INL/RPT-22-68990
Revision 1

Draft Methodology for Cybersecurity Analysis for Adoption of Wireless Technology in Nuclear Power Plants

November 2022

Koushik A. Manjunatha
Timothy R. McJunkin
Christopher P. Chwasz
Idaho National Laboratory

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance, LLC

DISCLAIMER

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

INL/RPT-22-68990
Revision 1

Draft Methodology for Cybersecurity Analysis for Adoption of Wireless Technology in Nuclear Power Plants

Koushik A. Manjunatha
Timothy R. McJunkin
Christopher P. Chwasz

November 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy Cybersecurity
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

EXECUTIVE SUMMARY

The report is delivered as DOE-NE Cybersecurity R&D Program Milestone M2CT-22IN1104014. The milestone is specifically to document a proposed process for developing guidance in support of industry's adoption of wireless communication technologies. Such a process may be useful to nuclear plant operators as they must develop a defensive strategy and propose that it satisfies regulatory requirements.

Secure and resilient wireless capabilities are required to transform the operation of nuclear power plants, including domestic light-water reactors, advanced reactors, microreactors, and fission battery, for grid and non-grid applications. In addition, to realize new operational concepts such as autonomous operation and remote monitoring, advanced sensor, and instrumentation, wireless technology is essential. However, industry implementation is low, and there is no technical basis for how to understand and address potential risks for wireless communications for critical plant functions. A methodology with a technical basis for implementing secure wireless communication is crucial.

This wireless adoption methodology is intended to assist in identifying an appropriate technological approach for securing wireless communications in nuclear power plants. However, this methodology does not provide regulatory guidance. This methodology provides a process for evaluating a proposed wireless implementation and drafting a plant change notification for an example use case. The example is a generic/non-proprietary version of the first test case of the methodology, which, if successfully implemented, is part of the consideration for protecting other functions' use of wireless in a cybersecure manner.

Disclaimer: Neither Idaho National Laboratory, the Nuclear Regulatory Commission (NRC), nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility that the method provided in this document meets any NRC requirements.

Page intentionally left blank

ACKNOWLEDGEMENTS

This report was made possible through funding from the U.S. Department of Energy (DOE)'s Nuclear Energy (NE) Cybersecurity R&D Program. We are grateful to Lon Dawson at Sandia National Laboratories, and Katya Le Blanc at Idaho National Laboratory for championing this effort. Idaho National Laboratory (INL) interacted with the Nuclear Regulatory Commission (NRC) for suggestions, comments, and feedback throughout this effort. We want to show our gratitude and thank NRC staff colleagues who provided their insights and expertise as part of this effort. We thank Rebecca N. Ritter at INL for the technical editing of this report.

Idaho National Laboratory

Arup Bhuyan

Shannon Eggers

Katya Le Blanc

Christopher M. Spirito

Sandia National Laboratories

Michael T. Rowland

Christopher Charles Lamb

Lon Dawson

NRC Research

Roy Hardin
Norbert Carte
Eric Lee
Mario Fernandez
Brian Yip
Erick Martinez Rodriguez
Ramon Gascot Lozada
Christopher Cook
Ismael Garcia
Michael Waters

Stakeholders

NEI Cybersecurity Task Force

Nuclear Energy Industry (Constellation)

Page intentionally left blank

CONTENTS

FIGURES

TABLES

ACRONYMS

CDA	Critical Digital Asset
CRC	Cyclic Redundancy Check
CSP	Cybersecurity Plan
CSS	Chirp Spread Spectrum
DA	Digital Asset
DAS	Distributed Antenna System
DFP	Data Flow Path
DOE	Department of Energy
DoS	Denial of Service
EMI	Electromagnetic Interference
GM	Gas Monitoring
HMAC	Hash Message Authentication Code
IP	Internet Protocol
LoRaWAN	Long-Range Wide-Area Network
M&D	Monitoring and Diagnostic
MAC	Medium Access Control
MIC	Message Integrity Code
NE	Nuclear Energy
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OSI	Open System Interconnection
PCN	Plant Change Notification
PSP	Physical Security Perimeter
RF	Radio Frequency
SINR	Signal to Interference Noise Ratio
SR/ITS	Safety Related and Important to Safety
UT	Ultrasonic-Testing
UTGM	Ultrasonic-Testing Gas-Monitoring
WCID	Wireless Capable intruding device
WSI	Wireless Security Institute
WSP	Wireless Security Perimeter

Page intentionally left blank

Draft Methodology for Cybersecurity Analysis for Adoption of Wireless Technology in Nuclear Power Plants

1. INTRODUCTION

The nuclear industry has already started to modernize its operations by utilizing wireless connectivity and is well poised to expand the use of wireless in an increasing number of use cases. In addition, advanced reactors and microreactors are expected to adopt new control and communication paradigms that will include wireless technology. The Nuclear Energy Institute (NEI) cybersecurity task force representing the current nuclear power plants (NPPs) operators and industries have identified secure wireless communication as a key area in modernizing various functions in the NPPs. The key focus areas of this work include:

- Understanding technological and regulatory barriers.
- Understanding the limitations/restrictions of the current security guidance.
- Exploring alternative processes and guidance to introduce wireless technology securely to a nuclear energy facility.

The objective of producing and socializing guidance for wireless security is intended to accelerate the cost-saving application of wireless communication by eliminating unnecessary barriers in cybersecurity programs and producing a process where the industry and regulators can identify necessary regulatory rulemaking to relieve constraints that impede implementation without improved security. In this regard, this document provides the following:

- A methodology that can be utilized by the industry to evaluate and secure proposed wireless systems
- Technical analysis and related regulatory analysis for secure and reliable wireless use
- Technical analysis that includes identifying threat scenarios arise at the wireless communication and providing/recommending additional cybersecurity controls
- A to-do list in utilizing the provided methodology with technical analysis to evaluate the use of wireless technology
- An example use case to demonstrate the use of methodology.

Once finalized, the methodology proposed in this document will be evaluated by the NEI or other industry stakeholders. The Department of Energy -Nuclear Energy (DOE-NE) Cybersecurity R&D Program will continue to assist NEI, DOE-NE research and development (R&D) programs, and the U.S. Nuclear Regulatory Commission (NRC) in identifying and conducting relevant wireless security research and supporting the use of the methodology as necessary. This document will also be utilized as a starting point for working with DOE-NE R&D programs for microreactors and advanced reactor technologies to identify the necessary research in wireless communications and communication security.

This report is organized as follows: Section 2 presents the wireless implementation methodology with technical analysis, comparison, a to-do list to implement wireless, and a use case analysis for the proposed methodology. Section 3 provides a comparison between the proposed cybersecurity controls in the methodology with the NIST 800-53 controls. Section 4 briefs about the outreach activities performed in FY-22. Section 5 describes the identified short-comings of the proposed methodology and path-forward to address them.

