Wireless Network Security in Nuclear Facilities*

J. Dion
United States Nuclear Regulatory Commission
Office of Research
Washington, DC 20555-0001
Jad4@nrc.gov

M.K. Howlader and P.D. Ewing
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37831 USA
howladermk@ornl.gov; ewingpd@ornl.gov

ABSTRACT

The U.S Nuclear Regulatory Commission (NRC) and Oak Ridge National Laboratories have been researching wireless communications as an emerging technology in nuclear facilities. This research is aimed at developing technical bases for regulatory guidance applicable to wireless technologies. A key element of regulatory guidance will be whether or not nuclear facilities can demonstrate data flowing in their wireless networks are secure. Wireless communications technology is not currently used in safety-related systems in nuclear facilities but is being used in non-safety related and business applications, many of which have not been under the purview of NRC's regulatory authority. In 2009, the NRC issued a cyber security rule requiring licensees to provide high assurance that critical systems and networks are adequately protected from cyber attacks [10 CFR 73.54]. Non-safety wireless networks that provide a potential pathway to critical digital assets must also be secured according to guidance set forth in Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities." If the nuclear industry continues to embrace the use of wireless communication technology, there could be more critical digital assets impacted by wireless systems.

The paper addresses the security issues of wireless networks relevant to instrumentation and control (I&C) applications in nuclear facilities. After presenting the relevancy of wireless systems in NPP, the paper briefly addresses the concerns about cyber security, wireless network security (WNS), and the necessary security controls. Finally, the paper presents the fundamental recommendations from Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities and their application to wireless systems.

Key Words: wireless network security, wireless communication, cyber security, nuclear facilities

* Disclaimer: This paper represents the personal opinions and viewpoints of the authors and is not intended to represent any official position of the U.S. Nuclear Regulatory Commission.

1 INTRODUCTION

The NRC has recognized wireless communications as an emerging technology for the nuclear industry. Wireless system security is of utmost importance for applications at nuclear facilities. Although wireless communications are not yet used for safety related or important to safety functions, one day they could be if they can be proven to meet the requisite design criteria. Although there are many technical issues with deploying wireless technology in nuclear facilities, this paper focuses only on the security issues.

The scope of the research has been focused on reviewing the state of the art in wireless network security (WNS) and studying the current WNS used to protect government and industrial systems. Wireless network vulnerabilities that may impact secure network operations were also investigated. Best practices and future directions will have been mapped into the nuclear environment and applied to recommendations for WNS at nuclear facilities.

1.1 Background

Recently, increasing numbers of wireless communications systems have been deployed in industrial environments such as nuclear facilities, where they are mainly used for monitoring purposes. When compared with wired systems, wireless systems have a number of benefits (e.g., lower installation and maintenance costs, reduced connector failure, and rapid deployment) [1-3]. Most wireless systems are based on new technologies, including wireless fidelity (Wi-Fi) (IEEE 802.11), Bluetooth (IEEE 802.15.1), and ZigBee (IEEE 802.15.4) [4].

The NRC has funded research of wireless communication technology as an emerging technology for nuclear facilities for several years. NUREG/CR-6882, "Assessment of Wireless Technology in Nuclear Facilities," documents the state of wireless technology in the 2003-2005 timeframe [5]. This document reviews the wireless standards in use during that time period, as well as the new standards under development. The report also discusses the deployment issues related to the use of wireless technology within nuclear facilities, deliberates on the potential impact of wireless technology on existing safety-related systems, and identifies potential resolutions for the suggested deployment issues. NUREG/CR-6939, "Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment,"details an interference study of the three most prominent wireless devices in the 2003-2006 timeframe, using computer models and simulations [6]. The goal was to determine whether Bluetooth, Zigbee, and Wireless Fidelity (WiFi) wireless devices could coexist in an industrial environment. The issue of wireless network security has not been thoroughly addressed by past NRC research for wireless technology.

Several advances in the area of cyber security regulations and guidance have been made over recent years. In 2009, the NRC issued a new cyber security rule requiring licensees to provide high assurance that critical systems and networks are adequately protected from cyber attacks (10 CFR 73.54) [7]. The NRC staff also issued guidance in Regulatory Guide 5.71, "Cyber Security Plans for Nuclear Facilities, [8]. While the approach in RG 5.71 is applicable for both wired and wireless networks, the special considerations for wireless security are not specifically called out.

