United States Nuclear Regulatory Commission
Protecting People and the Environment

TECHNICAL LETTER REPORT
TLR-RES-DE-2024-005

Analyzing the Impact of Using Wireless Technologies for Monitoring Safety-Related Critical Digital Assets

February 2024

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

E. Martinez Rodriguez, E. Lee, M. Fernandez, T. Marshall
U.S. Nuclear Regulatory Commission

A. Konkal, B. Barro
Oasis Systems, LLC

DISCLAIMER

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

CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENTS

The authors would like to acknowledge the hard work and commitment of all contributors to the research. The authors would also like to thank Leroy Hardin, Michael Brown, Kim Lawson-Jenkins, Ismael Garcia, Christopher Cook and Brian Yip from the United States Nuclear Regulatory Commission and Michael Shock and Kimberlee Edwards from Oasis Systems, LLC for their support and review of the report.

ACRONYMS

ADAMS	Agencywide Documents Access and Management System
ARM	advanced remote monitoring
BOP	balance of plant
CDA	critical digital asset
CFR	US Code of Federal Regulations
CSP	cybersecurity plan
CVE	Common Vulnerabilities and Exposures
DAQ	Data Acquisition
DOE	Department of Energy
DoS	Denial-of-service
EMI	Electromagnetic Interference
EP	emergency preparedness
EPRI	Electric Power Research Institute
FCC	Federal Communications Commission
I&C	instrumentation and control
I/O	input/output
ICS	industrial control systems
IDS	intrusion detection systems
IEEE	Institute of Electrical and Electronics Engineers
IPS	intrusion prevention systems
ITS	important-to-safety
KRACK	Key Reinstallation Attack
LCO	limiting condition for operation
LoRaWAN	Long Range Wide Area Network
LTE	Long Term Evolution
MAC	media access control
MiTM	Man-in-The Middle
NEI	Nuclear Energy Institute
NIST	National Institute of Standards and Technology
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NSR	non-safety-related
OT	operational technology
OTAP	over-the-air programming
OTAR	over-the-air-rekeying
RES	Office of Nuclear Regulatory Research
RF	Radio Frequency
RFI	Radio Frequency Interference
RG	regulatory guide
SIA	security impact analysis
SIEM	security information and event management
SP	Special Publication
SR	safety-related
SSEP	safety, security, or emergency preparedness
TLR	technical letter report
WAP	wireless access point
WEP	Wired Equivalent Privacy
WGRs	wireless gauge readers
WPA	Wi-Fi Protected Access

EXECUTIVE SUMMARY

With the rapid development of technologies, the nuclear industry has begun adapting wireless technologies to increase the efficiency and effectiveness of plant operations. For example, the industry is currently using devices that use wireless technologies to monitor the parameters and performance of equipment that perform non-safety-related (NSR) and some important-to-safety (ITS) functions. In addition, the nuclear industry is considering expanding the use of wireless technologies to safety-related (SR) and ITS systems by removing the wireless access restrictions in their cybersecurity plans (CSPs) as requested in Nuclear Energy Institute's (NEI's) letter titled "Wireless Security Guidance," dated March 2023 [1]. However, the use of wireless technologies has the potential to compromise the defense-in-depth cybersecurity posture at nuclear power plants (NPPs) that has been established to protect SR/ITS Critical Digital Assets (CDAs). The NRC staff needs to understand the potential cybersecurity vulnerabilities, risks, and potential changes to the defense-in-depth strategy that would be introduced if monitoring systems or equipment with wireless technologies are also implemented for SR and ITS systems at a NPP.

While wireless technologies may offer efficiencies to licensees, they can also invalidate one of the pillars of the defense-in-depth protective strategies, the isolation of SR and ITS networks from external networks and devices. Thus, before a device that uses wireless technologies is introduced, an analysis must be performed as part of the design change process to identify any cybersecurity risks caused by the use of a device with wireless technologies. This technical report documents research performed to gain knowledge on potential cybersecurity vulnerabilities and risks from introducing wireless technologies to monitor SR or ITS systems at a NPP and includes considerations that need to be addressed when performing an assessment to evaluate the implementation of wireless technology for monitoring of CDAs associated with SR/ITS functions. These identified risks must be managed so that introductions of a device with wireless technologies would not reduce the established cybersecurity posture of the plant's existing defense-in-depth protective strategies.

This report concludes with recommendations for future research to prepare the staff for any potential cybersecurity review and evaluation of wireless devices used for monitoring in NPP applications. Future research efforts will inform and prepare the staff to assess and evaluate potential future implementation of wireless technologies if introduced in a NPP environment, even only for monitoring SR/ITS parameters, to ensure these technologies do not reduce the established defense-in-depth protective strategy and that licensees address any vulnerabilities or risks associated with the introduction or implementation of this type of equipment.

1. INTRODUCTION

Title 10 of the Code of Federal Regulations (CFR) 73.54, "Protection of digital computer and communication systems and networks," also known as the cybersecurity rule, [2] requires licensees to establish, maintain, and implement a cybersecurity program that provides high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks. The cybersecurity rule is a performance-based regulation that requires licensees to submit a CSP for NRC's review and approval. As part of the NRC's oversight program, the staff inspects the implementation of the cybersecurity program per the CSP, which contains the licensing basis commitments associated with protecting nuclear power plants from cyber attacks. To comply with the cybersecurity rule, licensees could use the templates in guidance documents Appendix A of Regulatory Guide (RG) 5.71 "Cyber Security Program for Nuclear Reactors" [3] and NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors" [4] to construct a CSP. These guidance documents were reviewed and approved by the NRC.

A prominent part of licensees' CSPs is that it requires licensees to implement defense-in-depth protective strategies that includes a security architecture, the implementation of technical, management, and operational cybersecurity controls, and isolation of networks with SR and ITS systems from external networks and devices. This isolation is established by use of data diodes and prohibiting the use of wireless technology for CDAs associated with SR and ITS functions as required in licensees' CSPs and described in RG 5.71, Appendix B.1.17 and in NEI 08-09, Appendix D.1.17, "Wireless Access Restrictions." The cybersecurity protection provided by this isolation was one of the significant site-specific conditions that the NRC took into account to tailor cybersecurity controls that were specific for the nuclear industry.

The industry has expressed an interest in implementing advanced remote monitoring (ARM) equipment with wireless technologies for monitoring SR/ITS parameters. However, language in the CSPs is ambiguous in this aspect and to address this issue, the industry requested the NRC to evaluate a proposed alternate approach [1], as documented in NEI's letter titled "Wireless Security Guidance," dated March 2023. The NRC issued a letter in May 2023 titled "Response to NEI 'Wireless Cyber Security Guidance,' Dated March 2023" [5] in response to NEI's letter, which states in part that: "With respect to implementation of wireless devices used for monitoring equipment, licensees are required in accordance with 10 CFR 73.54(b)(1) and the NRC-approved CSPs, section A.3.1 "Analyzing Digital Computer Systems and Networks and Applying Cyber Security Controls," to perform an analysis and determine if technologies associated with monitoring that have wireless capabilities for data transmission (also known as ARM) are within the scope of the cybersecurity program." If ARM equipment or devices are determined to be within the cybersecurity program, licensees are required to perform a security impact analysis (SIA) prior to making a design change or configuration change to a CDA, or when changes to the environment occurs to manage risks introduced by the changes.[2] A SIA would be expected to be performed as part of the overall analysis to ensure that the plant's defense-in-depth protective strategies are maintained or if additional countermeasures are needed to address vulnerabilities or deficiencies.

