standards: ISA-100.11a and WirelessHART*." https://blog.isa.org/analysis-wireless-industrial-automation-standards-isa-100-11a-wirelesshart

F.3 EPRI TR-1019186, *Implementation Guideline for Wireless Networks and Wireless Equipment Condition Monitoring,*" Electric Power Research Institute, Palo Alto, California, December 2009.

F.4 H. M. Hashemian, C. J. Kiger, G. W. Morton & B. D. Shumaker (2011) "Wireless Sensor Applications in Nuclear Power Plants," *Nuclear Technology*, 173:1, 8-16, DOI: 10.13182/NT11-1.

F.5 He, W.; Hu, G.-Y.; Zhou, Z.-J.; Qiao, P.-L.; Han, X.-X.; Qu, Y.-Y.;Wei, H.; Shi, C. "A new hierarchical belief-rule-based method for reliability evaluation of wireless sensor network." *Microelectron. Reliab*. 2018, 87, 33–51.

F.6 Shukun Jin, Yawen Xie ,1 Yanzi Gao, Guohui Zhou, Wei Zhang, Shuaiwen Tang, and Wei He, "Data Reliability Analysis of Wireless Sensor Nodes considering Perturbation," Hindawi Journal of Sensors, Volume 2021, Article ID 5591187, 15 pages, https://doi.org/10.1155/2021/5591187.

F.7 IAEA Nuclear Energy Series No. NR-T-3.29, *Application of Wireless Technologies In Nuclear Power Plant Instrumentation and Control Systems*, International Atomic Energy Agency, Vienna, 2020.

F.8 A. Laikari, J. Flak, A. Koskinen, And J. Häkli, *Wireless in Nuclear, Feasibility Study*, Energiforsk Nuclear Safety Related I&C – ENSRIC, Report 2018:513, July 2018.

F.9 Steven G. Ferguson, *Electromagnetic Compatibility (EMC) for Equipment Qualification EPRI TR-102323 R4*, Washington Laboratories, Ltd., 2015.

F.10 Pangun Park, Sinem Coleri Ergen, Carlo Fischione, Chenyang Lu, and Karl Henrik Johansson, "Wireless Network Design for Control Systems: A Survey," August 24, 2017.

F.11 ISA-100.11a-2011, *Wireless systems for industrial automation: Process control and related applications*, International Society of Automation, 4 May 2011.

F.12 EPRI TR-1020562, *Program on Technology Innovation: Impact of Wireless Power Transfer Technology Initial Market Assessment of Evolving Technologies*, Final Report, Electric Power Research Institute, Palo Alto, California, December 2009.

F.13 Karen Scarfone, Derrick Dicoi, Matthew Sexton, Cyrus Tibbs, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, NIST Special Publication 800-48 Revision 1, U.S. Department of Commerce, National Institute of Standards and Technology, July 2008. http://dx.doi.org/10.6028/NIST.SP.800-48r1

F.14 Sheila Frankel, Bernard Eydt, Les Owens, and Karen Scarfone, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, NIST Special Publication 800-97, U.S. Department of Commerce, National Institute of Standards and Technology, February 2007.

F.15 EPRI 1011751, *Assessment of Wireless Technologies in Substation Functions, Part II: Substation Monitoring and Management Technologies*, Electric Power Research Institute, Palo Alto, California, March 2006.

F.16 A.J. Wileman and S. Perinpanayagam, *Failure mechanisms of radar and RF systems*, 2nd International Through-life Engineering Services Conference, CIRP 11 ( 2013 ) 56 – 61.

F.17 Axel W. Krings and Zhanshan Ma, *Fault-Models in Wireless Communication: Towards Survivable Ad Hoc Networks*, MILCOM 2006 - 2006 IEEE Military Communications conference, 23-25 Oct. 2006. https://ieeexplore.ieee.org/document/4086611

F.18 DOT/FAA/PM-83/18, *Failure Modes, Effects and Criticality Analysis (FMECA) of Type AN/GRN-27 (V) Instrument Landing System With Traveling-Wave Localizer Antenna*, February 1983.

F.19 AustroControl, Appendix F of AON67, *Failure Mode and Effect Analysis (FMEA) for Class I Unmanned Aircraft (courtesy translation)*. http://jarus-rpas.org/sites/jarus-rpas.org/files/f_fmea_1.1.pdf

F.20 *Top 7 Reasons for Wireless System Failure and How to Avoid Them***,** Marc Henshall | 24/04/2015, https://www.shure.com/pt-BR/shows-e-producoes/louder/top-7-reasons-for-wireless-system-failure-and-how-to-avoid-them

F.21 Don Boomer, *The Top Three Wireless Microphone Problems and How to Solve Them*. https://www.rfvenue.com/blog/2014/12/15/the-top-three-wireless-microphone-problems-and-how-to-solve-them

F.22 Howard Berkowitz, “Network Failure Prevention: Let's Get Physical,**”** *Computerworld* | Apr 19, 2006 12:00 am PST. https://www.computerworld.com/article/2554445/network-failure-prevention--let-s-get-physical.html

F.23 Bernard Fong, Nirwan Ansari, and A. C. M. Fong, “Prognostics and Health Management for Wireless Telemedicine Networks,” *IEEE Wireless Communications*, October 2012.

F.24 Gurpinar, E., Mohammad, M., Kavimandan, U., Asa, E., Galigekere, V. P., Ozpineci, B., Mukherjee, S., Tolbert, L., Bai, H., & Liu, Y (2021, August). *Failure modes and effects analysis for wireless and extreme fast charging* (Report No. DOT HS 813 137). National Highway Traffic Safety Administration.

# APPENDIX G. EXAMPLES OF COMMON EM THREATS

Interference of wireless networks and devices causing disruptions to other wireless networks/devices are generally unintended. After a discussion of what types of interference exist, examples of unintentional interference and intentional interference events are provided.

## G.1 INTERFERENCE

The common types of interference include co-channel interference (CCI), adjacent channel interference (ACI), electromagnetic interference (EMI), inter carrier interference (ICI), inter symbol interference (ISI), light interference, sound interference and so on [G.1].

CCI is the interference caused by two or more wireless systems transmitting at the same frequency. A frequency reuse concept is applied to handle large numbers of calls with limited number of channels frequency. In frequency reuse the same frequency is reused in multiple cells within their own boundaries without causing any interference. These cells are known as co-channel cells.

To reduce co-channel interference, co-channel cells must be separated by a minimum distance. When the cells sizes are approximately the same, then the following can be applied:

- Co-channel interference is independent of the transmit power.
- Co-channel interference is function of radius (R) of cell and distance (D) to the center of the nearest co-channel cell.
- By increasing ratio $Q$ (= $D/R$), interference is reduced.
- $Q$ is known as co-channel reuse ratio.
- For hexagonal geometry of cell, $Q = D/R = (3*N)^{0.5}$
- The larger value of $Q$ improves transmission quality because it will have smaller level of co-channel interference.

ACI interference is caused by leakage of frequencies from imperfect filters into passband of desired channel. Moreover, it is result of near-far effect. ACI can be reduced by careful filtering and channel assignments by RF planners. To achieve this, frequency separation between channels is kept large. Each mobile device transmitting the smallest power necessary to maintain a good quality link.

EMI interference caused by an EM signal at one frequency with the EM signal at the same frequency or at the other frequency is known as *EM interference*. An EM wave consists of electric field and magnetic field which are perpendicular to each other. EM interference can be between systems operating at the same frequencies or at different frequencies. These interference types are known as *co-channel* and *adjacent/alternate channel interference*.

In OFDM carriers are densely packed, where the peak of one sub-carrier is at null of other sub-carriers. This is referred to as *orthogonality*. To ensure that OFDM is modulating efficiently, subcarriers should be orthogonal to each other. Inter-carrier interference (ICI) is caused when sub-carriers lose orthogonality. ICI results from t following two reasons:

- Delay spread of radio channel exceeding the cyclic prefix (CP) interval (i.e., guard interval)
- Frequency offset at the receiver

ICI can be reduced or mitigated by estimating the frequency offset and correcting the sub-carrier spacing accordingly.

In OFDM-based systems, the transmission takes place symbol by symbol. Before the symbol transmission, symbols are packed with complex modulated data symbols. After the symbol is formed, CP is appended to each OFDM symbol. As the symbols travel one by one to the other end, the path from the transmitting to the receiving end will introduce delay spread in time domain. This results in the OFDM symbol becoming spread out and hence will interfere with consecutive OFDM symbols. This is referred to as *inter-symbol interference* (ISI). ISI can be mitigated or reduced using the CP concepts explained above. Here, CP length is chosen as more than channel delay spread.

Light interference occurs when light signals are at different wavelengths or at the same interference with each other. Light signals can also cause interference with other communication systems operating using other transmission media. Light waves can cause interference with other waves. This light interference is to the result of addition and subtraction of different waves when they overlap either in phase or out of phase.

Sound interference can be constructive or destructive based on whether the sound waves are in phase or out of phase with each, other respectively.

### G.1.1 Interference from 5G

The FCC recently reallocated a portion of the 3.7–4.2 GHz frequency band, making the frequency spectrum from 3.7–3.98 GHz available for flexible use, including 5G applications. The aviation industry noted that deployment of 5G networks in this frequency band may introduce harmful RF interference to radar altimeters on all types of civil aircraft currently operating in the globally allocated 4.2–4.4 GHz aeronautical band [G.2].

Radio Technical Commission for Aeronautics (RTCA) performed several tests to determine the *Interference Tolerance Threshold* on radar altimeters from 5G. The interference testing and technical analysis were conducted by the Aerospace Vehicle Systems Institute (AVSI). When addressing the complex coexistence issues in the 3.7–4.2 GHz band, RTCA determined that RF interference from 5G telecommunications systems in the 3.7–3.98 GHz band can cause harmful interference to radar altimeters that operate in the 4.2–4.4 GHz band. Interference can be received by radar altimeters that operate either within this band or within adjacent or nearby frequency bands.

5G emissions source include the following:

- Fundamental emissions: the wanted emissions within the necessary bandwidth of the source. The fundamental emissions may lead to blocking interference in the radar altimeter receiver, wherein a strong signal outside of the normal receive bandwidth cannot be sufficiently filtered in the receiver to prevent front-end overload or other effects.

- Spurious emissions falling within the 4.2–4.4 GHz band which fall within the normal receive bandwidth of the radar altimeter and which may produce undesirable effects such as desensitization due to reduced signal-to-interference-plus-noise ratio (SINR), or false altitude determination resulting from the erroneous detection of the interference signal as a radar return.

The fundamental and spurious 5G emissions are illustrated (not to scale) in relation to the radar altimeter band in Figure G.1 [G.2].

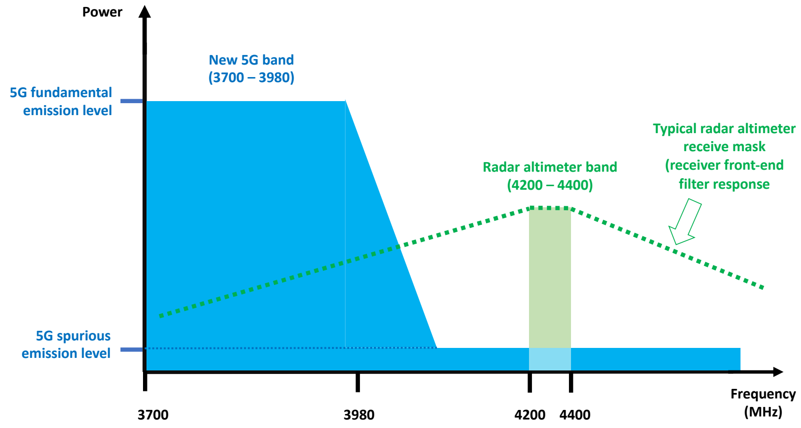


**Figure G.1. Spectrum illustration showing 5G fundamental and spurious emissions.**

RTCA determined the interference tolerance thresholds based upon the 5G fundamental emissions in the 3.7–3.98 GHz band and the 5G spurious emissions in the 4.2–4.4 GHz band. RTCA's conclusion was that 5G base stations present a risk of harmful interference to radar altimeters across all aircraft types, with far-reaching consequences and impacts to aviation operations. Specific operational impacts that affect safety include undetected erroneous readings or unanticipated loss of output from the radar altimeter on commercial or civil aircraft that use the radar altimeter for functions. Thus, any equipment in an NPP that operates in the 5G emission spectrum could be susceptible to harmful interference.

### G.1.2 Medical devices

Hundreds of incidents of RFI-induced medical device failures have been reported. The most likely source of those failures has been RFI from mobile radio transmitters. In one study, more than half of the medical equipment was shown to present some type of failure due to EMI at the more than 50 hospitals reviewed [G.3]. Many of these failures were believed to have been caused by RFI from mobile radio transmitters. The consequences have ranged from inconvenience to serious injuries and death. This history of medical device interference demonstrates a significant parallel to experiences in NPPs, where the need for constant vigilance of EMI-related interference is well justified.

NPPs uses administrative controls to limit RFI in certain areas of the plant. This vigilance may be defeated because of the increasing variety of medical devices that use wireless connectivity. For example, although it is well known that pacemakers use wireless communications, a wireless transmitter may even be in a medical implant located inside an employee's body. A medical micropower network (MMN) system uses a control unit and RF communications to receive or send data to implants in a person's body. An employee with an MMN network prescribed by a doctor could generate RFI signals in controlled areas.

Susceptibility concerns also arise with the increased use of emitters. Medical devices have experienced interference problems, and the emitter did not need to be close to the device to cause problems. Keebler and Burger [G.4] provide a summary of the interference with medical devices, as detailed below:

- Pacemakers and defibrillators have experienced failures because of cell phone interference. Nearby digital cellular phones can sometimes induce undesirable ejects. The dominant effect observed has been loss of pacemaker adaptive control, causing the device to deliver stimuli either irregularly or at a preprogrammed fixed rate. This is not usually detected by the patient, and when the cellular phones are moved away, the pacemaker resumes its normal operation.

