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

Technical Letter Report
TLR-RES-DE-2022-007

STUDY OF WIRELESS TECHNOLOGY IMPLEMENTATION IN ISOLATED, HIGH CONSEQUENCE NETWORKS

July 2022

Alexandria Haddad, Christopher Lamb, Jenna deCastro
Sandia National Laboratory

Koushik A. Manjunatha
Idaho National Laboratory

Erick Martinez Rodriguez, Anya Kim, Eric Lee
U.S. Nuclear Regulatory Commission

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

Prepared as part of the Task Order #31310021F0023, “Research on the Nuclear Security Implementation of Wireless Communication Technologies at Nuclear Power Plants” under Interagency Agreement Number #31310019N0005

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.

SANDIA REPORT
SAND2022-8874
Printed July 2022

Sandia National Laboratories

Study of Wireless Technology Implementation in Isolated, High Consequence Networks

Alexandria Haddad, Koushik A. Manjunatha (INL), Chris Lamb, Jenna deCastro

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185
in partnership with
Idaho National Laboratory
Idaho Falls, Idaho 83415

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

The U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) requested Sandia National Laboratories (SNL), Energy Security department to research potential cyber security risks affiliated with introducing wireless technology devices into a risk significant (safety/security critical) network isolated by either hardware-based data diode or air gap. Particularly, the NRC wanted SNL to understand the potential cyber risks based on experiences and insights gained by high consequence industries or government facilities who used wireless technology devices in their isolated safety/security critical networks.

At present, the U.S. operating fleet's cyber security plans (CSPs) prohibit the use of wireless technologies across security levels isolated by a data diode and prohibits the use of wireless technology for critical digital assets (CDAs) associated with safety-related and important-to-safety functions. Therefore, the use of wireless technology in domestic nuclear facilities is limited to CDAs that are not safety-related or important-to-safety and in parts of the network infrastructure that are not isolated with a data diode.

Wireless technology has become ubiquitous in everyday life, and with the upcoming Small Modular and Advanced Reactors, and digital controls, it seems certain that wireless technology will be considered for nuclear safety-significant applications. The NRC asked that SNL research both the nuclear industry and other high-consequence industries such as chemical, aviation, etc. and determine their use of wireless technology in their safety/security critical networks. If they do utilize wireless technology, to what capacity is that technology used, including the potential security risks and mitigations. This report documents SNL's research findings, including information gained from conversations the SNL team had with stakeholders in the nuclear and chemical industries and a select overview of wireless technologies.

This page left blank

ACKNOWLEDGEMENTS

NRC

Anya Kim
Erick Martinez Rodriguez
Eric Lee

Sandia National Laboratories

Lon Dawson
Doug Osborne

Canadian Nuclear Laboratories (CNL)

Dave Trask
Richard Brown

Electric Power Research Institute (EPRI)

Mike Thow
Matt Gibson
Jonathan Turner
Stephen Lopez
Paul Martyak

Cybersecurity and Infrastructure Security Agency (CISA)

Zeina Azar

Office for Nuclear Regulation (ONR)

Barry Hogan
Ian Begbie

Brenntag, North America

Matt Fridley

Dow

Scott Whelchel
Sandra Parker
Maulik Patel

Analysis and Measurement Services (AMS) Corporation

Chad Kiger

Constellation (Formerly Exelon Nuclear)

Michael Dack
David Olszewski

NuScale Power

Kevin Deyette

This page left blank

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
AC	Alternating Current
AES	Advanced Encryption Standard
AGR	Advanced Gas-cooled Reactors
ALOHA	Additive Links On-line Hawaii Area
AMS Corporation	Analysis and Measurement Services Corporation
AODV	Ad-hoc On-demand Distance Vector
AP	Access Points
APP	Application
AR	Advanced Reactor
ARQ	Automatic Repeat Request
ASI	Advanced Sensors and Instrumentation
AU	Austria
BLE	Bluetooth Low Energy
BPSK	Binary Phase Shift Keying
CBRS	Citizen's Broadband Radio Service
CCI	Co-Channel Interference
CISA	Cybersecurity and Infrastructure Security Agency
CNL	Canadian Nuclear Laboratories
CPU	Central Processing Unit
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CSP	Cyber Security Plan
CSS	Chirp Spread Spectrum
dBm	decibel milliwatts
DIMAS	Diagnostics- and Maintenance Server
DL	Downlink
DLL	Dynamic Link Library
DOE	Department of Energy
DP	Decentralized Peripherals
DSSS	Direct-Sequency Spread Spectrum
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
EDCA	Enhanced Distributed Channel Access
EMF	Electric and Magnetic Field
EMI	Electro Magnetic Interference

Abbreviation	Definition
EOC	Ethernet over Copper
EPRI	Electric Power Research Institute
FCS	Frame Check Sequence
FDL	Field bus Data Link
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FSAR	Final Safety Analysis Report
GPS	Global Positioning System
HART	Highway Addressable Remote Transducer
HCI	Host-to-Controller-Interface
HF	High Frequency
HMI	Human-Machine Interface
HPB	Hinkley Point B
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
IoT	Internet of Things
IP	Internet Protocol
IPSEC	IP Security
ISA	International Society of Automation
ISM	Industrial, Scientific, and Medical
KB	Kilo Bytes
LF	Low Frequency
LLC	Logic Link Layer
LoRaWAN	Long Range Wide-Area Network
LTE	Long Term Evolution
MAC	Medium Access Control
MBP	Manchester Bus Powered
MSI	Micro-Star International Co., Ltd
MU-MIMO	Multi-User Multi-Input Multi-Output
NA	North America
NAV	Network Allocation Vector
NE	Nuclear Energy

Abbreviation	Definition
NEET	Nuclear Energy Enabling Technologies
NET	Network
NIST	National Institute of Standards and Technology
NM	Network Manages
NP	Nuclear Power
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
O-QPSK	Offset-Quadrature Phase Shift Keying
OEM	Original Equipment Manager
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
ONR	Office for Nuclear Regulation
OPC UA	Open Platform Communications Open Platform Communications
ORNL	Oak Ridge National Laboratory
OSI	Open Systems Interconnection
PACS	Priority and Actuator Control Systems
PAH	Plant Automation Host
PHY	Physical
PROFIBUS	Process Field Bus
PROFINET	Process Field Net
PS/SAS	Protection Systems/Safety Automation Systems
PWST	Passive Wireless Sensor Technology
QAM	Quadrature Amplitude Modulation
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RFD	Reduced-Function Devices
RFI	Radio Frequency Interference
RFID	Radio Frequency Identification
RTS/CTS	Request To Send / Clear To Send
SCADA	Supervisory Control and Data Acquisition
SF	Spread Factor
SIMATIC	Siemens Automatic
SIVAT	Simulation Validation Test Tool
SM	Security Manager
SMR	Small Modular Reactor

