Wireless System Considerations When Implementing NERC Critical Infrastructure Protection Standards

Teja Kuruganti[1], Walter Dykas[1], Wayne Manges[1], Tom Flowers[2], Mark Hadley[3],
Paul Ewing[1], Thomas King[1]
[1]*Oak Ridge National Laboratory, Oak Ridge, TN 37831*
[2]*Flowers Control Center Solutions, Todd Mission, TX 77363*
[3]*Pacific Northwest National Laboratory, Richland, WA 99352*

February 25, 2009

Introduction

Energy asset owners are facing a monumental challenge as they address compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards (CIP-002 through CIP-009). The increased use of wireless technologies and their introduction into control center networks and field devices compound this challenge, as ambiguity exists regarding the applicability of the CIP requirements to wireless networking technologies.

The requirement to monitor and control a utility's Electronic Security Perimeter (ESP) is defined in CIP-005. While wireless is neither explicitly included nor excluded from the requirements, wireless technologies provide electronic access to utility networks and therefore must be considered under CIP-005. Selected requirements from CIP-005 include:

> **R1.1.** Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
>
> **R1.3.** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
>
> **R2.** Electronic Access Controls—The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> **R3.** Monitoring Electronic Access—The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) 24 hours a day, seven days a week.

Because the applicability of CIP Standards to wireless is ambiguous, compliance conflicts potentially exist among CIP Standards, other federal regulations (e.g., Federal Communications Commission [FCC] regulations), and a utility's normal or emergency operational protocol. Utilities will confront implementation challenges anywhere their regulatory constraints, legal implications, corporate information technology policy, and technological options clash.

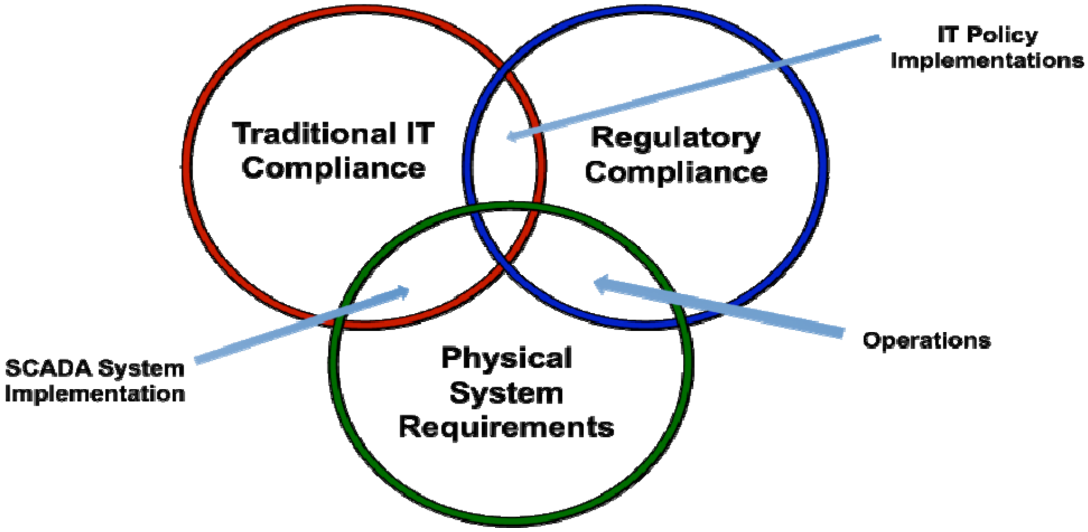

IT Policy Implementations
Traditional IT Compliance
Regulatory Compliance
SCADA System Implementation
Operations
Physical System Requirements

Figure 1. Security in critical infrastructure combines three domains

Figure 1 illustrates how IT compliance, regulatory compliance, and physical system requirements are all interdependent. CIP Standards potentially create conflict when their interpretation is unclear in the context of (1) normal and emergency operations; (2) wireless technologies; (3) control systems; and/or (4) ability to implement compensating controls meeting compliance, potentially creating conflict with FCC regulations.

This white paper examines the risks of wireless use within the ESP, presents a defense-in-depth model to monitor and control wireless, and presents technical solutions for each defensive layer that will assist with CIP-005 compliance. This paper also offers methods to reduce risk from numerous wireless threat scenarios, including approved wireless use, inadvertent wireless use, and covert wireless use.

Defining the Electronic Security Perimeter

A utility must first define its ESP before attempting to monitor and control wireless communications. In wired networking environments, the ESP encompasses the points of connection to other networks (e.g., corporate networks, remote access, Internet, etc.). These wired connection points are well defined and limited in number. Existing technical solutions such as firewalls, intrusion detection systems (IDSs), and packet inspection systems exist to secure the ESP against approved, inadvertent, and covert threats to the wired access points.

Wireless networking devices introduce the ability to connect control center networking devices within a utility’s ESP to other networks inside or outside the ESP using any computer on the wired control center network. The number of access points is only limited by the number of routable and serial ports that exist on the computing devices within the ESP. Figure 2 depicts a typical ESP for a utility. The control center network is contained within a physical security perimeter (PSP).