- An apnea monitor, later recalled, was extremely susceptible to low-level RF fields, including those from mobile communication base stations several hundred meters away and FM radio broadcast stations more than one kilometer away.
- An electrically powered wheelchair experienced unintended motion initiated by RFI from transceivers in nearby emergency vehicles, causing persons to be ejected from their wheelchairs or propelled into traffic.
- Recently, handheld digital cellular telephones that use pulse modulated time division multiple access (TDMA) have been found to disrupt the proper operation of in-the-ear hearing aids. Subjective perception of interference varies from that which is barely perceptible to annoying and loud, starting when the phones are within one meter of the hearing aid, and becoming louder when the phones are several centimeters away. This type of interference also occurs in behind-the-ear hearing aids, making it impossible for wearers of this device to be able to use this type of phone.
- Recent warnings have been published concerning the use of wireless communications equipment in the clinical environment. Hospitals worldwide have recommended that cellular phones and two-way radios not be used in intensive care units, operating theaters, and patient rooms where critical care medical equipment is in use.

### G.1.3 Interference from Radar

Radars have higher regulatory priority to the bandwidth. Regulations that apply to the 5 GHz band in certain regulatory domains require radio local area networks (RLANs) operating in the 5 GHz band to avoid co-channel operation with radar systems and to provide uniform utilization of available channels [G.5]. The dynamic frequency selection (DFS) service is used to satisfy these regulatory requirements.

The DFS service provides for the following [G.5]:

- Association of STAs with an access point (AP) based on the station's[22] supported channels.
- Quieting the current channel so it can be tested for the presence of radar with less interference from other STAs.
- Testing channels for radar before using a channel and while operating in a channel.
- Discontinuing operations after detecting radar in the current channel to avoid interference with radar.
- Detecting radar in the current and other channels based on regulatory requirements.
- Requesting and reporting of measurements in the current and other channels.

[22] A station is the logical entity that is a singly addressable instance of a medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).

- Selecting and advertising a new channel to assist the migration of a basic service set (i.e., overlapping service coverage area) after radar is detected.

Potential methods to enable regulations to be met even if DFS is not employed include independently detecting radar and ceasing operation on channels on which radar is detected.

If the distance to the radio horizon is taken as the limiting factor in determining the range over which a radar can cause interference to the RLAN, then there is a potential interference zone of approximately 50 km around every land-based radar and 350 km from the airborne radar [G.6].

The upper frequency bounds for the RE102 and RS103 tests are extended to 18 GHz, regardless of the EUT's highest generated frequency in the update to MIL-STD-461G. More than likely, this has a direct link to the types of systems (e.g., radar, communications) being deployed on military platforms [G.7].

If an NPP is located near a port or airport or another source of radar, then the radar will have priority and could interfere with the wireless network in the plant. If the distance to the radio horizon is taken as the limiting factor in determining the range over which a radar can cause interference to the RLAN, then there is a potential interference zone of approximately 50 km around every land-based radar and 350 km from the airborne radar [G.8].

#### G.1.3.1 Navy Radar Shuts Down SCADA Systems

In November 1999, the US Navy was conducting exercises off San Diego during which two commercial spectrum users experienced severe EMI to their SCADA wireless networks operating at approximately 928.5 MHZ [G.9].

The San Diego County Water Authority (SDCWA) and the San Diego Gas and Electric (SDGE) companies were unable to remotely actuate critical value openings and closings because of the EMI. This necessitated sending technicians to remote locations to manually open and close water and gas valves at the water and wastewater plants.

The source of the EMI at SDCWA and SDGE was determined to be radar operated on a ship 25 miles off the coast of San Diego [G.10]. More specifically, the cause of the EMI was determined to be a Navy AN/SPS 49 radar operating off the coast of San Diego.[23] This incident resulted in new restrictions in San Diego radar operation.

#### G.1.3.2 Other events caused by interference with radar

High-powered radar, whether from ships or ground stations, can cause interference to other ships, aircraft, and commercial systems.

MIL-STD-464D provides the following examples of how external transmitters, with their increasing power levels, can drive the overall system environment [G.11].

> *High-powered shipboard radars have caused interference to satellite terminals located on other ships, resulting in loss of lock on the satellite and complete disruption of communication. The interference disables the satellite terminal for up to 15 minutes, which is the time required to re-*

[23] The AN/SPS-49 is a very long-range air surveillance radar that operates in the 902-928 MHz band.

*establish the satellite link. Standoff distances of up 20 nautical miles between ships are required to avoid the problem.*

*An aircraft lost anti-skid braking capability upon landing as a result of RF fields from a ground radar changing the weight-on-wheels signal from a proximity switch. The signal indicated to the aircraft that it was airborne and disabled the anti-skid system.*

*Aircraft systems have experienced self-test failures and fluctuations in cockpit instruments, such as engine speed indicators and fuel flow indicators, caused by sweeping shipboard radars during flight-deck operations. These false indications and test failures have resulted in numerous unnecessary pre-flight aborts.*

*Aircraft on approach to carrier decks have experienced interference from shipboard radars. One such problem involved the triggering of false "Wheels Warning" lights, indicating that the landing gear is not down and locked. A wave-off or preflight abort could occur due to this EMI induced condition.*

*Currently there are numerous incidences of co-site, intra-ship, and inter-ship interference, as well as interference with the civilian community. For example, the Honolulu Airport air traffic control radars have been degraded by shipboard radars stationed adjacent to Pearl Harbor. A program manager developed a system without requesting spectrum certification. After development, it was discovered that the system had the potential to interfere with other critical systems. Costly EMC testing and operational restrictions resulted, impacting the ability to meet mission requirements. Both items could have been avoided if spectrum management directives had been followed.*

*A base communications officer funded the purchase of commercially approved equipment. The user was unable to get a frequency assignment because the equipment functioned in a frequency range authorized for only non-Government operation. A second system had to be purchased to satisfy mission requirements. A tactical user bought commercial items as part of a deployable communications package. Because ESC was not acquired and resulting host nation coordination for the use of that equipment was not accomplished, the user found that they were unable to use the equipment in the host European and Asian countries. This problem would have been identified prior to purchase had the proper coordination taken place. The user was unable to meet communication needs and had to buy additional equipment to satisfy requirements.*

## G.2 SABATOGE

### G.2.1 Maroochy Shire Sewage Spill

The incident at Maroochy Water Services in Australia shows what can happen when a wireless network is compromised. Maroochy experienced an insider attack on its sewage pumping stations through its wireless control system. A series of mysterious faults and communication breakdowns in a network of 150 computer-controlled sewage pumping stations were originally thought to be glitches in the new system [G.12]. Faults and communication breakdowns included:

- Pumps not running when they should.

- Alarms not being triggered and reported from the computers running each individual pumping station.

- Communications between the computers through a two-way radio link being lost.

Mr. Boden, a disgruntled ex-contractor employee, was hacking into the system to take control of the network of sewage pumping stations using a laptop computer and a radio transmitter. Boden caused 800,000 liters of raw sewage to spill out into local waterways, parks, rivers, and even the grounds of a Hyatt Regency hotel, over a three-month period. "Marine life died, the creek water turned black, and the stench was unbearable for residents," said a representative of the Australian Environmental Protection Agency.

R. Stringfellow, the civil engineer in charge of the water supply and sewage systems at Maroochy Water Services during the time of the breach, provided his analysis of the incident [G.13, G.14]:

- It was easier to blame installation errors for the problems with the new control system rather than admit a cyberattack.
- It is very difficult to protect against insider attacks.
- Radio communications commonly used in SCADA systems are generally insecure or are improperly configured.
- It is often the case that security controls are not implemented at all or are used improperly.
- SCADA systems must record all device accesses and commands, especially those involving connections to or from remote sites.
- Antivirus and firewall protection should be used, along with encryption.

### G.2.2 Disgruntled Employee Remotely Disables Cars

A man fired from a Texas auto dealership used an internet service to remotely disable ignitions, setting off the car horns of more than 100 vehicles sold at his former workplace. The ex-employee used a former colleague's password to access the Webtech Plus system operated by Pay Technologies. This system makes it possible for car dealers to install a box under the vehicle dashboards that responds to commands issued through a central website and relayed over a wireless pager network. Using the Webtech Plus system, the dealer can disable the car's ignition system or trigger the horn as a reminder that a payment is due. The Texas auto center received customer complaints when their car ignitions were disabled and horns were activated remotely. The vehicle owners could not operate their vehicles, and some owners had to have their cars towed. The issues subsided when the Texas Auto Center reset the Webtech Plus passwords for all employee accounts. The police obtained access logs from Pay Technologies and traced the activity to the ex-employee's IP address to determine that this was an act of sabotage.

## G.3 REFERENCES

G.1 Different Types of Interference in communication-CCI, ACI, EMI, ICI, ISI, light, sound, RF Wireless World [accessed April 22, 2022. https://www.rfwireless-world.com/Articles/Interference-basics-and-Interference-types.html]

G.2 RTCA Paper No. 274-20/PMC-2073, Assessment of C-Band Mobile Telecommunications Interference Impact on Low Range Radar Altimeter Operations, RTCA Inc., Washington, DC, October 7, 2020.

G.3 Oscar Gutiérrez, Miguel Ángel Navarro, Francisco Saez de Adana, Adolfo Escobar, María E. Moncada, and Claudio Marcelo Muñoz, "Study of Electromagnetic Compatibility in Hospital

Environments," *Journal of Electromagnetic Analysis and Applications*, 2014, 6, 141-155, 15 April 2014.

G.4 Philip Keebler and Stephen Berger, "Managing the Use of Wireless Devices in Nuclear Power Plants," *InCompliance Magazine*, November 1, 2011. https://incompliancemag.com/article/managing-the-use-of-wireless-devices-in-nuclear-power-plants/

G.5 IEEE Std 802.11-2020, *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," The Institute of Electrical and Electronics Engineers, Inc., New York, NY, Approved 3 December 2020.

G.6 ERC REPORT 15, Compatibility Study Between Radar And RLAN Operating At Frequencies Around 5.5 GHz, Madrid, October 1992.

G.7 Paul D. Ewing, Kofi Korsah, Thomas J. Harrison, Richard T. Wood, and Gary T. Mays, *Technical Basis for Electromagnetic Compatibility Regulatory Guidance Update*, ORNL/SPR-2016/108-R1, July 2017.

G.8 ERC REPORT 15, Compatibility Study Between Radar and RLANS Operating at Frequencies Around 5.5 GHz, October 1992.

G.9 Repository of Industrial Security Incidents (RISI) database. https://www.risidata.com/Database [Accessed July 7, 2022.]

G.10 Richard Supler, John Livingston, Connor Armstrong and Omran Samadi, Introduction to the Electromagnetic Pulse Issue in the Nuclear Power Industry, NPIC&HMIT 2021, June 14–17, 2021.

G.11 MIL-STD-464D, Electromagnetic Environmental Effects Requirements For Systems, Department of Defense, Washington, D.C., 24 December 2020.

G.12 The Age, "The cyberspace invaders," June 22, 2003. https://www.theage.com.au/national/the-cyberspace-invaders-20030622-gdvx44.html

G.13 M. Abrams and J. Weiss, *Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia*, August 2008. http://www.mitre.org/publications/technical-papers/malicious-control-system-cyber-security-attack-case-study-maroochy-water-services-australia

G.14 Slay, J. and Miller, M., 2008, "Critical Infrastructure Protection," *IFIP International Federation for Information Processing, Volume 253*, eds. E. Goetz and S. Shenoi; (Boston: Springer), pp. 73–82.

# APPENDIX H. USES OF WIRELESS TECHNOLOGY

## H.1 USES OF WIRELESS IN NPPs

The use of any wireless applications in NPPs is strictly regulated. Requirements and restrictions vary, depending on the country. In the United States, wireless technologies are currently not used for CDAs associated with SR/ITS functions. Because the likelihood of an individual packet being blocked or corrupted in a transmission is high [H.1], the use of wireless technologies may continue to be limited to nonsafety applications for the foreseeable future. Nevertheless, with increased use, the further exploration of its potential use in SR/ITS related applications is likely.

However, there is significant interest within the nuclear industry to implement wireless technology in applications that can enhance plant safety or reduce maintenance costs. Standards that provide guidance on the use and types of wireless communication technologies currently available (Wi-Fi, Bluetooth, 5G, Zigbee, etc.) are available from IEEE, ISA, WirelessHART, and IEC. However, wireless technology continues to change very rapidly, which can lead to hesitation to procure equipment that may rapidly become obsolete. In addition, because of the long lead time to develop an approved standard, it is not surprising that the standards and guidance from standards development organizations are slow to release new reports, except for IEC and ISA.

The strategy for maintaining the component/system as is or modifying/replacing it is directly correlated to the licensee's aversion to risk [H.2], which is also applicable to the use of wireless technology:

- Conservative decision makers exhibit a risk-averse behavior that has a low cost to implement and would have very low project risks, but this stance maintains a very high commitment to long-term maintenance and does not provide any productivity or reliability improvements.

- Less conservative decision makers may use an aggressive replacement/upgrade strategy with the potential to increase productivity and reliability and decrease long-term maintenance while requiring a high initial investment. This approach is more likely technology-driven, in that they want the current components/systems.

- Neutral decision makers exhibit a risk-neutral behavior and would generally make small, incremental changes. A neutral strategy would identify tactical upgrades with moderate project risks and high long-term maintenance needs, low-to-moderate productivity and reliability improvements, and low-to-moderate initial investment.

Worldwide, NPPs have taken advantage of wireless technologies in several ways in nonsafety-related applications that include [H.3]:

- Voice over internet protocol (VoIP[24]) phones for voice communications throughout the plant.

- The use of laptops or personal digital assistants to upload data to the plant network, general network access and data communications.

[24] VoIP is an internet phone service that is delivered over the web. VoIP uses packet-switched protocols, and if there is a VoIP compatible network such as a LAN, the packets can be transmitted anywhere. When others receive the digital packet, it reconverts to analog so that others can hear the caller's voice.

- Condition monitoring such as wireless vibration sensors for traditional condition monitoring of rotating equipment and facilities monitoring.

- In-service inspections (such as containment integrated leak rate tests) that use many temporarily installed sensors to gather data.

- Wireless cameras for physical security purposes, analogue gauge readings or personnel monitoring, which has been shown to be helpful in reducing operator workload.

- Wireless personnel dosimetry.

- Wireless controls for crane operation.

- System performance monitoring.

Sample wireless technologies in use worldwide for NPPs include [H.4, H.5]:

- Cognitive radio systems.[25]

- WSN trials in Comanche Peak Nuclear Power Plant and Arkansas Nuclear One.