2. WIRELESS IMPLEMENTATION METHODOLOGY

2.1 Summary of the Methodology

This methodology guides nuclear power plant operators through a process of evaluating a proposed implementation and drafting a plant change notification for a new or redesign of a wireless system in several steps:

- Provide a detailed description of the system that will be designed or modified to use wireless communications.
- Guide the plant operator through a technical analysis to show the detection and mitigation of threats to the wireless communication system. The technical analysis procedure includes following steps as described in Figure 1:
  - Decompose the entire wireless system into its structural or logical components. Derived system components can be processes or elements that communicate internally or separate systems that communicate externally. Components reveal functionalities, relationships, and interactions among them.
  - Identify and draw a diagram of the data flow path (DFP), including each component and associated interface in the data flow from the source to destination. Identify any other related systems that utilize the DFP to allow all potential impacts that could be affected through the wireless communication channel.
  - Determine the impacts that can occur in the wireless communication channel to systems that are identified as being supported by the DFP.
  - Plan cybersecurity controls based on the defense strategies to mitigate the identified threat impacts to the wireless channel and functions.
  - Evaluate the performance of the identified cybersecurity controls. If technical gaps are identified, the cyber controls will be reevaluated and retested. This process continues until a satisfactory performance is met across all attack vectors.
- Document the cybersecurity defense mechanism and technical security controls implemented to mitigate cyber threats to provide secure wireless communication.
- Provide a summary of the implementation for the hardware procurement, installation, and operation that execute the required cybersecurity controls.

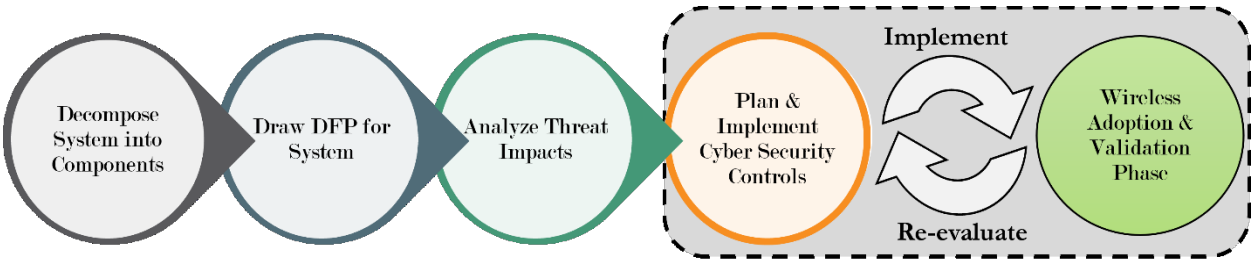

Figure 1. Cybersecurity of wireless communication technical analysis flow diagram

In addition to the methodology, a model plant change notification (PCN) for an example use case is provided.

The example is a generic/non-proprietary version of the first test case of the methodology, which, if successfully implemented, may show a path for protecting other uses of wireless in a cybersecure manner. Ultimately, this methodology may provide a basis for revising industry guidance to establish a standard for considering wireless communications.

2.2 Summary of the Function

In the "Summary of the Function" section of the PCN, the operator should provide a full scope description that includes the following:

- Describe the systems, their planned use, and a periodicity of observations including *acceptable latency.* The acceptable latency is determined by the time expectation before the deadline for data-driven decision-making. Acceptable latency sets the time constraint for confirming data validity or resolving issues with transmission of data that may be a result of cyberattacks. This is an important factor in evaluating the risks involved with using wireless communication. The wireless specific latency depends on the availability of a wireless channel. The acceptable latency of the CDA function can be affected by a wireless channel's availability and system impairments, while the wireless specific latency could be due to the unavailability of a wireless channel. Thus, acceptable latency should be larger or equal to the wireless specific latency.
- Identify the plant network to which the wireless receiver is connected. The plant operator needs to account for the non-wireless communications involved in the executing the system function to identify other impacted functions.
- Describe all communication interfaces with the system (nuclear power plant operators may want to add a graphic to detail these connections and clearly capture the "scope" of the wireless security analysis).
- Describe the physical space in which the wireless communication can take place, referred to in this methodology as the wireless security perimeter (WSP). A wireless capable intruding device (WCID) must enter the WSP to access the wireless communication channel. The relative position of a physical security perimeter (PSP) will determine whether the applicable access controls can be considered a defensive mechanism for securing wireless communication. Also, the WSP should be within the PSP boundary. While radio frequency (RF)-based wireless communication is expected to be the primary media for this methodology, similar perimeters can be considered for acoustic/optical communication.
- As per the generic wireless communication diagram shown in Figure 2, the sensor is connected to a wireless node through a cable/wired connection, and the wireless node is connected to a wireless gateway through a wireless technology. The wireless gateway is connected to a plant network through a wired connection. For a plant operator to take credit for physical security controls, the WSP must be within the PSP. The representation here is generic; the plant operator needs to identify the specific network and the wired data path to the end use point, for example, when the connection extends to destination via data diode. The operator needs to understand if there are any other plant functions that may be supported on this data path in order to adequately understand, and address, the risk of utilizing wireless communications to connect to the plant network. A WSP can be established and ensured through link budget analysis involving signal strength measurement around the PSP and ensuring the signal strength is weak outside of the PSP to decode the signal.

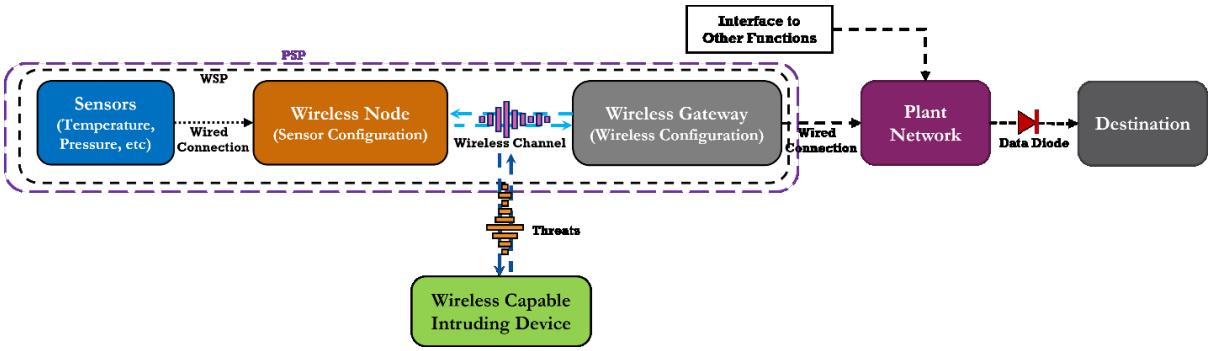

Figure 2. A generic diagram of wireless communication for a DA function in a plant.

2.3 Technical Analysis of Wireless Implementation

The operator will use this section to provide guidance for how to analyze and populate the technical analysis, threat, and impact section of the wireless implementation.

2.3.1 Decompose System into Components

Figure 2 illustrates a generic implementation diagram of components with wireless communication, sensors, transmitters, receivers, and components and connections that are part of the DFP. Based on Figure 2, the system consists of the sensor nodes, wireless network interface, wired network interface, and data diode (if part of the DFP). Also indicated is the possibility of a WCID that would be the initiator of an attack on the wireless communication portion of the DFP. Decomposing into components is necessary to identify the interfaces and interconnection of the system with the plant network and other plant functions supported by the DFP as shown in Figure 2. Identifying other plant functions, particularly those that either use wireless or wired network, is necessary for the operator to understand the plant functions that could be at risk with this implementation. Note that the number of components can change based on the plant infrastructure. Also, the wireless threat analysis does not consider the physical components not susceptible to cyberattacks via wireless communications. Each component processes the input and generates output, which may feed into the input of another component.