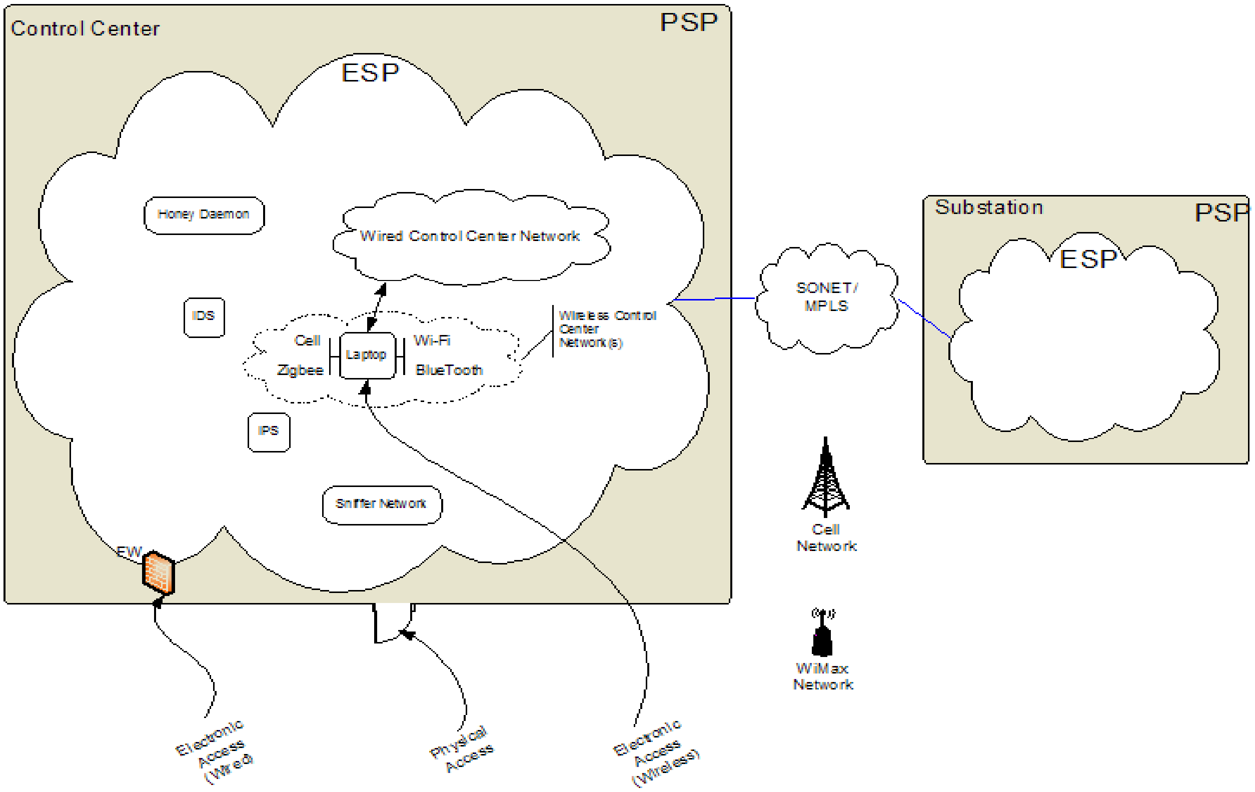


Figure 2. Typical electronic security perimeter (ESP) for a utility

Figure 2 also shows how a utility can define multiple, distributed ESPs. In this example, a routable protocol is used to communicate between the ESPs. A routable protocol could also be used for communication within each ESP. The use of routable protocols makes the network subject to CIP requirements, increasing the security impact. CIP-002 applies as follows:

> **R3.1.** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
>
> **R3.2.** The Cyber Asset uses a routable protocol within a control center.

The Challenge of CIP Compliance

CIP compliance is challenged when mobile devices, capable of unauthorized wireless connectivity with wired and wireless interfaces, are able to access a CIP-protected cyber asset within the ESP. For example, many utilities routinely permit the operation of cell phones, pagers, wireless bar code readers, and wireless local area network (WLAN) connections in or near their control centers or substations. Because devices operating within the PSP of the control center are not necessarily within the logical bounds of the control center's ESP, many utilities do not routinely consider them problematic for CIP compliance. Cell phones and pagers are prime examples. They are physically within the PSP but not connected to any computing devices; however, they are still a threat because they could potentially establish a connection.

Many wireless devices of concern discussed in this paper are initially unmanaged and unauthorized to access cyber assets per the responsible entity's CIP guidelines. It is their capability for wireless connectivity with multiple wired and wireless interfaces that poses a threat.

An example scenario in which CIP compliance is challenged within the control center ESP follows: The cyber assets in the control center are NERC CIP compliant and CIP operation authorized. The control center is physically accessed by authorized personnel, whether part of the local organization (of the cognizant responsible entity) or from an outside organization. To accomplish their assigned tasks, these employees use a variety of communication and computing devices, including laptops with multiple network interfaces and connection capabilities, such as universal serial bus (USB), wired network, Bluetooth, infrared, business WLAN (e.g., 802.11a/b/g), cell modem (e.g., Wireless Fidelity [Wi-Fi]), and physical media read/write capability. Because of their proximity to the ESP, individuals equipped with these devices have the potential for: (1) unintended or intended unauthorized access, interception, movement, or disruption of information or assets, by either wired or wireless connection to cyber assets within an ESP or PSP; or (2) interception of wireless network traffic from cyber assets within the ESP.

As previously stated, threats can stem from three situations:

- Approved use of wireless technology
- Inadvertent use of wireless technology
- Covert use of wireless technology

Threat: Approved Wireless Use

Scenario: A utility staff member has been tasked with monitoring syslog files associated with a new cryptographic application deployed in the control center. The key update process is being monitored to determine if it is the cause of an increase in data loss from the telemetry process. The staff member attaches a USB Wi-Fi adapter to the syslog server and configures it to connect to the corporate Wi-Fi network. The staff member can now access the syslog information from his computer on the corporate network and perform his analysis. While the Wi-Fi connection performs as expected, it provides an access path to the syslog server.