---

[1] Terms "safety-related," and "important-to-safety," for CDAs are defined in NEI 10-04 "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 3.

[2] As stated in NEI, 08-09, Revision 6 "Cyber Security Plan for Nuclear Power Reactors," Section 4.4.2 "Cyber Security Impact Analysis of Changes and Environment," 2010, Agencywide Documents Access and Management System (ADAMS) Accession No. ML101180437.

The focus of this technical letter report is to inform staff about the impact of implementing equipment with wireless capabilities to monitor SR/ITS systems without bypassing any one-way deterministic device or airgaps that segregate SR or ITS CDAs; provide an overview of some of the risks and vulnerabilities from the use of these wireless monitoring equipment (Section 3); considerations for the use of wireless communications, specifically for ARM equipment (Section 4); and criteria and elements necessary for a SIA that would help assess the implementation of such wireless technologies for monitoring SR/ITS systems (Section 5).

The authors note that this report does not address the implementation of wireless technologies to control the function of SR/ITS systems and that specific use for wireless technologies in NPPs was not within the scope of this report. This report only evaluated the use of wireless technologies for monitoring SR/ITS systems without bypassing a one-way deterministic device or airgaps that segregate SR or ITS CDAs. The considerations required to address an implementation of wireless technologies to control a function was beyond the scope of the current cybersecurity framework to protect a wireless control system from attack. Further research efforts and/or additional information will be needed to understand any impending implementations of specific wireless technologies related to controlling the functions of SR/ITS in the nuclear industry. It is important to recognize that wireless technologies in the context of this technical letter report refers to wireless technologies such as Wi-Fi, Bluetooth, Zigbee, satellite, cellular, etc.

2. BACKGROUND

The cybersecurity program for the nuclear power industry evolved from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 “Security and Privacy Controls for Information Systems and Organizations” [6] and SP 800-82 “Guide to Industrial Control Systems (ICS) Security” standards. [7] The “high impact” baseline security controls described in NIST SP 800-53 and NIST SP 800-82 were tailored to develop guidance for the nuclear industry to provide an acceptable method to comply with 10 CFR 73.54. This led to the development of the NRC RG 5.71 and the NEI 08-09 guidance documents. Both documents provide the nuclear industry a construct that licensees can use to develop their CSPs to meet the requirements of 10 CFR 73.54.

Licensees CSPs require the implementation of a network defensive architecture having protective levels of security, separated by security boundaries devices such as firewalls and diodes. For example, RG 5.71 provides a conceptual approach of a cybersecurity defensive architecture that has five security levels. In this approach, Levels 0 – 2 have been designated as the lower security levels and levels 3 and 4 are the higher security levels, with level 4 being the highest protected level. Critical systems and CDAs associated with safety and security functions reside and are protected in security level 4 and are isolated from external communications using a one-way deterministic device (e.g., data diode) or where it is feasible, critical systems and CDAs are air-gapped. In addition, the defense-in-depth approach requires the implementation of overlapping technical, management, and operational security controls identified in Appendix B and C of RG 5.71 or the security controls in NEI 08-09, Appendix D and E (depending which guidance was used for the construct of the CSP) and wireless technologies restrictions for

CDAs associated with SR/ITS functions.

Allowing any wireless communications to CDAs protected by a one-way deterministic device invalidates the fundamental principle behind the structure of the licensees' NRC-approved CSP because implementation of wireless communications to control the functions of SR/ITS systems renders the licensee's network defensive architecture ineffective. However, there is a need and a concern that introducing new technologies with wireless capabilities to transmit data for monitoring SR or ITS critical systems may invalidate the established defense-in-depth protective strategies and render the security controls implemented ineffective.

The NRC Office of Nuclear Regulatory Research (RES) staff performed research, alongside technical experts from Oasis Systems LLC, to better understand the cybersecurity issues related to wireless technologies in other safety-critical industries. This research is document in a Technical Letter Report TLR-RES-DE-2022-007 "Study of Wireless Technology Implementation in Isolated, High Consequence Networks" [8] which was published in July 2022. This report documents the findings on the cybersecurity aspects from the use of wireless technologies in other safety-critical industries and identifies some barriers or challenges to the wider adoption of wireless technologies.

2.1 Common Terminologies

Throughout this technical letter report, the following terminology is used consistent with the definitions in RG 5.71, Revision 1.

- **Attack Pathway–**Pathway (including physical access, wired connectivity, wireless connectivity, supply chain, or portable media and mobile devices) used or that may be used to gain access to a digital asset.

- **Attack Vector–**Means, method, mechanism, or technique (or combination thereof) used or might be used by an adversary to gain unauthorized access to, exploit a vulnerability in, produce a malicious outcome on, or otherwise cause adverse impact to a digital asset, network, or system.

- **Attack Surface–**The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.

In the context of cybersecurity, attack vectors and attack pathways are related, but are two distinctly different concepts. The attack vector is the specific method or technique used by an attacker, while the attack pathway refers to the communication medium an attacker takes to conduct their objective within a target system or network. Understanding both, attack vectors and attack pathways within the context of the NRC regulatory framework is crucial for cybersecurity professionals in finding and mitigating potential risks and vulnerabilities.

Section 3 of this technical letter report discusses some of the risks and vulnerabilities that would need to be considered for the potential introduction or implementation of equipment with wireless communications for monitoring SR/ITS systems.

3. RISKS OF WIRELESS COMMUNICATIONS

Wireless technologies present a greater security risk than other network mediums. Wired networks are bound in part by the physical characteristics of the wire and by placing physical barriers around the wire (e.g., conduit, room access controls, locked cabinets). However, with wireless mediums there are little to no physical barriers to eliminate or mitigate unwanted or unauthorized access to a wireless communication to prevent a cyberattack.

RG 5.71 and NEI 08-09 provide a framework for the protection of digital computer, communication systems and networks. The protection of those digital assets is accomplished by the implementation of defense-in-depth protective strategies that includes a security architecture and implementation of the applicable technical, management, and operational security controls, and countermeasures. The defense-in-depth protective strategies, when properly implemented, would include 1) physical and logical network designs with security levels separated by boundary control devices with segmentation within each security level, and 2) supporting tools, technologies, and processes to effectively perform timely detection of, protection against, and response to a cyberattack.[3]

The security architecture as well as the security controls need to be reassessed when introducing wireless technologies to monitor SR or ITS critical systems to ensure that CDAs remain protected and that a cyberattack can still be detected or prevented. For instance, data diodes currently implemented in NPPs could be bypassed if wireless communications are inadequately implemented and CDAs become part of the wireless network. While a data diode can be an important element of an acceptable defensive architecture, the introduction of wireless technologies could allow an attacker to circumvent the protection provided by the data diode implementation, so an air-gap or an isolation strategy alone does not provide the necessary restrictions to ensure a robust security architecture maintains defense-in-depth. Other security controls like the use of conventional intrusion detection systems (IDS) can only monitor traffic after it has been processed through a wireless-to-wired gateway. The protection of SR/ITS and other associated CDAs in the nuclear power industry rely heavily on physical restrictions and placing these assets in security levels logically behind a data diode. Wireless technologies circumvent some of these existing countermeasures by the nature of wireless being an invisible and penetrable communication pathway. NIST 800-154 "Guide to Data-Centric System Threat Modeling" [9] provides some insight into wireless technology threats. Defending attack pathways created from using wireless may require additional countermeasures that may not be common to all digital assets, so knowledge of the potential risks associated with the introduction of wireless communications is vital.