2.3.2 Draw a Data Flow Path for System

The sensor nodes are typically connected by an electric wire or attached to the wireless node itself. The wireless network has components such as a wireless node (to which the sensor is attached), wireless gateway, antennas, and interfaces to plant network. The wireless gateway and the wireless node have their respective signal processing modules attached to their respecting transmission and reception antennas. The wireless gateway contains wireless elements such as antennas, distributed antenna system (DAS), and the gateway node of the wireless technologies (such as long-range wide-area network (LoRaWAN) and radio frequency identification. Also, the wireless gateway has a port to connect to a plant-wired network interface. The wireless nodes incorporate sensory metadata (e.g., data/type, configuration, protocols, and data-reading/sending frequency) and enable wireless connectivity with wireless gateways.

Wired plant networks are implemented with a defense architecture described in operators' CSPs using switches, routers, and boundary devices such as data diodes and firewalls. The plant network will also interface with other plant functions or other plant subnetworks, including wireless infrastructure. Like wireless networks, wired networks also have data processing at routers and at switches to forward data to its destination. Data diodes are one-way deterministic devices that typically take data via an IP endpoint and then pass it one-way to a corresponding endpoint on the "other side" which is then translated back into IP packets that are moved to another destination. Data diodes are often located between network levels in secure architecture designs to ensure data or signals cannot traverse from less secure levels into more secure levels. Following the Regulatory Guide 5.71 nomenclature, data diodes are typically located between Level 4 and Level 3 devices as well as Level 3 and Level 2 devices to ensure one-way data flow from control networks (Level 4) to plant networks (Level 3) to local business networks (Level 2). There is typically bi-direction data flow within each level, as well as between Level 2 and outward-facing levels. The secure architecture design and use of hardware-based data diode eliminate wired attack vectors from external network including the local business network.

The means that are available for the exploiting the wireless communication channel are represented in Figure 2 as:

- A WCID that is placed in the WSP and may try to decieve the node and/or gateway to look like a legitimate device.
- A WCID that is temporarily brought into the WSP that has the ability to spoof and reconfigure aspects of the plant that would impact the security posture impacting the system supported by wireless or another plant function.

- A WCID may try to send jamming/interference signal to deny/distort communication between sensor node and gateway node.

To limit the opportunity for these means to be exploited, the boundaries of the WSP need to be identified and apply specific controls given in this methodology for monitoring and restricting access to detect any WCID which attempts to communicate along with access process and procedure controls that apply to the plant.

Also as per Figure 2, the whole wireless communication path is intended to be unidirectional except at the wireless communication between the wireless gateway and the wireless node. Two-way communication is required for authentication and authorization of the wireless node, but data transmission is unidirectional. Also, two-way communication due to authentication and authorization can be avoided by implementing static authentication and authorization procedures at the origin (e.g., wireless gateway) before deploying a wireless node.

2.3.3 Identify Potential Threat Impacts on Wireless Communication and Effect on DA Functions

To ensure that the wireless communication is secure, "what and how things can go wrong" in the wireless communication channel should be considered. This methodology uses a model that considers the following threats or mechanisms that can lead to the undesirable impacts given in the previous section. Considering various threats of the intruding device on the wireless communication, a threat analysis is essential to understand and mitigate the threats on wireless communications. To perform threat analysis, it is necessary to identify possible attack impacts (or threat consequences) of a threat source by exploiting DFP, based on the expert knowledge. The threat actors exploit wireless communication infrastructure to attack both wireless infrastructures, and/or the functions. All the potential impacts are classified under 4Ds as deny, distort, disclose, and deceive. Each impact parameter is detailed in Table 1. Also, Table 2 provides the mapping of different attack classes to 4D threat impacts.

Table 1. Threat impact definition with examples

Impact	Security Property Violated	Impact Definition	Example including adverse effects on DA functions. (These are generic adverse outcomes. The PCN should identify specific outcomes and the effects on functions if not mitigated by defenses)
Deceive	Authenticity	Intruding device is able to attach to wireless node and fool the node into believing it is authorized.	A wireless communication enables an intruding device to affect other DFP-supported functions by acting as a gateway to the network supporting CDAs for those other functions. Impacts on functions could have a broad range depending on the functions and details of how the system compromises. Intruding device sends incorrect data/message. Misrepresentation can cause no action to be taken when necessary or inaction or wrong action when it is necessary. The function will be affected adversely by an incorrect decision or control (e.g., incorrect decision leads to unplanned maintenance performed when not required or function component is damaged, or the taken control action impacts safety).
Deny	Availability	The legitimate device cannot transmit data.	The data is lost or received after acceptable latency has elapsed. The decision or control action cannot be taken in the time required causing a potential for a function to fail. Acceptable latency is determined from the need of desired function data.
Disclose	Confidentiality	Sensitive information is disclosed to threat source.	Attacker gains knowledge about the plant and the communication mechanism to improve future attack capability.

Distort	Integrity	Received data is corrupted or modified.	Causes data to be altered between the wireless transmission and reception that creates a misrepresentation of the system state. As per current wireless communication standards, distorting the data is very difficult. The encryption and data correction mechanisms can address data distortion while recovering data. Same outcomes that are possible for deceive or delay can occur with distort. It is delineated from them due to the difference in attack mechanism and the means for detecting and mitigating.

Table 2. Attack classes for each of the 4D threat impact.

Impacts	Attack Classes	Description
Deny	Network jamming	Attacker jams communication between sensor node and gateway by overloading the communication channels.
	Obstacles	Attacker can put some obstacle to disrupt line-of-sight communication between sensor node and the gateway.
Deceive	Identity spoofing	Attacker can spoof as the legitimate device in the environment and cause multiple attacks such as denial of service, false request, etc.
	Impersonation attack	A malicious wireless node can bypass the authentication protocol to gain unauthorized access to the system/network and perform malicious activity.
Disclose	Network profiling	An intruding device can profile the wireless network to get ideas about the current network topology, data transmission frequency, location of the nodes, current occupancy of available resources, etc.
	Eavesdropping	An intruder listens to the ongoing data transmission from wireless node to gateway.
	Snooping on storage	An attacker accesses the operation settings of the wireless node or the sensed data upon gaining access to the wireless node.
	Man-in-the-middle attack	An attacker is placed in between wireless node and the gateway and intercepts and repeats the data transmission.
Distort	Data sniffing	An attacker uses unprotected wireless communication channel to sniff and tamper with the ongoing communication data from sensor node to wireless gateway.
	Data alteration	An attacker may update or alter data collection and transmission settings within the wireless node or gateway.

2.3.4 Plan and Implement Cybersecurity Controls

System function may be adversely affected by an attack exploiting the vulnerabilities in the wireless network identified in the preceding steps. Not adopting sufficient defense mechanisms, which detect or mitigate the threat, is a source of vulnerability the threat actor can exploit. The vulnerabilities in the wireless network are not just specific to the physical layer of the open system interconnection (OSI), but also through the wireless channel, the attack sources can exploit vulnerabilities in other layers (such as data link layer, network layer, transport layer, presentation layer, session layer, and application layer). Thus, it is essential to adopt defense mechanisms at all the OSI layers in the wireless network to detect and mitigate threats capable of producing any of the 4Ds impacts. Accordingly, the defense mechanisms to protect against 4D impacts are explained in detail in Table 3. Each defense mechanism is subsequently explained in detail.

The recommended defense mechanisms are listed in Table 3. Some of those listed are built into every wireless technology. For example, timestamps, sequence number, and source and destination IDs are

integrated into all wireless technology. Other defense mechanisms (such as resource prioritization and signal masking) are added to the wireless technologies. Also, some defense mechanisms (such as RF monitoring and restricted access) are isolated from the wireless technology but need to be deployed to protect/monitor wireless technology. This methodology suggests the operator should make sure that along with the default defense mechanisms, all the add-on defenses, as well as isolated defense mechanisms, are also adopted to adequately protect wireless communication.