Threat: Inadvertent Wireless Use

Scenario: A vendor brings a laptop into the control center while assisting with an upgrade to the site's energy management system (EMS). The laptop contains a cell modem that the vendor uses to connect to his office to obtain files and information necessary to support the asset owner. The asset owner does not allow USB flash drives and other removable media into the control center. To transfer files from the vendor's laptop to the EMS, the laptop is connected to the control center wired network. The laptop is not configured to prohibit bridging (the act of connecting networks over different media or interfaces). After downloading files, the vendor does not disconnect from his network before plugging in the cable to transfer the files for the asset owner. The wireless cellular network is now able to communicate with the wired control center network, effectively bypassing all ESP monitoring and control mechanisms.

Threat: Covert Wireless Use

Scenario: While checking a problem with a server in the computer room supporting the EMS, a disgruntled employee attaches a cellular broadband modem to an Ethernet port on a server. The cell modem is small and can be easily attached and hidden to avoid detection. The cell modem provides an attack pathway for the employee that bypasses wired electronic security controls. The employee plans to use the cell modem to launch an attack on substation intelligent electronic devices and also cause a denial of service to make recovery more difficult.

Threat: No ESP Threat

Scenario: A utility staff member brings a Blackberry within the ESP to communicate with the Federal Emergency Management Agency during a response to a hurricane. The Blackberry is never connected to the wired control center network. This Blackberry supports both voice and data communication. Since these capabilities can be abused, the threat persists even though connectivity, at a given moment in time, does not exist.

Defense in Depth

No single defense is adequate to secure any wired or wireless network. Defense-in-depth security is a process that requires an array of security measures at all layers of a utility, including people, technologies, the cyber realm, and physical controls. Each defensive layer contains multiple controls to mitigate risk—however these controls may also contain risks that need to be mitigated by other layers. Security measures in the personnel controls layer might include a training program to educate staff on the policies and procedures governing appropriate use of wireless technologies. The physical controls layer might require a perimeter fence around the control center building, locks on the control center network doors, locked cabinets within the control center to house sensitive cyber assets, and guard patrols.

Figure 3 depicts various defensive layers used to monitor and control the ESP from wireless networking devices. The technical solutions available differ with each wireless technology. For example, commercial products exist to monitor, locate, and control Wi-Fi communication; however, commercial solutions may not be available for ZigBee, Wireless HART, or ISA100 for many years. As a result, asset owners must use a combination of defensive techniques, including those available on the wired network, to identify anomalous communications. That said, the most successful mitigation is for the asset owner to prohibit the use of wireless technologies until they can be adequately monitored and controlled.

Figure 3 also shows several access attempts and attack pathways that exemplify the need for a layered defense. Two are explored further here as examples. One is the covert wireless attack, in which an adversary attempts to use a utility-operated Wi-Fi network to access control center devices. Though the personnel and physical layers are breached by the adversary, the utility has implemented an 802.1X network registration scheme for its Wi-Fi network. The adversary’s PC is not known to the 802.1X environment and is denied access. In the second attack attempt, a malicious employee tries to access the control center to install a wireless cell modem onto a control center computer. The employee ignores the personnel controls, but the proximity reader controlling physical access denies the employee entrance to the control center network.

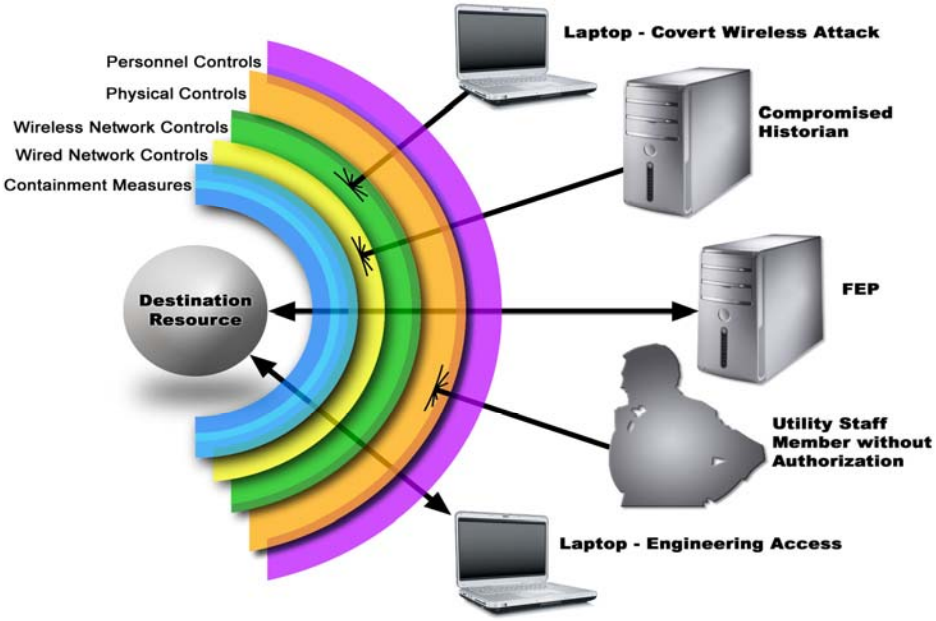

Personnel Controls
Physical Controls
Wireless Network Controls
Wired Network Controls
Containment Measures
Destination Resource
Laptop - Covert Wireless Attack
Compromised Historian
FEP
Utility Staff Member without Authorization
Laptop - Engineering Access

Figure 3. Access attempts and attack pathways

The authors make the following assumptions:

- A defense-in-depth approach provides the greatest opportunity to stop both known and unknown vulnerabilities.
- Despite best efforts, vulnerabilities will always exist that cannot be mitigated by a defense-in-depth model.
- Each security layer is equally important.