Wireless networks include small operators and community networks, cellular networks over shared spectrum, mesh networks, ad hoc networks, and personal area networks. Initially, the networks were mostly centralized, but they have since been followed by the distributed type. They are now moving toward self-organizing networks capable of adjusting themselves, or at least requiring minimum human interaction, for optimum network efficiency. Hence, security architectures must be redesigned accordingly because the increasing programmability of the devices increases the risk of attacks. The

growing number of small, embedded computing devices will likely lead to additional vulnerabilities and new attacks. As networks are changing from fixed to ad hoc, increasing the "security distance" between devices and infrastructure will lead to an increased temptation for cyber attacks.

1.2 Wireless technologies in Nuclear Facilities

Although wireless devices are increasingly being used in nuclear facilities, in general, they are not being used for the transfer of safety critical data. However, the NRC anticipates the nuclear industry to consider plans to substantially expand the use of wireless systems in applications such as data transmissions that affect systems or functions which must be protected under the cyber security requirement, 10 CFR 73.54. Existing non-safety wireless systems, which potentially provide a pathway to wired critical digital assets, should also be protected critical digital assets even if those wireless systems are not directly performing a safety, security or emergency preparedness function.

The current use of wireless communications deployed in nuclear facilities is limited to nonsafety-related and business applications. Present applications of wireless communications in power generation facilities include voice and data communications to employees and field crews, distribution of supervisory control and data acquisition to substations and line devices, wireless local area networks (WLAN) devices for office use, automated intelligent metering, work management based on the geographical information system, alarm systems, and emissions monitoring.

Wireless systems are considered intentional emitters and should adhere to the exclusion zone guidance set forth in Regulatory Guide 1.180 [9]. Unlicensed wireless devices (i.e. wireless access points, laptops, wireless sensors) operate under 1W power restrictions, equating to an exclusion zone of less than 1 meter. Two-way radios and cell phones with higher power outputs may have exclusion zones equating to several meters.

For safety-related applications, wireless may one day be a candidate for safety system communications for process control, however they would also have to satisfy the NRC regulations in Part 50, "Domestic Licensing of Production and Utilization Facilities," of Title 10 of the Code of Federal Regulations (10CFR50) [10]. The existing regulatory framework, as described in Chapter 7 of the Standard Review Plan (NUREG 0800) [11], for safety-related digital computers and communications would also apply for safety-related wireless systems.

Although wireless communications could be an option for safety-related I&C applications, there has been no industry study addressing that issue. In addition, there are no other known examples of safety critical wireless applications in other industries. However, the safety issue and analysis framework for wired networks may be fully compatible and applicable for wireless communications. Wireless communications do not bring any new types of communications errors. The common error types for wired systems (repetition, deletion, insertion, incorrect sequence, corruption, delay, too early, jitter, masquerade, and inconsistency) cover all communication errors of wireless systems as well. One difference is that the probabilities of the various error types are different in wireless systems. For example, a corruption error is more probable due to higher bit error rates caused by a fading environment, mobility, and interference from other wireless users. Short-term deletions occur more often due to poor connections. It can also be anticipated that a masquerade error is more likely because the air interface is more vulnerable to intentional or unintentional jamming. Therefore, authentication and cryptographic techniques are more likely to be needed if a wireless communications system is applied.

2 NETWORK SECURITY FOR WIRELESS SYSTEMS

2.1 General Cyber Security

In general any information system incorporating wireless technology should fulfill some basic security objectives. The typical taxonomy of security properties can be described by confidentiality, integrity, and availability (CIA). The relative importance of these security parameters in process control is different from that in information technology applications. The relative importance of CIA is also related to the criticality and performance requirements of the specific application. Violations of these security parameters typically arise through known attack mechanisms. These attacks can be categorized in terms of attackers' function. A useful categorization of these attacks is in terms of passive attacks and active attacks.