- Wireless radiation monitoring.

- Seismic monitoring systems at NPPs.

- UWB transmission pilot at the MIT research reactor.

- Pilot for an NPP wireless ERS.

- WSN for temperature and humidity monitoring at Sadhana Loop, India.

- EPRI project on distributed antenna systems at Catawba.

- IAEA coordinated research project on application of wireless technologies in NPP I&C systems.

- Emerging ICON project for the design of a wireless nuclear control system in the United Kingdom.

- Nuclear decommission using wireless applications in Sellafield and Magnox in the United Kingdom.

- Use of robotic techniques in NPPs that can reduce exposures to workers by having the operator control the device from a safe distance, which makes them ideal for use in hazardous areas. Robots can also be used in the decommissioning phase.

[25] A cognitive radio system includes a radio that is programmed to handle unanticipated radio channels and events. Cognitive radios can sense RF spectrum, geographical surroundings, and user 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.

The eight applications of wireless technology in NPPs that were identified [H.6] are on the risk averse end of the tolerance spectrum:

- Voice communications.
- Data communications through laptops and personal digital assistants (PDAs).
- Wireless dosimetry.
- Equipment monitoring.
- Equipment condition monitoring.
- Process monitoring.
- Camera monitoring.
- Heavy equipment operation.

Examples from both ends of the spectrum include Comanche Peak Nuclear Power Plant that maintains 100% wireless coverage across the entire facility for communications [H.6], whereas Diablo Canyon has limited wireless technology installed in the facility, and the installation of a wireless network is not currently planned for the areas in the power block (i.e., the turbine building, auxiliary building, control room, and any other equipment necessary for plant operation) [H.6].

The concerns and limitations regarding the use of wireless technologies in SR/ITS systems in other countries across the world is similar to that seen in the United States. In Finland "No solutions based on wireless data transfer may be used in the safety functions" [H.7]. Additionally, applications must evaluate EMI caused by wireless transmissions (e.g., human action, telephone systems, repair, maintenance and measuring devices). In Finland's nonsafety systems, the Radiation and Nuclear Safety Authority of Finland (STUK) requires that "A device or a system comprising wireless control shall be designed such that the control action is possible only through a connection signal designed for the control and that the system or the device goes quickly enough in a state preferable from the safety point of view in case the control signal breaks off" [H.8]. The same approach used in Finland has been also adopted in Sweden. The Nordic NPPs (Olkiluoto, Loviisa, Hanhikivi, Ringhals, Oskarshamn, and Forsmark) do not currently use wireless technologies in their operations [H.5].

NPPs that have implemented wireless technology use it for multiple applications, and each application may use a different technology. For example, the wireless technology used for voice communication is not the same as that used for equipment monitoring. Each of these applications is reviewed below.

At the Comanche Peak Nuclear Power Plant [H.5], an IEEE 802.11b wireless network infrastructure incorporates wireless sensors for equipment condition monitoring and diagnostics. Presently, approximately 100 wireless sensor nodes have been installed in the plant to collect information for monitoring purposes on nonsafety-related system equipment.

ANO has one of the more extensive wireless networks and is using wireless for both voice and data communications [H.6]. The site has ~145 access points outside containment allowing site-wide access to the wireless network. Omnidirectional antennas are used primarily for the network coverage inside the building. ANO also has wireless vibration sensors that are used to monitor the condition of the containment cooling fans. The system is designed to acquire and transmit vibration data once a day. Previously, the data were collected manually during refueling and maintenance outages.

Diablo Canyon has limited wireless technology installed in the facility [H.6]. Since the RF interference associated with the use of a walkie-talkie cause the plant to trip, the plant has been hesitant to implement wireless technology and has restrictions preventing the use of most wireless systems within the power block. However, some uses of wireless technologies exist at the plant such as wireless dosimetry during plant outages. There is also a wireless paging system. Walkie-talkies are used by security personnel outside known exclusion zones. Lastly, there is a Wi-Fi wireless network in on-site building excluded from the power block.

The Farley NPP uses wireless technology in many areas of the plant [H.6]. It uses two-way radios throughout the plant, and based on EMI/RFI site survey data, there are exclusion zones for the use of those devices. Farley also uses a low-power wireless digital paging system throughout the plant as well as a wireless phone system using VoIP technology. Farley also uses wireless web cameras for security and operations monitoring.

SONGS has installed wireless devices for equipment condition monitoring [H.6]. Because clogged intakes to the circulation control motors on the secondary side of the plant were preventing sufficient cooling and subsequently overheating and damaging the motors, a Wi-Fi 802.11b network was installed to monitor the motors for prognostic purposes. According to SONGS, maintenance can be scheduled and can be performed in 1.5 days while at 80% power. If a motor fails unexpectedly and needs emergency repairs, replacement take 3.5-4 days. This represents a 60% increase in labor savings.

STP has installed an 802.11 wireless network with ~125 access points in all the administrative buildings with more than 300 access points to be installed [H.6]. This expansion is expected to include the power block as well. The applications will most likely be used for voice and data communications and can be extended to temporarily include a wireless network inside containment during outages.

The INPP in Lithuania has a seismic early warning system that uses wireless seismometers to transmit seismic vibration data to the plant [H.5]. This allows plant operators to recognize and mitigate the potential effects of an earthquake.

An UWB system was piloted at the MIT research reactor. UWB temperature transmitters were placed in various challenging locations inside the equipment room [H.5]. The receiver was placed inside the control room behind a closed door. The signal had to pass through a concrete wall (1.2 m thick), a heavy metallic channel in the equipment room, and a closed metallic door. The tests showed that UWB signals successfully propagated through heavy metallic and concrete structures.

The Canadian Nuclear Safety Commission (CNSC) [H.9] anticipates numerous wireless technology advances as advanced reactors seek licensing approvals. It is expected that more control will be given to automated systems, and there will be extensive use of remote monitoring. For example, wireless systems could provide remote voltage and current monitoring of batteries. In addition, extensive use of near-field communication (NFC) / radiofrequency identification (RFID) relays will allow for short range in-field monitoring of important component parameters (e.g., voltage, frequency, vibration, radiation, flow) by plant personnel. As NFC is a method of wireless data transfer operating at the 13.56 MHz frequency range that allows smartphones, laptops, tablets, and other devices to share data when in very close proximity, this is an effective and relatively easy to implement method that will provide valuable data for plant monitoring.

### H.1.1 Audio Communications

Because of the increased demand and availability for mobile wireless communications, the use of voice communications is no longer dedicated to wired connections. Instead, voice conversation can be through walkie-talkies, cell phones, or a wireless network. Services can be fixed or mobile.

Wireless communications can affect plant systems. In 1983, the use of portable radio transmitters (commonly referred to as walkie-talkies) caused system malfunctions and spurious actuations. NRC IN 83-83 [H.10] states that the solid-state devices were responsible for all the known cases of RFI generated by portable radio transmitters.

The use of portable radio transmitters or walkie-talkies has been common at many operating NPPs, and for the most part, NPPs have shown themselves to be largely, although not entirely, invulnerable to the RFI that these radios generate. When this type of RFI has been demonstrated to be a problem, NPPs have successfully addressed it by prohibiting their use in certain areas. Nevertheless, the vulnerability of safety and nonsafety systems to inadvertent actuation or malfunction poses a significant threat to safe plant operation if measures to prevent use of radio transmitters fail during emergency situations.

Emergency situations in which posted restrictions on the use of portable radio transmitters are likely to break down include those instances when individuals other than plant-operating personnel may be present or when operating personnel are performing nonroutine functions. Such situations include but are not limited to firefighting, bomb searches, and local operation of equipment normally performed from the control room.

Plans for dealing with such emergency situations require consideration of the possibility for RFI if the NPP has a demonstrated or implied vulnerability. When solid state equipment is retrofitted into an existing plant, the potential for RFI vulnerability suggests that the licensee should evaluate the impact on plant operation and safety.

Cellular technologies currently in use are 2G (second generation), 3G (third generation), 4G (fourth generation), and 5G (fifth generation). With the availability of cellphones, utilities may rely on them increasingly to transmit voice communications and data.[26] However, the growing reliance on cellphones for data should be factored into an overall wireless strategy. Most wireless public service providers cannot be relied upon during general emergencies because it is very likely that their air interfaces will be congested [H.11].

Wi-Fi, Bluetooth, Z-Wave, and ZigBee are technologies that use radio waves to transmit information across a network to a wireless access point or hub that can provide a connection to the internet. Voice communication is primarily in the lower portion of the radio spectrum (i.e., any frequency below 2.4 GHz).

The wireless network at Arkansas Nuclear One (ANO) includes all business buildings, the entire site inside the fence, and the power block. The ANO wireless network for voice communications uses VoIP instead of walkie-talkie systems [H.6]. The wireless network can be temporarily expanded to include inside containment if needed.

[26] Most 2G networks based on GSM use 850–1800 MHz or 900–1900 MHz bands. 3G networks use bands between 850–1900 MHz or 900–2100 MHz. Some carriers have already sunsetted their 2G and 3G networks. The main reason for network shutdowns is that the carriers have limited spectrum available for expansion. 4G LTE will be available for at least a decade to come and will co-exist with 5G networks.

Farley Nuclear Plant uses wireless two-way radios throughout the plant, as well as a low-power digital paging system. The wireless phone system uses VoIP technology. The VoIP phones use WPA for authentication and encryption security [H.6].

The South Texas Project (STP) uses radios and pagers and allows the use of cell phones and BlackBerry devices onsite. However, there is a lack of coverage for personal cell phone and BlackBerry devices [H.6]. However, the Bluetooth standard IEEE 802.15.1-2005 became inactive 7-5-2018.

Comanche Peak Nuclear Power Plant maintains 100% wireless coverage across the entire facility for communications [H.12]. The wireless network for voice communications at Comanche Peak is based on the 802.11b standard and is used in conjunction with VoIP phones that allow plant personnel to be contacted throughout the entire plant [H.6].

Diablo Canyon has limited wireless technology installed in the facility [H.6]. The plant currently has restrictions preventing the use of most wireless systems within the power block. The power block includes the turbine building, the auxiliary building, the control room, and any other equipment necessary for plant operation. The installation of a wireless network is not currently planned for this area. Additionally, cell phones—even when in the off position—are not allowed in the power block.

The Forsmark NPPs in Sweden have a limited use of wireless technology [H.13]. Current uses include communication using DECT and Tetra, wireless (radio) control for cranes/traverse (refueling floors, turbine hall, etc.), card readers for access to systems (RFID), including access to refueling floors, some use in the physical protection system, and internet access by Wi-Fi in administration areas. There are no plans for additional wireless applications at Forsmark at present. Possible uses in the future could include (1) using the existing wired infrastructure to create a temporary wireless access point in a room to allow the use of wireless equipment such as wireless cameras, (2) collecting data on the status of equipment through wireless temporary measurements during an outage , (3) taking measurements that require flexibility in location, duration, or other factors, or (4) using radiation measurement systems to take measurements on refueling floors during outages or during fuel handling and teledosimetry for certain tasks. Forsmark identified the following challenges for expanding the use of wireless technology: cybersecurity issues; EMC concerns, mostly regarding existing equipment that was installed prior to most EMC standards; less-than-optimal building layouts for wireless, thick, concrete walls; large number of rooms; minimal equipment in each room; and modern equipment that is sensitive to radiation.

### H.1.2 Data Transfer and Communications

Wireless networks can be used to provide data to personal computers (PCs), PDAs, or a network, or they can be used to increase access to information for workers in the field. Examples of efficiency gains include the use of tablet-based work orders and calibration procedures, wireless access to plant engineering documentation, voice communication anywhere in the plant, temporary or permanent installation of wireless cameras, and equipment condition monitoring using wireless sensors. These efficiency gains can minimize paperwork and work hours.

Future applications of wireless systems at Public Service Enterprise Group (PSEG) (Salem and Hope Creek generating stations) include providing mobile workers in the field with a tablet PC [H.14].

The wireless network at ANO is used in containment with the radiation survey system. The system allows the rad technicians to wirelessly update radiation readings in real time using a tablet computer or PC [H.6].

The wireless network at the Comanche Peak Nuclear Power Plant can be accessed by laptop computers and wirelessly enabled devices to view and upload data in real time [H.6].

### H.1.3 Wireless Dosimetry

The use of wireless dosimeters can help control radiological exposure by tracking personnel and exposure at key locations (such as the reactor, fuel, turbine, and control buildings) more frequently than has typically been possible in the past. Besides being more flexible than a cabled system, a wireless radiation monitoring system can also be easier to expand and maintain. Wireless dosimeter monitoring inside the plant area could provide additional security and an early warning of possible problems. Combined with access control systems, wireless dosimeters it could also be used to ensure that all persons in areas where dosimeters are required are carrying them [H.5].

Wireless dosimeter devices use hands-free technology (pass-by data exchange) for communication and dose accountability, providing a dose tracking tool to help maintain exposure to workers, the public and the environment as low as reasonably achievable (ALARA). In addition, portable and fixed instrumentation offers real-time personnel radiological monitoring from control stations and central access points, as well as equipment, component, area, and boundary monitoring. This provides live, on-line radiological data for work planning (ALARA, maintenance), pre-job briefs, and general viewing from any network-connected computer [H.15].

As part of its wireless plant applications [H.14], Exelon plans to install dose rate monitoring, tracking, and automated survey map updates.

South Texas Project (STP) uses wireless dosimeters for personnel and area/process radiation monitoring. These radiation monitoring devices use different radio transmitters/antennae from the Wi-Fi 802.11 backbone at STP [H.6].

The Salem and Hope Creek generating stations at the PSEG will include wireless dosimetry in the upgrades.

Although the wireless network is not installed in the power block (i.e., turbine building, auxiliary building, control room, and any other equipment necessary for plant operation), wireless dosimetry is used in a limited fashion during plant outages [H.6].

Other NPPs outside the United States are also using wireless networks for radiation monitoring. The Kalpakkam nuclear complex in India is deploying a WSN for radiation monitoring. The system comprises 17 sensor nodes, 29 router nodes, and 1 base station. Zigbee has been reported to be used as for the wireless communication [H.5].