This Section provides some details of the risks associated with wireless communications but is not intended to be inclusive of all the potential risks. Licensees still need to identify all known risk factors (attack vectors) and provide high assurance, through the implementation of security controls and countermeasures, that those risks have been mitigated or eliminated.

The following subsections identify some of the existing risks specific to the implementation of wireless devices.

---

[3] As stated in RG 5.71, Revision 1 “Cyber Security Program for Nuclear Reactors,” Section 3.2 “Defense-in-Depth Protective Strategies,” 2023, ADAMS Access No. ML22258A204.

3.1 Wireless Shielding

Wireless technologies are designed to broadcast and receive their signals for effective and efficient communications even in physically challenging environments without the necessity to install conduct and wiring. Due to the nature of the wireless medium, it is inherently difficult to restrict access to the wireless signals. An adversary, using readily available wireless equipment, can easily attack a wireless network. Protecting attacks on a wireless network requires implementing barriers that restrict the radiation and reception of wireless signals from outside its operating environment. This becomes challenging in the environment of a nuclear power plant.

The barriers required to restrict wireless network signals to a specific area could also restrict communication systems used by plant personnel. Restricting plant personnel from communicating outside these areas would present operational risks (safety, radiation control, emergency preparedness, security). For example, if shielding is placed in a space to reduce the emissions of the wireless network, the same shielding could effectively limit the ability of plant personnel to communicate via their radios to perform daily and/or emergency operations. These conditions would need to be addressed in the security impact analysis, so that site personnel are aware of the potential limitations of implementing shielding in those areas.

3.2 Electrical Isolation

Implementing wireless technologies for monitoring purposes on digital assets could potentially have an adverse impact on the monitored device. It is not uncommon for instrumentation and control (I&C) systems to share a real-world sensor (e.g., pressure, flow, voltage, current) with multiple displays or indicators. When shared connections are not properly isolated from one another they could affect the accuracy of measurements. Sharing an electrical connection with a wireless device may also present a vulnerability. If the configuration of wireless devices is managed through their wireless network, it could also expose these devices to a cyberattack. For example, electrically interfacing a wireless transmitter to an existing sensor shared with an SR/ITS function without proper isolation could create an attack vector. The compromise of the wireless transmitter could even interfere with the shared connection causing the sensor to produce incorrect or incomplete values. Therefore, the sensor being relied upon to monitor a SR/ITS system must be isolated to ensure that a wireless monitoring device would not bypass any one-way deterministic device or air-gapped networks and compromise SR or ITS CDAs.

3.3 Electromagnetic Interference/Radio Frequency Interference

NPPs are required to meet Electromagnetic Interference/Radio Frequency Interference (EMI/RFI) requirements for safety systems. The electromagnetic conditions at the point of installation for SR I&C systems should be assessed to identify any unique EMI/RFI or power surge sources that may generate local interference[4]. This is generally met by distancing or shielding EMI/RFI sources from the equipment performing an SR/ITS function. The required distance is based on the level of interference from the source. The guidance in RG 1.180, Revision 2 “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” [10] establishes the use of exclusion zone distance calculations to identify the minimum distance between the point of installation of SR I&C equipment and the location of portable EMI/RFI emitters. This is part of the

[4] As stated in RG 1.180, Revision 2 “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” 2019, ML19175A044.

administrative controls that need to be established to provide an acceptable level of protection to separate wireless EMI/RFI emitters and safety systems. [11]

The Radio Frequency (RF) power and operating frequencies emitted by a wireless device are also governed by the Federal Communications Commission (FCC). However, many wireless devices are configurable to operate in many countries where power restrictions and frequency bands are different than those authorized by the FCC. The configuration of these devices is often managed through the transmitter's software configuration attributes. As a result, a cyberattack could target and make changes to these attributes, changing the expected RF power or operating frequency of a device. Wireless devices designed to operate in diverse environments may also have the ability to operate using multiple frequency bands simultaneously. As a result, one cybersecurity risk is that the compromise of a wireless transmitter could cause the transmitter to operate at power levels or frequencies that exceed the design basis for an installation, which could potentially cause interference to a SR/ITS system. One example of a cyber threat related to this would be an electromagnetic side-channel attack, where unintentional electromagnetic emissions could be used for eavesdropping on plant operations and data of safety systems. [12] Without adequate cybersecurity controls that ensure monitoring systems are installed and configured properly and in place, such configuration changes have the potential to go unnoticed until they create an adverse impact on a SR/ITS system. Furthermore, depending how wireless devices are physically connected or attached to SR/ITS equipment, their connectivity, and electrical attributes, there could be EMI/RFI effects (e.g., intended or unintended electrical or RF interference to a control function) on the SR/ITS function created by the compromise of the wireless device(s).

3.4 Physical Restrictions

Figure 1. Wireless Gauge Reader

Equipment such as wireless gauge readers (WGRs), as seen in Figure 1, are pieces of equipment that can be physically attached to analog gauges to read and convert the readings to digital. These WGRs can sometimes obscure the view of the analog readings. Operators that are required to log readings from these gauges would be forced to record the digital values provided by the WGR. In this case, for example, it could require licensee to assess the WGRs to see if these should be classified as CDAs because the analog reading is no longer available. Due to their wireless connectivity, WGRs within that network would also require an analysis to determine the impact to SR/ITS equipment and to the rest of the network. As part of an EPRI Modernization Technology Assessment report [13], one of the cybersecurity risks from WGRs is that if the device "is not properly segmented and implemented, potential cybersecurity deficiencies may result in an increase in vulnerability to cybersecurity threats." Introducing potential cybersecurity deficiencies to the environment from the use of wireless equipment like WGRs would decrease the defense-in-depth strategy that protects from cybersecurity threats.

3.5 Data Confidentiality, Integrity, and Availability

Cybersecurity basic principles protect the confidentiality, integrity, and availability of digital data. Protecting the confidentiality, integrity, and availability of digital data requires addressing the attack pathways and attack vectors of the network infrastructure by eliminating the attack pathway (i.e., does not exist) and/or mitigating the attack vectors through a defense-in-depth strategy applying multiple layers of protection for each attack pathway. An attack vector can be eliminated if it can be demonstrated that an attack pathway does not exist. For example, if a

digital asset does not have any networking capability (hardware for networking is not present in the device), then a network attack is not possible; therefore, the attack pathway does not exist. If a digital asset is part of a network, the attack vector(s) can be transmitted via the network pathway and cannot be eliminated. The protection of the networked assets would require attack pathway mitigation and implementing multiple countermeasures to address the attack vector so that defeating a single countermeasure (security control) would not allow the successful compromise of the digital asset.