Abbreviation	Definition
SNL	Sandia National Laboratories
SPACE	Specification and Coding Environment
SR/ITS	Safety-Related or Important to Safety Systems
SYS	System
SZB	Sizewell B
TAI	International Atomic Time
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
TPMS	Tire Pressure Monitoring System
TWT	Target Wakeup Time
TXS	Teleperm® XS™
UDP	User Datagram Protocol
UHF	Ultra-High Frequency
UK	United Kingdom
UL	Uplink
US	United States
UTC	Coordinated Universal Time
UWB	Ultra-Wide Band
WinCC	SIMATIC SCADA HMI system
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
Z-AODV	Zigbee Ad hoc On Demand Distance Vector

1. INTRODUCTION

As analog systems and equipment becomes obsolete, it has become increasingly difficult, especially for the current nuclear power plant operating fleet to acquire equipment that is analog or does not come with some form of wireless capability. Furthermore, other industries have found that the implementation of wireless technologies such as satellite, wireless, 5G/4G, Bluetooth, Wi-Fi, etcetera, increases staff and operational efficiency while often reducing overhead costs. The use of wireless technology is prohibited in nuclear power plant CDAs associated with safety-related or important-to-safety functions, which is defined in Revision 3 of NEI 10-04 "Identifying Systems and Assets Subject to the Cyber Security Rule," in the NRC-approved licensees' cyber security plans.

The NRC, as the licensing and regulatory agent for US civilian Nuclear Power Plants (NPP), needs to gain a better understanding on security risks associated with the use of wireless technologies in a mission, safety, security, or consequence critical industries or facilities. To accomplish this, the report looked at other high-risk industries and their approach to wireless implementation.

The first step was to conduct a literature review of other high-risk industries, such as Chemical and Biological, to determine:

a) Whether these industries use wireless technology in their high-risk (safety and/or security) networks, and,

b) if so, to what extent and capacity is the technology used. Or, if not, why not.

If wireless technology is used in these facilities, the second part of the report identifies and includes security risks associated with introducing wireless technologies into a high-risk (safety/security) network.

After conducting an extensive literature review of the publicly available information listed in Section 6. References, the team found that there are no known examples of the use of wireless technology in critical functions or applications for other safety-critical industries and/or high-risk facilities.

There are many examples of wireless implementation in non-safety critical areas found during the interviews, such as administrative and manufacturing, but not safety-critical areas as defined by the nuclear industry (see Section 3 for further discussion).

The project team also spent some time conducting interviews of professionals within government bodies, nuclear stakeholders both domestic and international, and a few high consequence industries. These interviews revealed a plethora of information, primarily a consensus that high-consequence industries have not used wireless technology. However, some of these industries are starting to consider the implications and benefits of wireless use in high-risk areas and are starting to reassess the perceived risks. Sandia also found that high-consequence industries, such as chemical and nuclear, are beginning to look towards existing frameworks and methodologies (such as reports already available from EPRI [1] [2] [3] [4] [5] and IAEA [6]) providing guidance on the implications, benefits, and potential consequences of implementing wireless in high-consequence areas.

Despite this need, during the stakeholder interviews, the perceived risk of compromise of a wireless network outweighed rapid adoption in the nuclear and chemical industry. The

interviews identified the following main challenges associated with the expanded implementation of wireless technologies:

1. Ability to efficiently (such as cost) and effectively address cyber security challenges associated with using wireless technology for high risk systems such as SR/ITS systems.
2. Lack of technical implementation guidance on suitable wireless technologies along with the acceptable implementation examples.

Other barriers included signal interference with proper plant operation, lack of understanding on providing security for wireless technologies used in industrial control systems, and concerns of potential cyber attacks that could (1) bypass the isolated safety (of risk significant) networks and (2) eavesdrop on wireless communications and (3) prevent wireless communications. Although the securing of wireless technology is well researched and documented for IT, there is a need for more research in OT. This indicates future opportunities to research and test cyber security implications and mitigation options for wireless technology.

2. OVERVIEW OF WIRELESS TECHNOLOGY

Wireless communication has been around since the late 19th century, although first demonstrations happened earlier, with the first complete wireless system patent and communication in 1897 by Guglielmo Marconi. [7] Wireless transmission continued with the telegraph, radio, television, and most recently cellular service. Today, when talking about wireless, this usually means digital communication and information transfer via different protocols such as satellite (GPS), cellular, Wi-Fi, Bluetooth, or Zigbee to name the most well-known technologies. Wireless communication is covered in the IEEE 802 series. The current standard for Wireless Wide Area Networks (WWAN) and Wireless Local Area Networks (WLAN) such as cellular and Wi-Fi is 802.11ax. Wireless Personal Area Networks (WPAN) such as Bluetooth and Zigbee are covered in 802.15 (802.15.1 for Bluetooth and 802.15.4 for Zigbee).

As the research for this report is concerned with cyber security risks that arise when introducing wireless technology into a risk significant (safety/security critical) network at an NPP, this report focuses on only those wireless technologies that would reasonably be used in NPPs, such as wide, local, and personal area network technology.

2.1. Types of Wireless

The focus of this report is on local and personal area networks (WLAN and WPAN) and the applicable technology used in each type of wireless network where they are used as designed. The main difference between different types of wireless networks is the coverage area. Table 1 provides a brief overview of these two network types, the applicable IEEE standard, applicable protocols, and approximate range of each technology.

NOTE: There are other wide range wireless networks, e.g., Wireless Metropolitan Area Network (WMAN) and Wireless Wide Area Network, which are not applicable for the purposes of this report.

Table 1 Wireless Networks Overview [8]

	Standard	Protocols	Range	Overview
WLAN	802.11	Wi-Fi	<1 Km	Wireless communication (e.g., internet) within a building or small outdoor area.
WPAN	802.15	Bluetooth, Zigbee	<100 meter	Wireless communication between nearby devices.

Additional supplemental information on some, but not all, of the wireless technologies discussed in this report can be found in Appendix A "Cyber Security Considerations of Select Wireless Technologies" and Appendix B "Technical Description of Wireless Protocols."

2.2. Adaptation in Industry

The industry's desire to use wireless technology for SR/ITS system is (1) to minimize wiring costs, (2) to reduce the cost of updates, (3) to increase the options for replacing analog parts (e.g., most digital replacements include wireless), and (4) to manage SR/ITS systems more efficiently. Although studies have been done by Electric Power Research Institute (EPRI) regarding balance of plant systems demonstration [5], and Luminant Energy's balance of plant wireless flow loop sensing [9], the research for this report reaffirmed that the implementation of wireless in safety/security critical networks has yet to be realized.