In 2003, the PAKS NPP in Hungary made use of a portable standalone radiation monitoring system using a gamma dose rate detector equipped with a solar cell, a rechargeable battery, and a radio modem for wireless communication [H.5].

Olkiluoto in Finland uses wireless radiation measurement in the plant perimeter [H.5].

### H.1.4 Equipment and Process Monitoring Conditions

The benefits of wireless monitoring have resulted in real-time data regarding plant equipment and conditions while eliminating the need for hands-on data collection.

Advantages of wireless monitoring include fast transmission speeds although simultaneous access to the RF channel from numerous sources could result in slower data transmission; inexpensive installation in existing locations, flexible connections; and handshaking to ensure accurate data transmission, even if data must be resent. Wireless monitoring is ideal for use in remote or hazardous locations, and multiple protocols enable a wide range of solutions to allow usage in widespread or congested environments. Disadvantages include it is susceptibility to interference and its requirement for strong security.

EPRI has launched numerous efforts over the last few years to examine the potential of wireless sensors for use in equipment condition monitoring and other applications in fossil plants and nuclear power reactors [H.16].

Equipment condition monitoring in industrial processes depends on measurement of vibration, acoustics, temperature, pressure, strain, humidity, and other parameters. For rotating equipment, the first indication of a problem is a change in the equipment's vibration amplitudes and/or frequencies. These changes can sometimes be observed months before a failure occurs [H.12]. As the equipment continues to degrade, acoustic or ultrasonic noise develops within weeks of the failure. Then the equipment begins to overheat, producing a rise in the temperature within days of the failure. Finally, smoke or even fire can develop because of increased friction within minutes of equipment failure. Often, no sensors are installed on or near the equipment to provide these measurements for condition monitoring applications. Of course, new sensors can be installed on or near the equipment or the process, but the wiring costs are prohibitive, especially in nuclear safety applications. Wireless sensors provide a cost-effective alternative and are being used more and more for equipment and process condition monitoring, as well as various other industrial applications.

The wireless DAS will include the ability to acquire, qualify, analyze, store, and display data from wireless sensors. The prototype system will also be flexible and will allow for information from existing wired sensors available through the plant computer to be integrated into the analysis and display of wireless sensor data.

The process for installing the wireless system will be based on satisfying the regulatory requirements relating to wireless sensors in NPPs [H.15] and demonstrating to the host site that all considerations for successful implementation of the wireless system have been fulfilled. This includes satisfying cybersecurity requirements, examining the effects of EMI/RFI, providing plant design modification documentation, and testing for coverage and reliability of the wireless network.

Although the information may be the same as for hard-wired applications, the acquisition, qualification, storage, and display of data from wireless equipment differs in the following areas:

- A description of the design modifications necessary for a wireless system installation.
- A coexistence assessment of the wireless network with existing plant systems.
- A description of a module to interface with the plant computer to send and retrieve sensor data.
- Example algorithms and software packages used for sensor data qualification and analysis.

Each manufacturer has its own proprietary software that receives the wireless data from its sensors and provides the data to the user. This software is embedded in a receiver module that is often referred to as a "gateway." The gateway contains software and hardware to receive the data from wireless sensors and to send them out to the user. The transmission from the gateway to the user is usually accomplished through hard wires (i.e., a local area network). What is critically missing in this scenario is a general means to interface with the gateway to extract and store the wireless sensor data for subsequent plotting, trending, monitoring, or analysis.

The wireless sensor data must be available to the plant computer. Once the data are stored in the plant computer, they can be readily accessed, qualified, and analyzed based on the application at hand (e.g., condition monitoring, diagnostics and prognostics, asset management, security monitoring, redundant measurements, backup for wired sensors, etc.). For qualification, the data are stripped of artifacts from the wireless communication link, and any gaps in the data caused by sensor communication or receiver errors are removed. Additional data qualification measures such as checking the data for Gaussian distribution and normality will be integrated with wireless data qualification routines. Once qualified, the data may be stored for subsequent analysis or displayed on a computer screen.

The following questions must be answered regarding the interaction of wireless sensors with a typical nuclear reactor environment [H.12]:

1. What is the impact of wireless transmission on the signal quality of a traditional wired sensor?

2. What is the impact of multiple wireless sensors on a single wireless network?

3. How does the inclusion of wireless sensor data affect the throughput of a wired data network?

4. What are the effects of EMI/RFI from industrial equipment on wireless sensors, and vice versa?

5. How does the harsh industrial radio-frequency industrial environment affect the coverage and signal quality of a wireless network?

6. What sampling rates can be achieved through wireless transmission?

7. What obstacles are encountered when a traditional wired sensor is instrumented with a wireless transmitter?

8. What are typical failure modes of equipment that can be identified using wireless sensors, and in which types of measurement does the failure present itself first (process, environmental, vibration)?

Through the implementation of a plantwide 802.11b wireless infrastructure, Comanche Peak has been able to incorporate numerous wireless technologies, including data communications, camera monitoring, and equipment condition monitoring. About one hundred wireless sensor nodes have been installed in the plant to collect information to monitor varieties of nonsafety-related system equipment [H.5]. After the initial installation of the 802.11 network, Comanche Peak added about 60 vibration and temperature sensors on critical pumps, motors, and structures in Unit 2. Besides monitoring vibration, devices will also monitor current partial discharge, motor speed, and other key variables. Before the wireless sensors were implemented, data were manually collected on targeted equipment once per month. Data are now being sent wirelessly at least once per day. Direct benefits are labor savings from manual data collection and manual database entry [H.6]. Comanche Peak plans to expand the use of this technology on safety-related equipment [H.6]. This would be the first implementation of wireless technology on safety-related equipment in the nuclear industry.

PSEG has indicated that the wireless capabilities to be installed will help with equipment monitoring to support its reliability analyses [H.14].

At San Onofre Nuclear Generating Station (SONGS), wireless devices were installed for equipment condition monitoring to solve a problem of clogged intakes to the circulation control motors on the secondary side of the plant [H.6]. The system was initially installed at Unit 3 and then was installed at Unit 2. Since the Wi-Fi 802.11b was installed in 2003, not a single pump has failed during plant operations covered in the EPRI report (circa 2003–2009). Because of this, the plant receives indications of wear-out, so plans can be made to replace these pumps during an outage or during low-power operations. This significantly reduces the cost of maintenance for these pumps. Subsequently, it was concluded that the Wi-Fi system was somewhat complicated and expensive for this specific application, which only requires low-frequency data. There were plans to convert to a Zigbee-like system, but it is unknown if this was done before the plant was permanently shut down in 2013.

To collect data on the high-pressure turbine inlet pressure for Unit 2, SONGS planned to use the WirelessHART communication protocol based on 802.15.4, which transmits at a lower power than the 802.11 Wi-Fi signal. With the use of these wireless devices, SONGS estimated a 75% cost savings compared to traditional methodologies, with improved accuracy provided by the technology. Before successful completion of the pressure transmitters, SONGS identified a possible 500 additional locations where wireless pressure reading would have been of value. The network was to be a mesh network [H.6], but because SONGS was permanently shut down in 2013, it is unknown if this was implemented.

The Limerick Generating Station, a two-unit plant owned by Exelon, has had two wireless applications: one to monitor a large overhead crane, and the other to monitor turbine exhaust fans [H.17]. The crane application involved vibration monitoring of the wheel bearings of a 125-ton crane used to pull reactor vessel heads, floor plugs, and reactor components on the fuel floor during refueling outages. The crane's availability during these outages is critical. Limerick had experienced problems with an overhead crane on the fuel floor. After a seized wheel bearing on the refuel floor overhead crane delayed a refueling outage for 24 hours, the plant's maintenance team sought a way to monitor the crane's condition to ensure its reliability. The team found that a conventional vibration monitoring setup would require at least 16 vibration channels, a speed sensor, a recorder, cabling, low-frequency sensors, man lifts, harnesses, fall protection, and other equipment. All of the equipment would have to be taken into and out of the contaminated area, strung over a large area, and attended while the crane was moving heavy loads. Instead, Limerick chose to deploy a wireless vibration probe [H.18]. The system uses battery-powered wireless sensors mechanically mounted to each piece of equipment. These sensors gather vibration and temperature data and transmit that information to a transceiver using a 2.4 GHz DSSS signal. Funding was received, and the equipment was ordered from CSI. Twenty sensors and one battery-powered transceiver were ordered at a cost of approximately $20,000. In this system, the signal is downloaded to a handheld data collector, which in turn downloads to a laptop for display.

Another application of wireless technology at the Limerick plant involved fans used to exhaust turbine enclosures. The fans were experiencing maintenance problems and were inaccessible to technicians while the plant was online [H.19]. Installation of vibration and temperature sensors on the fan motors has resulted in reductions in (1) the time and costs of document control and tracking, (2) data conversion/transcription, and (3) error checking.

Exelon plans to expand its wireless network to include [H.14]

- DAS monitoring devices on/near SR/ITS for equipment health monitoring.
- DAS monitoring devices on/near SR/ITS components for equipment performance data collection without local observation.
- Use of DAS throughout the plant using RF through an installed plant radio antenna system.

ANO is using wireless vibration sensors to monitor the condition of the containment cooling fans [H.5]. STP has installed an 802.11 wireless backbone with access points in all administrative buildings, the turbine building, the diesel building, the fuel handling buildings, the electrical auxiliary building, and the reactor building [H.6].

### H.1.5 Spent Fuel Pool

On March 12, 2012, the NRC issued Order EA-12-051 [H.20] that requires, in part, that all operating reactor sites have a reliable means of remotely monitoring wide-range SFP levels to support effective prioritization of event mitigation and recovery actions in the event of a beyond-design-basis (BDB) external event.

On August 29, 2012, the NRC issued JLD-ISG-2012-03 [H.21] to describe methods acceptable to the NRC staff for complying with Order EA-12-051. The ISG endorses, with exceptions and clarifications, the methods described in Nuclear Energy Institute (NEI) 12-02, Revision 1, [H.22], which states that

> *Wireless and other advanced technologies may be used provided that an evaluation is performed to address their interaction with other plant systems, failure modes, and impact on plant cyber security controls. The use of such wireless technology must be evaluated for any possible adverse impact it may have on other plant equipment likely to be in use at the same time as the wireless SFP instrumentation is functioning. Licensees should also consider the ability of a wireless communication link to perform in the environment (e.g., high humidity, radiation) in which it may be called upon to function. Wireless technologies must meet the same requirements as wired technologies as specified in this guidance document [Section 3.1 in NEI 12-02].*

After the March 11, 2011, earthquake and resulting tsunami at Fukushima Daiichi, the NRC determined that several near-term actions were needed at US commercial NPPs. Documentation of the NRC staff's efforts is contained in SECY-11-0124, "Recommended Actions To Be Taken Without Delay From the Near-Term Task Force Report," dated September 9, 2011, and SECY-11-0137, "Prioritization of Recommended Actions To Be Taken in Response to Fukushima Lessons Learned," dated October 3, 2011.

EA-12-051, *Order Modifying Licenses with Regard to Reliable Spent Fuel Pool Instrumentation (Effective Immediately)*, notes that SFP level instrumentation at US NPPs is only capable of monitoring normal and slightly off-normal conditions because the instrumentation typically covers a very narrow range. The NRC staff determined that an external BDB event could challenge the ability of existing SFP instrumentation to provide emergency responders with reliable information on the condition of SFPs. Reliable and available indication is essential to ensure plant personnel can effectively prioritize emergency actions. Therefore, the NRC has determined that all power reactor licensees and construction permit holders must have a reliable means of remotely monitoring wide-range SFP levels to support effective prioritization of event mitigation and recovery actions in the event of a BDB external event.

> *All licensees ... shall have a reliable indication of the water level in associated spent fuel storage pools capable of supporting identification of the following pool water level conditions by trained personnel: (1) level that is adequate to support operation of the normal fuel pool cooling system, (2) level that is adequate to provide substantial radiation shielding for a person standing on the spent fuel pool operating deck, and (3) level where fuel remains covered and actions to implement make-up water addition should no longer be deferred.*

RG 1.227, *Wide-Range Spent Fuel Pool Level Instrumentation*, replaced JLD-ISG-2012-03 and provides guidance for demonstrating compliance with NRC regulations to provide a reliable means to remotely monitor wide-range SFP levels to support implementation of event mitigation and recovery actions. RG 1.227 endorses, with exceptions and clarifications, the methods and procedures promulgated by the NEI in NEI 12-02.

JLD-ISG-2012-03, *Interim Staff Guidance (ISG), Japan Lessons-Learned Project Directorate* ***(JLD),*** *Compliance with Order* ***EA-2012-051***, *Reliable Spent Fuel Pool Instrumentation*, provided interim staff guidance to describe methods acceptable to the NRC staff for complying with Order EA-12-051. The ISG stated that the methodologies and guidance provided in NEI 12-02, Revision 1, subject to certain clarifications and exceptions, are an acceptable means of meeting the requirements of Order EA-12-051.

NEI 12-02, *Industry Guidance for Compliance with NRC Order EA-12-051, To Modify Licenses with Regard to Reliable Spent Fuel Pool Instrumentation*, provides guidance on implementing NRC Order EA-12-051, directing licensees to provide a reliable means of remotely monitoring wide-range SFP levels. The guidance notes that “wireless and other advanced technologies may be used provided that an evaluation is performed to address their interaction with other plant systems, failure modes, and impact on plant cybersecurity controls. The use of such wireless technology must be evaluated for any possible adverse impact it may have on other plant equipment likely to be in use at the same time as the wireless SFP instrumentation is functioning.” Implementation of a wireless monitoring system must consider the operating environment. The guidance also notes that any wireless technologies that might be used in either the permanent or backup water level instrument channels are not CDAs as defined in NEI 08-09, *Cyber Security Plan for Nuclear Power Reactors*.

Examples of the implementation of wireless monitoring of the water level in the SFP, Palo Verde is using the 900 MHz, industry, scientific, and medical (ISM) band, from 902 to 928 MHz, to meet NRC Order EA-12-051. The frequency hopping spread-spectrum (FHSS) technology facilitates system operation without interference with 900 MHz communication equipment or other plant systems. No other plant systems use the 900 MHz ISM band. The FHSS technology allows for multiple wireless channels to be operating at the same time without interference. The wireless components will be located in the auxiliary building (transmitters) and in the main control room and operations support center (OSC) (receivers) and will be capable of operating in the respective environments during a BDB event resulting from loss of SFP cooling.