Most passive attacks on wireless networks involve an attacker with access to the wireless link. In passive attacks, the attacker monitors network communications for data, including authentication credentials or transmissions that identify communication patterns and participants. Regardless of the network types, these passive attacks can occur at any point in the wireless link. Active attacks rely on an attacker's ability to intercept and inject network communications. Active attacks can also include intentional jamming of wireless transmissions. Attackers can alter the message by deleting, adding, or changing it. The basic security control features include encryption, cryptographic hashes, device authentication and data origin authentication, replay protection, wireless intrusion detection, and physical security. All of these measures, especially various encryption and authentications, intrusion detection, and physical security, jointly secure the wireless networks.

2.2 Wireless Security Concerns

Wireless networks have no inherent physical protection. Physical connections between devices are replaced by logical associations. Physical access to the network infrastructure (e.g., cables, hubs, and routers) is not required for sending or receiving messages. Wireless usually means radios, which broadcast through the air. Thus, transmissions can be overheard by anyone within range. Although it is not the typical case, an intercepting receiver can receive the target signals because standardized commercial communication protocols are readily available. Also, anyone can generate transmissions that can interfere with other nearby transmissions or prevent their correct reception (jamming). The Federal Communications Commission (FCC) only regulates products sold in the US and a jamming radio can easily be built if all of the information about the communication protocols is available. Of course, the jammer or the interceptor has to be in close proximity for adequate reception of the signal. Thus, a secure communication system should not be built using commercially available wireless devices. Best practices from the Department of Defense should be adopted for using commercial wireless devices or in-house devices. Eavesdropping, injecting harmful messages into the network, replaying previously recorded messages, unauthorized access to the network and its services, and denial-of-service by jamming are all easier in wireless networks. In addition, all the vulnerabilities that exist in a wired network also exist for a wireless network.

Although wired and wireless networks face similar vulnerabilities to attack, there are some fundamental differences between the significance and the nature of the threats and their detection. Attacks on a wired network can originate at remote locations of the wire, whereas the attacking points on the wireless network need to be local and within range of the attacker's wireless devices. The local attacker can, however, be positioned anywhere within range. This relative ease of access to a wireless network makes the detection of an attacker more challenging. The security features of a wireless network are

typically weaker because wireless networks usually can afford fewer resources and wireless devices are less computationally complex.

Since wireless signals are broadcast, each packet that arrives at a receiver is of unknown provenance and must be verified for authenticity. Even if authenticity is verified at the beginning of a session, an intruder could still potentially hijack the session. Information transmitted with weaker encryption or without encryption is vulnerable to interception. Also, an intruder can use a wireless connection to bypass firewall protections and thus obtain unauthorized access to protected information assets.

2.3 Security controls for Wireless Networks

The security concerns discussed in the previous section require various remedies, including confidentiality, authenticity, integrity, access control, replay detection, and protection against jamming, for ensuring proper information transmission. First, messages sent over wireless links must be encrypted to maintain confidentiality, because information transmitted with weaker or no encryption is vulnerable to interception by an intruder, and the origin of messages received over wireless links must be verified for authenticity. Then, the integrity and the freshness of messages received must be verified. Also, access to network services should be provided only to legitimate entities. However, it is not enough to check the legitimacy of an entity only when it joins the network and its logical associations are established because logical associations can be hijacked.

Current state-of-the-art practices in wireless security rely on vendors to supply robust security protocols for wireless devices to guard against potential attacks and, in the case of a security breach, to detect and prevent the attack. It falls to individual organizations to adopt security measures and practices according to their security needs. The Federal Information Security Management Act requires that all federal agencies (U.S. civilian departments, agencies, and government/agency contractors) develop and implement agency-wide information security programs to safeguard their information technology assets and data. Federal Information Processing Standard (FIPS) 199 [12] offers a standardized methodology to assess the risks to the confidentiality, integrity, and availability (CIA) of unclassified systems. The NIST SP 800-53 sets the baseline management, operational, and technical controls that must be incorporated into a system to minimally ensure the security of low-, moderate-, and high-risk systems [13]. Before the deployment of a wireless network, an organization should assess its security needs and the possible consequences of a security breach. In performing the assessment, the organization should consider existing security policies, known threats and vulnerabilities, legislation and regulations, safety, reliability, system performance, security related life-cycle costs, and technical requirements.

The deployment strategy for wireless systems is quite different from that of wired systems. At a minimum, it is recommended that the following steps be implemented, in order, before any deployment of a wireless system.