One licensee mentioned during their interview that they use wireless to monitor some of their analog gauges to provide data, but they "do not take credit" for the use of wireless, i.e., they still use manual monitoring in addition to the wireless monitoring and they do not make any decisions based on the wireless feedback (see Section 4.2.4 Constellation). Another push towards wireless is the ubiquity of digital devices, and the difficulty finding non-digital replacements for worn out analog devices. During ONR's interview, they stated that one of the challenges for EDF Energy while building Hinkley Point C has been ensuring that the digital devices are all wi-fi disabled, since they usually come with wireless capabilities built-in.

Additionally, according to an Idaho National Laboratories (INL) report on the application of digital twins, the use of digital technology application in future NPPs will rely heavily on wireless communication applications to "monitor and control plant systems, structures, and components (SSCs) and for decision making supporting operations and maintenance." The INL report mentioned several potential digital applications for wireless implementation in NPP including gauge readers, cameras, advanced [wireless] sensors (e.g., vibration), communication, and data transfer. [10]

One of the Department of Energy-Nuclear Energy's (DOE-NE) initiated Nuclear Energy Enabling Technologies (NEET) programs, Advanced Sensors, and Instrumentation (ASI), has wireless featured prominently in their Instrumentation Deployment research area. Specifically, both INL and Oak Ridge National Laboratory (ORNL) are working on projects related to wireless communication application in NPP. [11]

There are many benefits to using wireless technology in NPPs, for example, the work being led by ORNL is looking at Passive Wireless Sensor Technology (PWST). These sensors do not require a power source, are "ultra-miniature," low cost, customizable, easy to deploy and replace, and provide both physical and chemical sensing. [12]

The next sections of this report focus on current regulatory guidance, research in this area that was available, and international guidelines. Following that, Section 4 covers what was learned during discussions with nuclear industry and other high-consequence cyber security stakeholders. The closing section concludes the report and discusses potential topics for further study and discussion.

Finally, during the document review, and later during interviews with industry stakeholders, Sandia found that the definition of Safety-related and Important to Safety could mean different things in different industries. The closest definition to the nuclear industry's definition, both national and international was the chemical industry's definition. This is discussed in the following sections.

3. INDUSTRY REGULATIONS AND GUIDANCE

3.1. Nuclear

For the domestic nuclear industry, cyber security is regulated under Title 10 of the Code of Federal Regulations (CFR) Part 73, Physical Protection of Plants and Materials. Section 73.1 outlines the design basis threat of (a)(1) Radiological sabotage and (a)(2) Theft or diversion of formula quantities of strategic special nuclear material, by several methods including (a)(1)(v) and (a)(2)(v) A cyber attack. Section 73.55(b)(2) clarifies that power reactors must defend against the design basis threat of radiological sabotage, which includes implementation of the cyber security rule in described in Title 10 CFR §73.54 "Protection of digital computer and communication systems and networks." [13]

The cyber security rule establishes the requirements to defend against the Design Basis Threats (DBT) via cyber attack and to implement and maintain a cyber security plan that implements the cyber security program requirements of the regulation. The rule is applicable, and specifically calls out four functions and their support systems that must be protected in §73.54(a): [13]

(1) The licensee shall protect digital computer and communication systems and networks associated with:

(i) Safety-related and important-to-safety functions;

(ii) Security functions;

(iii) Emergency preparedness functions, including offsite communications; and

(iv) Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Since the cyber security rule, 10 CFR 73, is a high level performance based rule, the rule does not provide how performance objective of the cyber security rule is achieved. However, the rule requires licensees to submit their CSPs for NRC's review and acceptance. The NRC accepted licensees' CSPs describe how the cyber security programs are implemented to comply with the cyber security rule. The NRC accepted CSPs includes the prohibition of use of wireless technology. The CSP templates included in RG 5.71 "Cyber Security Programs for Nuclear Facilities" as referenced earlier in this report in and in the industry's guidance NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors" prohibits use of wireless technology for CDAs associated with safety-related and important-to-safety. For example, the regulatory guide 5.71 states that the [Licensee/Applicant] is responsible for the following:

- only allowing wireless access through a boundary security control device and treating wireless connections as outside of the security boundary,
- prohibiting the use of wireless technologies for CDAs associated with safety-related and important-to-safety functions,
- disabling wireless capabilities when not utilized,
- establishing usage restrictions and implementation guidance for wireless technologies,
- documenting, justifying, authorizing, monitoring, and controlling wireless access to CDAs and ensuring that the wireless access restrictions are consistent with defensive strategies and defensive models, as articulated in RG 5.71, and

- conducting scans [no less frequently than once every week] for unauthorized wireless access points, in accordance with this document, and disabling access points if unauthorized access points are discovered.

Of particular importance is the second bullet which expressly prohibits wireless technology use in a safety-related or important to safety CDA.

Industry guidance NEI 08-09, Section D 1.17, Appendix B also provides "Wireless Access Restrictions" that the industry adopted in their CSPs, prohibiting wireless technology use in SR/ITS systems. Licensees must maintain compliance with their Cyber Security Plan (CSP). However, licensee can make changes to their CSP via LAR or 50.54(p)(2). Additionally, CSP section 3.1.6 allows the licensee to implement and use an alternate countermeasure for the CSP controls if the countermeasure mitigates the attack vector the control was intended to protect. However, to apply Section 3.1.6, the licensees need to recognize and address cyber security concerns stems from the following:

- The CDAs located inside the plant and behind the data diode inherited the protection provided by the prohibition of the wireless technology
- The use of wireless technology may provide attack vectors that can be exploited by an adversary to bypass the data diode from external networks or devices. These attack vectors were eliminated by the prohibition of wireless technology usage.,
- The baseline security controls provided in the licensees' CSP are tailored from NIST SP 800-52 and SP 800-83 based on that the CDAs associated with safety and security would have limited attack surface due to the established deterministic network isolation from external networks by:
    - Implementing data diodes to force one-way communication out to the business networks
    - Prohibit the use of wireless technology for CDAs associated with safety functions.

Additionally, although wireless technology is not specifically addressed, RG 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, provides acceptable NRC methodologies cyber-security of digital computers for the four functions from §73.54(a)(1). [13]

3.2. Chemical

The domestic chemical industry's regulatory guides can be found in Title 6 CFR Chapter 1 Part 27, Chemical Facility Anti-Terrorism Standards with the Department of Homeland Security (DHS) acting as the Chemical Sector Risk Management Agency (SRMA). [14] The Cybersecurity and Infrastructure Security Agency (CISA) branch of DHS maintains the Chemical Facility Anti-Terrorism Standards (CFATS). [15] The focus of the regulatory guidance is to prevent chemical release, theft or diversion, or sabotage from "high-risk chemical facilities to ensure security measures are in place to reduce the risk of certain hazardous chemicals being weaponized." [16]

The International Organization for the Prohibition of Chemical Weapons (OPCW) defined chemical safety as "measures to prevent non-deliberate releases of toxic chemicals into the environment and to mitigate the impact if such events occur" and chemical security as "measures to prevent deliberate releases of toxic chemicals and to mitigate the impact if such events

occur." [17] For the purposes of this paper, the chemical industry uses "security" in similar manner as the nuclear industry uses "safety-related," as it pertains to the DBT. During conversations with chemical industry cyber security professionals, this also seemed to be the case (see Sections 4.1.2 and 4.1.3).