Another example is wired networks protected by a data diode. If part of the defense-in-depth approach includes isolating a network with a data diode, improper implementation of wireless technologies can create a data diode bypass decreasing the defense-in-depth strategy or even rendering the network defenseless. Therefore, careful implementation of wireless technologies is essential in addition to implementing countermeasures to detect compromise and for data protection would be expected to be part of a defense-in-depth protective strategy.

3.5.1 Data Confidentiality

Data confidentiality is the protection of information, data, that flows on a network or is processed on a digital device. Data confidentiality on a wireless network is a more difficult objective to achieve than protecting a wired network. Defending the confidentiality of data on a wireless network is challenged by the lack of ability to restrict access to the wireless signals. There are methods such as data encryption that may help mitigate accessing the data. However, due to the vulnerabilities of an exposed wireless network, a skilled adversary could capture the encryption credential and use it to access the network. Unlike a wired network, which would require an adversary to physically have access to the network to capture encryption credentials, the wireless network signals are exposed allowing a skilled adversary to observe the handshaking process required to initiate data encryption and potentially capture credentials to gain access to the data.

3.5.2 Data Integrity

Data integrity is the ability to maintain trust in the information being communicated. An exposed wireless network presents attack vectors which could allow an adversary to inject false data into the communication pathway. Methods used to ensure data integrity such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA-2 were once effective, but these methods have now been compromised and are no longer considered effective. WPA-3 is the new standard of protection. However, the industrial wireless network device industry is very slow in adopting new standards [14]. Man-in-The Middle (MiTM) and Evil Twin attacks are common methods used to compromise the integrity of information communicated over wireless networks.

3.5.3 Data Availability

Data availability is the most difficult to defend on a wireless network. The most prevalent method of denying access to data is signal jamming. Jamming prevents wireless systems from receiving data from wireless sensors, thus eliminating the availability of the data required to monitor the status of a critical system.

Wireless communication pathways can be established over long distances using readily available equipment. Once a communication pathway has been established, signal jamming or other attacks are possible. Signal jamming could even be accomplished from 237 miles away.

This was demonstrated in 2007 by Ermanno Pietrosemoli, a professor of telecommunications at the University of Andes in Venezuela. The professor successfully established a wireless connection between two locations approximately 237 miles apart using modified commercial off-the-shelf equipment [15]. In July 2004, Ben Corrado, Andy Meng, and Justin Rigling achieved Wi-Fi wireless communication between two computers some 55 miles apart with unamplified equipment [16]. This is far beyond the bounds of the protected area in all NPPs. Although these are extreme examples, this shows what was once not economically or technologically possible is now readily achievable.

3.6 Wireless Attacks

Implementing wireless in an open environment, such as in a NPP, creates a physically unbounded attack pathway. Implementing physical boundaries (i.e., protective shielding) can effectively reduce the transmission of a wireless signal (i.e., RF energy). Distance and environmental conditions, such as building construction, affects the distance in which RF energy propagates. However, an RF signal is never diminished to a state of non-existence. Therefore, with the proper equipment, and knowledge, a wireless signal can be detected and decoded from even the smallest amounts of energy. The attack pathway to a SR/ITS system using wireless technologies can take a direct or an indirect route as discussed in the next sections.

3.6.1 Direct Attacks

A direct attack pathway is an exploit that would directly affect a SR/ITS system. A direct attack pathway or exploit sequence would lead to a direct and deleterious effect on a SR/ITS function. Examples of a direct attack are as follows:

1. Disruption of the wireless transmission pathway (i.e., jamming)

    a. Disruption of wireless data flow is conducted from outside the network environment using commercially available equipment. Disruption of wireless data flow that is conducted from outside the network environment using commercially available equipment can cause the corruption or complete loss of data that may be critical to performing a SR/ITS function.

2. Denial-of-service (DoS)

    a. A DoS attack differs from signal jamming in that it does not disrupt the signal but uses the 802.11 standard series wireless protocol to flood the network with traffic until the target cannot respond or crashes, causing a partial or total loss of network services. Signal jamming disrupts the wireless signals on a broad scale targeting the frequency or frequencies used by the wireless devices. Signal jamming requires a higher level of transmit power by an adversary to overwhelm the wireless receivers and may be easier to detect. Whereas a DoS attack is an attack that is integrated within the data flow and can target specific devices or the entire network, denying services and communications. Wireless protocols are defined by various communication standards that enable the transfer of data among devices. Each protocol has varying degrees of vulnerability and resilience to DoS attack that should be analyzed and addressed if wireless communications, even for monitoring, are used. Some of the more common wireless standards are Wi-Fi, Zigbee, Bluetooth, Long Term Evolution (LTE) and Long Range Wide Area Network (LoRaWAN).

3. MiTM

    a. A MiTM attack can be launched from outside a wireless network environment. A common MitM attack is when an adversary or third party gets in the middle of wireless communication between two endpoints and intercepts, changes, replaces or modifies (i.e., spoofs) the messages. In a MitM attack, an adversary spoofs the identify of a wireless node. The adversary can then compromise the confidentiality of the data by eavesdropping, the integrity of the data by modifying, or destroying data altogether. An adversary could also assume the identity of a connection to create a rogue connection to inject malware or falsified information in the data streams. Such an attack can be mitigated by employing an authentication protocol to ensure that communications reach their intended recipients [17].

4. Media access control (MAC) spoofing

    a. MAC spoofing is another method to introduce a rogue connection to a wireless network. A MAC address is a unique identifier that is assigned to every network interface controller in a digital device for use as a network address in communications within a network. MAC spoofing, in simple terms, is a technique for changing or masking a MAC address to avoid detection or hide activity within the network. Although you cannot change the physical address on a device, MAC spoofing can be accomplished with software and other tools to fool operating systems or devices in the network. This technique is used by adversaries to gain access to networks so they can hide the identity of a rogue device, or to avoid being tracked or traced. MAC spoofing is technically a more effective hack against a wireless network than on a wired network because no physical access to a device is needed to attack the wireless signal. For example, MAC filtering is a security control that is often used to allow communication between authorized devices within a network. However, MAC filtering could more easily be bypassed by sniffing a wireless network and spoofing a known MAC address. Then a device with the spoofed MAC address can communicate with other devices in the network. Often the MAC address is used to negotiate the wireless connection prior to engaging encryption. One vulnerability of wireless communications is that once an adversary gains a foothold on to the wireless network, they could pivot onto any other vulnerable node on the system.

3.6.2 Indirect Attacks

Indirect attacks using the wireless attack pathway are those attacks that do not interfere directly with the data flow but exploit the weaknesses in wireless technologies to escalate an attack. An indirect attack can also enumerate the network and give information to an adversary that could be used to develop an attack later.