To help utilities mitigate wireless cyber security risks and comply with CIP Standards, the authors introduce several technical and personnel controls in tables 1 and 2 that can be used to build a defense-in-depth approach to security. The “defensive layer” column in Table 1 describes the point within the infrastructure where the defense technique can be employed; for example, physical controls are applied at the point or proximity where a wireless device can be introduced into the facility or near an ESP (e.g., building access, lock boxes). The existence and visibility of these controls may provide some deterrent by acting as a reminder to a forgetful employee or by averting discovery by a malicious adversary. Physical controls are applied near the facility; however, they can be bypassed by a determined adversary. The “technical availability” column in Table 1 defines which wireless technologies can benefit from the defensive technique. The recommended technical controls target specific and known wireless technologies or protocols; multiple and updated controls would be required to address multiple technologies. Nontechnical controls, however, are typically available for all wireless technologies, especially personal wireless devices. The NERC CIP Standards specifically require utilities to “monitor” or “control” cyber assets and perimeters; the “Critical infrastructure protection requirement” column in table 1 indicates the function each technique serves. The “Threat” column in Table 1 indicates the type of threat that the defensive technology addresses within a critical infrastructure site, with covert threats being the most difficult and expensive to address. The three columns in table 2 labeled “Security benefits,” “Security limitations,” and “Organizational impact” address, respectively, the benefit, risk, and cost associated with the defensive technology.

Table 1. Defensive techniques: defensive layers, technical availability, critical infrastructure protection requirements, and threats

Defensive technique	Defensive layer	Technical availability	Critical infrastructure protection requirement	Threat
Building access controls (e.g., locks, fences, cameras)	P, S	W, B, Z, C, S, O	M, C	A, I
Appropriate-use signs (e.g., only company-owned cell phones allowed)	P, S	W, B, Z, C, S, O	C	A, I
Network design	W, D	W, B, Z, C, S, O	M, C	A, I, C
Lockboxes for wireless devices	P, S	O	M, C	A, I
Wireless-use training	P	W, B, Z, C, S, O	M, C	I
Security guards	P, S	W, B, Z, C, S, O	M, C	A, I
Physical search	P, S	W, B, Z, C, S	M, C	A, I, C
Signature-based IDS	W, D	W, B, Z	M, C	A, I
Anomaly-based IDS	W, D	W, B, Z	M, C	A, I, C
Device registration	W, D	W, B, Z	M, C	A, I, C
RF spectrum analysis	W	W, B, Z, C, S	M, C	A, I, C
Dual DNS	W, D	W, C	M	A, I
OSI physical layer security	W, D	O	M, C	A, I, C
Wireless technology cryptographic protections (e.g., WEP, WPA, AES)	W	W, B, Z, C, S	M, C	A, I
Third-party cryptographic communication protection	W, D	W, B, Z, C, S	M, C	A, I, C

Abbreviations:

AES: advanced encryption standard	D: wired	B: Bluetooth	C: control	A: approved
DNS: domain name server	P: physical	C: cellular	M: monitor	C: covert
IDS: intrusion detection system	S: personnel	O: other		I: inadvertent
OSI: open system interconnection	W: wireless	S: SCADA radio		
RF: radio frequency		W: Wi-Fi		
WEP: wired-equivalent privacy		Z: ZigBee		
WPA: Wi-Fi–protected access				

Table 2. Defensive techniques: security benefits, security limitations, and organizational impacts

Defensive technique	Security benefits	Security limitations	Organizational impact
Building access controls (e.g., locks, fences, cameras)	Prevents accidental damage	May not find all devices	High cost to implement
Appropriate-use signs (e.g., only company-owned cell phones allowed)	Prevents accidental mistake	Limited to trusting people	Very low impact
Network design	Different technologies	Denial of service	High cost to implement and practice
Lockboxes for wireless devices	Visual presence provides reminder of wireless prohibition	Limited to trusting people	Low cost to implement, low impact, and provides a perceived benefit of protecting an individual's wireless devices if not allowed in an ESP
Wireless-use training	Prevents inadvertent violations; increases vigilance of individuals monitoring for violations	Limited to preventing inadvertent violations	Personnel training is generally considered the lowest cost and most effective security control
Security guards			High cost for implementing a security guard force, but is likely available for property protection and personnel access
Physical search	Prohibits unauthorized devices	May not find all devices	High cost to implement
Signature-based IDS	Will mitigate known threats	Cannot find zero-day attacks	Low-to-medium cost to implement
Anomaly-based IDS	Prevents cyber physical attacks	Initial damage cannot be prevented	Medium cost to implement
Device registration	Prevents unauthorized attack	Devices can be spoofed	Medium-to-high cost to implement
RF spectrum analysis	Actual wireless activity can be monitored	Not commercially available	High cost to implement
Dual DNS	Unauthorized wireless bridging	Not comprehensive	High cost to implement
OSI physical layer security	LPI/LPD	All/nothing	High cost to implement
Wireless technology cryptographic protections (e.g., WEP, WPA, AES)	Accessible to all technologies	Known vulnerabilities	Low cost to implement
Third-party cryptographic communication protection	Robust	Proprietary	High cost to implement