3.3. Literature Review

The team reviewed hundreds of papers and reference documents, listed in Section 6 References. Although there is a large amount of research and documentation relating to securing wireless in information technology networks, there was little documentation the team could find that spoke specifically to high-consequence isolated networks that used wireless technology. The team's premise was confirmed during interviews with Nuclear and Chemical industry subject matter experts and stakeholder interviews. Wireless has yet to readily adopted in high-consequence industry, and if it is used, it is not documented publicly.

The Sandia team conducted a literature review of publicly available information and scholarly, peer reviewed articles and reports. The team initially searched for documentation specifically referencing high-consequence industry use of wireless technologies *within isolated (air-gapped or data diode) networks*. After finding no information, the search was broadened to use of wireless in high-consequence industries, regardless of isolation, with safety and security concerns like the nuclear industry and again, there was no reference to a specific industry. Although this search uncovered many research papers, reports and general guidance speaking to how to secure wireless for high security IT networks, search did not find any publication providing information regarding how wireless technology was implemented into secure, isolated networks in risk significant facilities.

3.3.1. EPRI Technical Reports

A study was conducted by EPRI in 2017 titled "Use of Cellular Network and Distributed Antenna Systems to Improve Connectivity and Increase Data Transfer." [18] The SNL team reviewed the study and spoke with the EPRI authors. This study specifically addresses the need to increase coverage areas of "Wi-Fi technologies (as designated by IEEE 802.11a, b, g, and n) that operate at 2.4-GHz and 5-GHz frequencies." While the report provides great information about using wi-fi technologies in NPP, it is focused on cellular networks only and amplifying the range of those networks using distributed antenna systems.

For implementing wireless technologies in SR/ITS in NPP, EPRI suggested their "Cyber Security Isolation for Maintenance, Monitoring, and Diagnostic Applications in Nuclear Power Plants," Technical Report #300-200-8206 [19] would be of better use. There are many additional reports developed by EPRI that are also related to the implementation of wireless in power plants. Please see Section 6 References for a list of some of their publications that informed this report. [19] [1] [2] [4] [3]

3.3.2. IAEA Technical Report

The IAEA report, Application of Wireless Technologies in Nuclear Power Plant Instrumentation and Control Systems (IAEA No. NR-T-3.29) [6] is an international nuclear industry reference to the implementation of wireless in NPP. From 2015 to 2017 the International Atomic Energy Agency (IAEA) conducted a Coordinated Research Project (CRP), comprising a diverse group of industry experts on the use of wireless technologies in the NPP industry. In 2020 the CRP

published a technical report as part of the IAEA Nuclear Energy Series, titled Application of Wireless Technologies in Nuclear Power Plant Instrumentation and Control Systems NR-T-3.29. [6] The objective of this technical report was to "…develop and demonstrate advanced wireless communication techniques for potential implementation within the I&C systems of NPPs…" Additionally the scope was "An overview of wireless technology concepts such as network topology, signal propagation, EMI/RFI and energy source considerations is presented, along with related concerns or limitations in an NPP environment." [6]

According to this report, "owing to challenges such as computer security, electromagnetic and radiofrequency interference and coexistence, power source/battery use, and response time issues, the nuclear industry still has not adopted" [6] wireless technology in a broad sense. The IAEA report supports adopting wireless in NPPs (both current fleet and upcoming builds such as AR/SMR), because of the potential benefits and improvements which include increased safety, more reliable communication, enhanced productivity, reduced operation, and maintenance costs, among other enhancements. However, the industry has been reluctant to adopt this potentially beneficial technology, as previously mentioned, because of lack of information and challenges related to EMF interference, power availability, and cyber security concerns such as the proper protection of wireless communications to prevent ransomware attacks, eavesdropping via RF transmitters, or jamming of wireless signals, to name a few areas of concern.

This report was also focused on implementation of wireless in a facility, and therefore the findings, while interesting for follow on work, were outside the scope of this project.

4. INSIGHTS ON THE SURVEY ON WIRELESS TECHNOLOGIES

Over the course of several months, Sandia personnel conducted several interviews of industry experts, members of other industries, and key stakeholders in the NPP space. General trends that emerged from the interviews are that other agencies are researching the same issues, a general distrust of wireless technology being used in critical or safety functions, an understanding that manufacturers are slowly forcing NPPs to purchase equipment with wireless capabilities, and an overall desire for guidance regarding how to securely implement wireless into an NPP. At this time, the interviews uncovered only two use cases of wireless being used in safety functions, and both of these were in the research phases at a plant in the United Kingdom (see Section 4.2.2 ONR – United Kingdom, on page 31. Otherwise, critical infrastructure industries, i.e., nuclear, chemical, or biological, and other facilities are avoiding use of wireless until additional acceptable implementation guidance is published and/or research can prove that wireless can be just as safe as analog and wired systems.

Table 2 provides the date of each interview, interviewee information, and associated organization. The following sections provide more detailed information the interviews and insights. Because of the open, free-flowing style of discussion during the interviews, Sandia was able to gain insights that would have otherwise been missed.

Table 2 Interview Highlights1

Interview Date	Attendees	Role	Org
11/16/21	Dave Trask	Cyber Security	Canadian Nuclear Laboratories

[1] All of the external organizations and people interviewed asked for copies of the paper when it was published.