- Determine the quality of service (QoS) to be provided (i.e., the guarantee of a certain level of performance for the particular wireless application).
- Select the wireless technology and protocols.
- Select network topology and information formats.
- Choose between licensed, unlicensed, or combination systems.
- Obtain complete information (terrain data) about the deployment environment’s large-scale fading characteristics.
- Use models to study the performance of the system. Example models include Hata and Nakagami.

- Study the coexistence performance of the system. These coexistence studies are available from standards organizations, e.g., IEEE and NIST.
- Analyze the cyber security of the system thoroughly according to the needs of the organization. Regulatory guides and related policy recommendations detail the defined goal and the process to obtain cyber security. Is the system adequate to fulfill the cyber security requirement?
- Measure the system performance and adjust the design. The performance matrices include QoS, BER, delay, and throughput. A Monte Carlo experiment can be conducted to measure the appropriate metric. Adjusting the position of the wireless devices, the network architecture, or device parameters (code rate, antenna gain, filters taps, etc.) might improve the performance.
- Perform an integrity check of the system by perturbing the input parameters. Input parameters include antenna alignment, distance between two wireless devices, transmitted power, and available BW.
- Use simulations to address "what if" scenarios. Undesired cases, including some extreme scenarios, can be evaluated using simulations without suffering the consequences of an actual test. Test cases include maximum transmitted power, optimal positioning of the receiver, and DoS.
- Ensure that the system meets all the redundancy requirements to obtain the required reliability value.
- If replacing an existing wired system, involve the system's experts early enough in the process to maintain similar security for the system. For example, IT personnel can help to determine any changes in the existing security due to wireless deployments.
- Deploy the system and perform a final evaluation. For example, can the system transmit a minimum data rate of 10 Mbps over 1 km if that is required?
- Ensure that at no point will the wireless transmitter power be permitted to exceed the maximum allowable power. This is generally regulated by the standards organizations and assured by the device manufacturers. Attempts to exceed this limit during operation might cause interference to other users/devices.

Any addition or modification to the system would engender coexistence and cyber security studies as if it were a new system. NIST SP 800-48, 48 (rev 1), 94, 97, and 98 detail various recommendations for WNS, especially for IEEE 802.11, Bluetooth, and RFID devices [14-18]. Many of the specific details of the security protocols discussed in this report are derived from those documents and their original references.

Many of the security features are available in open network standards such as IEEE 802.11i [19]. The standards provide various options for some features, according to system needs. Some of the features also have upgrade options to improve the overall security. However, the guidelines in the NIST recommendations and the IEEE standards are general and might require altering according to an organization's security needs. Security challenges are increasing because wireless technologies are changing rapidly and newer systems, with more capabilities, are continually emerging. As a result, the standards themselves and the associated recommendation guides also need frequent revisions. Standards and related documents are typically for information only, and every organization should have its wireless network policy tailored to its security needs, although in reality, many of the security features are shared by most organizations and can be supplemented with a few specific ones.

Neither this report nor the referenced NIST documents establish minimum standards of acceptable risk or a specific set of mitigation measures that must be used. Any set of specific standards would be rapidly outdated as wireless technologies changed, new threats emerged, new mitigation tools became available, and regulatory requirements changed. The emphasis in this document is on the existing practices of WNS

that can be applied for nuclear facilities. The following are basic security control features for all wireless networks [17, 15].

1. **Encryption of communi cations**—using cryptography to encrypt wireless communications prevents exposure of data through eavesdropping.
2. **Cryptographic hashes for communications—** calculating cryptographic hashes for wireless communications allows the device receiving the communications to verify that the received communications have not been altered in transit, either intentionally or unintentionally. This prevents masquerading and message modification attacks.
3. **Device authentication and data origin authentication—** authenticating wireless endpoints to each other prevents man-in-the-middle attacks and masquerading.
4. **Replay protection—**adding devices such as incrementing counters, timestamps, and other temporal data to communications to detect message replay.
5. **Wireless intrusion detection—** monitoring events in network or computer systems and analyzing them for a possible violation of the network security or simple standard policies.
6. **Physical security—**limiting physical access within the range of the wireless network to prevent some jamming and flooding attacks.