Abbreviations:
AES: advanced encryption standard
DNS: domain name server
IDS: intrusion detection system
LPD: low probability of detection
LPI: low probability of interception
OSI: open system interconnection
RF: radio frequency
WEP: wired-equivalent privacy
WPA: Wi-Fi–protected access

Summary

Increasing use of wireless technologies in the control systems environment will present a growing challenge to energy asset owners as long as monitoring and control technologies for wireless usage lags. Meeting requirements to both monitor and control the ESP is difficult even when technical solutions are available for a wireless technology. New and emerging wireless technologies will only add to the challenge. To best secure the network and comply with NERC CIP Standards, utilities must implement a defense-in-depth approach to infrastructure and cyber security and restrict the use of wireless technologies to those that can be properly monitored and controlled. The technical and personnel controls (defensive techniques) presented in tables 1 and 2 are intended to assist asset owners in achieving regulatory compliance.

The tables also indicate where further research in the area of wireless security is needed. It is the hope of the authors that this paper will help identify technical gaps, assist with the creation of a research and development roadmap, lead to inherently secure wireless technologies that integrate in multiple Open Systems Interconnection (OSI) layers (physical to application), and also encourage the collaborative development and testing of wireless security solutions in laboratory environments.

References

1. Reliability Standards for the Bulk Electric Systems of North America; March 26, 2008:
   a. Cyber Security – Electronics Security Perimeter(s), CIP-005-1, ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-005-1.pdf
   b. Cyber Security – Critical Cyber Asset Identification; CIP-002-1
   c. Cyber Security – Security Management Controls; CIP-003-1
   d. Cyber Security – Physical Security of Critical Cyber Assets; CIP-006-1/1a
   e. Cyber Security – Systems Security Management; CIP-007-1
   f. CIP-008-1 Incident Reporting and Response Planning
   g. Communications – Telecommunications; COM-001-1
   h. Communications – Communications and Coordination; COM-002-1
2. Todor Cooklev, “Wireless Communication Standards – A Study of IEEE 802.11, 802.15, and 802.16,” IEEE Press
3. NERC 1200 and CIP-002 through CIP-009 Comparison; Updated: January 30, 2006; Nick Lauriat and Adam Lipson (Network and Security Technologies)
4. FIPS 140-2; May 2001; Security Requirements for Cryptographic Modules
5. Applying NIST SP 800-53 to Industrial Control Systems; Stuart Katzke/et al; National Institute of Standards & Technology, September 16, 2006
6. Government Accountability Office (GAO) report, March 2004, Critical Infrastructure Protection Challenges and Efforts to Secure Control System.

APPENDIX A. CHARACTERISTICS AND USE OF TYPICAL WIRELESS TECHNOLOGIES

A variety of wireless technologies can be used to support communications where wired communication is costly or where mobility is required. Numerous wireless technologies, including mainstream communication devices like cell phones and wireless modem technologies, are presently being used in control center environments. The Critical Infrastructure Protection (CIP) Standards require utilities to identify all of their cyber assets (including wireless devices), list their location, and document their communication within and outside the ESP. To comply with CIP Standards, utilities must monitor and control wireless access to the network using both procedural and personnel controls (e.g., training, awareness, policies, procedures) in addition to technical controls. This includes monitoring both the physical and electronic space around an asset. This appendix introduces the wireless technologies, standards, and protocols that apply to contemporary control room environments, showing at the same time the challenges and possibilities for monitoring for wireless technologies within a CIP-compliant ESP.

Wireless applications vary in range (e.g., short-range wireless sensor networks, local-area data acquisition systems, long-range distributed control systems). Consequently, wireless networks are typically defined by their nominal transmission distances, with wireless personal area networks (WPANs) operating over a coverage area of a few tens of meters, wireless local area networks (WLANs) operating over a coverage area of hundreds of meters, wireless metropolitan area networks (WMANs) covering several kilometers, and wireless wide area networks (WWANs) covering hundreds of kilometers. Much of the success of wireless networks can be directly attributed to the successful development and adoption of the Institute of Electrical and Electronics Engineers (IEEE) 802 standards. Figure A-1 illustrates the relationship of the IEEE 802 wireless standards and their associated technologies.

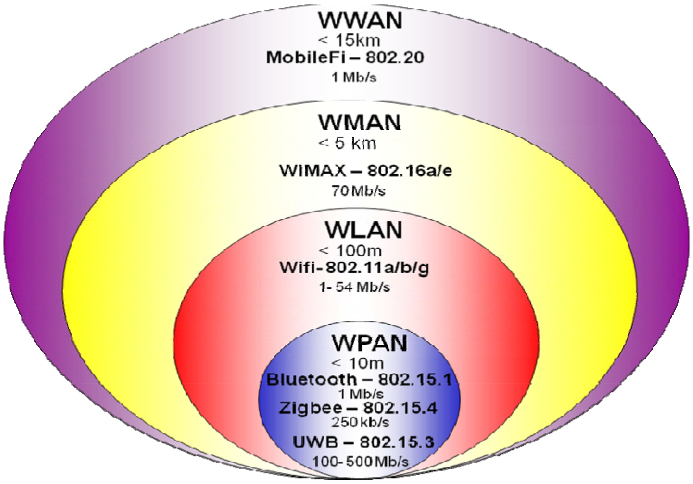


Figure A-1. Wireless standards and associated technologies

WPANs are covered by the IEEE 802.15 series of standards and include the Bluetooth (IEEE 802.15.1), ZigBee (802.15.4), and UltraWideband (UWB; 802.15.3) technologies. Bluetooth is a technology that was developed for short-range cable replacement. Table A-1 describes the various 802.15 networks. A consortium of companies with similar needs, known as the Bluetooth Special Interest Group (www.bluetooth.org), collaborated and decided to generate a new and universal mode for which data transfer could be accomplished without wires and without sacrificing the speed of the transfer. The cornerstone for Bluetooth-compliant devices to date has been their ability to communicate with a personal computer. Bluetooth products include keyboards, mice, printers, and devices that can be used in conjunction with computers, such as personal digital assistants and cell phones. Bluetooth has a data rate of 1 Mb/s and operates in the 2.4 GHz Industrial, Scientific, and Medical (ISM) frequency band.