The wireless technology used for the primary and backup SFP level measurements at Callaway also uses the 900 MHz SM band from 902 MHz to 928 MHz [H.23]. The wireless system incorporates frequency hopping spread-spectrum (FHSS) techniques, with the pre-determined hopping pattern controlled by hardware "keys" plugged into the wireless transmitter and receiver modules. The wireless transmitter is limited to 1 watt of power, and antenna gain is 7 dbi [decibels-isotropic]. Implementation of the wireless signal provides for up to 256-bit, advanced encryption standard (AES) encryption. An individual, single-frequency transmission can be dropped without disruption or loss of the measurement signal. FHSS technology facilitates system operation without interference with 900 MHz communication equipment or other plant systems. The FHSS technology allows for multiple wireless channels to be operating at the same time without interference. The wireless components will be located in the Auxiliary Building and will be capable of operating in the environment during a BDB event resulting from loss of SFP cooling. The wireless implementation meets the same requirements established for wired implementation in NEI 12-02. Battery capacity for each of the SFP level measurement channels is sufficient to provide continuous operation for 72 hours.

Similarly, the wireless technology at Palo Verde will also use the 900 MHz, ISM band from 902 MHz to 928 MHz [H.224]. In its letter, Palo Verde stated that the “Implementation of the wireless signal provides for up to 256-bit encryption. An individual, single-frequency transmission can be dropped without disruption or loss of the measurement signal. FHSS [frequency hopping spread-spectrum] technology facilitates system operation without interference with 900 MHz communication equipment or other plant systems. No other plant systems use the 900 MHz ISM band. The FHSS technology allows for multiple wireless channels to be operating at the same time without interference.

The wireless components will be located in the auxiliary building (transmitters) and in the main control room and OSC (receivers) and will be capable of operating in the respective environments during a BDB event resulting from loss of SFP cooling. The wireless implementation meets the same requirements established for wired implementation in NEI 12-02, Section 3.1.

In addition, the licensee stated that "The [spent fuel pool instrumentation system] is a stand-alone system with no connection into other parts of the plant instrumentation and control systems and it is not a critical digital asset as defined in NEI 08-09, Cyber Security Plan for Nuclear Power Reactors. Failure of a wireless component will affect only the signal for which it is used. The SFPIS does not provide a path for entry of malicious code into any part of the plant instrumentation and control systems and has no impact on plant cyber security controls."

The use of equipment and process monitoring is not limited to operations. Wireless instruments were installed in the Sellafield and Magnox plants in the United Kingdom to aid monitoring during plant closure and decommissioning [H.5]. A seismic early warning system was installed in INPP in Lithuania that transmits the measured values from the field seismic monitoring system (SMS) seismometers to the power plant by radio communication using ultrahigh frequency (UHF) band [H.5].

Wireless sensors were installed at the Ontario Power Generation (OPG) Pickering Nuclear Generating Station (PNGS) to increase online monitoring capabilities to enable condition-based monitoring [H.26]. The wireless network uses Bluetooth 5.0 low-energy and 900 MHz wireless sensors. Wireless sensors were installed on multiple secondary side pump/motor sets and standby generator batteries. These sensors monitored vibration, humidity, temperature, and battery health parameters such as cell voltages, ambient temperature, and humidity of the battery cabinet.

### H.1.6 Monitoring Devices (Visual Communications, Cameras)

Identification and monitoring devices include still and video cameras, motion sensors, vibration sensors, heat sensors, biometric authentication or recording devices, and a variety of other devices [H.26]. They do not by themselves specifically control or limit access to a physical location or system. The design and intended use of these devices is specific to detecting, identifying, or recording physical entities, including the state of physical presence of individuals, vehicles, systems, or other identifiable physical objects.

Applications for the use of cameras include physical security, operations monitoring, monitor outages, personnel traffic, to obtain gauge readings in remote locations, to monitor fire watch patrol carts, and so on.

Cameras with wireless technology can provide remote monitoring of equipment. Portable carts containing sensors and cameras can perform some of the work of fire watches, providing continuous monitoring of certain parts of the plant, serving as a replacement for hourly visits made by personnel. Such carts are already in use in several US NPPs [H.27]. Video and cameras can also be remotely controlled, can be fixed in place or movable, and can even be infrared.

From a practical perspective, new video over WLAN products allows facility managers to place cameras in remote locations without the need to install ethernet cabling or conventional video wiring. At an NPP, for example, cameras could be used to monitor an outlying restricted area and stream video back to a command post or forward it to an internal company intranet. Vendors are also providing monitoring devices that can receive video and display it on a Wi-Fi–equipped PDA, allowing mobile resources to review the video.

An internet protocol (IP) camera can be connected directly to a transceiver to transmit video signals over a range of several miles. No special hardware, software, or adapters are required between the camera and the radio. Instead of being carried over the internet, signals are transmitted over the radio channel to a second IP/ethernet-ready device where the images can be displayed on a connected PC. The setup of this type of architecture can include two or more remote cameras that transmit images to a single access point [H.11]. Digital video recorders (DVRs) allow users to monitor live cameras, review stored video data, capture images and video clips, and connect remotely via ethernet or other standard networking connections and protocols [H.28].

At an NPP, a WLAN with a camera can be used to monitor radiation protection efforts when employees enter a radiation area. The WLAN with wireless cameras can help reduce exposure time, and operators can also log and monitor the equipment.

Comanche Peak uses the wireless camera feeds to view areas during outages, to monitor personnel traffic, and to obtain analog gauge readings in remote locations. Gauges are monitored by sending a snapshot of video data rather than streaming a live video feed [H.6].

Farley Nuclear Plant uses wireless web cameras for security and operations monitoring [H.6]. For example, cameras are used to monitor the water level in the circulating water canal by remotely displaying the water level against a footage mark on the canal. The camera allows a quick assessment of the water level. Another use of the wireless cameras at Farley is real-time gauge voltage reading at the switch house.

Exelon has installed camera monitoring of in-plant equipment in difficult-to-access areas and uses a fire watch patrol cart for in-plant hourly fire watch patrol [H.14].

The wireless network at ANO uses wireless cameras when performing outage work [H.6].

### H.1.7 Heavy Equipment Operation

Wireless remote controllers used for operating heavy equipment provide several advantages compared to hard-wired controllers. A wireless controller provides more freedom of movement because the device or machine can be operated without interfering with cables. Operating by wireless remote control allows the operator to move more freely, providing the best viewpoint of the work being performed, more freedom of movement without a cable, and the ability to avoid direct contact with a running machine. Operators can be positioned at a safer distance, farther away from moving parts, harmful dust, radiation, noise, vibration, or falling debris.

Although wireless controls still require maintenance, cable controls for hard-wired systems usually require more maintenance because cables tend to wear out more quickly in industrial environments. In addition, it is relatively easy to install a remote control on an existing wired control.

A wireless remote control can lead to increased efficiency because work can continue without the operator being exposed to a harsh environment such as a high radiation field. The machine takes all the risk, allowing the operator to remain in a safer location. This not only saves time by allowing continued operation, but it also increases operational safety. Furthermore, wireless control systems can include a wireless emergency button to shut down operations if needed. Incorporating remote-controlled equipment reduces reliance on manual labor, resulting in more significant labor cost savings.

Remote-controlled systems cause less fatigue to equipment than traditional manual machine operations. Vibration and noise, which also contribute to fatigue, are also eliminated or decreased by using remote-controlled equipment.

NPPs are taking advantage of remote controls for heavy equipment to operate overhead crane systems. For example, the primary pieces of equipment used in the overhead heavy load handling system (OHLHS) at the US Advanced Pressurized Water Reactor (US-APWR) are the spent fuel cask handling crane in the fuel handling area and the polar crane in the prestressed concrete containment vessel (PCCV) [H.29]. Other OHLHS equipment may include, but is not limited to, monorail-type hoists, bridge cranes, and jib cranes. The OHLHS is in fuel handling area and the PCCV of the reactor building.

The complete operating control system and the emergency control features are in the cab on the OHLHS. Additional wireless remote-control stations are also provided for OHLHS remote operations. The wireless remote-control stations include the same controls as the cab-mounted controls, including emergency, features. The individual control stations are interlocked so that only one station is operable at a time.

PSEG also uses wireless technology for crane operations [H.14].

### H.1.8 Future Uses

Numerous wireless devices are in a test or trial phase at NPPs at this writing. Successful test conclusions may lead to a push for more wireless technology to be incorporated in NPPs to create additional information paths to the operator or to other analytical devices. One example is a radiation- and temperature-tolerant wireless transmitter being developed by Westinghouse [H.30] that operates inside a fuel assembly’s top nozzle. The device is powered by radiation in the core and is capable of continuously transmitting neutron flux data during light-water reactor (LWR) plant operation. This technology would allow every fuel assembly to be instrumented, leading to an increase in operating margin. This would also have implications on the amount of power delivered from a given fuel load. Research on the technology was funded by DOE and tested at the Penn State Breazeale Reactor.

Other wireless applications under investigation by Westinghouse include [H.30]:

- An integral fuel rod real-time wireless sensor to provide real-time data such as centerline fuel temperature, fuel pellet elongation, and rod internal pressure to enhance reactor operation
- A gas void monitoring system to monitor gas voids within safety-related systems, to reduce personnel dose, and to reduce labor costs

Exelon [H.31] is investing in wireless infrastructure at its plants to provide a cost-effective method to utilize wireless sensors and innovative monitoring and predictive technologies. Data are collected through a DAS. This is intended to replace high-cost, time-based maintenance with centralized performance monitoring. The technology discussed has come to be known as digital twins of key components. The example for Exelon was the creation of a digital twin of a condensate booster pump at one of its plants. At the time the associated paper was presented, Exelon had wireless sensors in place to monitor several parameters on the pump:

- Motor/pump failure modes,
- High bearing temperature,
- High motor winding temp,

- Worn thrust bearing,
- Motor bearing lubrication,
- Worn motor opposite drive end (ODE) bearing, and
- Worn pump drive end (DE) bearing.

Exelon is also interested in adding wireless sensors to expand the centralized monitoring capability. Added sensors would allow the following parameters to be monitored:

- Worn pump internals,
- Shaft misalignment,
- Shaft imbalance,
- Power supply harmonics,
- Power cable damage,
- Rotor bars broken,
- Stator winding fault,
- Rotor eccentricity,
- Loose foundation,
- Pump cavitation, and
- Supply line power problem.

Other wireless technologies being investigated by Exelon for online monitoring include:

- Noncontact vibration sensor,
- Online thermography,
- Online oil particle counter, and
- Wireless gauge reader.

## H.2 USES OF WIRELESS TECHNOLOGY IN NON-NUCLEAR APPLICATIONS

Many wireless technologies being used in industry are diverse and allow for better communications, monitoring, and process control, as well as production automation. In fact, networks could be self-organizing so that each device acts as a data source and/or connector, improving the reliability of communication.

Either WirelesssHART or Wi-Fi standards are used to create a plant wireless network, which is usually connected with data centers for measurement data integration, analysis, and process control. To prevent wireless eavesdropping and other external attacks, all data transmissions are robustly encrypted with provision for user authentication. Wireless technologies are also used to track the location of assets and personnel to improve operational efficiency and security. Technologies used for location tracking include Wi-Fi, RFID, GPS, and UWB, depending on specific applicable needs and restrictions. For personnel communications, voice over WLAN (VoWLAN, VoIP) as well as cellular networks, are the dominating technologies.

Industrial uses of wireless technology are expanding rapidly. Wired serial links are being replaced with Bluetooth wireless links between pieces of equipment such as intelligent electronic devices (IEDs), power equipment sensors, power system equipment controllers, security monitoring sensors and actuators, and video cameras. These industrial uses are typically non-critical, or they have alternate communication backups [H.11].

A feasibility study on the use of wireless in the nuclear field identified where the technology is being used in non-nuclear industries [H.5]:

- Transportation and logistics (maritime, aviation, land),
- Healthcare,
- Industry, factories,
- Energy,
- Smart cities,
- Environment,
- Agriculture,
- Mining,
- Emergency,
- Military, and
- Office, home, and consumer.

The ISA committee, ISA100, was formed in 2005 to establish standards and related information to define procedures for implementing wireless systems in the automation and control environment with a focus on the field level [H.32]. ISA standards cover process applications (ISA100.11a), wireless backhaul backbone network (ISA100.15), trustworthy wireless (ISA100.14), people and asset tracking and identification (ISA100.21), and WirelessHART & ISA100.11a converged network applications (ISA100.12). ISA100 provides an example list of applications that use ISA100 wireless standards [H.5]:

- Machine health monitoring,
- Basic process control,

- Monitoring of well heads,
- Remote process monitoring,
- Leak detection monitoring,
- Diagnosis of field devices,
- Condition monitoring of equipment,
- Environmental monitoring,
- Tank level monitoring,
- Gas detection,
- Fuel tank gauging,
- Steam trap monitoring,
- Open loop control, and
- Stranded data capture.

The Energiforsk Nuclear Safety Related I&C Research (ENSRIC) feasibility study on the use of wireless in the nuclear field provided example cases where wireless is being used in non-nuclear industries [H.5]:

- Machine health monitoring,
- Basic process control,
- Monitoring of well heads,
- Remote process monitoring,
- Diagnosis of field devices,
- Condition monitoring of equipment,
- Environmental monitoring,
- Tank level monitoring,
- Gas detection,
- Fuel tank gauging,
- Steam trap monitoring,
- Open loop control, and

- Standard data capture.

Occasionally, unintended consequences arise with the use of wireless technologies, such as the challenge of maintaining security and privacy to communication networks. Encryption standards and network architectural design can provide for secure, reliable data transmission. Such approaches are accepted in other industries to communicate highly sensitive information.

### H.2.1 Mining Industry

The Mine Improvement and New Emergency Response (MINER) Act of 2006 amended the Federal Mine Safety and Health Act of 1977 to provide greater protections for underground coal miners and to improve emergency preparedness [H.33]. The MINER Act requires mine operators to adopt underground communications and electronic tracking systems that meet specific performance goals, and it provides updated requirements for emergency response, incident C&C, mine rescue teams, and incident notification. WSNs can also improve efficiency and safety in underground operations by providing condition monitoring of temperature, humidity, and gas detection [H.5].