3 CYBER SECURITY PLANS

Regulatory Guide (RG) 5.71, *Cyber Security Programs for Nuclear Facilities,* provides an approach that the NRC believes is acceptable for meeting the requirements of 10 CFR 73.54: provide high assurance that digital computer and communication systems and networks within nuclear facilities to be adequately protected against cyber attacks [7, 8]. This requirement is applicable to systems/networks associated with (1) safety-related and important-to-safety functions, (2) security functions, (3) emergency preparedness functions, including offsite communications, and (4) the functions of any support systems or equipment that could adversely impact safety, security, or emergency preparedness functions. RG 5.71 provides guidance for licenses to establish, implement, and maintain a comprehensive cyber security program that includes cyber controls, defense-in-depth strategies, attack mitigation measures, and incident response and recovery processes. The technical basis for RG 5.71 encompasses related NRC orders, reports, and regulatory guides, as well as special publications by the Nuclear Energy Institute (NEI), the Institute of Electrical and Electronics Engineers (IEEE), and the National Institute of Standards and Technology (NIST).

Irrespective of the communication media—wired, wireless, or both—the security measures described in RG 5.71 are the guiding principles for network security in nuclear facilities. Though not specifically called out, many of the security control techniques and network management methods developed for wired networks are also useful for wireless networks. However, the primary difference is that information from the various units in wireless networks uses a shared medium rather than a designated path, and interference abatement is a dominant design issue. This makes the wireless network architecture and security implementation different from that of the wired network. Indeed the types of attacks on wireless networks are essentially the same as those on wired networks, but the techniques might differ. The overall guidance in RG 5.71 applies to wireless networks and can appropriately be supplemented with additional guidance on the issues specifically applicable to wireless networks.

3.1 Defense in Depth Strategy

In general, nuclear facilities need to deploy a protection strategy for their communications infrastructure that incorporate multiple layers of defense, to and including the protection of wireless

devices. To that end, achieving a defense-in-depth strategy will require several complementary steps. First, for the overall system design, an internal zone of defense with various intrusion detection techniques should be used to detect and prevent security breaches in the event of the failure of the security controls at the boundary. Second, boundary security measures should not be limited to monitoring business-process transaction links, but should also include peripheral process control links, as an insider attack might be originated within the facility. Finally, some form of security should be implemented at the device level by the manufacturer, and these inherent device-level security capabilities should be tested before actual deployments.

3.2 Deployment of wireless nuclear facilities

RG 5.71 recommends that a licensee conduct a site-specific analysis of digital computer and communications systems and networks to identify critical digital assets (CDAs). A CDA may be a wireless network, which is essentially a wireless pathway. Since a wireless communications pathway is a shared medium characterized by its surroundings, an accurate propagation study of the site is necessary before the deployment of the network. For wireless networks, site-specific analyses are very critical before and during their operation. Any changes in the facility layout might change the wireless communication channel and an update of the analysis should be recorded in the event of changes in the surroundings. The wireless medium is interference and fading limited. Thus, the deployment of new equipment or updates in existing equipment should not cause interference to the overall wireless network.

3.2.1 Physical Security

Wireless networks have no inherent physical protection. Physical connections between devices are replaced by logical associations. Physical access to the network infrastructure (e.g., cables, hubs, and routers) is not required for sending or receiving messages. However, given these concerns, one method to secure wireless networks is physical security or distance. For example, if wireless sensors are used inside of a metal building, it should be quite difficult for an adversary to intercept the communications if he or she can be kept out of the building. Even if the wireless transmitters are not protected by a metal shield, distance can be an effective shield. If the strength of the transmitter and the perimeter distances are such that the signal strength outside the perimeter is sufficiently low, it should also be quite difficult for an adversary to intercept the signals.

3.2.2 Directional Transmission and Low Power Signals

Another method that can be used is directional transmission. Transmitting the data directly towards the intended receiver reduces the locations from which the transmissions may be received. If this method is combined with low power signals, it can be even more effective. A further optimization of this technique could involve multiple access points utilizing phased array antennas. The signal can be multiplexed between the access points so that parts of the signal are transmitted from each access point directly toward the receiver. In this way, an eavesdropper would not be able to intercept the entire signal without having at least one antenna located in line with each transmitter and receiver.