Interview Date	Attendees	Role	Org
	Richard Brown	Cyber Security	
12/14/21	Mike Thow Matt Gibson Jonathan Turner Stephen Lopez Paul Martyak	Program Manager Technical Executive Principal Project Manager, I&C Principal Technical Leader Sr. Technical Leader	Electric Power Research Institute
12/15/21	Zeina Azar	Section Chief	Cybersecurity and Infrastructure Security Agency
1/4/22	Barry Hogan Ian Begbie	Nuclear Safety Principal Inspector Nuclear Security Inspector	Office for Nuclear Regulation, UK
1/5/22	Matt Fridley	Director of Safety and Security	Brenntag NA, Inc.
1/5/22	Doug Osborne	DMTS, Nuclear Engineer	Sandia National Laboratories
1/10/22	Scott Whelchel Sandra Parker Maulik Patel	Chief Security Officer Global Improvement Director Cyber Security Sr Director - Digital M&O IT/OT	Dow
1/2/22	Chad Kiger	EMC Engineering Manager	AMS Corp.
1/2/22	Michael Dack David Olszewski	Cyber Security Manager, IT Central Design Engineering Manager	Constellation, (FKA Exelon)
2/10/22	Kevin Deyette	Program Manager, Nuclear Security and Emergency Preparedness	NuScale

While only one hour was allocated for each interview, every single group interviewed was willing to assist and collaborate for follow-on work. At a high level, the interviews provided the following insights:

- The chemical industry, like the nuclear industry, has been very risk averse to using wireless in its high-consequence areas. As of the writing of this report, neither of the two industry leaders interviewed have implemented wireless outside of administrative and manufacturing areas. Brenntag doesn't even allow use digital assets in their high-consequence areas.
- The reasons given for not using wireless in these high-consequence areas, were the same reasons listed in the IAEA report discussed in Section 3.3.2. Additionally, not knowing how to secure wireless technology with 100% certainty was a concern.
- The Banking industry, Aviation industry, DoE, and DoD all use wireless extensively. DoD and DoE even allow some exceptions to the use of wireless in their upper-level classification Sensitive Compartmented Information Facilities (SCIFs). This information is discussed in more detail in the upcoming sections.
- Most interestingly, and another vector for future work, CISA is in the process of updating the CFATS to include information and guidance about using wireless in high-consequence areas of chemical plants. Scott Whelchel, the Chief Security Officer for Dow, previously worked on the National Radiological Emergency Preparedness (NREP)

team for his local region and was very excited about potential collaboration with CISA (CFATS) and NRC to update regulatory guidance.

- And finally, CNL is starting research and development into wireless implementation into SR/ITS areas and assets. This is another avenue for potential collaboration.

4.1. Other Industries and Organizations

As previously touched on in the introduction, there is (little to) no public information on how specific industries have implemented their wireless networks and applied security controls in their more secure areas. This is to be expected, for if the information was easily available, Advanced Persistent Threats (APTs – the bad guys) would be able to easily hack into the very system the cyber security specialists are trying to protect. Because of the lack of published information, it was decided to do personal interviews. This also had its own set of challenges, as the team is very well connected in the nuclear industry but less so outside of that area.

The team did attempt a few cold requests, with no response. Understandably, the fear of a fake request, or good practices to guard against social engineering, were likely contributors to the lack of response to the cold requests. The Nation is in a state of hypersensitivity to cyber attacks on critical infrastructure, albeit disappointing, it was also encouraging that people were being cautious. Fortunately, the NRC had a contact, and provided an introduction to a CISA representative, which led first to a contact at Brenntag and then to Dow.

4.1.1. United States Cyber Security and Infrastructure Agency

The Chemical Facility Anti-Terrorism Standards (CFATS) is the nation's first regulatory program focused specifically on security at high-risk chemical facilities. Managed by the Cybersecurity and Infrastructure Security Agency (CISA), the CFATS program identifies and regulates high-risk facilities to ensure security measures are in place to reduce the risk that certain dangerous chemicals are weaponized by terrorists. Because of this and looking for contacts and connections to industries other than nuclear, the team was introduced to Zeina Azar, a Section Chief, at CISA. What the team was hoping to find was insight into other high-consequence industries are managing cyber security with respect to wireless communication, as well as gaining connections to those industries.

The CFATS program is currently conducting research into use of wireless technology, especially with respect to security of high-risk chemical facilities from terrorist exploitation, as although the CFATS risk-based performance standard for cybersecurity [15] does cover remote access at a high level, it doesn't specifically call out wireless and cellular.

The Agency is currently considering what things should be included in a potential update, but at this moment does not have a deep enough analysis to encompass current wireless/mobile threats. They are having similar challenges the nuclear industry is having regarding technology growing so fast and the need to update regulatory guidance and recommended security best practices quickly. CISA believes that the CFATS model of performance-based regulation does help in these instances as a capability can be described for industries to meet rather than specific security measures; however, that approach does not account for all future technological changes that may occur and regulatory guidance will need to be prioritized for completion.

Their research efforts have centered around reviewing the National Institute of Standards and Technology (NIST) best practices framework for wireless access and associated practices for securing access. [22] [23] [24] [25]

4.1.2. Brenntag, North America

The team scheduled a meeting with Matt Fridley, the Director of Safety and Security for Brenntag North America (BNA) on January 5, 2022. Brenntag, a German chemical distribution company, is the largest chemical distributor in the world. In addition to his position at Brenntag, NA, Matt also served as:

- Member of U.S delegation for chemical security at the G7 Summit [26];
- Current Chairman of NACD Government Policy and Advocacy Committee;
- Member of Global Congress on Chemical Security and Emerging Threats [26]; and
- Current member of INTERPOL's Global Advisory Group on chemical security.

Matt was very generous with his time and spoke quite frankly with the team about Brenntag's decisions around wireless technology. He explained that Brenntag is extremely judicious in the use of wireless technology within the facility. Brenntag does not allow any industrial control systems to operate on their sites. Systems are all operator controlled to reduce risk of cyber intrusion. Safety or security systems such as camera surveillance, intrusion detection, fire alarms, etc. are kept separate from the other business operations by running two separate connections into each facility. Their business network exists behind a firewall and all other non-business-related traffic moves through a separate line. Both are behind a firewall and monitored. Everything is separated physically. If there was a virtual Wi-Fi system, that would eventually direct back to a security internet server that is managed through the server.

The only systems that have any external connection are telemetry for a few tanks, like nitrogen. This allows the vendor to see on demand what tanks needs to be serviced and is only allowed for chemicals that are not critical or regulated by DHS anti-terrorism standards [15]. Any chemical on the Appendix A [21] list is not connected to the outside world. For example, systems used to monitor/make bleach are physically disconnected through the wire and re-connected if technicians need to do a service. If that happens, all hoses to system are physically disconnected so an attack cannot take place during a service.

The interview team asked if BNA used wireless technology in any physically closed system, either physically isolated or separated by data diode. The response was "rarely." Matt said that BNA does have two systems in the U.S. that they are using for testing, to determine if they can be built safely. He reiterated that these "test systems" do not have any external connections and they are testing with a lot of engineering and operational controls during non-business hours when the operational system is shut down.

Matt then mentioned that quite a bit of the wireless risk aversion at Brenntag stems from the May 2021 cyber-attack by the APT DarkSide ransomware (gang), targeting the North American division. "As part of this attack, the threat actors encrypted devices on the network and stole unencrypted files." The attack cost the company over $4.4 million in Bitcoin to "receive a decryptor [sic] for encrypted files and prevent the threat actors from publicly leaking stolen data." [27] Although the information that was stolen was not business critical fortunately

("unlike the attack on facilities in Florida" [28]) Brenntag cannot risk having their chemical systems attacked.