One goal of the MINER Act is to provide wireless communications and location information between underground workers and surface personnel following an underground accident. The wireless technology used in mines differs from that used in industry. RF interference and protection of I&C devices is not a concern in mines. Rather, the concern is communications and knowing workers' locations. Although the technology may not directly apply for use inside an NPP, it could be useful outside the plant and at other nuclear facilities. Therefore, this the technology is discussed in detail here.

Capabilities of a wireless network in the mining industry must cover a very large area and must handle a significant amount of traffic for communications and tracking. The technology is very different than that used in NPPs, but the needs are also very different. However, large areas outside the plant, such as an independent spent fuel storage area, may benefit from the technology used in mines, tunnels, and aircraft.

### H.2.2 Communication technologies

There are primarily four different wireless communications technologies used in mines today [H.34]. The fundamental difference between them is their frequency bands of operation. Each frequency band uses a different mechanism for propagation of EM waves, and each system has the advantage of permitting the miner's radio to be untethered.

#### H.2.2.1 Leaky feeder systems

One option for underground communication is the leaky feeder system, which consists of a set of long cables connected to the transmitters. The cables run along the main corridors in the mine [H.5] (Figure H.1). The cables' accompanying signal amplifiers act both as signal conveyors and as long antennas. The main components of a leaky feeder communications system include the base station, a leaky feeder cable, amplifiers, a power supply, and a barrier. The leaky feeder system overcomes range limitations by extending the receiver antenna (the leaky feeder cable) to the general area of the handheld radio, allowing surface personnel to talk with distant underground miners.

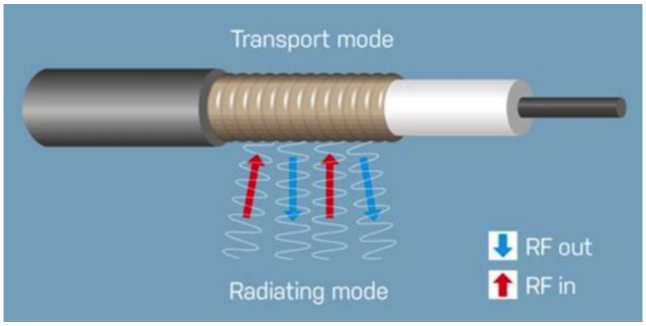


**Figure H.1. Leaky feeder cable [H.35].**

The leaky feeder cable is a specially designed coaxial cable [H.34] that "leaks" the radio signal in or out along its length, thus creating a continuous coverage area along the tunnels where the cable is strung. The coaxial cable has regular openings in the outer shield that allow RF energy to enter or leave the cable. The radio transmits the RF signal which is received by the leaky feeder cable if the radio is within range. The signal travels down the cable, radiating as it travels. If the receiving radio is within RF range of the cable, then it receives the signal and makes the connection. It can receive and transmit signals down its entire length. Leaky feeder cable is installed down the mine's entries to the mine at locations where communications are needed. The center conductor of the cable transports the RF signal, and it also carries the DC power (typically 12 volts) for the amplifiers.

Leaky feeder systems operate at the frequency conventionally used by two-way voice radio communications. Leaky feeder systems for coal mines usually operate at VHF (~150 MHz) or UHF (~450 MHz) bands. At these operating frequencies, handheld radios can establish a physical communications link through air, but the range is very limited underground.

The leaky feeder system is also used for underground mobile communication in mass transit railways and can be used to allow reception of onboard GSM and Wi-Fi signals on passenger aircraft. Leaky feeders are used in hotels, warehouses, and other industrial buildings where it is difficult to get Wi-Fi coverage using normal access points. Some installations have 50–75 meters of leaky wire connected to the antenna output of access points.

#### H.2.2.2 Node-based system

Another option for communicating in a mine is to use a robust mesh network. In this system, the node detects when a miner's radio is in range and provides an automatic connection to the network. In node-based systems, the access link is the first link, and it is made through the air from the miner's handheld radio to a node in the system [H.34]. The *access node* provides the communications service or link to the miner's radio. The *backhaul* is the communications path from the access node to the surface. The *backhaul links* are the connections between nodes—through wires, the air, or both. These systems communicate with the gateway node located at the mine operations center through the access nodes. The backhaul link connects the access node to the gateway node through wires, fiber, or other radio links.

Node-based communications systems for coal mines can use UHF, Wi-Fi and WLAN. In the underground coal mine environment, UHF radios can communicate directly with each other over significant distances up to as much as 1,000 feet. The means by which a UHF radio wave travels through the air in a coal mine is different from the way it travels through the air above ground [H.34]. In an underground mine, the tunnel opening guides the UHF waves, which bounce off the walls, floor, and roof. The tunnel acts as a guide or pipe for transporting the radio waves. This guiding effect is important, because it contributes to a loss of signal power in the RF link through the air, which determines the effective range of the communications link.

#### H.2.2.3 Medium frequency system

In medium frequency (MF) communications systems, the radio signals couple onto metallic conductors such as pipes or power lines, wire lifelines, other electrical wiring, and metal pipes, which can easily extend its working range up to kilometers without the need for a repeater or amplifier [H.34]. The conductors play the same role as that of the coaxial cable in a leaky feeder system—as conduits for the radio signal. MF radio signals travel along the conductor. Because many mine entries already have conductors, and because installing simple conductors is inexpensive, the MF communications distance easily extends over miles without the need for a repeater or amplifier.

In addition, the conductor acts as a distributed antenna, transmitting and receiving signals continuously along its length, just like a leaky feeder cable. However, MF radios and antennas are considerably larger and heavier than VHF/UHF/Wi-Fi radios, so they are usually limited to use as secondary (redundant) communications system or a system used for emergencies.

MF communications systems typically operate at around 500 KHz.

#### H.2.2.4 Through-the-earth systems

Through-the-earth (TTE) communications technology is the only technology that can transmit an EM signal between a sender and receiver with a worker underground and another on the surface without relying on a network [H.34]. Most EM waves reflect off the earth or rapidly weaken as they pass into the earth, penetrating only a few feet below the surface. However, at frequencies less than about 10 kHz, the waves can propagate more than 1,000 feet through the earth.

Several factors limit potential applications for TTE in underground coal mines: antenna design, low frequencies necessary to transmit the signal, and other noise sources. These factors are discussed below.

Antenna design has a significant impact on TTE systems. The practical antennas for TTE communications are much smaller than a wavelength limiting its efficiency. An advantage of a TTE communications link is that it is highly survivable. Given the constraints on antenna size, signal power, message size (very low bitrate), and delivery delay, TTE systems are only used in emergencies [H.5].

Because TTE communications are limited to low frequencies, the amount of information transmitted in the message is also limited, so receipt of the message may be delayed by several minutes. This limited information flow makes it very difficult to use TTE for voice communications and to include TTE communications links in a network.

Various natural and manmade noise sources exist at these low frequencies—including EM energy from power lines and EM noise naturally occurring in the atmosphere These noise sources further limit the range and information flow of a TTE communications link.

### H.2.3 Tracking Systems

The ability to know workers' locations is especially important in an emergency. Tracking systems can be manual, or they may use RFID-based or WLAN systems.

### H.2.3.1 Manual tracking systems

Tracking systems record which people are underground and where they are located. The mine operations center displays this information so that rescue workers can effectively plan operations in the event of an underground emergency. The manual tracking system relies on workers to indicate their locations and to update that information if they change locations.

Manual tracking has several limitations [H.34]. A miner may report a location as being within a working section, but a section might cover two square miles. Occasionally, a miner forgets to notify the dispatcher when changing work locations.

### H.2.3.2 Reader-based tracking systems

Reader-based tracking systems typically use RFIDs to track the locations of underground miners [H.34]. An active tag is used to extend the tag-to-reader range. Active tags have an internal battery to power the signal transmission. Each miner wears a tag that transmits a unique identifier. When the miner passes within the RF range of a reader, it interrogates the tag. The reader relays the detection information to a central location (usually the mine operations center) over wires, through fiberoptic cable, or even wirelessly. Each RFID reader has its own identification and a location associated with that identification. When a given reader interrogates a tag and then forwards the information to the operations center, personnel at the center know that the miner is within a certain distance of that reader's location.

A zone-based RFID only detects tags within its RF range or zone. Another tracking method is for the RFID readers to transmit their location information to a leaky feeder cable, which then transfers the information to the operations center.

A representative RFID reader range is about 300 feet. The RFID reader requires line of sight with the tag (i.e., an unobstructed straight-line path between the tag and reader). The resolution of a tracking system is determined by reader spacing. If greater resolution is required, then more readers will be required.

In a reverse RFID system, each miner wears an RFID reader, and the tags are in fixed, known locations [H.34]. The reader has a radio transmitter that periodically transmits the miner's location data to the mine backhaul. The backhaul could be a UHF leaky feeder system.

Using a more sophisticated approach than simply recognizing when a miner is in a certain zone can further enhance location accuracy. If a miner is within RF range of two RFID tags at the same time, then comparing the received signal strengths from the two tags can determine the miner's location within 50 feet. A comparison of the rates of change of signal strengths at the RFID tags pinpoints the miner's location and an analysis of this comparison also determines the miner's speed and direction of travel. This technique is referred to as *received signal strength indicator* (RSSI).

### H.2.3.3 Radio node-based tracking systems

Radio node-based tracking systems use the same physical components as the node-based communications systems. Radio node-based tracking uses the known locations of the fixed position nodes as reference points. Each handheld radio is assigned with a unique identifier that is associated with a specific miner. A fixed node with a known location is linked to a radio with a unique ID and is assigned to a specific miner, so the location of the miner is known [H.34]. Like RFID systems, resolution is limited to node spacing.

Applying the same concept of comparing radio signal strengths (RSSI), which is used in the reverse RFID technique, RSSI can be used to determine how far the miner's radio—and thereby the miner—is from the node. In a reverse RFID system that uses RSSI, the tags are in fixed, known locations, and the miner wears a receiver that detects and measures the signals radiated by the tags. Because a node-based UHF communications system has all the necessary components to implement the RSSI technique, it does not require RFID tags. In a node-based system, the access node and/or the miner's radio makes the signal strength measurements; hence, the node-based system provides both communications and tracking in a single system.

### H.2.4 Transport

Wireless technologies are widely used in the transportation sectors (i.e., maritime, aviation, and land transport) to improve the efficiency and safety. Each sector implements the type of technology that supports their needs. Wireless networks for the transportation sectors must cover a very large area and must handle a significant amount of traffic. The wireless networks may use the same technology used at NPPs (e.g., WSN, Bluetooth, Wi-Fi, Zigbee), or they may use satellite communication systems because of the distances involved.

#### H.2.4.1 Maritime

A very important aspect of harbor management is the real-time tracking of goods [H.36]. Wireless networks used for maritime transportation can be short range for harbors or long range for the open sea.

The short-range networks must obtain large amounts of data, so some require thousands or tens of thousands of sensors [H.36]. The wireless networks may use a WSN, Bluetooth (WPAN), Wi-Fi, or Zigbee. WiMAX is used for other types of data transfer (including internet access for passengers), RFID is used for identification and location tracking of personnel/equipment or shipment containers, and cellular networks are used for voice and data transfers, Terrestrial Trunked Radio (TETRA) is used for personnel communication. VHF, UHF and satellite communications with ships may also be used.

On the open sea, there is no coverage of typical cellular networks, so communications links are limited to satellite systems (long-range ship-to-ship and ship-to-shore super-high frequency [SHF] and satellite communications [SATCOM]), commercial satellite (e.g., international maritime satellite [INMARSAT] B), UHF/VHF LOS, HF extended line of sight (ELOS), and high frequency (HF) beyond line-of-sight (BLOS) [H.5]. Satellite communication can provide high bandwidth, but at high delay and high costs. However, VHF/UHF links have small capacity and cannot support high data rate applications, so multiple attempts are made at developing maritime wireless mesh networks (MWMNs) with ships, buoys, and land stations forming the nodes to convey the communications [H.37]. MWMNs can be based on the above-mentioned technologies, as well as new alternatives such as WiMAX in the sub-GHz bands that were released after the migration from analogue to digital terrestrial TV (especially 698–862 MHz, but possibly also 450–470 MHz). Naturally, the ships are usually equipped with satellite positioning/navigation systems such as a global positioning system (GPS), a global navigation satellite system (GLONASS) and Galileo, a global navigation satellite system.

#### H.2.4.2 Aviation

Multiple wireless technologies are inherently supporting the airport operations, depending on the application. Passengers are provided with access to cellular networks and Wi-Fi for typical voice and data communication. However, many more technologies are used for airport management and basic operations. TETRA-based systems are used for high-reliability ground personnel and safety communication. RFID, super-sensitive GPS, and/or a real-time locating system (RTLS) can enable accurate location of a vehicle, mobile personnel, and equipment, all of which are crucial for efficient management of resources, access, incidents, and service disruptions. For wireless networks, VHF AM multimode radio and UHF digital radio can be used for ground-to-air communication.

### H.2.4.3 Land transport

The wireless networks used for land transport applications may include navigation, traffic signal control systems, container/vehicle fleet management systems, variable message road signs, automatic number plate recognition, and speedometer cameras (radar). Specific systems are used by authorities and safety agents because of their reliability. For these applications, the widely used technologies are TETRA and Dedicated Short-Range Communications (DSRC) [H.5]. DSRC is based on the IEEE 802.11p amendment to the 802.11 (WLAN) standard for operating in the licensed (dedicated) frequency band of 5.9 GHz. Moreover, in Europe there is a dedicated GSM-R band (873–880 MHz UL, 918–925 MHz DL) of spectrum for railway applications.

## H.2.5 Electric Utility

An electric utility operates facilities to generate electric power, transmits that power through the transmission system, and distributes electricity to public and industrial consumers via the distribution system. The capabilities of wireless networks for an electric utility must cover a very large area and must handle a significant amount of traffic. Grid management, teleprotection, and wireless substations use LTE[27] networks that can be upgraded to and are compatible with 5G. The networks are based on the LTE standards rather than the IEEE standards used for NPPs.

The grid, which was built in the 1890s and improved upon as technology advanced through each decade, consists of more than 9,200 electric generating units with more than 1 million megawatts of generating capacity connected to more than 300,000 miles of transmission lines [H.38].