Table 3. Defense mechanisms against 4Ds. In the table, (*) indicates default defense mechanisms, (+) indicates add-on defense mechanisms, and (^) indicates isolated defense mechanisms.

Defense	Threats			
	Deceive	**Distort**	**Disclose**	**Deny**
Sequence Number (*)	√	√		
Timestamp (*)		√		√
Time Expectation (+)		√		√
Resource Prioritization (+)				√
Connection Authentication (*)	√	√	√	
Encryption (*)	√	√	√	
Hash (+)	√	√		
Optimized Radio Resource Allocation (+)		√		√
Source & Destination IDs (*)	√	√		
Signal Masking (+)	√	√	√	
Restricted Wireless Access (^)	√	√	√	√
RF Monitoring (^)	√	√		√
Directional Transmission (+)	√	√	√	√

The following provides a detailed description of each defense mechanisms and security controls:

- **Sequence Number [1]:** The data in a wireless network are transmitted as packet/frame. Each packet/frame will have a sequence number. Packets with duplicate sequence or invalid sequence will be discarded. Sequence numbering helps to guard against off-path spoofing attacks attempting to inject packets with forged source addresses (for data injection or reset attacks). That is, arbitrarily injected packets are to be discarded at the receiver due to invalid sequence numbers. On the other hand, tampering distorts the data in a packet/frame, and the receiver cannot decode packet/frame accurately. The receiver can request retransmission of distorted packet/frame using the sequence number.
- **Timestamp [2]:** The timestamp permits a receiving node/gateway to validate the received signed messages. Consequently, a signed message, injected by an unauthorized node, arriving with a timestamp discrepancy MUST be dropped. The message injection by an unauthorized user can happen as a tampering attack, repudiation attack, or denial of service. The timestamp discrepancy is pre-negotiated between sender and the receive node.
- **Time Expectation [3]:** Latency describes the difference between the time when data is expected versus when it is requested**.** Data are sent based on a schedule, and the receiver knows when to expect the data. By setting a time expectation in a scheduled or unscheduled transmission, the receiver can determine if the data are being inserted, deleted, or delayed if the data are not received in the expected or pre-defined time window. The data received outside the time window can be considered as compromised and MUST be dropped.
- **Resource Prioritization [4]:** For the desired system function using wireless, setting up a transmission priority enables nodes to be given a desired wireless resource to transmit data. One

potential approach for setting a transmission priority is through defining the delay requirement of data transmission. The transmissions with low (high) delay requirement will have higher (lower) priority to access the radio channel. This technical cybersecurity control configures digital assets to limit the use of resources by priority thus preventing lower-priority processes from delaying or interfering with servicing of any higher-priority process as described in NEI 08-09 Appendix D.3.5.

- **Connection Authentication [5]:** Necessary and proper authentication and authorization protocols must be developed/adopted to add devices to the network for data transmission. For a faster response, solutions such as digital signatures or a cryptographic-based solution should not be computation heavy. The adopted protocols should also ensure mutual authentication to verify the identity of both communicating parties. This permits actions to be traceable to a verified identity and strengthens non-repudiation on the DA function. Hash Message Authentication Code (HMAC) can be used to authenticate both the source of a message and its integrity. The receiver computes the hash on the received message using the same key and compares the results. If they are same, then the receiver can be assured that the message was correctly received from an authentic sender when static symmetric key is not used.
- **Encryption [1]:** Encryption provides data confidentiality by scrambling the data, and it can only be unscrambled with the knowledge of the key and the algorithm used to scramble. Encryption can be employed in two ways:
  - **Symmetric cryptography** uses a shared secret key for both encryption and decryption, which is shared between the sender and receiver.
  - **Asymmetric cryptography**, also known as public-key cryptography, uses a pair of different keys; a private key and a shareable public key. The public key will be used to encrypt the data which can only be decrypted by the private key. The public key can be known by anyone, but the private key must be kept secret by the owner.
- **Hash [6]:** A function that compresses an input of arbitrary large length into a fixed small size hash code is known as hash function. Input to the hash is message data, and the out is called message digest. Hashes are used to ensure data integrity, data authentication, and digital signature.
  - Cyclic redundancy check (CRC) is a type of hashing that can provide some assurance of data integrity method that calculates checksum for received data as an error-detection mechanism. Particularly, CRC is used as error check for any data transmission including wireless. The CRC check is also used as a performance metric.
  - Message Digest and Secure Hash algorithms use mathematical functions to provide 128 to 512 bits digital representation, which are unique to each message. These algorithms are secure because, for a given algorithm, it is computationally and mathematically infeasible to find a message data that corresponds to message digest or to find two messages that produce the same message digest.
- **Optimized Radio Resource Allocation [7]:** To ensure availability of the sensor data at the right time, the availability of the radio resources is essential. Radio resource allocation includes allocating enough bandwidth to the transmission and setting up access priority over radio resources. In addition, RF channel switching, and a hopping mechanism should be adopted to enable coordinated transmission across multiple devices and also to tackle potential jamming/interference attacks. The resource allocation includes disabling unutilized wireless capabilities and also periodically scan for unauthorized access points and disabling them as described in NEI 08-09 Appendix D.1.17.
- **Signal Masking [8]:** Signal masking is an approach against unintentional disclosure of information to protect the confidentiality of the data transmission. Strong signal masking covers the intended signal by using known signals with strong power characteristics, which not only ensures receiving accuracy of cooperators but also increases receiving difficulty of non-cooperators and reduces accuracy of intercepted data. Common techniques for signal masking include:
  - Padding messages so that they are always the same size regardless of content

- Padding the network by sending dummy messages when there is no legitimate information to send.

Padding techniques should be constructed such that padding information cannot be easily separated from legitimate information.

- **Source and Destination IDs [3]:** Messages that include a unique source and/or destination identifier describing the logical addresses (such as internet protocol [IP] address and medium access control [MAC] address) of the sender allows the receiver to determine if the message was intended for itself and if it came from an expected source. The message is rejected if either condition is not met.
- **Restricted Wireless Access [3]:** It is important to ensure the procedures are in place to keep the unauthorized devices/users from gaining access to network connection without denying access to authorized devices. To provide access, a graded approach should be taken involving the least privileged access to the network. For new connections multi-factor authentication should be used. Also, mechanisms such as override with higher privilege and session time out on network access could be adopted to avoid a denial-of-service situation.

  Each piece of hardware connected to a network has a MAC address. Access to network can be filtered by these MAC addresses [9]. Consult your user documentation for specific information about enabling these features. Utility can also utilize the "guest" account, which is a widely used feature on many wireless networks particularly on WLAN. This feature allows you to grant wireless access to unauthorized or guest users on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials [9].
- **RF Monitoring:** A network of RF receivers can be installed in DA function area at a utility to continuously monitor the RF spectrum in real time. RF monitoring can provide alerts when a unusual or unwanted signal is detected. In addition, the detected signal can be further investigated, and unauthorized devices can be localized. This also provides *geofencing* to ignore transmissions outside the DA function area to minimize false alarms [10]. Effective RF monitoring includes:
  - **Quantifying** what RF devices are on the plant site including those that are mobile and carried in by staff and visitors
  - **Assessing** what communication is taking place between devices on the installed wireless technologies: Cellular, WLAN, LoRaWAN, Bluetooth, etc.
  - **Real-time monitoring and alerting** of detected unwanted signals with a low false alarm rate, feeding into with situational awareness
  - **Establishing RF-restricted zones** where only a set of validated and authorized devices are allowed in that area.
- **Directional Transmission:** Transmitting the data directly toward 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.