1. Exfiltration of data using wireless communication

    a. The exfiltration or sniffing of data through a compromised wireless network may not create a direct impact on a SR/ITS function. However, exfiltrated data or information could aid an adversary in planning an attack. For example, an attacker or malicious actor could place a receiver within range of a wireless transmitter and “sniff” for data, such as usernames and passwords. If such data

are available, they could be used to capture valid login information, which can then be used to access the network and disrupt operations.

The attacker can use open-source or commercially available tools to sniff and capture traffic (data packets) useful for analysis of the wireless network. The use of encryption can be a deterrent to the sniffing of data since it requires additional tools and resources to decipher. However, operational technology (OT) devices are vulnerable or susceptible because the industrial control system (ICS) industry is slow in implementing the latest encryption technology, partially due to the limited processing capabilities of most wireless sensors. This limitation makes implementing robust encryption a challenge. For example, WPA2 is widely used as the defacto encryption method. However, vulnerabilities associated with WPA2 are well known such as Key Reinstallation Attack (KRACK), which is a group of vulnerabilities that when successfully exploited could allow an attacker to intercept and steal data from a wireless network.

b. The Evil Twin is another method of stealing data. The attacker sets up a fake wireless access point (WAP) with the same name as an authorized point so that it appears to users as the authorized and legitimate WAP. This causes the wireless clients to connect to the fake WAP. By connecting to the fake WAP, the user is exchanging login and authentication credentials with the fake WAP. The adversary takes advantage of this by capturing login and authentication information from the devices that connect to the fake WAP to attack the targeted network. The Evil Twin will broadcast a stronger signal than the legitimate WAP forcing the wireless client to connect to the fake WAP. The Evil Twin is considered a direct attack if it is used to disrupt data flow or inject malware.

The consequence of either type of direct or indirect attack would result in the loss or degradation of the wireless network.

Lastly, inadequate implementation of wireless technologies or equipment with wireless technology in the high security levels of a NPP network would eliminate the established deterministic network isolation that is part of the defense-in-depth protective strategies required per the current licensees' CSPs. Implementing wireless technologies on CDAs associated with SR/ITS functions, even only for monitoring equipment, would require licensees to perform an in-depth analysis to identify the risks and vulnerabilities that could be introduced to ensure defense-in-depth is maintained.

4. POTENTIAL USE OF WIRELESS COMMUNICATIONS FOR MONITORING (ADVANCED REMOTE MONITORING)

Organizations such as NEI and the Department of Energy (DOE) are working together assessing plant operations where the potential increased use of wireless technology can be effective and efficient. Examples include the Advanced Remote Monitoring (ARM) project effort, to improve data collection, save on operations and maintenance costs, and to reduce operator utilization [18]. The use of ARM is an industry initiative to consolidate the monitoring of plant systems to reduce human resource utilization and improve maintenance cycles. Introducing ARM equipment with wireless technologies to monitor SR/ITS systems would provide a new attack pathway. This attack pathway, if compromised, could impact the information transmitted

from the monitoring devices providing false data that could potentially impact the operation of high consequence CDAs, more specifically those associated with SR/ITS functions.

Because wireless technologies present a greater security risk than other network mediums, special consideration must be given to the implementation of ARM that uses wireless technologies. The nuclear industry has already embarked upon implementing ARM for cost effectiveness and/or operational reasons. In February 2022, the Utilities Service Alliance announced that the ARM project team continues to modernize nuclear business practices [19]. An industry study was conducted by Energiforsk in 2022 that identified multiple licensees expanding their wireless infrastructure [20]. Utilities participating in the ARM project have reportedly completed the following activities:

- Implementation of Advanced Monitoring and Diagnostic Centers;
- Installation of additional monitoring capability enabling online thermal performance analytics and large transformer monitoring;
- Development of intelligent algorithms (Process Anomaly Detection) aligned with the Institute of Electrical and Electronics Engineers (IEEE) standards for monitoring transformers;
- Setting up a laboratory with prototypes for the design and development of (1) Surveillances Automation; (2) Automation of Operator Rounds; (3) Remote Radiation Area Monitoring; and (4) Online Thermal Cycle Isolation Monitoring.

These areas are examples that raise the question of whether the digital devices used for ARM should be considered CDAs. These activities may be relied upon or support SR/ITS functions. For equipment surveillances and operator rounds crediting ARM, the licensee must consider the impact of the loss or compromise of the data produced and transmitted with ARM equipment. The risks introduced by wireless technologies mentioned above could potentially impact the confidentiality, integrity, and availability of the data and the ARM equipment.

4.1 Considerations on the Use of ARM

If the use of wireless communications for monitoring SR/ITS equipment is considered, licensees need to know first what information should be included and assessed to determine if the ARM equipment using wireless technologies is a CDA. Second, if the ARM equipment is a CDA, a SIA needs to be performed in accordance with the licensee's CSP. To consider if any equipment that uses wireless technology is a CDA, a licensee can follow the guidance in NEI 10-04, Revision 3, "Identifying Systems and Assets Subject to the Cyber Security Rule" [21]. NEI 10-04, Section 5, which states "a digital device that communicates to a CDA need not be classified as a CDA simply due to the connectivity pathway. If the compromise of the digital asset can be used to compromise a CDA, then the digital asset should be classified as a CDA."

In NEI 10-04, Section 5, under SR/ITS systems, item 5 provides guidance to "identify NSR systems and equipment that functionally interface (including digital pathways) with the SR systems and equipment," and to "[d]etermine if a compromise by cyberattack of the NSR system and equipment interfacing with the SR function could prevent or adversely impact the performance of the SR function, then identify the NSR equipment as a CDA for protection as a SR equipment." Similarly, item 9 of Section 5, addresses ITS equipment and provides guidance to "identify NSR systems and equipment that functionally interface (including digital pathways)

with the Important-to-Safety equipment" and to "[d]etermine if a compromise by cyberattack of the NSR equipment interfacing with the ITS equipment could adversely impact the ITS function, then identify the NSR equipment as a CDA for protection as ITS equipment."

The guidance in NEI 10-04 emphasizes that any digital device, connected in any way to a SR/ITS system, whose compromise could adversely impact a SR/ITS function should be assessed as a CDA. When considering implementing wireless technologies, it is important to fully understand the technology, its weakness, vulnerabilities, hidden features, and functions. The use of wireless communications for any CDA may impact more than just the connected systems. Licensees should reassess if the implemented baseline protections eliminate or mitigate the wireless attack pathway(s) (i.e. data and/or device compromise, DoS attacks) to protect against a cyber attack, in addition to considering other factors such as EMI and RFI concerns. NEI 13-10, "Security Control Assessments," [22] provides additional guidance on how CDAs using wireless technology should be assessed. In summary, CDAs using wireless technology may not be considered of low consequence to SSEP functions, if compromised; therefore, a full assessment is required to determine an adequate level of protection.