Wireless networks have a significant impact on monitoring and control at substations. New standards in device control and management provide guidance. LTE converges connectivity for the power grid and the substation (Figure H.2). Flexibility in the use of the LTE spectrum increases capabilities that bring low latency and reliability within the substation and enables monitoring of the distribution and consumer grid.

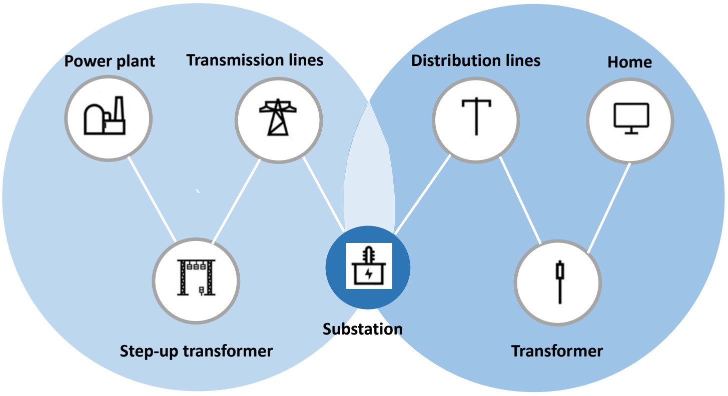


**Figure H.2. LTE converges connectivity for power grid and substation [H.39].**

[27] LTE is a 4G wireless broadband standard. LTE technology offers faster data connection and lower latency than 4G. Additionally, LTE allows for more phones to connect to the same network at one time. The main difference between 4G and LTE is that LTE has faster upload and download speeds.

### H.2.5.1 Distribution of power

The electrical power grid comprises a series of components: the site where the power is generated (the power plant), the transmission of that power throughout the grid, substations to ensure that the generated power is distributed efficiently, and the distribution substations that transmit the power from the grid to industries, offices, and homes.

In the United States, power is usually generated at about 69 kV at the power generation stations. Transmission substations, which are located closer to power stations, increase this to 138–768 kV to minimize transmission losses over long distances and to provide for interconnection to other parts of the power grid. Closer to the consumers, distribution substations reduce the transmission to 26–69 kV to serve three classes of consumers: industrial at 11–69 kV, commercial at 4–11 kV, and residential at 120–240 V).

#### *a. Grid management*

Communication and WANs are used to manage the grid. Grid management and telemetry systems are designed for centralized control and SCADA. The round-trip latency for centralized control is 50–100 ms, which is well within the capabilities of the 20–80 ms latencies available on LTE networks [H.39].

#### *b. Teleprotection*

Teleprotection is a system that monitors the condition of the grid and isolates faults to prevent damage to other components on the grid or large-scale failure of the grid itself. Teleprotection involves direct control of devices that carry high voltages, and it requires round-trip latency on the order of 10–20 ms to allow for instantaneous fault isolation. This can be achieved with dedicated 4G wireless transport like present-day microwave or with 5G new radio (NR)[28] bearers using high-band spectrum.

Teleprotection performs as a physical interface between the telecommunication infrastructure and the protection relays (Figure H.3). When a fault occurs, the protection system can realign switches, circuit breakers, or reclosers to prevent a fault from cascading throughout the network. Furthermore, in the event of an outage, teleprotection helps restart the power to that part of the grid.

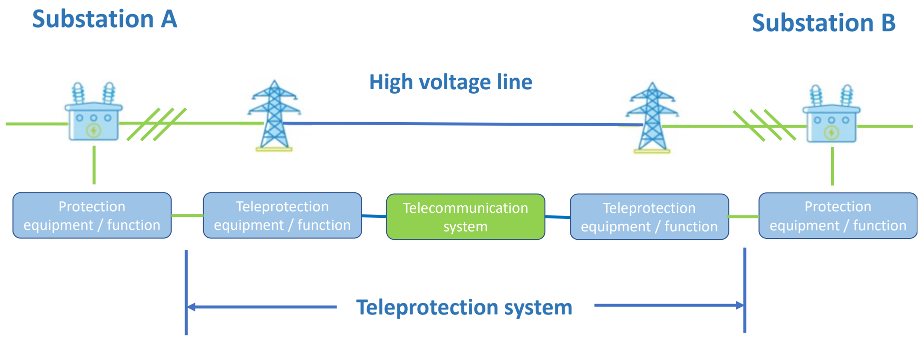

Substation A
Substation B
High voltage line
Protection equipment / function
Teleprotection equipment / function
Telecommunication system
Teleprotection equipment / function
Protection equipment / function
Teleprotection system

**Figure H.3. Teleprotection system [H.41].**

[28] 5G NR is a new radio access technology (RAT) developed by 3GPP for the 5G mobile network. It was designed to be the global standard for the air interface of 5G networks.

A self-contained LTE radio access network (RAN)[29] and core network installed at the substation ensures that one-way latencies are available for teleprotection at the substation.

### *c. The "Last Mile"*

That so-called *last mile* in the power grid is where power enters the consumer domain—the connection from the distribution substation to consumers. LTE enables more real-time monitoring of power grid components when high power lines enter a neighborhood. This monitoring can also be used to determine how consumer power generation affects and enables the power grid [H.40].

The real-time feedback from LTE wireless in the last mile enables utility companies to ensure power grid security and to be more proactive in staying ahead of potential faults in the neighborhood grid in some of the following ways:

- Substations receive the information needed to isolate smaller parts of the neighborhood grid, avoiding instability and blackouts in the larger grid.
- Safety is enhanced by proactive monitoring of a weather-stricken infrastructure.
- A real-time analysis of consumption and prosumer generation allows for more efficient onboarding of distribution energy resources across transmission and distribution substations in the power grid.

### H.2.5.2 Wireless substations

Transmission substations control the input of the power onto the grid. This control could be through isolation or switching of power generation sources using breakers, switches, and relays. Transmission substations could be located in remote areas far away from the control centers.

Distribution substations ensure continuity and reliability of power towards industrial, commercial, and residential consumption by switching power sources based on demand and fault detection/isolation. Distribution substations are typically closer to population centers: that is, closer to the consumption.

Wireless technology enhances substation control with its flexibility in latency and performance. From a performance standpoint, wireless networks at a substation can provide smart video monitoring.

The higher the power/voltage, the more critical the latency requirements are for direct control of substation equipment [H.42]. Devices operating at high voltages in substations must operate quickly to minimize the danger of sending high voltage on a compromised transmission line. Mesh networks are often custom built and lack the consistency and flexibility in latency offered by a single multipurpose LTE network [H.43].

The switchyard and control room are the main areas of focus for the wireless substation:

- The switchyard is where the incoming and outgoing power lines arrive and the electrical power operating equipment and primary control elements are located. These elements include power

[29] A RAN) is the part of a telecommunications system that connects individual devices to other parts of a network through radio connections. A RAN provides access and coordinates the management of resources across the radio sites. A handset or other device is wirelessly connected to a backbone or core network, and the RAN sends its signal to various wireless endpoints so it can travel with other networks' traffic.

transformers, circuit breakers, reclosers and instrument transformers, which provide a scaled down version of voltage and current.

- The control room is where secondary equipment such as relays and protection control of the primary elements are implemented.

With current analog technology, a control center cannot observe in real time whether a circuit breaker is working properly. Evolving standards like IEC 61850 [H.44] address the evolution from serial/analog to digital packet-based protocols, aligning more toward wide area control and communication. This establishes the protocol architecture for introduction of the standardized communication architecture offered by 3GPP wireless.

LTE networks can easily add capabilities of wireless 4G or 5G solutions to enhance or expand existing data connections and offerings.

Advantages realized through LTE modernization of the substation include [H.43] the following:

- LTE provides a multipurpose IP infrastructure, allowing the utility to define separated virtual networks for different primary control elements in the switchyard. All of these virtual networks can be defined on the single set of wireless bearers between the switchyard and the control room.

- The private network established to monitor and control the switchyard control equipment can multitask with employee smartphones, providing converged mission-critical and enterprise access.

- Deploying a common LTE network between the substation and WAN that is serving the surrounding power grid allows for enhanced control and transparency between mission-critical operations (within the substation's control) and monitoring, operations of the surrounding grid, which would have sensors on the same network, outside the substation's control.

- Upgrading the LTE network to 5G is relatively easy. As economies of scale and the ecosystem progress in 5G, integration of 5G into the LTE that has been deployed at substations and surrounding WANs is usually considered part of a wireless network evolution strategy.

- When power grid and substations are on a common LTE/5G network, the security environment for the power grid would extend into and encompass both the power grid and the substations that control the power grid.

### H.2.6 Military

Communication is a vital part of military operations, providing the distribution of commands, logistical information, and data from sensors. The data collected from sensors can be distributed through WSNs. The capabilities of the WSN for military applications must cover a very large area and must handle a significant amount of traffic. The majority of current military communications systems rely heavily on commercial protocols at the network and transport layer. IP version 4 (IPv4) is the predominant network layer technology within military networks. Commercial routing technologies such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) are the predominant routing technologies within military networks. Transmission control protocol (TCP) and user datagram protocol (UDP) are the predominant transport layer technologies within military networks. Future military networks are expected to adopt IPv6[30] as their network layer technology. (IPv6 is sometimes referred to as *IP Next Generation* or *IPng*.)

Historically, technologies for military applications have led the development beyond state-of-the-art, and their commercial adoption has followed (e.g., radars, satellite communications, GPS) [H.5]. In recent decades, however, the progression has been in the opposite direction, and the military solutions are currently adopting commercial-off-the-shelf (COTS) technologies [H.45].

The secure wireless local area network (SWLAN) is a US Army program that will use IEEE 802.11 standard waveform that has been modified to meet military needs for reliability and security. The SWLAN will provide a mobile networking alternative to present fiber optic connections between tactical operations center (TOC) vehicles at the brigade and battalion levels. The SWLAN is designed to allow secure wireless ethernet communications.

The Two-way Robust Acquisition of Data (2-RAD) program investigated and defined a WLAN architecture to enable high-speed data acquisition and command of mobile platforms. A candidate architecture was deployed using COTS equipment that conforms to the IEEE 802.11 b WLAN standard.

The majority of next-generation military communications systems are being designed to provide QoS capability to tomorrow's warfighter. It is expected that commercial QoS and traffic engineering techniques such as Integrated Services (IntServ), Resource Reservation Protocol (RSVP), Differentiated Services (Dimem), and multi-protocol label switching (MPLS) will play a significant role in traffic management for future military networks.

### H.2.7 Other Industry Examples

An article in *Power Engineering 2011* lists five case examples of wireless usage in power plants [H.46]:

- *San Diego Gas & Electric wanted to implement a wireless architecture throughout the Palomar Energy Center combined cycle plant to access data that was previously unattainable through traditional wired solutions. Emerson installed five applications of its WirelessHART network, which have been used to provide access to additional plant and process data and [were] helpful in improving operational efficiencies.*

- *Verizon Wireless deployed BlackBerrys integrated with SAP [Systems, Applications, and Products] at a utility's power plant. This capability gave the workforce access to tools leading to increased production.*

- *A power plant in Europe recently used Honeywell wireless temperature transmitters to measure steam used for heavy oil burners. The transmitters were used to replace a wired solution that would have taken two months to install. The wireless solution, however, took two days to install.*

- *A Nebraska power plant installed Honeywell wireless technology to monitor its remote oil tanks. The plant is now able to efficiently monitor water runoff where electricity is not available.*

- *Central Iowa Power Cooperative (CIPCO) collects power measurements each month for both billing purposes and planning initiatives. The cooperative was previously using a process called*

[30] IPv6 became a Draft Standard for the Internet Engineering Task Force (IETF), which subsequently ratified it as an Internet Standard on 14 July 2017. RFC 1883, *Internet Protocol, Version 6 (IPv6) Specification*, replaces RFC 791, *Internet Protocol* (IPv4). IETF is a non-profit standards organization whose purpose is to create voluntary standards to maintain and improve the usability and interoperability of the internet.

> *probing that required field workers to physically collect meter data using an analog phone. The process was costly and time-consuming. CIPCO decided to install Sierra Wireless' AirLink Raven XT solution, enabling remote management, configuration and troubleshooting capabilities. The system has enabled CIPCO to monitor and control its network of wireless gateways from one central location, lowering the total cost of ownership.*

Below are some examples of wireless technology usage selected from various sensor and system vendor reference cases [H.5]:

- The RWE Westfalen power plant in Germany uses an environmental monitoring system to measure temperatures and water levels in the plant's perimeter. The system is powered by solar panels, and data are transmitted via a wireless mesh network using a license free 2.4 GHz channel to the plant central system.

- The Niederhausen hydro plant in Germany wirelessly measures water levels in the reservoir, as well as flood and groundwater pump states. Data are wirelessly transmitted to the dam towers and are further transmitted with wireless single-pair high-speed digital subscriber line (SHDSL) modems to the plant. A wireless mesh solution is used by the Glendale Power & Water municipal utility located in Los Angeles County, California, to collect remotely read data from 84,000 electric and 30,000 water-smart meters remotely.

- Suncor Energy in Canada uses a wireless mesh network to secure refinery operations with access control and video. The network is installed in the middle of a metal storage tank farm, which is a difficult environment for wireless communications.

EPRI combined two technologies to demonstrate OLM capabilities to assess equipment condition from signals obtained from plant components during operation. Vibration signals from the pulverizer roller bearings were provided via wireless network, in combination with the existing process signals, to provide early warning of failure. The equipment's predictive monitoring software and wireless technology vibration sensors were able to provide more information for early detection of coal pulverizer failures than conventional vibration analysis alone [H.47]. Wireless technologies reviewed for the demonstration included Bluetooth, IEEE Standard 802.11b, and 900 MHz systems with the IEEE 802.11b wireless standards chosen based on signal strength and range within a power plant environment, as well as providing nearly real-time data transfer capabilities. The network-capable application processor system operates at 2.4 GHz with a 100 mW signal having a range of up to 300 ft. The Access Point wireless system receiver uses an ethernet connection with the plant's LAN, where a dedicated desktop computer receives the data and provides an interface with the plant data archive server. The combination of vibration signals and process variables, when monitored by the predictive monitoring system, increases the number of detectable failure modes from 11 to 46%. The value proposition is that the technology could achieve up to a 12-hour early warning of impending failure.