Table 4 provides mapping of proposed defense mechanisms for secure wireless communication to NEI 08-09 technical cybersecurity controls described in Appendix D section 2 and 3 for wireless. Table 4 does not address all the cybersecurity controls provided in operator's CSPs, including NEI 08-09 Appendix E Section 10.5, "Security Impact Analysis," for replacing an existing asset with a digital asset that uses wireless technology. Based on the guidance provided in this report, each operator must comply with its CSP if the operator decides to implement a new digital asset with wireless technology.

Table 4. Mapping of proposed defense mechanisms for secure wireless communication to NEI 08-09 technical cybersecurity controls described in Appendix D section 2 and 3 for wireless. [**Green**: defense

strategy that may detect an attack, **Orange**: defense strategy mitigates the attack, and **Grey**: proposed new cybersecurity controls].

NEI 08-09, "Technical Cyber Security Control"	Defense												
	Sequence number	Timestamp	Time expectation	Resource prioritization	Connection authentication	Encryption	Hash	Optimized radio resource allocation	Source and destination IDs	Signal masking	Restricted wireless access	RF monitoring	Directional transmission
D.2.8 Time stamps		√		√									
D.3.2 Application partitioning/security function isolation								√					
D.3.3 Shared resources			√					√					
D.3.4 Denial-of-service protection				√				√					√
D.3.5 Resource priority			√	√				√					
D. 3.6 Transmission integrity	√		√			√	√						
D.3.7 Transmission confidentiality						√							√
D.3.8 Trusted path		√	√					√					√
D.3.9 Cryptographic key establishment and management						√							
D.3.17 Session authenticity	√				√		√	√	√				
Radio resource management								√		√			√
RF monitoring											√	√	
RF-restricted zones											√	√	√

For the proposed cybersecurity control additions, the control description is as follows:

- **Radio Resource Management:** This technical cybersecurity control ensures the availability of radio resources, protection against denial of services, and accessibility to legitimate devices when required

for data transmission, as follows:

- Control and coordinate other devices to occupy the same frequency spectrum
- Use redundant radio channels to reduce and avoid RF interference
- Use priority-based radio resource allocation to other devices/functions
- Adopt multiple access technologies with directional transmission to create multiple and directed spatial streams to reduce RF interference.

- **RF Monitoring:** This technical cybersecurity control detects unauthorized access points and devices present in the WSP as well as the physically protected area.
  - Continuously conducts scans for unauthorized wireless access points/devices in accordance with this document and disables access points/devices if unauthorized access points/devices are discovered. RF monitoring should be connected via wired connection else it will also be a critical digital asset (CDA).
  - Synchronized with safety related and important to safety (SR/ITS) transmissions to validate correct data is received without over-the-air modification.
- **RF-Restricted Zones:** This technical cybersecurity control protects the WSP by controlling transmission power of nodes and employing directional signal transmission to reduce a RF signal leakage outside the physically protected area.
  - Place antennas close to the sensor nodes and perform link budget analysis to set transmission power settings of the sensor node.
  - Use directional antennas to reduce transmission power leakage outside the line-of-sight of sensor node.

2.3.5 Wireless Adoption and Validation

The wireless adoption and validation method includes wireless technology selection and wireless deployment evaluation by incorporating required cybersecurity controls and defense mechanisms. Wireless technology selection considers the outcome of components analysis with cybersecurity requirement and technological objectives of the system. Wireless technology, which satisfies the highest total of technical and cybersecurity requirements, is finally selected as the best candidate. Finally, the selected wireless technology is evaluated for the electromagnetic interference (EMI), RF planning, operation, maintenance, and the identified cyber controls. Deployment evaluation helps to identify any modification or customization to technology, cybersecurity controls, or maintenance approach. The findings or modifications to cyber controls are then reevaluated, modified, and further validated to ensure system is adequately protected.

2.4 Comparison Between Wired and Wireless Network Cybersecurity Control Implementations

This section is provided to show a comparison of the cybersecurity controls that need to be applied to wireless versus wired networks. Apart from comparison Table 5is also indicative of the cybersecurity controls that can be applied for wireless from the existing NEI 08-09, Appendix D's cybersecurity controls. This is an information-only section for stakeholders to understand the relative requirements for implementing a wireless over wired communication. Data sent through wireless networks are more prone to physical access of transmission media by the attackers as compared to wired networks. Also, both the wired and wireless network operate on a packet-based (collection of data in bits) digital transmission system, Thus, a wired network will also have same or similar cybersecurity defense mechanisms as a wireless network except for the defense mechanisms to protect the air gap. Table 5 shows the comparison of cybersecurity defense mechanisms that are available in wired and wireless technologies with reference to NEI 08-09, Appendix D's cybersecurity controls.

Table 5. Cybersecurity defense mechanism comparison between wired and wireless network

NEI 08-09, "Technical Cyber Security Control"	Wired Network	Wireless Network
D.2.8 Time stamps	√	√
D.3.2 Application partitioning/security function isolation	√	√
D.3.3 Shared resources	√	√
D.3.4 Denial-of-service protection	√	√
D.3.5 Resource priority	√	√
D. 3.6 Transmission integrity	√	√
D.3.7 Transmission confidentiality	√	√
D.3.8 Trusted path	√	√
D.3.9 Cryptographic key establishment and management	√	√
D.3.17 Session authenticity	√	√
Radio Resource management		√
RF monitoring		√
RF-restricted zones		√

2.5 Operator To-Do List

Based on the technical analysis, the operator should execute certain tasks at every phase in the cybersecurity analysis to ensure successful implementation, validation, and testing of wireless communication for the intended function. The operator to-do lists are listed in Table 6.

Table 6. Operator To-do list

Information	To-do list
Decompose System into Components	
DFP, interfaces	Identify components including interfaces for wireless communication deployment. Components include gateways, antennas, and wireless-to-plant network (level 1 or 2) interfaces.
Draw DFP for System Components	
Interfaces and communication components	Draw unidirectional data traversing a path from sensor node to destination.
	If wireless section is bi-directional: Plan cybersecurity controls which adequately protect bi-directional communication.
	Identify physical protection area and WSP. Make sure that WSP is well within the PSP.
	Address non-wireless or other attack vectors by following existing cybersecurity control procedures.
Analyze Threat Impacts	
DFP, interfaces, and impacts	Identify all the potential impacts which can be achieved by attack through the wireless communication channel.
	Consider worst-case effects on the function for each of the 4D impacts.

Table 6. (continued)

Information	To-do list
	Identify wireless components/devices which are susceptible to such impacts.
Plan & Implement Cybersecurity Controls	
Threats and impacts	Ensure the defense mechanisms provided for detection as well as mitigation.
	Ensure defense mechanisms protect data path as well as hardware and software services.
	Plan component procurement: 1. Verify hardware components; verify and validate component specifications and configurations; firmware and software specifications 2. Verify network customization capabilities (e.g., allocating RF channels and bandwidths and modifying encryption mechanisms) and access to wireless related information such as signal strength.
Wireless Adoption and Validation	
Defense/cybersecurity evaluation	Perform: (1) realization of application through simulation or experimental testbed, (2) safety, security, and performance evaluation of the function using wireless communication, and (3) modification, update, and retrofit of security controls and technical specifications of the wireless technology.
	Generate results and document cybersecurity implementation performance. The resulting generation includes: (1) the security evaluation, (2) the performance evaluation in terms of QoS, system latency, etc.