3.3 Deployment of wireless in nuclear facilities

The following are two hypothetical scenarios for deploying wireless in nuclear facilities: (1) the deployment of wireless for non-safety systems and (2) the deployment of wireless for safety systems. Each scenario refers to the concentric cyber security defensive levels described in RG 5.71 which correspond to the physical security areas at a nuclear facility.

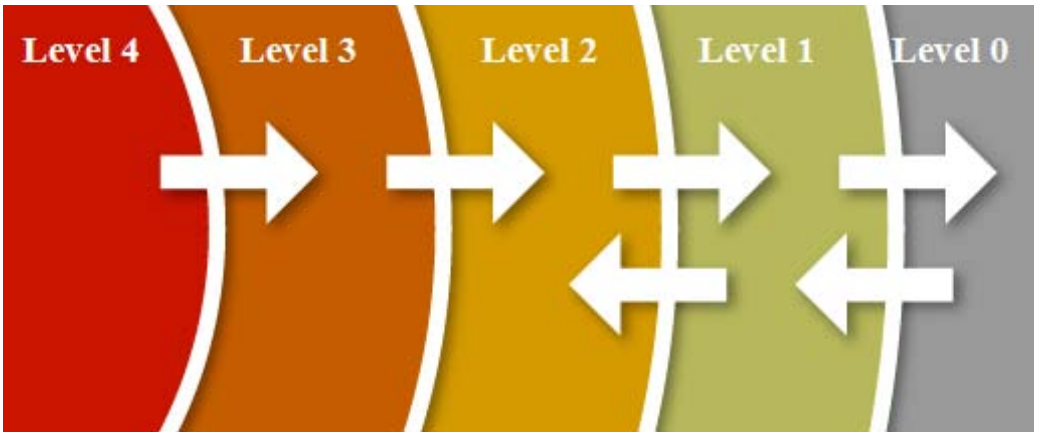

Figure 1 Simplified cyber security defensive architecture (from RG 5.71) [8]

3.3.1 Deployment of non-safety wireless I&C systems

RG 5.71 recommends prohibiting the use of wireless technologies for CDAs and ICSs associated with safety-related and important to safety functions. However, a licensee might have wireless CDAs for non-safety systems. For non-safety wireless CDAs, data from a wireless network will go into a security control device at the wireless to wired network boundary. This control device can completely block the incoming wireless signals and therefore address concerns with interference and interception. However, wireless communications networks might be used to deliver data required by CDAs and ICSs outside of the security boundary. The required reliability of the wireless CDA link should be commensurate with the reliability of safety related communications, as described in DI&C-ISG-04 [20], because the accuracy of the data delivered to the CDAs and ICSs is critical for maintaining the security at the boundary.

Although the CDAs and ICSs located in levels 3 and 4 are not utilizing any wireless technology, these logical boundaries might allow data flowing from wireless devices through their security control devices. For example, a safety system in level 4 might broadcast non-safety information through a wireless link to systems in level 3. Of course, this data will not flow through the safety network or should not have any role in safety decisions. Another example is for wireless CDAs located in levels 0-2. For this case, an appropriate decision strategy should be established before accepting the data. If the data meet the appropriate reliability, survivability, and quality of service (QoS) values, the data should be acceptable. These wireless devices should employ proper security controls, e.g., robust firewalls and sophisticated intrusion detection and prevention techniques for the real-time monitoring of data.

Since wireless networks might deliver data to CDAs and ICSs for non-safety systems inside and outside of the logical boundary of the safety system, the reliability of the data and the wireless network are important. The wireless network architecture is also important because gradual levels of security measures can be established within the wireless network itself. More vulnerable and flexible portions of the network should be located at the lowest security levels. The physical boundary should be placed at the higher levels to prevent interception. The wireless medium inherently prevents remote interception because the wireless signal's power level drops off rapidly with distance. Proper network management and strict access regulation (the need-to-know rule) will minimize the interception of the signal. The physical and administrative security controls should be implemented jointly with the physical security program.

Communications networks typically consist of wireless links and non-wireless (wired) links. If the design protocols are open to adversarial attack, wireless links might be more prone to interception.