Table A-1. 802.15 networks

Name	Description
802.15.1	WPAN based on Bluetooth (1.1 and 1.2)
802.15.2	Co-existence of WPAN with other systems in the 2.4 GHz band
802.15.3	High-rate WPAN (11-54 Mbps)
802.15.4	Low-rate WPAN (12-250 Kbps)
ISA100	Wireless standard for industrial automation
Wireless HART	Wireless protocol for process measurement and control

ZigBee is a collection of major corporations committed to standardizing cost-effective, low-power, wirelessly networked monitoring and control products based on an open global standard. IEEE 802.15.4 is supported by the ZigBee Alliance (www.zigbee.org) and targets applications that do not need high data speeds or share large amounts of data. In return, ZigBee devices do not consume large amounts of power. ZigBee devices operate in the 2.4 GHz ISM frequency band at a data rate of 250 kb/s. ISA100 and Wireless Hart are two emerging standards for wireless sensors based on the IEEE 802.15.4 radio. ISA100, developed by ISA (www.isa.org), a leading global nonprofit organization of industrial automation professionals, allows the deployment of a single integrated wireless infrastructure platform that can simultaneously communicate over existing application protocols (e.g., HART, FOUNDATION Fieldbus, Modbus, and Profibus). Wireless HART combines the well-established HART communication protocol with IEEE 802.15.4 radios and is supported by the HART Communication Foundation (www.hartcomm.org), an independent not-for-profit organization providing worldwide support for the HART technology.

IEEE 802.15.3 uses UWB technology for low-cost, low-power, high-speed wireless multimedia applications for portable consumer electronic devices. These applications include wireless connections to surround-sound speakers, portable video displays, flat panel displays, digital video cameras, and digital still cameras. UWB devices also operate in the 2.4 GHz ISM frequency band but at data rates from 100 to 500 Mb/s. The benefits of WPAN include ubiquitous sensing and enhanced process visibility.

Denial of service remains the biggest risk or concern for these low-power devices. With careful implementation, the devices can respond to a denial of service attack by self-locating interference sources and rerouting messages through mesh networking.

WLANs are covered by the IEEE 802.11 series of standards. They are typically called the Wireless Fidelity (Wi-Fi) standards and are supported by the Wi-Fi Alliance (www.wi-fi.org). Table A-2 describes the various 802.11 networks. Three of the Wi-Fi standards are enjoying widespread use today: 802.11a, 802.11b, and 802.11g. The most prominent of the three IEEE 802.11 protocols is IEEE 802.11b, which has been successfully deployed in business offices, university buildings, and homes around the world for many years. IEEE 802.11b can transmit data at rates up to 11 Mb/s and operates in the ISM frequency band at 2.4 GHz. IEEE 802.11a offers a fivefold increase in data rate over IEEE 802.11b by transmitting up to 54 Mb/s. To increase its output bit rate, IEEE 802.11a takes advantage of the 300 MHz of bandwidth available in the 5 GHz Unlicensed National Information Infrastructure (UNII) band. IEEE 802.11g is the most recent standard, and products have been appearing in the marketplace for the last few years. It is capable of maintaining IEEE 802.11a-type data rates up to 54 Mb/s and is essentially a version of 802.11a (with slight differences) placed in the 2.4 GHz ISM band.

Table A-2. 802.11 amendments

Number	Description
802.11a	Phy layer for the 5GHz ISM band, 6-54 Mbps
802.11b	Phy layer for the 2.4GHz ISM band, 5.5 and 11 Mbps
802.11c	Supplement to support MAC bridge operation
802.11d	Specification for operation in different regulatory domains
802.11e	Enhancements for Quality of Service (QoS)
802.11f	Inter access point protocol
802.11g	Phy layer for operation in 2.4GHz band (OFDM)
802.11h	Spectrum and power management operations to 802.11a
802.11i	Security enhancements
802.11j	Enhancement to 802.11a for operation in 4.9–5.0GHz in Japan
802.11k	Radio resource management
802.11m	Technical corrections and classifications
802.11n	High-throughput enhancement (OFDM, MIMO)

Abbreviations:
MAC: media access control
OFDM: orthogonal frequency division multiplexing
MIMO: multiple input multiple output

In the industrial environment, Wi-Fi networks are regularly used for sensor data acquisition, Internet connectivity, and enterprise-wide connectivity. All the laptops used in the field or within control centers are likely equipped with any or all of the WLAN types. While providing mobile/instantaneous Internet access for authorized users within the facility, using WLAN technology poses the biggest risk for unauthorized access to the enterprise or control center networks. A benefit of WLAN technology is rapid Internet connectivity for nonstationary authorized users (e.g., field engineers assembled in control centers during a crisis). The risk includes the potential for unauthorized access to a control center's enterprise network and possible access into the ESP. Careful implementation of defense-in-depth security is required to separate authorized stationary users, authorized nonstationary users, and unauthorized users and reduce the risk of a wireless attack on a control center network.