2.6 Case Study

This section provides a generic breakdown of the PCN applying the wireless implementation methodology for a ultrasonic-testing (UT) gas-monitoring (GM) (UTGM) system. Some details of the implementation are proprietary to the operator and are left as blocks to be completed by the operator.

2.6.1 Summary of the Function

UTGM is used to check for voids in the process fluid of emergency core cooling and decay heat removal system piping in NPPs per TSTF-523, “Tech Spec Surveillance Requirement” that the piping be sufficiently full of water. Voids in the fluid can lead to water hammer effects and damage to safety-related equipment. Void monitoring has previously been performed by field technicians. Hence, UTGM transitioning from field technicians to a remote sensor system may be categorized as SR/ITS. (For the purpose of this example, PCN, the wireless void detector, is assumed to be SR/ITS.) The sensor system requires a communication channel to allow data to be transferred, recorded, and used by the personnel evaluating the data and using it to inform maintenance decisions. The use of wireless communications to deliver a UT sensor’s data thus requires a thorough investigation on considering wireless technologies to transmit data to plant’s monitoring and diagnostic (M&D) center.

2.6.2 Technical Analysis

The technical analysis provides the cybersecurity evaluation of most impactful threats on wireless communication used in a UTGM function. Cybersecurity controls and procedures for supply chain, wired

network interface, etc. are addressed by the current CSP and cybersecurity policies and procedures.

2.6.2.1 Decompose System into Components

The UTGM sensors will be attached to the piping at location(s) that will provide the necessary data to meet TSTF-523 requirements. The sensors have wireless communication capability with LoRaWAN technology and will be used to connect to a DAS antenna. To the DAS at the backend, the LoRaWAN gateway is connected using cables. The LoRaWAN network configurations are maintained at the LoRaWAN gateway. The LoRaWAN then connects to the NPP communication network (wired network). The wired network is a hub and interface to other plant functions and facilitates data transmission to M&D center through data diode. A diagram of the system illustrating that information path is show in Figure 3.

2.6.2.2 Draw DFP for System Components

The communication between the UT sensor node and DAS antenna is bi-directional (only during the device authentication process). During data transmission, the communication is unidirectional. Secondly, the communication from DAS antenna to the LoRa Gateway, and then further to wired network gateway, it is fully unidirectional. With the use of data diode, the communication with wired network and M&D center is ensured to be unidirectional plus no external data can be sent into the plant network.

The RF-protected area (WSP) starts from the DAS antenna to the UT sensor nodes.

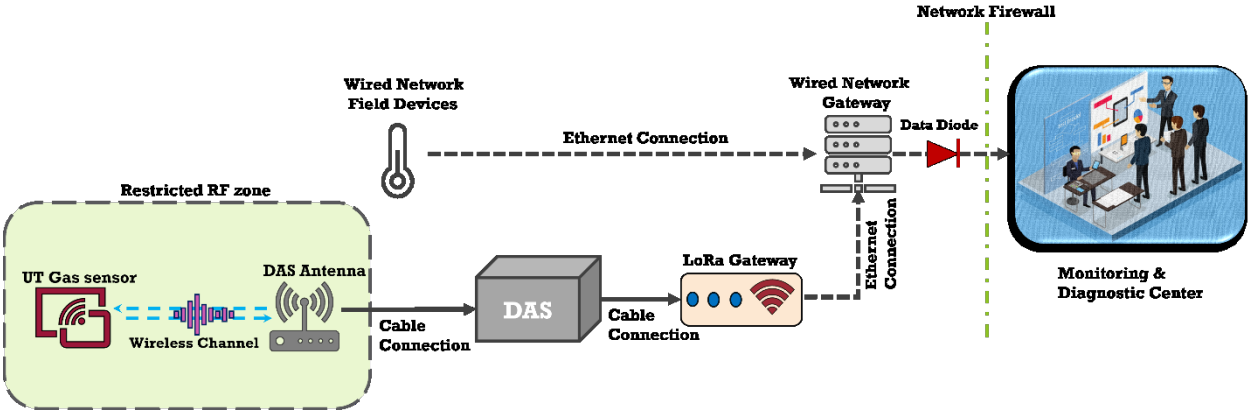

Figure 3. Data flow from UT sensor node to actuator using LoRa Gateway.

2.6.2.3 Analyze Threat Impacts

The 4D impacts due to attack on UTGM is presented in Table 7. Each of the impacts are mapped to corresponding attack and presented with the most impactful attack scenario on UTGM.

Table 7. Impact analysis.

Impact	Example (Worst-Case Consideration)	Objective Violated
Deny	UT sensor node cannot get a wireless channel to transmit data. Receiving data is delayed until the attack can be resolved.	Availability (A)
Distort	Distorted UTGM data can cause no action to be taken (i.e., false negative) when attention is necessary to avoid serious consequences.	Integrity (I)
Disclose	Unauthorized or an outside entity getting access to the UTGM data could compromise confidentiality of the plant information or lead to information gathering for use in another attack.	Confidentiality (C)
Deceive	The attacker gains access to a UT gas-sensor device identities, such as an IP address and session ID, and may provide incorrect data (same as “Distort Impact”) or provide access to other functions supported by	Authenticity (A)

	the plant communication network.	

2.6.2.4 Plan and Implement Cybersecurity Controls

The operator has identified following security protocols with the LoRaWAN technology, which can be adopted to adequately protect functionality (Table 8).

Table 8. LoRaWAN implementation and its security control protocols.

NEI 08-09, "Technical Cyber Security Control"	LoRaWAN Technical Specifications	Threats			
		Deceive	Distort	Disclose	Deny
D.2.8 Time stamps	Timestamp: "**tmst**" in payload		✓		✓
D.3.2 Application partitioning/security function isolation	• Chirp spread spectrum (CSS) with frequency hopping (FH) • DAS with a low-power transmission	✓	✓	✓	✓
D.3.3 Shared resources	• CSS with FH • DAS with a low-power transmission	✓	✓	✓	
D.3.4 Denial-of-service protection	• CSS with FH • DAS with low-power transmission				✓
D.3.5 Resource priority	Set **PRIORITY="HIGH"** in payload				✓
D.3.6 Transmission integrity	• Frame counters: **FCntUp** & **FCntDown** • HMAC with SHA256 + message integrity code (MIC) with AES-128	✓	✓		
D.3.7 Transmission confidentiality	• Symmetric AES-128 • CSS with FH		✓	✓	
D.3.8 Trusted path	• Network ID: **NetID** and device address: **DevAddr** • Frame counters: **FCntUp** & **FCntDown**	✓	✓		
D.3.9 Cryptographic key establishment and management	• Symmetric AES-128 • SHA256		✓	✓	
D.3.17 Session authenticity	• Frame counters: **FCntUp** & **FCntDown** • **OTAA** (over-the-air activation) • Network ID: **NetID** and device address: **DevAddr**	✓			✓
Radio Resource management	CSS with FH	✓	✓	✓	✓
RF monitoring	RF monitoring (additional to LoRaWAN)	✓	✓		✓

Table 8. (continued)

NEI 08-09, "Technical Cyber Security Control"	LoRaWAN Technical Specifications	Threats			
		Deceive	Distort	Disclose	Deny
RF-restricted zones	DAS with low-power transmission	✓		✓	

2.6.2.5 Wireless Adoption and Validation

Wireless adoption and validation have actions including (1) realization of application through simulation or experimental testbed, (2) safety, security, and performance evaluation of the function using wireless communication, and (3) modification, update, and retrofit of security controls and technical specifications of the wireless technology. These steps are detailed in Table 9.