However, techniques are available to monitor and secure the wireless segments of the overall communication network. Advanced encryption and intrusion detection techniques can be used to make a wireless link highly reliable. Also, physical security can augment network security. The reliability of the link can meet the DI&C-ISG-04 recommendations by using the appropriate communication protocols. Since the communication medium is invisible, a physical attack to the medium (cutting the wire) is not possible. Several proven sources of diversity (space, time, frequency, code, polarization) can be used to improve the probability of interception significantly. The integration of diversity, security controls, and intrusion detection can build a trustworthy (reliable, resilient, and secure) wireless link.

3.3.2 Potential deployment of safety-related wireless critical digital assets

Wireless systems can be highly reliable, robust to jamming, and have a significantly low number of errors, which might lead to the conclusion that they could be acceptable for functions associated with safety systems.

Consider a hypothetical scenario where wireless technology will be used for safety and important to safety systems located in levels 3 and 4 of the logical boundary of the network security controls. These wireless environments can be treated as large industrial deployment sites. Accurate channel modeling is the first step in deploying a wireless system, as described in Chapter 5 of NUREG/CR-6939, "Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment," [6]. When infrared and free-space laser communications are used, there is no need for a channel modeling study because the signal always has a line-of-site (LOS) path, though these are wireless systems too.

The mobility of wireless devices, such as laptops and wireless sensors, should be minimized because physical movement might impact the network performance. For example, if Bluetooth or Zigbee wireless devices are used for collecting sensor data or connecting closely located wireless devices, their position can change within the range of the connecting wireless devices as long as their new location does not suffer more interference from nearby wireless devices or more fading from nearby obstacles (i.e. steel beams, concrete wall, etc). Therefore it is desirable to limit the mobility of wireless devices used in important to safety and safety-related systems.

Properly designed or selected protocols for wireless devices could possibly satisfy the QoS requirements of safety and safety-related systems. Various error types and QoS of safety and safety-related systems for digital I&C are described in NUREG/CR-6991, "Design Practices for Communications and Workstations in Highly Integrated Control Rooms," [21]. Potential wireless communication systems for important to safety and safety systems must guarantee these criteria.

Diversity is a design objective of the communication network in safety systems for improving robustness and reliability. Wireless protocols can choose the most desired diversity technique or multiple ones among the numerous available options. These include time, space, code, frequency, polarization, and relay for the physical layer and various network architectures, such as mesh, at the network layer. Interference and interception are the two main constraints in the development of wireless protocols. Unintentional interference is a design issue which can be overcome with the design of a robust transceiver system and its proper deployment. Intentional interference is a security challenge which can be controlled using the combination of various techniques. Anti-jamming is widely used in military communication systems. Adversaries can build a jamming transmitter if the protocols are known to them. A secure version of commercial protocols should be used or proprietary standards should be developed for the wireless communication systems in safety systems. Again, military communication systems are built on this principle. The main objective is to keep the protocols unknown to adversaries and include enough randomness in the design that even a known protocol is hard to jam, e.g., as with spread spectrum systems. Finally, wireless signals are generally secure from adversaries located outside of the wireless system's physical range of operation. Although it is theoretically possible for a remotely located

adversary to intercept or interfere with wireless signals, the likelihood of a successful interception or interference is significantly low. Physical security and the security policy in levels 3 and 4 can augment the network security to minimize the probability of jamming. Also, at some carrier frequencies signals attenuate rapidly, thus secure communication systems can be designed at these frequencies. Of course, other parameters, such as reliability and QoS, also need to be considered when selecting the carrier frequency, modulation and coding techniques, the network architecture, and security controls. Finally, robust intrusion detection techniques should be deployed for protecting wireless installations.

In summary, the three issues of highest concern for wireless communication systems are fading and multipath, interference, and interception. In turn, these issues can be overcome by accurate channel modeling, anti-jamming, and intrusion detection techniques, respectively. Wireless systems can be designed with better and robust diversity techniques compared to those of wired system. Thus, wireless systems can offer improved reliability and more operating flexibility. However, wireless safety systems will have to meet the extensive regulatory requirements in place for safety systems under 10CFR50 [10]. These requirements can be found in Chapter 7, Instrumentation and Controls, of NUREG-0800 and include design criteria, acceptance criteria, and guidance for evaluation of conformance [11].