The following considerations need to be addressed when performing an assessment to determine if ARM equipment using wireless communications is a CDA. These considerations are not to be considered official guidance or regulation, or elements of a complete analysis, but provide a starting point based on published guidance:

- Document that the ARM equipment is either electrically isolated or has no connectivity to CDAs associated with SR/ITS and the proximity of any wireless device that radiates RF energy could not have an adverse impact on a SR/ITS system.
    - Does it create communications between security levels?
- Ensure that the ARM equipment does not create a data diode bypass or allows external communications in networks that are air-gapped.
    - Does it provide a potential pathway that would allow external networks or devices to connect to a device, system, or network that are directly or indirectly connected to the SR or ITS CDAs that is located behind a data diode?
    - Can it create any vulnerabilities or conditions that could change the defense-in-depth approach of the environment where SR/ITS CDAs reside as specified in the licensees' CSPs?
- Determine if the ARM equipment will be a CDA (NEI 10-04 Guidance).
    - Is the ARM equipment credited in the site's licensing basis?
    - Is it relied upon to make safety or ITS decisions to support operations or operator rounds?
- Document how the data or information generated by the ARM equipment will be used and if the information will be sent to other networks or systems?
    - If data are collected and sent to another device, how are the data and the receiving device protected?

- Does the ARM equipment create communications between security levels?
- Can the operator trust the data being received (e.g., addressing risks like data corruption)?
- How is ARM equipment protected from existing cyberattacks such as denial-of-service, data exfiltration, MiTM attacks, etc.?

The information above would assist both the licensee and NRC staff during inspections to evaluate if any ARM equipment installed is a CDA, and considerations for the security control assessment to ensure the defense-in-depth protections are maintained.

If the ARM equipment becomes a SR or ITS CDA, a more detailed SIA is required prior to making any change to a digital asset or its environment per the CSP to manage the risks caused by a change such as the introduction of wireless devices. Specifically, a SIA is performed to capture the following: (1) identify potential vulnerabilities caused by introducing a wireless CDA (mitigation verse elimination), (2) determine the risks to the established cybersecurity posture and reliability of CDAs, and (3) identify and implement mitigation measures that manage risks caused by introducing ARM equipment. Section 5 of this technical letter report provides an overview of the expected criteria or elements of a SIA to address the vulnerabilities and risks from the use of ARM equipment with wireless communication to monitor SR/ITS systems.

5. CRITERIA OR ELEMENTS OF A SECURITY IMPACT ANALYSIS

The guidance in NEI 08-09, Section 4.4.2, “Cyber Security Impact Analysis of Changes and Environment,” states that a SIA must be performed prior to making a design or configuration change to a CDA, or when changes to the environment occur, to manage the risks introduced by those changes. NEI 08-09, Section 4.4.2 further states that SIAs “are performed as part of the change approval process to assess the impacts of the changes on the cyber security posture of CDAs and systems that can affect SSEP functions.” As a result, licensees committed as part of their CSPs to perform a SIA to manage the risks introduced that may challenge the plant’s cybersecurity defense-in-depth protective strategies. This section captures some of the criteria or elements that the authors expect would be needed to perform an adequate SIA, specifically to assess a NSR system that uses wireless technologies to monitor parameters of a SR/ITS system.

NIST 800-128 “Guide for Security-Focused Configuration Management of Information Systems,” [23] dated August 2011, provides guidance for developing a SIA. Specifically, Section 3.3.3 “Conduct Security Impact Analysis” details a five-step process for documenting an SIA. These five steps include: (1) understanding the change, (2) identifying vulnerabilities, (3) assessing risks, (4) assessing the impact on existing security controls, and (5) planning safeguards and countermeasures. Additionally, Appendix I and Attachment I of NIST 800-128 provide useful information on what a comprehensive SIA should include and questions an inspector may ask to identify any gaps in the SIA. The details of how NIST 800-128 may apply to the inspection process are beyond the scope of this technical letter report. NIST 800-128 is not a regulatory requirement or considered regulatory guidance. However, the information contained in that document provides insights that may be useful in assisting an inspector when auditing an SIA.

An area of concern when introducing wireless in a NPP is that the licensee needs to understand and address all the risks associated with the wireless implementation. Section 3 of this technical letter report provides some details of the risks associated with wireless but is not inclusive of all the potential risks. Performing a comprehensive SIA is important to identifying all known risk factors (attack vectors and pathways) and to provide high assurance all security controls and countermeasures are in place to mitigate or eliminate those risks. In addition, a well-documented SIA should provide information about potential new or emerging threats and vulnerabilities introduced by changes in the system, network, and environment.

RG 5.71 and NEI 08-09 do not provide details or specifics about the depth and scope of a SIA. One of the objectives of this TLR is to provide criteria or elements that provide a starting point and considerations to prepare a SIA so licensees that are planning to implement ARM equipment to monitor SR/ITS systems can provide detailed information during inspections. The criteria or elements below were developed for the limited cases regarding the use of wireless technologies to monitor SR/ITS parameters such as the possible implementation of ARM equipment in its own isolated network (i.e., ARM with wireless capabilities not connected to the networks behind the data diode). However, an inspector evaluating implementation of ARM with wireless technologies may have a better understanding of the impact wireless could have on its implementation and a SIA may be scaled in accordance with the safety and security categories of the systems.

If ARM equipment with wireless technologies is implemented to indirect, balance of plan (BOP), and emergency preparedness (EP) CDAs, it should also be noted that NEI 13-10, Section 5, baseline security control criteria would need to be reassessed and additional countermeasures may be needed to address the implementation of wireless technologies. Therefore, the expectation is that a full security control assessment would have been done to demonstrate adequate protection of CDAs implementing wireless technology.

The following criteria or elements are needed to perform an SIA to evaluate the implementation of wireless technology for monitoring of CDAs associated with SR/ITS functions. These criteria are not to be considered official guidance or regulation. The following should be documented:

1. The baseline documentation for the proposed wireless network implementation.

    a. The expected as installed baseline configurations, including manufacturer documentation for each type of device, such as the use of any wireless-to-wired gateways, routers, and firewalls or other boundary devices. This information is useful to determine the attack surface.

    b. The acquisition of devices that have wireless (enable or disabled) and the policies and procedures the plant uses to maintain those devices, as well as the qualifications of personnel installing such devices. This information is necessary to assess any possible misconfigurations in the installation and maintenance of wireless devices.