Table 9. Wireless adoption and validation steps.

Inputs	Activities	Example (UTGM)
Realization of Application		
1. Wireless Technology 2. Cybersecurity Controls	Select wireless technology will be adopted or customized to meet security assurance.	LoRaWAN in 900MHz band will be selected. Add a control channel to manage settings of UT sensor node.
	Realization including all subsystems (other safety or non-safety functions as well as existing wireless technologies) operating together	Test feasibility of using UT sensor nodes along with other existing safety or safety-related functions.
	Realization of selected wireless technology on other safety or non-safety applications, which are already adopted on other existing wireless technology/infrastructure	Determine the effect of LoRaWAN on other technologies. Particularly operating in the same spectrum.
	Evaluate EMI or RF impact on other existing wireless infrastructures and associated applications.	Evaluate RF and EMI interferences between LoRaWAN technology and other 900MHz wireless technologies.
	If the realization is on the existing wireless infrastructure, evaluate the impact of adopted security strategies and customizations on other safety or non-safety applications, which are already on the existing wireless infrastructure.	Evaluate the security approaches defined for UTGM on other data transmissions which also use LoRaWAN.
Wireless Deployment, Safety and Security Validation, and Operation and Maintenance Planning		
3. Findings from Realization	Wireless deployment planning includes spectrum allocation for the safety application, determining operating parameters such as signal to interference noise ratio (SINR), transmit power, frequency selection, etc. Also includes licensing and commissioning.	Set transmission power, data transmission interval for UT gas-sensor node to transmit data.

Table 9. (continued).

Inputs	Activities	Example (UTGM)
	Safety validation should consider • The environment conditions in which the safety system operates. • Assessing the safe transmission of the data using performance measures, wireless channel models, and security protocol evaluation. (Simulation approaches are necessary.) • The co-existence of multiple wireless technologies.	Validate that the received UT sensor data is meeting QoS requirements with minimum SINR (-20dB) level and latency (utility dependent) in the NPP environment.
	Operation and maintenance planning include: • Develop alternative approaches in case of wireless infrastructure failure • Develop interference mitigation plan: spectrum allocation among multiple wireless technologies, scheduling of data transmission intervals from safety system node • Develop a resource allocation and scheduling strategy among multiple applications including both safety and non-safety applications • Develop interoperability interfaces (e.g., integrating LoRaWAN to DASs) and protocols • Develop spectrum monitoring plan.	If there is already LoRaWAN deployed and serving other functions, determine effect of LoRaWAN on other technologies. Particularly operating in the same spectrum.
Overall Modification and Retrofit		
4. Operation and Maintenance Planning	Based on findings from wireless network operation and maintenance planning, update wireless technology adoption in terms of: • Changing the interface • Data collection frequency • Selection of RF channel frequency • Customization of security protocols	Set transmission power, data transmission interval for UT gas sensor.

3. COMPARISON OF CYBERSECURITY CONTROLS WITH NIST 800-53

The NRC controls are majorly adopted from NIST 800-53 [11]. A mapping and a comparison of wireless controls mentioned in NIST 500-83 with the cybersecurity controls are described in this document. A brief comparison of such controls is provided in Table 10. The comparison indicates that the cybersecurity controls listed in the methodology well correlate with the wireless controls specified in NIST 500-83.

Table 10. NIST controls mapped to proposed cybersecurity controls.

NIST 800-53 Controls		Description	Proposed Controls
Access Control			
AC-17: Remote Access	Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods	RF monitoring
	Adopt Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions	Encryption
	Managed Access Control	Route remote access through authorized and managed network access control points	Connection authentication and hash
	Disconnect or Disable Access	Provide capability to disable or disconnect remote access	Restricted wireless access
AC-18: Wireless Access	Wireless Access	Protect wireless access to the system using authentication and encryption	Restricted wireless access
	Disable Wireless Networking	Disable wireless network, when not intended for use when embedded within system components	Restricted wireless access
	Transmission Power Levels	Calibrate transmission power levels to avoid wireless access point can be received outside organization-controlled boundaries	Directional transmission
AC-19: Access Control for Mobile Devices		Prohibit the use of unclassified mobile devices and enforce restrictions	Restricted wireless access
Physical and Environmental Protection			
PE-18: Location of System Components		Position system components within the facility to minimize the opportunity for unauthorized access	Establish restricted physical access with PSP
System and Communication Protection			
SC-2 Separation of System and User Functionality		Separate user functionality, including user interface services, from system management. Separate network components, network address, additional access controls.	Restricted wireless access, source and destination IDs
SC-5 Denial-of-Service (DoS) Protection	Restrict Ability to Attack Other Systems	Restrict the ability of individuals to launch a DoS attack against other systems by restricted access and excessive use of wireless resources	Restricted wireless and Directional Transmission

	Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding DoS attacks	Optimized radio resource allocation
	Detection and Monitoring	Employ organization defined monitoring tools and keep track of resources for their availability to effective DoS attacks	RF monitoring
SC-6 Resource Availability		Protect the availability of the resources by allocating (organization defined access priorities and quotas with predetermined number of resources)	Resource prioritization
SC-40: Wireless Link Protection	Electromagnetic Interference	Implement cryptographic mechanisms that achieve protection against intentional attacks	Encryption Hash Signal Masking
	Reduce Detection Potential	Implement cryptographic mechanisms to reduce detection of wireless links	
	Imitative or Manipulative Communication Deception	Implement cryptographic mechanisms to identify and reject imitative or manipulative communication deceptions using signal parameters	
System and Information Integrity			
SI-4: System Monitoring	Wireless Intrusion Detection	Employ a wireless intrusion detection system to identify rogue wireless device and detect attack attempts and potential compromises	RF monitoring
	Wireless to Wireline Communication	Wireless intrusion detection to identify traffic as it passes from wireless to wireline networks	Source and destination IDs Timestamp Time expectation Sequence number
	Correlate Monitoring Information	Correlate information from monitoring tools and mechanisms employed throughout the system	
	Optimize Network Traffic Analysis	Provide visibility into network traffic at external and key internal system interfaces	RF monitoring Timestamp Time expectation Sequence number
SI-10: Information Input Validation	Review and Resolve Errors	Review and resolve errors within organization defined time-period	Hash Timestamp
	Predictable Behavior	Verify that the system behaves in a predictable and documented manner when invalid inputs are received	Source and destination IDs Timestamp Sequence number Time expectation RF monitoring
	Timing Interactions	Account for timing interactions among system components in determining appropriate responses for valid inputs.	Timestamp Time expectation

	Restrict Inputs to Trusted Sources and Approved Formats	Restrict the use of information inputs to designated sources and/or in designated formats.	Restricted wireless access
	Inject Prevention	Prevent untrusted data injections.	Signal masking Directional transmission

4. OUTREACH

In addition to research on technical and regulatory analysis, the secure wireless R&D area also engaged in outreach throughout FY22 as information exchange, methodology review, and comments. A frequent and periodic engagement on the development of the methodology was involved with NEI, industry such as Constellation Energy, NRC Research, and DOE-NE Cyber team. A list of major outreach activities is included in Table 11. These outreach efforts revealed remaining challenges with the methodology that may be addressed by future work. These challenges are discussed in Section 5.