4.1.3. Dow

The Dow Chemical Company is multinational corporation based in Michigan, US. According to the Chemical and Engineering News, it is the third largest chemical company in the world. [29] The team was able to meet with three top executives at Dow to discuss the company's use of wireless technology on January 10, 2022:

- Scott Whelchel, Chief Security Officer,
- Sandra Parker, Global Improvement Director Cyber Security, and
- Maulik Patel, Sr Director - Digital M&O IT/OT

Scott described the multi regulatory agencies, including US Environmental Protection Agency (EPA), US Occupational Safety and Health Administration (OSHA), US Coast Guard, and CISA. According to the Dow team, the company has been investigating the use of wireless throughout its facilities. However, currently, in high-consequence areas where Dow is concerned about leakage or theft, wireless and even Programable Logic Controllers (PLCs) are not used. Dow is taking a stepped approach, from least to more consequential, to make sure all networks are available and secure and meet all cyber security requirements. They started with their administrative areas and are now working on adding wireless technology to their manufacturing industrial areas.

Maulik specified that Dow's scope is global and there are different options available for industrial wireless connectivity based on the location of the plant, they have developed two different forms of wireless technology implemented in facilities internationally. For this discussion, as this was an NRC funded study, the conversation was kept to how Dow is developing connectivity in the US. Currently Dow has developed and implemented an industrial wireless network and a private LTE network.

The industrial wi-fi network is used in digital manufacturing domain, not in high-consequence areas. Deployment has been difficult, expensive, and requires numerous access points for ubiquitous coverage. Dow representatives declined to talk about their industrial wi-fi any further because of these challenges and the belief that it would not benefit Sandia's research. The other technology currently in use is a citizen's broadband radio service (CBRS) which is a private cellular LTE network which has the same speeds and bandwidth available to the public. The CBRS allows facilities to augment Wi-Fi and cellular coverage, reduces the number of antennas with omnidirectional coverage, but does require a significant amount of effort to ensure the network is fully complaint with cyber security principals such as CISA's CFATS regulatory program.

Dow employees are aware of the EMI/RFI issues encountered by UK licensees and conducts routine checks to ensure that wireless devices are not interfering with critical equipment. Dow engineers are also working to develop a network which is available but also secure which meets all cyber security requirements. Engineers are working to implement wireless in areas of least consequence and are working towards implementation in high-consequence areas.

Another interesting topic which was discussed was Dow's use of tabletop exercises for the identification, classification, and response processes and systems and their latest efforts to incorporate cyber security into their crisis management exercises. As they conduct these exercises, they have continued to learn and consequently developed two classifications of cyber intrusion responses, one which is more draconian than the other. They use both internal and external resource for benchmarking etc. Additionally, they also participate in Cyber Storm, "CISA's biennial exercise series, provides the framework for the most extensive government-sponsored cybersecurity exercise of its kind. The exercise series brings together the public and private sectors to simulate discovery of and response to a significant cyber incident impacting the Nation's critical infrastructure." [30]

Sandra and Maulik both spoke to Dow's formal security risk assessment that is a complex deliverable to set up the controls to ensure that data can be accessed only by approved individuals in Dow. Because of security concerns they did not go into detail, however, they did say that they are using a security design-based approach to make sure right principals are integrated from the beginning and everything can be traced back to well-known standards. Additionally, none of the untethered or other mobility solutions can access their network without some type of VPN.

4.1.4. Analysis and Measurement Services Corporation (AMS)

The AMS Corporation supplies the nuclear industry with instrumentation and control (I&C) system testing equipment, training, and services. The team spoke with Chad Kiger, EMC Engineering Manager, on February 1, 2022. Chad's work is with frequency and electromagnetic interference. He mentioned that if deploying wireless in a SR/ITS area, IEC Standard 62988, Nuclear power plants - Instrumentation and control systems important to safety - Selection and use of wireless devices, should be consulted. He also mentioned implementation of wireless may be difficult to achieve without a better understanding, however wireless technology would be a significant cost savings for the industry. Comparing cost of implementation with overall cost savings of wireless vs wired is another area for future study.

Chad did not know of any domestic nuclear facilities using wireless in SR/ITS applications. However, AMS has noticed that some NPPs have deployed cellular networks, specifically LTE, and have installed and use sensors for monitoring and insight into plant activity outside of SR/ITS functions. Additionally, there has been a push for sites to implement wireless capabilities for monitoring purposes to save operators from conducting rounds to collect data, again, leading to significant cost savings.

4.1.5. Aviation

While the team didn't have an opportunity to personally interview anyone in the aviation industry, there is quite a bit of information available to determine that yes wireless is used in the industry and that wireless cyber security is big business for this industry. Wireless technologies used in the Federal Aviation Administration's (FAA), Transportation Security Administration (TSA), and in aircraft both commercial and private.

The literature review revealed that the industry definitions for security were more in-line with the NRC definition of safety-related and their restrictions on wireless. For example, the National Air Transportation Association (NATA) explains that safety is governed by the FAA's "safety

standards and rules to stop unworthy pilots from flying and keep faulty aircraft on the ground," while the DHS agency TSA is the governing body for the "security of the infrastructure." [31]

Although the definitions were helpful, there are several organizations and initiatives that are addressing cybersecurity in the aviation industry. The FAA's Air Traffic Group (ATO) has multiple initiatives in cyber security, one is the Aviation Cyber Initiative (ACI), whose stated mission is "to reduce cybersecurity risks and improve cyber resilience to support safe, secure, and efficient operations of the Nation's Aviation Ecosystem." [32]

The FAA's regulatory guidance, JO 1370.118 - Air Traffic Organization Wireless Policy, with the stated intent of "is to optimize the number of devices based on organization and mission, without compromising the operational needs of the agency." [33] An article from RF Wireless World stated that, "Various wireless technologies are used for air traffic management and control in aeronautical communication applications. It includes measurement of distance, aircraft collision avoidance, surveillance beaconing etc." [34] A Globe New Wire article from 2021 projected that the aviation cyber security market is projected to be worth upwards of $5 Billion by 2030. [35]

4.1.6. Banking

Does the banking industry use wireless communication technology? If you have ever deposited a check using your cell phone, you will know that the answer to this question is a resounding yes, this industry does use wireless technology. As with the aviation industry, Sandia did not get a chance to talk to anyone in person about how they use and secure wireless technology. The banking industry may allow wireless technology for limited application (e.g., what the NRC could consider as non-safety CDAs). The research did not identify any issues with respect to the use of wireless technology in financial critical (non-customer access) data, which would be like those areas considered to be safety or high consequence as defined by the nuclear and chemical industry. Nevertheless, there was quite a bit of information about cyber security and wireless on mobile banking, specific to IT.