2. The characterization of the attack surface for each wireless device and associated wired pathway, including:

    a. Total number of nodes in the network to determine whether all potential vectors and pathways of attack have been identified.

b. Characterization of the wireless asset and network to determine whether the licensee has considered all the potential attack vectors and pathways, not just the ones operating under normal conditions. The characterization of the wireless transmitting and receiving capabilities that help identify normal and expected activity of the wireless devices. Transmitters operating at higher or reduced power or transmitting at more frequent intervals are signs of abnormal activity. Changes in receiver signal strength or an increase in noise conditions are indications of rogue devices or unauthorized scanning activity. Some of the information that could help characterize the attack surface of a wireless communication is:

   i. Knowledge of the operational RF spectrum(s) used by the wireless technologies, including the spectrums the device is capable of operating to understand what the expected RF operating frequencies are. Any RF signals detected outside the normal operating spectrum may be an indication of unauthorized scanning or attempts to establish back channels into the wireless network. The RF spectrum should be monitored so that security controls or processes can be taken to mitigate a cyber threat.

   ii. Characteristics from the wireless transmitter and receiver used by a system. Knowledge about the characteristics and capabilities of the transmitters and receivers can aid an adversary to develop targeted cyber threats to a system, such as signal jamming. Information such as the transmitter power range (i.e., the average and peak amount of RF energy per unit power emitted by the transmit antenna) or the receiver sensitivity (i.e., the minimum signal strength, Signal to Noise Ratio, or Signal-to-Noise-And-Interference Ratio required by a receiver to decode an incoming transmission). The transmit power may indicate and affects the area covered by a wireless transmitter, so proper configuration management of components is important for securing a wireless network. A signal may also be jammed by electronic means by targeting a jamming beam at the receiver using a particular known operating frequency that the receiver can sense.

   iii. Wireless protocol(s) (used and unused), which are required to be documented for all CDAs as part of the CSPs. Unused or insecure protocols can become attack vectors that must be addressed and mitigated.

   iv. External antenna placements. It is useful to understand where the potential risks are for broadcasting wireless data further than is necessary for a particular function. Wireless communications can sometimes go beyond the necessary range needed to transmit/receive the data and could provide an opportunity for unauthorized reception of information or unauthorized access to the network. The placement and directionality of radiating antennas also goes to supporting the requirements to preventing any EMI or RFI impact from wireless technologies on SR/ITS systems.

c. All input/output (I/O) capabilities both digital and analog. This information is part of the baseline configuration and it is needed to identify any potential attack pathways to associated systems.

d. Firmware versions and methods for updating. Documenting firmware revisions is

a baseline control requirement. Documenting the methods for updating firmware could factor into portable media management, vulnerability management, software quality assurance, and supply chain requirements.

e. Device management capability to determine whether the licensee has considered all the attack vectors that could be used to alter the configuration or function of the wireless device. This should include:

    i. Methods or operational programs used to manage the individual device configuration settings.

    ii. Methods or operational programs used to change or update the device operational settings, such as those having the following capabilities:

        a. Over-the-air programming (OTAP)–A capability that allows a device or devices to be reconfigured or reprogrammed once it is deployed.

        b. Over-the-air-rekeying (OTAR)–A capability in which data signal encryption keys are updated in secure information systems by conveying the keys through encrypted wireless communication channels.

f. The data flows between the wireless nodes and any wired pathways, including analog connections from digital assets that may influence either connection.

g. The wireless topology (e.g., star, point-to-point, mesh, ad hoc, etc.) to understand the wireless data flow and whether all potential attack vectors associated with each type of network topology have been considered. For example, the techniques required to monitor a mesh network for intrusion is different than that of a star or point-to-point network.

h. Information to estimate the potential signal levels and coverage at the highest capable emitter setting for each device (e.g. Heat maps) to determine the overall coverage of the wireless network. This is important to monitor for rogue connections and to know the extent of the signal range that has to be considered to counter an adversary's ability to monitor network traffic remotely.

i. Equipment required to scan for rogue wireless devices. This is necessary to maintain the capability to effectively monitor the wireless network in all potential modes of the device operation. For example, some devices may have the capability to operate on different RF bands simultaneously. The monitoring equipment should be capable of detecting all modes of operation whether they are configured or not.

    i. Not all wireless sensor networks use conventional 802.11.x frequencies or protocols. Compliance with the control requirements must ensure the capability to monitor for rogue wireless connections regardless of the technology deployed.

3. Common Vulnerabilities and Exposures (CVEs) and manufacture alerts and

advisories associated with each unique asset.

4. Shared sensor connections. This information is useful to determine the effect shared monitoring devices may have on a CDA associated with a SR/ITS function. For example, two monitoring devices sharing the same sensor should be electrically isolated to prevent one device from compromising or causing a failure that would interfere with the other device. Additionally, a wireless device shared with a wired device, if improperly configured by error or by compromise, may create RF interference with the wired device.

    a. Connections shared between a wireless device and a wired sensor used on a SR/ITS system. Shared sensors, if not electrically isolated, could adversely affect the integrity of the sensor readings for both the wired and wireless pathways.

5. The wireless devices physical connections, mechanical and/or electrical to the SR/ITS system to determine how an operator obtains information from the component required to be surveyed under their limiting condition for operation (LCO) requirements. Measurements that were once available by directly reading an analog gauge and are read through digital means would need to be assessed by the licensee to determine if they should be considered a CDA (such as the use of ARM equipment).

    a. The mechanical attachment of a wireless device such as a WGR can obscure the viewing of the analog gauge under it. Obtaining the value of the gauge may require reading the digital value of the WGR. Should an operator require this value for making operational decisions, the licensee would need to determine whether the WGR may be considered a CDA. Therefore, it may be possible that all digital devices within the wireless network could be treated as CDAs by the licensees to protect this attack pathway.

    b. Any electrical connectivity from a wireless device to a SR/ITS system represents a potential attack pathway. Many sensor devices are built on programmable components, that if manipulated by compromise, can alter their designed function. An analog input connection could become an analog output connection. A wireless device which passes an analog signal through to an SR/ITS system could be manipulated to cause an adverse impact.

    c. Document shared electrical connections with SR/ITS sensors. This information would be valuable to understand how a wireless device and SR or ITS Data Acquisition (DAQ) system or indicator shares a single sensor. If the shared connections are not properly isolated from one another, the compromise of the wireless device may result in causing intended or unintended interference with the SR/ITS function.

6. The mitigations (i.e., technical and programmatic controls applied) to detect, protect, and respond to each element of the attack surface with sufficient defense-in-depth and demonstrate an adequate cybersecurity posture. This is a fundamental requirement of the licensees' CSPs.

    a. Document the placement and locations of mitigations for wireless devices. Some mitigations such as wireless shielding may cause interference with normal plant

communication requirements and must be identified so compensating actions are identified when operating in a shielded space. Other mitigations such as wireless IDS and intrusion prevention systems (IPS), continuous monitoring, and security information and event management (SIEM) tools can also be utilized. However, a lack of knowledge of wireless threats and specialized training to manage the monitoring tools could lead to unmitigated attack vectors.

7. The evaluation of the effectiveness of any installed controls or mitigations for wireless devices. Such an evaluation should address the effect that devices with wireless capabilities have on other security controls performed as part of the licensees' CSPs.

6. CONCLUSION

The introduction of wireless technologies into a NPP would introduce risks and vulnerabilities that may not be well-understood. The NRC-approved CSPs include licensees' commitments to implement defense-in-depth protective strategies that include the isolation of networks where SR and ITS systems reside from external networks or devices. This isolation has been established by the use of data diodes and the implementation of wireless access restrictions as required in licensees' CSPs and described in RG 5.71 and NEI 08-09. However, due to the unique attack characteristics of wireless technologies, the concern becomes that introducing wireless technologies at an NPP to monitor SR or ITS critical systems may invalidate the established defense-in-depth protective strategies, which include a defense-in-depth architecture that isolates SR and ITS networks from external networks and devices.