Table 11. Outreach and collaboration activities during FY22.

Activity	Purpose	Date(s)
NEI and Constellation	Briefing about the wireless adoption guidance plan and also discussion on the UT monitoring of gas use case including technical specifications with respect to wireless communication	October 2021
NRC Research	Briefing about the wireless adoption guidance plan and review by the NRC research team	November 2021
NEI Cybersecurity Task Force	Addressing comments and discussion on the wireless adoption flowchart	January 2022
NRC Research	Briefing of wireless adoption flowchart and review and feedback by the NRC research team	February 2022
NEI Cybersecurity Implementation Workshop	Briefing NRC staff on the wireless adoption guidance	March 2022
NRC Drop-in	Presentation on wireless adoption methodology	May 2022
DOE-NE Cyber Team Meeting	Discussion and review of wireless adoption draft	June 09, 2022
NEI Cybersecurity Task Force Meeting	Wireless communications discussion	June 29, 2022
NRC Cyber Fallout Training Course	Wireless security briefing to the NRC inspectors at an INL hosted cybersecurity workshop for NRC staff	July 2022

5. REMAINING CONCERNS ON LIMITATIONS OF THE METHODOLOGY

This section contains a summary of methodology limitations and concerns from members of the DOE-NE Cybersecurity and informal comments from NRC research program. It is anticipated that the industry will explore the use of a form of this methodology in SR/ITS functions in public meetings where the NRC may provide official comments. The following are issues that were identified during

development of the methodology for which a clear satisfactory resolution has not be achieved.

5.1 Testbed Demonstration of a Use Case

At the NRC cyber-fallout presentation, several NRC staff expressed interest in seeing a real demonstration of the methodology on a use case. The demonstration should validate the cybersecurity controls recommended in the methodology and the performance of the system to meet its requirements (e.g., acceptable latency).

5.2 Ability of the Methodology to Differentiate Wireless Applications

The methodology evaluates the wireless communication path separate from the related plant function(s). This means that the analysis does not provide insights into how failure or compromise of the wireless communication path affects the plant function. This is especially important for critical plant functions. To be technically complete, the methodology should evaluate impact of compromise of the wireless channel in the context of the plant function, including how to provide defense-in-depth to protect the function.

5.3 Evaluation of the Methodology with Different Use Cases

UTGM serves a safety-related function by preventing gas that will degrade cooling pumps to accumulate in plant cooling systems. It replaces a manual process currently completed during outages and has a very long maximum latency in data delivery. Thus, the generalizability of the methodology to different SR/ITS function of the current fleet needs to be verified.

In FY23 we plan to work with the NEI and advanced reactors to identify and evaluate higher risk use cases that may clearly delineate where risk of utilizing wireless is and is not acceptable. We will continue to engage with industry and the regulator in this effort. In the first quarter of FY23, we will socialize this guide with industry stakeholders and identify other proposed wireless communications technologies and use cases. Other use cases will be selected for further evaluation and applicability of the guide in the last half of FY23.

5.4 Insufficient Alternative to Current SR/ITS Prohibition on Wireless

This methodology presents an approach, using Section 3.1.6 of NEI 08-09 Appendix A, to define alternative controls to the prohibition of the use of wireless communication for SR/ITS functions in NEI 08-09 rev 6 D1.17. However, introduction of cybersecurity controls that address only the wireless channel may not sufficiently address the intent of the prohibition in its entirety. This is a persistent comment from the engagement with the NRC including comments made during the May 2022 NEI cybersecurity task force “Drop in” with the NRC. This method limits the wireless boundary to a physically secure area and prevents the connection of a rogue device. However, these practices may not be a sufficient regulatory argument regardless of the completeness of the technical adequacy of the controls and defensive strategies.

In FY23, work will continue the process of understanding the basis for the prohibition and assist, if possible, to establish a technical approach that addresses the basis for prohibition. Note: the NRC will not provide official guidance or decision in “drop ins” or discussions held with staff by DOE-NE Cybersecurity R&D Program under the memorandum of understanding between DOE and NRC. Official positions will only be possible in public meetings or during an official review of operator action.”

5.5 Consistency with SR/ITS QA requirements

The methodology described above only considers security considerations and some performance requirements. However, the methodology lacks an approach on how to validate the performance of the wireless link and its robustness factors against cyber-attacks. The methodology needs to consider development of a suite of tests to confirm the performance of the wireless link and associated impacts on system functions. These tests should be considered as part of SR/ITC QA requirements and demonstrate

that 4D impacts cannot be achieved by the adversary.

Wireless for SR/ITS is a new application, and does not meet the form, fit and function of wired networks. In cases, where the WSP extends beyond the data diode, or can be disrupted from outside of the WSP, the use of wireless invalidates the protection of a data diode against remote network-based attacks. This attribute needs to be extensively covered in the FY23 efforts.

6. CONCLUSION

This report presents a wireless implementation methodology intended to assist nuclear power plant operators in identifying an appropriate technological analysis for securing wireless communication for a NPP function. The methodology includes a technical analysis to identify the cybersecurity threat points and their types in a wireless communication channel. Then provided detection and mitigation mechanisms using NEI-08-09 Appendix D cybersecurity controls and additional wireless specific security controls were also recommended. The cybersecurity controls were also compared with NIST 800-53 controls for the completeness. The methodology was validated considering UTGM use case. Finally, the shortcomings/findings from the methodology were identified and described, and path-forward steps were also discussed.

7. REFERENCES

[1] M. A. a. H. R. Hoque, "Towards a threat model for vehicular fog computing," in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics \& Mobile Communication Conference (UEMCON)*, 2019.

[2] D. E. a. S. G. M. Denning, "Timestamps in key distribution protocols," *Communications of the ACM,* vol. 24, pp. 533-536, 1981.

[3] D. a. M. M. a. J. C. Trask, "Cyber security for remote monitoring and control of small reactors," Atomic Energy of Canada Limited, 2014.

[4] M. R. a. K. R. Al Asif, "Cyber security threat modeling of a telesurgery system," in *2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, 2020.

[5] D. a. V. A. H. a. C. P. a. M. A. Sattar, "A STRIDE Threat Model for 5G Core Slicing," in *2021 IEEE 4th 5G World Forum (5GWF)*, 2021.

[6] C. Engvall, *Security in Wireless Sensor Networks for Open Controller,* 2013.

[7] S. Baseer, "Heterogenous networks architectures and their security weaknesses," *International Journal of Computer and Communication Engineering,* vol. 2, p. 90, 2013.

[8] X. a. J. T. Xu, "Design of Strong Signal Masking Covert Communication Transmission Scheme Based on OFDM System," in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, 2019.

[9] CISA, "Security Tip (ST05-003) Securing Wireless Networks," 08 May 2020. [Online]. Available: https://www.cisa.gov/uscert/ncas/tips/ST05-003.

[10] CRFS, "Keeping Data Centers Secure Against RF threats," [Online]. Available: https://www.crfs.com/applicationstory/keeping-data-centers-secure-against-rf-threats/.

[11] J. T. Force, "Security and privacy controls for information systems and organizations," NIST Special Publication (SP) 800-53 Rev. 5 (Draft)., 2020.