The IEEE 802.16 standards enable the development of WMANs by incorporating broadband wireless access technology. This technology is typically referred to as Worldwide Interoperability for Microwave Access (WiMAX). The proliferation of WLAN hotspots based on the IEEE 802.11 standards is driving the demand for broadband connectivity back to the Internet, with the term "broadband" simply meaning that the wireless system is capable of delivering a transmission rate greater than 1.5 Mb/s. Originally, the WMAN was intended to be a fixed wireless access system capable of providing the desired last-mile broadband access. WMAN has since developed into broadband access for hard-to-reach areas for wired infrastructure, or where high installation costs make broadband access prohibitive. The IEEE 802.16 standards now include both fixed and mobile wireless broadband technology and are supported by the WiMAX Forum (www.wimaxforum.org). IEEE 802.16a addresses fixed non-line-of-sight point-to-multipoint transmissions in the 2 to 11 GHz band, and IEEE 802.16e addresses portable applications in the 2 to 6 GHz band. Looking toward the future, an emerging IEEE 802.20 working group has been tasked with developing standards for mobile broadband wireless systems designed to be used in WWANs that cover hundreds of kilometers.

CONTROL AND MANAGEMENT OF TYPICAL WIRELESS TECHNOLOGIES

Unintentional noise sources, such as rogue unlicensed ISM-band devices and microwave ovens, can often become wireless network interference sources and can cause noticeable increases in bit error rates. Intentional jamming sources can also be used to target a certain channel or band of frequencies, hence disrupting the network. The networks that are increasingly being used for supervisory control and data acquisition (SCADA) monitoring applications (e.g., IEEE 802.15.1, IEEE 802.15.4, IEEE 802.11, and ISA100) are low-power types and hence use very low radio frequency (RF) transmission power, typically on the order of 0–10 dBm. As a result, an inexpensive jammer for such networks is easy to implement and build with commercial off-the-shelf components. On the other hand, IEEE 802.11 networks can severely degrade the performance of IEEE 802.15 networks if their deployment is not efficiently planned (coexistence issues).

Figure A-2 shows a frequency sweep of wireless networks from 150 kHz to 3 GHz. RF detection systems, while expensive, can be constructed to monitor activity in multiple bands of operation (using multiple receiver hardware) and digitally search for unauthorized access and suspicious activity patterns. Table A-3 describes the frequency ranges of some of the popular wireless networks. Signatures exist for each of the network types and describe their operational activity. Figure A-3 shows the frequency and a spectrogram of an 802.11b waveform centered at 2.41 GHz. The spectrogram provides the frequency vs. time snapshot. The channel occupancy pattern is derived from the transmission duty cycle (e.g., beacons, data, sync). Sophisticated pattern recognition systems can be deployed to observe the RF activity to comprehensively monitor authorized and unauthorized channel access. The RF emissions from a transmitter are typically nonstationary, and the signal statistics can provide spatial and temporal data to identify the transmitter (including the make and model). Similarly, noise floor analysis can detect wideband transmitters. Techniques can be developed to snapshot the baseline model of a plant’s RF activity and to monitor its spectrum for abnormalities.

Several commercial off-the-shelf tools exist for 802.11-based networks for developing OSI layer-2-based and layer-3-based IDS (e.g., Kismet, AirDefense, Cisco). These tools can be effectively used in conjunction with RF monitors to detect rogue devices that are, for example, spoofing Media Access Control (MAC) addresses, dual port operations, or unauthorized access.

Technologies exist for developing layer 1 and layer 2 and above IDS. System-level integration and algorithm development are required to design and deploy comprehensive IDS to monitor wireless networks of interest.