Other examples of the uses of wireless instrumentation and sensors in the non-nuclear industry include [H.4, H.5]:

- The Gudrun platform, where the wireless network measures parameters such as temperature, pressure, and vibration using WirelessHART.

- Because the harsh environment underground resembles the demanding environment in the NPPs, the Modern 2020 Project has conducted tests and studies concerning radioactive influence on monitoring using a wireless network [H.48].

- In Borlänge, SSAB Tunnplåt AB runs a 15,000 m$^3$ warehouse for steel coils in three warehouse buildings. In these warehouses, manually operated forklift trucks were replaced with driverless stacker trucks and crab cranes on the ceiling that use wireless failsafe communication. Both standard and safety communication were integrated into the same wireless system using real-time and TCP/IP communication. Navigation of the automated stackers is accomplished by rotating lasers on top of the stackers, which are in contact with the mirrors distributed throughout the warehouse.

- Nokia is using its own factory in Oulu, Finland, as a living laboratory for factory-of-the-future (FoF) and industrial IoT system trials. Wireless technologies used in the concept include narrow band IoT, LTE, Wi-Fi, and emerging 5G networks. Testers, instruments, sensors, robots, and actuators are planned to be connected to the network. Some implemented wireless applications include monitoring of environmental parameters and engineering support in the final assembly line using smart wearables.

WirelessHART, narrow band IoT, LTE, Wi-Fi, long range (LoRa), and 5G wireless networks are in use.

### H.2.7.1 Emergency

Emergency services require two types of communications: one-to-one, and one-to-many (broadcasting) [H.4]. An example of one-to-many communication is when authorities issue alerts or provide information and instructions to the public concerned. One-to-many communications can be provided by special broadcast interruptions on TV, radio, and cellular networks. Also, specific, dedicated information websites can help offload the one-to-one communications traffic with typical emergency call centers such as the 911 system. Moreover, additional means are needed for emergency services (police, firefighters, army, medical) to communicate with each other during rescue actions in case of disasters. TETRA is the main type of wireless system used for this purpose. It is designed specifically for such services, providing point-to-point and broadcasting channels. Satellite communication can also be used at very distant locations. For daily routines, however, rapidly developing cellular networks provide emergency services personnel with sufficient means for communication.

### H.2.7.2 Healthcare

The healthcare domain currently spans over two main environments—patient homes and hospitals. At home, small medical devices can monitor a patient's parameters; Bluetooth is typically used to send the data to a computer or mobile phone for local analysis, or data are conveyed to a doctor at a remote location [H.5]. Hospitals have more data to track in a much more complex environment. RFID and near-field communication (NFC)[31] technologies are used for identification and location tracking of equipment (intravenous pump machines, respirators, wheelchairs, etc.) or personnel (nurses, doctors, guards, technicians, cleaners), as well as for restricted access control. Smartphones and tablets provide instant access to medical records in centralized databases, thus removing the need for manual data inputs and file transports. Room environment conditions (temperature, humidity) can be remotely monitored and controlled using RFID or Wi-Fi networks. Also, patient status is often monitored wirelessly in real time using Bluetooth or Wi-Fi communications. These applications of wireless technologies present a number of security issues, including data confidentiality and possible interference with medical electronic equipment.

[31] NFC is a short-range wireless connectivity technology that lets NFC-enabled devices communicate with each other.

### H.2.7.3 Office, Home, and Consumer Applications

Modern wireless office applications use a variety of wireless applications. Examples from home, office, and consumer applications are not the primary candidates to be considered, as the nuclear industry is moving to the wireless technology usage [H.5]. However, it is useful to follow the progress of wireless applications in this segment because in the later phase, consumer applications could also be adopted by the nuclear industry with some modifications.

## H.3 REFERENCES

H.1 ISA-TR84.00.08-2017, *Guidance for Application of Wireless Sensor Technology to Non-SIS Independent Protection Layers*, International Society of Automation, Approved 24 April 2017.

H.2 Pratik Pingle, *Selection of obsolescence resolution strategy based on a multi criteria decision model*, Master's Thesis, Iowa State University, 2015.

H.3 IAEA Nuclear Energy Series No. NP-T-1.13, *Technical Challenges In The Application And Licensing Of Digital Instrumentation And Control Systems In Nuclear Power Plants*, International Atomic Energy Agency, Vienna, 2015.

H.4 Arto Laikari, *Wireless in nuclear feasibility study*, VTT Technical Research Centre of Finland Ltd, 8.3.2018.

H.5 A. Laikari, J. Flak, A. Koskinen, And J. Häkli, *Wireless in Nuclear, Feasibility Study*, Energiforsk Nuclear Safety Related I&C – ENSRIC, Report 2018:513, July 2018.

H.6 EPRI 1019186, *Implementation Guideline for Wireless Networks and Wireless Equipment Condition Monitoring*, Electric Power Research Institute, Palo Alto, California, December 2009.

H.7 STUK Guide YVL B.1 (2019) *Safety design of a nuclear power plant*. STUK. ISBN 978-952-309-047-7.

H.8 STUK Guide YVL 5.5 (2002) *Instrumentation systems and components at nuclear facilities*. STUK. ISBN 951-712-622-0.

H.9 Ramzi Jammal, *Regulating Innovative Nuclear Technologies*, CNSC, Pacific Basin Nuclear Conference, 2018.

H.10 *Information Notice No. 83-83: Use of Portable Radio Transmitters Inside Nuclear Power Plants*, US NRC, December 19, 1983.

H.11 EPRI TR-1011751, *Assessment of Wireless Technologies in Substation Functions, Part II: Substation Monitoring and Management Technologies*, Electric Power Research Institute, Palo Alto, California, March 2006.

H.12 H. M. Hashemian, C. J. Kiger, G. W. Morton & B. D. Shumaker (2011) Wireless Sensor Applications in Nuclear Power Plants, *Nuclear Technology*, 173:1, 8-16, DOI: 10.13182/NT11-1

H.13 Emil Ohlson, WIRELESS IN NPP, Current situation and Future expectations for wireless in NPP, 2018-03-08.

H.14 Nuclear Energy Institute, *Use of Wireless Technologies for Plant Modernization*, February 20, 2020.

H.15 EPRI TR-1007448, *Guidelines for Wireless Technology in Power Plants, Volume 2: Implementation and Regulatory Issues*, Electric Power Research Institute, Palo Alto, California, (2002).

H.16 EPRI 1016724, *On-Line Monitoring for Equipment Condition Assessment*, Electric Power Research Institute, Palo Alto, California, (2008).

H.17 EPRI 1010468, *Automation in Power Plants and Wireless Technology Assessments*, Electric Power Research Institute, Palo Alto, California, December 2005.

H.18 EPRI TR-1004905, *Wireless Technology Power Plant Applications*, Electric Power Research Institute, Palo Alto, California, December 2003.

H.19 EPRI TR-1013485, *Revised Guidelines for Wireless Technology in Power Plants, Volume 1: Benefits and Considerations*, Final Report, Electric Power Research Institute, Palo Alto, California, December 2006.

H.20 NRC Order EA-12-051, *Issuance of Order to Modify Licenses with Regard to Reliable Spent Fuel Pool Instrumentation*, US Nuclear Regulatory Commission, (Agencywide Documents Access and Management System (ADAMS) Accession No. ML12054A679).

H.21 JLD-ISG-2012-03, *Compliance with Order EA-12-051, Reliable Spent Fuel Pool Instrumentation*, US Nuclear Regulatory Commission, August 29, 2012 (NRC ADAMS Accession No. ML12221A339)

H.22 NEI 12-02, Revision 1, “Industry Guidance for Compliance with NRC Order EA-12-051, 'To Modify Licenses with Regard to Reliable Spent Fuel Pool Instrumentation,” August 2012 (NRC ADAMS Accession No. ML12240A307)

H.23 Letter from Carl F. Lyon to Adam C. Heflin, “Callaway Plant, Unit 1 -Interim Staff Evaluation and Request for Additional Information Re: Overall Integrated Plan in Response to Order EA-12-051, Reliable Spent Fuel Pool Instrumentation (TAC NO. MF0773),” US Nuclear Regulatory Commission, November 25, 2013 (NRC ADAMS Accession No. ML13323A111)

H.24 Letter from Jennie K. Rankin, NRC, to Randall K. Edington, Arizona Public Service Company, “Palo Verde Nuclear Generating Station, Units 1, 2, and 3-Interim Staff Evaluation and Request for Additional Information Regarding the Overall Integrated Plan for Implementation of Order EA-12-051, Reliable Spent Fuel Pool Instrumentation (TAC NOS. MF0774, MF0775, AND MF0776),” US Nuclear Regulatory Commission, October 29, 2013 (NRC ADAMS Accession No. ML13296A006)

H.25 EPRI 3002017641, *EPRI Research Helps Ontario Power Generation (OPG) Deploy Its First Wireless Sensor Network at One Plant*, Electric Power Research Institute, Palo Alto, CA, Dec 23, 2019.

H.26 ANSI/ISA-TR99.00.01-2007, *Security Technologies for Industrial Automation and Control Systems*, International Society of Automation, Approved 29 October 2007.

H.27 Muhlheim, M. D., et. al., *Developing a Technical Basis for Embedded Digital Devices and Emerging Technologies*, NUREG/CR-7273, US Nuclear Regulatory Commission, March 2021.

H.28 EPRI 1003584, *Guidelines for Wireless Technology in Power Plants, Volume 1: Benefits and Considerations*, Final Report, Electric Power Research Institute, Palo Alto, CA, December 2002.

H.29 *Design Control Document for the US-APWR, Chapter 9, Auxiliary Systems*, MUAP-DC009, Revision 2, October 2009 (NRC ADAMS Accession No. ML093070259)

H.30 Eva Gustavsson, *Wireless in Nuclear – Nuclear Radiation-Tolerant Wireless Transmitters*, WAAP-10784, Rev. 1, Westinghouse Electric Company Sweden AB, 2018.

H.31 Bill Ansley, *Wireless in Nuclear at Exelon*, Exelon Digital Plant Innovation, 2018.

H.32 Mike Hopfe and Wayne Manges, *The ISA100 Standards Overview & Status*, 2008.

H.33 PUBLIC LAW 109–236—JUNE 15, 2006

H.34 The National Institute for Occupational Safety and Health (NIOSH), *Basic Tutorial on Wireless Communication and Electronic Tracking: Technology Overview.* https://www.cdc.gov/niosh/mining/content/emergencymanagementandresponse/commtracking/commtrackingtutorial1.html

H.35 https://duckduckgo.com/?q=leaky+feeder+cable&t=newext&atb=v319-1&iax=images&ia=images&iai=http%3A%2F%2Fgetbfbs.com%2Fsites%2Fdefault%2Ffiles%2Fstyles%2F800px_wide%2Fpublic%2Fright_hand_side_images%2FLeaky-Feeder-800x400.png%3Fitok%3DYmEOblQH

H.36 M.G.C.A. Cimino et al., *Wireless communication, identification and tensing technologies enabling integrated logistics: a study in the harbor environment*, 2015. https://arxiv.org/abs/1510.06175

H.37 M. Manoufali, H. Alshaer, P.-Y. Kong, S. Jimaa, *Technologies and networks supporting maritime wireless mesh communications*, 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), 2013. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6549005

H.38 *The Smart Grid*. https://www.smartgrid.gov/the_smart_grid/smart_grid.html

H.39 Gautam Talagery, *The wireless power substation: transformation towards power grid sustainability*, Nov 01, 2021. https://www.ericsson.com/en/blog/2021/11/the-wireless-power-substation-transforming-the-journey-towards-power-grid-sustainability-and-modernization

H.40 Gautam Talagery, *Why LTE wireless brings power grid security, convenience, and convergence to the last mile*, Dec 06, 2021. https://www.ericsson.com/en/blog/2021/12/why-lte-wireless-brings-power-grid-security-convenience-and-convergence-to-the-last-mile

H.41 *Teleprotection*, SGRwin, September 2, 2020. https://www.sgrwin.com/protecting-power-systems/

H.42 Gautam Talagery, *Wireless brings low latency, high performance to interconnect generation, distribution in the power grid*, Oct 01, 2021. https://www.ericsson.com/en/blog/2021/10/wireless-for-power-grids

H.43 Gautam Talagery, *Always on, always plugged in, Mission-critical wireless connectivity and the journey to power grid modernization*, Ericsson, April 2022. https://www.ericsson.com/498244/assets/local/enterprise/reports/14042022-utilities-blog-pov-paper.pdf

H.44 IEC 61850 uses an object-oriented protocol that use a hierarchical data structure to monitor families of devices.

H.45 J.L. Burbank, W.T. Kasch, *COTS communications technologies for DoD applications: challenges and limitations,* Military Communications Conference, MILCOM 2004. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1495111

H.46 Lindsay Morris, *Power Engineering*, 2011 volume 115, “Wireless at Power Plants,” 9.1.2011.

H.47 EPRI TR-1004902, *On-Line Predictive Condition Monitoring System for Coal Pulverizers Application of Wireless Technology*, Electric Power Research Institute, Palo Alto, California, October 2003.

H.48 José Luis García - Siñeriz, Wireless in nuclear applications, 8 March 2018, STOCKHOLM, Swedish Radiation Safety Authority office, Solna Strand väg 9, Stockholm, EU project Modern2020.

Closeout for RAR-NRR-2021-014 DATE October 17, 2023

DISTRIBUTION:
JZhao, NRR/DEX/ELTB
NCarte, NRR/DEX/EEOB
LHardin, RES/DE/ICEEB
SWyman, NRR/DEX/EEEB
CCook, RES/DE/ICEEB
MWaters, NSIR/DPR
RStattel, NRR/DEX/EEOB
TMartinezNavedo, NRR/DRO
JMcKirgan, RES/DE
NTaylor, R-IV/DRS/EB2

**ADAMS Accession No.: ML21117A273; ML23222A166**

| | | | | |
|---|---|---|---|---|
| OFFICE | RES/DE/ICEEB | RES/DE/ICEEB | NSIR/DPCP/RSB | |
| NAME | LHardin *LH* | CCook *CC* | MSampson *MS* | |
| DATE | Sep 27, 2023 | Sep 28, 2023 | Oct 17, 2023 | |

***OFFICIAL RECORD COPY***