4 CONCLUSION

The NRC has recognized wireless communications an emerging technology in the nuclear industry. The many benefits of wireless communications must always be appropriately balanced with safety and security requirements. If the nuclear industry continues to embrace the use of wireless technology, adequately protecting critical systems and functions at a nuclear facilities will be become a high priority. Under the current security requirements, some non-safety wireless systems may also need to be secured to protect wired critical digital assets.

Current industry best practices do not address availability (denial-of-service), non-repudiation, or traffic analysis for Wi-Fi networks. If these security services are required in a nuclear facility, additional layers of network security above and beyond commercial best practices would be required

It is important to note that security protocols and practices deemed effective today will be outdated in few years. New vulnerabilities in emerging hardware, software, and protocols will be discovered, and tools will be published allowing unsophisticated attackers to break into networks still using dated equipment and protocols. Thus, even if wireless solutions are deployed securely at the outset, unless provisions are made to patch, maintain, and update the wireless systems, their security posture will degrade over time.

For additional offerings of improved performance, the core technologies for wireless communications are rapidly changing, sometimes with a new paradigm of solutions. These changes pose increased security challenges for wireless networks.

The NIST 800.x documents represent the current best understanding of wireless network security for several types of wireless applications [13-18]. These documents recommend that if the very latest protocols are implemented, taking into account subtle implementation considerations, then wireless systems can be deployed with reasonable confidence that authentication, access control, and message confidentiality can be achieved.

5 REFERENCES

1. Willig, K., K. Matheus, and A.Wolisz, "Wireless technology in industrial networks," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1130–1151, June 2005.
2. Pellegrini, F., et. al., "On the use of wireless networks as low level of factory automation systems," *IEEE Transactions on Industrial Informatics*, vol. 2, no. 2, pp. 129–143, May 2006.
3. Tang, K., K. Man, and S. Kwong, "Wireless communication network design in IC factory," *IEEE Transactions on Industrial Electronics*, vol. 48, no. 2, pp. 452–459, April 2001.
4. Laboid, H., H. Afifi, and C. D. Santis, *Wi-Fi, Bluetooth, ZigBee, and WiMaX*, Springer, 2007.
5. *Assessment of Wireless Technologies and Their Application at Nuclear Facilities*, NUREG/CR-6882, Oak Ridge National Laboratory, July 2006.
6. *Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment*, NUREG/CR-6939, Oak Ridge National Laboratory, July 2007.
7. "Protection of Digital Computer and Communication Systems and Networks," Code of Federal Regulations, Title 10, Part 73, Section 54.
8. Regulatory Guide 5.71, Rev 1, *Cyber Security Programs for Nuclear Facilities*, January 2010.
9. Regulatory Guide 1.180, Rev. 1, *Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems*, U.S. Nuclear Regulatory Commission, October 2003.
10. "Domestic Licensing of Production and Utilization Facilities," Code of Federal Regulations, Title 10, Part 50.
11. Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, NUREG-0800, March, 2007.
12. Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199, National Institute of Standards and Technology, February 2004.
13. Recommended Security Controls for Federal Information Systems, NIST 800-53, National Institute of Standards and Technology, February 2005.
14. Wireless Network Security for 802.11, Bluetooth and Handheld Devices, NIST SP 800-48, National Institute of Standards and Technology, November 2002.
15. Wireless Network Security for IEEE 802.11a/b/g and Bluetooth, NIST SP 800-48 (rev. 1), National Institute of Standards and Technology, August 2007 (draft).
16. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, NIST SP 800-97, National Institute of Standards and Technology, February 2007.
17. Guide to Intrusion Detection and Prevention Systems (IDPS), NIST SP 800-94, National Institute of Standards and Technology, February 2007.
18. Guidelines for Securing Radio Frequency Identification (RFID) Systems, NIST SP 800-98, National Institute of Standards and Technology, April 2007.
19. Black, U., *Network Management Standards: SNMP, CMIP, TMN, MIBs, and Object Libraries*, McGraw-Hill, New York, NY, 1995.
20. Interim Staff Guidance 4, "Highly Integrated Control Rooms- Digital Communication Systems." Revision 1, March 2009.
21. "Design Practices for Communications and Workstations in Highly Integrated Control Rooms," NUREG/CR-6991, February 2009.