Depending on the application, the industry keeps financial information safe using a variety of controls such as: [36]

- Anti-virus and anti-malware protection.
- Firewalls.
- Secure Socket Layer (SSL) encryption.
- Cookies.
- Multi-factor authentication measures.
- Credential confidentiality.
- Automatic logout.
- Biometric authentication.
- Limited liability.

Overall, the team was not able to find any publicly available information that the banking industry is using wireless technology in high consequence areas.

4.1.7. Other Government Agencies

The team spoke to an SNL SME that works with the corporate network as well as hearing from a Navy representative involved with a Navy Research Lab (NRL) wireless program. Most national laboratories, with some exceptions, do not allow wireless, mobile, or Bluetooth devices in the limited areas. In higher classification secure Sensitive Compartmented Information Facilities (SCIFs) there is almost a complete ban of any wireless technology. Note that this discussion is focused on Information Technology (IT) and less on Operational Technology (OT).

There are a variety of reasons why wireless transmitters and even receivers are not allowed in or near high-security environments. Some of the specifics are sensitive and even classified.

The first concern is Operational security (OPSEC). Radio Frequency (RF) transmitters intentionally introduced into a high-security environment can be used for eavesdropping purposes. Therefore, it is obvious that reducing the number of RF transmitters in a high-security environment is a good thing in terms of information protection. Information is fragile – it can be copied without the original going missing or being modified, and once any copy is compromised the damage is done.

Separation of RF of different classifications, or TEMPEST concerns. “TEMPEST is a U.S. National Security Agency (NSA) specification referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations. TEMPEST covers both methods to spy upon others and how to shield equipment against such spying. The protection efforts are also known as emission security (EMSEC), which is a subset of communications security (COMSEC).” [37]

Electricity is the flow of electrons and electrons in motion create an electromagnetic field. Hence, any electrical or electronic device emanates RF energy. This RF energy inevitably is modulated in some way by the information observed or processed by the device – voices in the case of phones, data in the case of computers. Although modern devices do a good job of reducing the types and power of these RF emanations, they can be directly observed over the air.

However, if these RF emanations become coupled to nearby wires, which can act as antennas, their RF signals can travel longer distances until they can be observed by an eavesdropper. In high security environments, electronic devices are required a certain amount of physical separation between classified and unclassified devices (the minimum physical distances required between unclassified and classified devices are OUO). RF transmitters exacerbate TEMPEST concerns. If an RF transmitter is nearby such a device, it becomes even easier for an eavesdropper to obtain the information contained within those emanations from much greater distances.

Strong RF signals can be used to power otherwise passive eavesdropping devices. The most famous example of this is the passive cavity resonator that the Russians managed to sneak into a US embassy back in the 1940s and 1950s. The "thing," as they called it, does not have its own power source and, when not being powered by an external RF source, it is completely benign and useless. But when powered remotely by a high-enough power RF source, it begins modulating the radio waves that power it enough that these waves contain useful information for eavesdropping (e.g., room audio). [38] The technology is old but has only improved with time, of course.

Radio Frequency signals of sufficient strength and character can cause data integrity concerns. Just as an electron in motion creates an electromagnetic field, the opposite is also true: an electromagnetic field can cause an electron to move. Even though modern devices are engineered to some degree to reject unwanted interference from external RF sources through things like shielding, it is completely possible for an attacker to use an RF transmitter to alter data being processed by a device. The work required of an attacker here is complicated, but it is known that this is not an impediment for adversaries with a lot of capability and patience.

The more RF energy in a physical space the harder it is to sort out. In high-security environments, there are teams of technical professionals who hunt for worrisome RF emanations (bugs, leaky capacitors in equipment, unauthorized transmitters). This is a difficult job, but it is even harder the more sources of RF emanations that are in or nearby a physical location. Reducing the number of such sources makes the job a bit easier, which means these teams can cover more court. (Note that just about any details of any other government agency's Technical Security Countermeasures programs will be OUO at minimum.)

In other high-security situations (not for data protection), RF transmitters are highly regulated for safety reasons. In many areas where energetic materials (e.g., explosives) are stored, for example, transmitters are either banned completely or highly regulated because the RF energy can cause such materials to become unstable. RF transmitters also require energy sources (e.g., batteries) to function and efforts to eliminate all unnecessary energy sources are prioritized.

4.2. Nuclear Energy

4.2.1. CNL – Canada

CNL is conducting similar research into the use of different technologies and is looking at all protocols and locations inside and outside the plant walls.

CNL is not limiting their investigations to any single technology, instead they are investigating all options and are more concerned about the risks that each option poses. The cyber risks that are being considered are access protocols and how those protocols impact the facility's attack surface, as defined by the NIST glossary. They are also concerned with cyber security at the application security level and are working to limit the number of trusted devices that have access to their network.

CNL's research and investigations are still in the early stages but the team is investigating a variety of different technologies ranging across cellular, satellite, wireless, and Bluetooth. Currently, CNL's researchers are operating under the assumption that all off-the-shelf wireless devices are not to be trusted as they are concerned about access protocols, application security and trusted devices, and reliability to withstand jamming or scrambling.

4.2.2. ONR – United Kingdom

In the UK, it is incumbent on the licensee to prove that wireless technology is safe. UK Licensees have researched signal interference. Two use cases:

1. Wireless operation of a polar crane
2. Wireless operation of autonomous vehicles.

Like US nuclear facilities, those in the United Kingdom are also expressing interest in implementing wireless technology. However, ONR interviewees noted that UK licensees are

responsible for proving that their implementation of wireless technology is secure. ONR does not provide direct guidance to licensees regarding wireless technology. As EPRI staff noted in their interview, this is a costly endeavor and as such, adoption of wireless technology in UK NPPs has been slow. Interviewees recognized that the market is forcing NPPs to adopt wireless technology so there is an urgent need to understand how these technologies impact a facility's attack surface as well as any impacts on equipment within the facility.

The research that has been conducted in the UK has been mainly centered around electromagnetic and radio frequency interference (EMI/RFI).

Recently ONR noted that there was a gap in advanced gas-cooled reactors (AGR) regarding EMI/RFI. Spectrum testing at Hinkley Point B (HPB) revealed that passive RFI emissions activated a nearby fire alarm. As a result, HPB created a safety[2] case around the following five points:

1. On-site, periodic, passive measurement of RFI emissions at various areas of the station to determine the current level of threat at that moment and particular location.
2. A review of equipment classification, categorization, and qualification status at each site.
3. EMI/RFI hazard employee briefings and training at each site.
4. Administrative arrangements to mitigate the risk - specific to each site.
5. Add additional shielding/protection against EMI/RFI to equipment. This decision is based on an assessment of that equipment.