Recently, the nuclear industry has expressed an interest in utilizing wireless technologies to increase the efficiency and effectiveness of plant operations, such as the implementation of ARM equipment for monitoring SR/ITS parameters. This technical letter report provides some details of the risks associated with the use of such wireless communications, including the need to consider and protect against various vulnerabilities such as wireless attacks like jamming, disruption of communications or the exfiltration of data. Implementing wireless technologies on, even only for monitoring SR/ITS parameters, would require licensees to perform an in-depth analysis to identify all the risks and vulnerabilities that could be introduced and need to be addressed to ensure defense-in-depth is maintained.

If the use of wireless communications for monitoring SR/ITS equipment is considered, licensees need to know what information should be considered and assessed to determine if the ARM equipment needs an SIA and if the device using wireless technologies is a CDA or not. Licensees commit as part of their CSPs to perform a SIA to manage the risks introduced that may challenge the plant's defense-in-depth protective strategies. Section 5 of this report captures some of the criteria or elements that the authors expect would be needed to perform an adequate SIA specifically to assess a NSR system that uses wireless technologies to monitor parameters of a SR/ITS system. These criteria or elements of a SIA as captured to illustrate what would be some of the expected best practices for an adequate SIA. Performing a comprehensive SIA is important to identifying all known risk factors (attack vectors and pathways) and to provide high assurance that all security controls and countermeasures are in place to mitigate or eliminate those risks. Ultimately, licensees still need to understand and address any risks to ensure that ARM equipment does not create a bypass to the data diode or airgaps that segregate SR or ITS CDAs, and the need to perform analysis to determine if wireless technologies associated with monitoring are within the scope of their cybersecurity programs.

7. FUTURE WORK

Future research efforts would help prepare the staff for any potential cybersecurity review and evaluation of wireless devices used for monitoring in NPP applications. Further research would help to better understand the associated cybersecurity concerns and regulatory implications from the expanded use of wireless communications in NPPs. The following are recommendations for further research efforts to:

1) understand any impending implementations of specific wireless technologies in the nuclear industry, such as Wi-Fi, Zigbee, cellular, etc.,
2) assess how existing guidelines such as the guidance in NIST 800-128 or other similar standards could be used by the nuclear industry to improve the development of a SIA when introducing wireless communications in a NPP environment,
3) identify the benefits and challenges of using wireless-specific security or monitoring controls, such as the use of wireless IDS and/or IPS systems in a NPP for monitoring SR/ITS functions,
4) review encryption protocols for wireless technologies, to understand and/or demonstrate how they could be used to maintain adequate security for wireless communications, and
5) assess if additional cybersecurity controls and/or guidance may be required to address the new attack vectors introduced by wireless technologies.

These future research efforts would inform and prepare the staff to assess and evaluate potential future implementation of wireless technologies introduced in a NPP. Even if wireless technologies are used only for monitoring SR/ITS parameters, these future research efforts could ensure implementation of these technologies do not reduce the established defense-in-depth strategy or that licensees address any vulnerabilities or risks associated with the introduction or implementation of this type of equipment.

REFERENCES

1. Nuclear Energy Institute (NEI), “Wireless Security Guidance,” 2023. (ADAMS Accession No. ML23060A327)

2. Title 10 Code of Federal Regulations (CFR) §73.54 “Protection of Digital Computer and Communication Systems and Networks.”

3. U.S. Nuclear Regulatory Commission (NRC), Regulatory Guide (RG) 5.71, Revision 1 “Cyber Security Program for Nuclear Reactors,” 2023. (ML22258A204)

4. NEI, NEI 08-09, Revision 6 “Cyber Security Plan for Nuclear Power Reactors,” 2010. (ML101180437)

5. NRC, Response to NEI “Wireless Cyber Security Guidance,” March 2023. (ML23118A268)

6. National Institute of Standards and Technology (NIST), NIST SP 800.53 “Security and Privacy Controls for Information Systems and Organizations,” 2020.

7. NIST, NIST SP 800.82 “Guide to Industrial Control Systems (ICS) Security,” 2015.

8. Haddad, A., Lamb, C., deCastro, J., Manjunatha, K. A., Martinez Rodriguez, E., Kim, A., & Lee, E., Technical Letter Report TLR-RES-DE-2022-007 “Study of Wireless Technology Implementation in Isolated, High Consequence Networks” July 2022. (ML22180A008)

9. NIST, SP 800-154, “Guide to Data-Centric System Threat Modeling,” 2016

10. NRC, RG 1.180, Revision 2 “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” Washington, DC, 2019. (ML19175A044)

11. Muhlheim, M., Belles, R., & Hardin, R. (2023). Criteria for Determining the Safety of Wireless Technologies at Nuclear Power Plants. Retrieved [Online] from https://www.osti.gov/servlets/purl/1996676

12. Sayakkara, A., Le-Khac, N. A., & Scanlon, M. (2019). A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. Digital Investigation, 29, 43-54.

13. Electric Power Research Institute (EPRI). (2020). Modernization Technology Assessment MTA-EN-001 “Reduce Maintenance Costs Using Wireless Gauge Readers.” Retrieved [Online] from https://dotcomstorage.blob.core.usgovcloudapi.net/plantmodernization/mta/MTA-EN-001.pdf.

14. Sagers, G. (2021, December). WPA3: The Greatest Security Protocol That May Never Be. In 2021 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE (pp. 1360-1364), doi: 10.1109/CSCI54926.2021.00273.

15. World Guinness Book of Records, “Longest Broadband Wireless Connection.” Retrieved August 25, 2023, from https://www.guinnessworldrecords.com/world-records/longest-broadband-wireless-connection#:~:text=In%20April%202007%2C%20Ermanno%20Pietrosemoli,mountains%20in%20the%20Venezuelan%20Andes

16. World Guinness Book of Records, “Longest Wi-Fi Connection at Ground Level.” Retrieved August 25, 2023, from https://www.guinnessworldrecords.com/world-records/longest-wi-fi-connection-(ground-level)

17. Bhushan, B., Sahoo, G., & Rai, A. K. (2017, September). Man-in-the-middle attack in wireless and computer networking—A review. In 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall) (pp. 1-6). IEEE.

18. Idaho National Laboratory. “U.S. Energy Department invests in Advanced Remote Monitoring project.” May 28, 2020. Retrieved [Online] from https://inl.gov/nuclear-energy/u-s-energy-department-invests-in-advanced-remote-monitoring-project/

19. Utilities Service Alliance (USA) Communication. (February 21, 2022). “ARM Project Update.” https://www.usainc.org/arm-project-update-february-2022/

20. Energiforsk. ENSRIC report “Wireless in Nuclear Applications in the US,” Report 2020:683. August 2020. Retrieved [Online] from https://energiforsk.se/media/28293/wireless-in-nuclear-applications-in-the-us-energiforskrapport-2020-683.pdf

21. NEI, NEI 10-04, Revision 3, “Identifying Systems and Assets Subject to the Cyber Security Rule.” 2021. (ML21342A168)

22. NEI, NEI 13-10, Revision 5, “Cyber Security Controls Assessments.” 2017. (ML17046A658)

23. NIST, NIST 800-128, “Guide for Security-Focused Configuration Management of Information Systems.” 2019. https://doi.org/10.6028/NIST.SP.800-128.