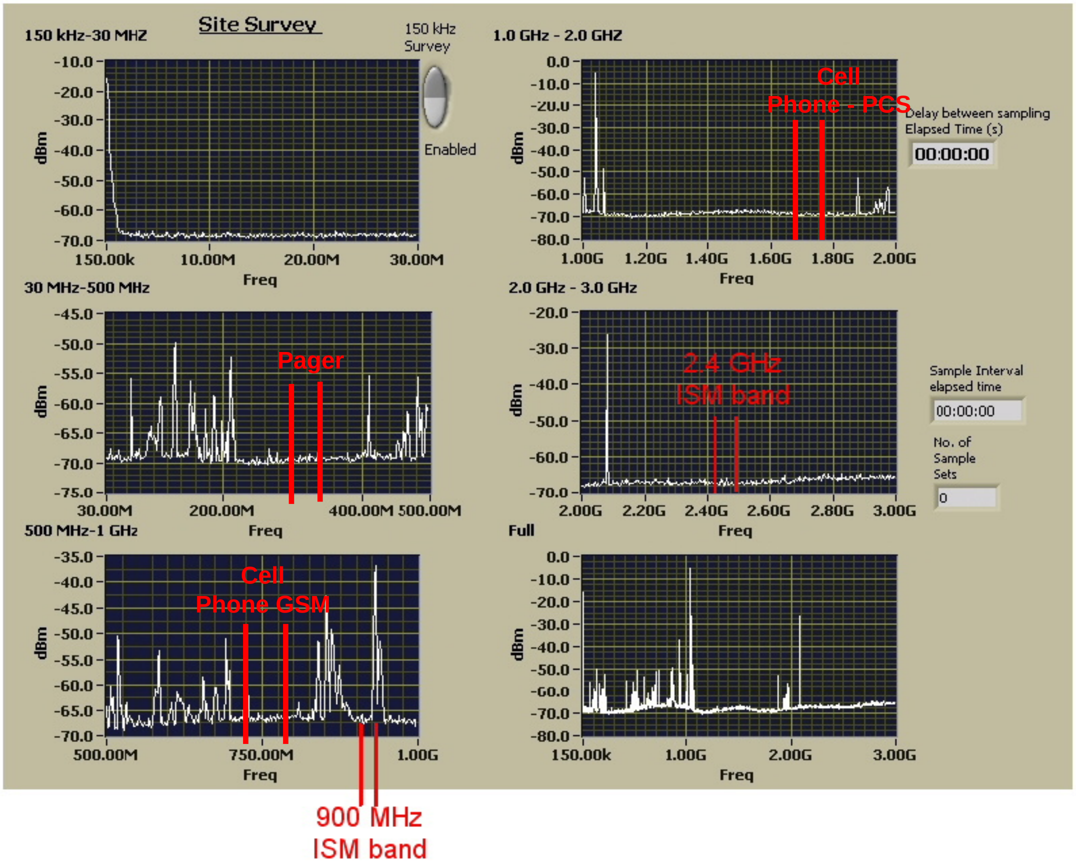
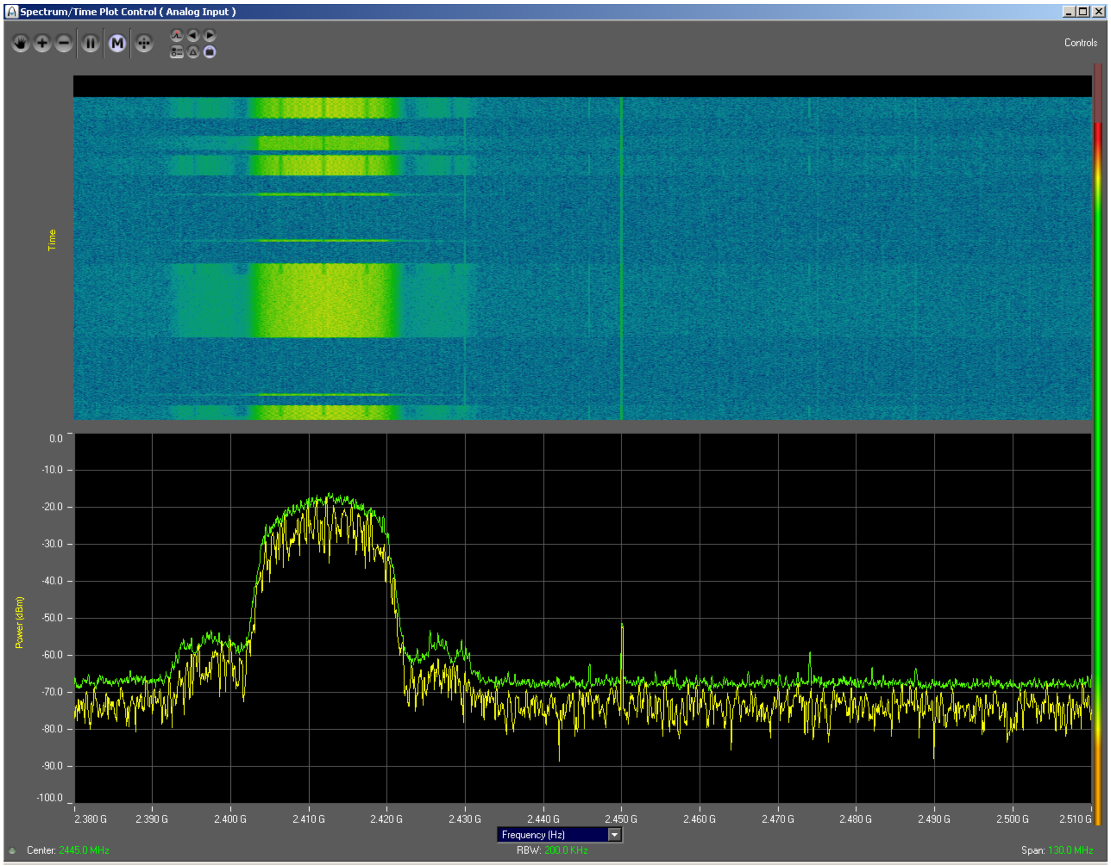


Figure A-2. Frequency sweep of 150KHz – 3GHz

Table A-3: Frequency ranges of operation for popular wireless networks

Technology	Frequency Bandwidth	Application
AMPS, GSM, IS-95 (CDMA), IS-136 (D-AMPS)	824-849 MHz 869-894 MHz 896-901 MHz 935-940 MHz	Cell phone data and communication networks
	1850-1910 MHz 1930-1990 MHz	Personal communication networks
3G, 4G	698-806 MHz 1710-1755 MHz 2110-2170 MHz	Advanced wireless services
4G	2500-2690 MHz	Cell phone – multimedia, digital video, etc.
ISM*	433.05–434.79 MHz 902–928 MHz 2400–2483.5 MHz 5725–5875 MHz	

*Other, less popular ISM bands include 0.765–6.795 MHz, 13.553–13.567 MHz, 26.957–27.283 MHz, 40.66–40.70 MHz, 24–24.25 GHz, 61–61.5 GHz, 122–123 GHz, 244–246 GHz



Center: 2445.0 MHz
RBW: 200.0 KHz
Span: 130.0 MHz

Figure A-3. Time-frequency sweep of 802.11b network