Another licensee, Sizewell B (SZB) facility created a safety case for the use of wireless in equipment important to nuclear safety; namely the use of wireless technology to control the polar crane at SZB. SZB has demonstrated that risks have been reduced to as low as reasonably practicable in the operation of the polar crane using this device whether unintentional (poorly conceived or implemented modification) or intentional (adversary utilizing the Wi-Fi to take control of the polar crane). Additionally, the licensee has had to provide confidence that other safety systems implementing nuclear safety functions in the vicinity of the polar crane will not be inhibited by either RFI or EMI in delivery of their nuclear safety function.

One last use case revealed by ONR is the use of wireless to control autonomous vehicles as they move drums throughout a contaminated/hostile environment in a waste processing site. The use of wireless technology prevents wiring harnesses from degrading and therefore removes the need for maintenance to be performed in a contaminated environment.

4.2.3. SNL – Physical

Divisions within Sandia National Laboratories (SNL) have investigated the use of wireless in physical security environments. One key concern that was raised was how to protect against adversaries jamming wireless signals. This interview uncovered research which conducted by other DOE labs and briefed to Sandia personnel. There was, however, some uncertainty surrounding if the technology which was briefed would be useful for advanced reactors. The work was conducted for the Department of Homeland Security and the Department of Justice Prison System but may be useful for some NPPs in the existing fleet.

[2] ONR defines a safety system as 'A system that acts in response to a fault to protect against a radiological consequence' see Safety Systems in Document NS-TAST-GD-003 Revision 9 https://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-003.pdf

4.2.4. Constellation

Constellation (formerly Exelon Nuclear) has been working to develop wireless antenna networks across their systems. These networks fully operational in a few sites and are solely for systems which are not associated with either safety or high-consequence functions.

Constellation has started installing wireless monitoring devices on equipment, however an equipment operator is still dispatched to verify signals, since the wireless devices seems to only be used to provide additional monitoring capabilities. Any data collected via wireless monitoring devices is never accepted without verification.

Constellation is also currently engaging with DOE and the NRC, to development an entirely digital control room at Constellation's Limerick generating station. The project is still in its infancy and will likely take another five years to reach completion.

4.2.5. NuScale

Unlike many of the licensees interviewed for this project, NuScale wants to implement wireless capabilities everywhere possible. NuScale recognizes that using wireless technology would be beneficial for many different aspects of the plant's operations. First, pulling cabling for networking is costly and time consuming and secondly, the use of wireless devices will streamline plant processes. However, it is worth noting that the NuScale design is claimed to have a lower risk than operating nuclear power plants, so this also needs to be taken into consideration when contemplating the use of wireless.

NuScale is in the process of investigating allowing operators to use tablets to make maintenance inspections more efficient, implementing machinery component monitoring devices, as well as a method to use wireless for distributed control systems to balance of plant systems. NuScale understands that there needs to be a secure method with a well-defined cyber security plan prior to implementing any of these options and has started research into developing a use case.

4.2.6. EPRI

During the initial interview, much of the initial conversation was focused on the fact that researching the use of wireless in critical or safety functions is sorely needed. This type of research will take years and be costly.

EPRI has been working with CNL to research CNL's Cyber Security Plan (CSP) requirements but haven't focused on wireless technology specifically in their assessment. Because EPRI is conducting similar research, interviewees did not have answers to the interview questions but did offer important insights and recommendations from their own experiences.

Most importantly, the team at EPRI noted that future research investigating the feasibility of using wireless technology in critical functions is a long-term project which will require significant funding. Furthermore, they recommended that future work include an operationalized definition of "safety critical system/function," which would provide the opportunity to develop better research answers.

This page left blank

5. CONCLUSION

After several months of research, an extensive literature review and one-on-one interviews the research team at Sandia found that although wireless technology is used in all industries in almost every capacity, high-risk facilities within the US, such as chemical and nuclear, have yet to implement wireless capabilities in critical function applications. However, both industries do use wireless capabilities in low-consequence operations such as administrative and manufacturing. This conclusion supports the NRC's current risk-informed decision of approving licensees' CSPs that prohibit the use of wireless technology for CDAs associated with safety-related and important-to-safety functions. Both industries named that their ability to address regulatory constraints and security challenges as the main reasons for the lack of implementation of wireless technology in their safety related and important to safety operations. However, representatives and stakeholders that were interviewed talked about the desire to move to using wireless in these SR/ITS areas to improve the efficient operation of their plants, e.g., reducing costs, improving communication, and facilitating technology upgrades.

Over the course of several months, Sandia personnel conducted interviews with industry experts, individuals in other high-consequence industries, and key stakeholders in the NPP field as well as the chemical industry. As discussed during the interviews from Section 4, many organizations, such as CNL, ONR and US CISA, are researching the need for and challenges associated with wireless implementation in SR/ITS systems. The people interviewed expresses a general uncertainty around securing wireless for use in SR/ITS systems, as well as an understanding that replacing aging analog equipment is challenging as most digital components often include wireless capabilities.

Security issues were one of the most prominent barriers to entry for implementing wireless in SR/ITS areas. Finding and retaining talent with wireless application and security experience was listed as one of the biggest challenges to implementing wireless technology, especially in the operational technology sector. Although there is plenty of information about wireless technology implementation and security for information technology, there is not as much for operational technology. Having experienced professionals is not only necessary, but required, as there is no tolerance for risk of cyber security or other mishaps.

The researchers were hoping to find some information in the literature review related to how other industries have integrated wireless technology is currently implemented into risk significant facilities, comparable to a NPP SR/ITS network, however there was no publicly available information. During the interview with Dow Chemical revealed the researchers learned that the lack of information is more than likely because of security, as Dow did not want to share any detailed specifics for how they were integrating wireless into their manufacturing facilities.

The critical infrastructure industries interviewed (nuclear, chemical, and biological), have avoided the use of wireless, until further research and guidance can prove that wireless technology can safely and securely replace analog SR/ITS systems. An area of future study that could aid NPPs and their desire to implement wireless technology is a comparison of implementation costs compared to the overall savings of wireless versus wired technologies.

Areas mentioned that need further research and verification are the vulnerabilities associated with EMF interference, new attack vectors introduced to a network by use of wireless technology, wireless eavesdropping via RF transmitters, or jamming of wireless signals. Other concerns stemmed from difficulties of ensuring the availability, confidentiality, integrity, and

repeatability of wireless communications. A more in-depth analysis of a representative isolated safety/security network, with system level testing and development, providing strong information informing the implementation of wireless in NPP critical networks may be needed to further understand the security risks of using wireless in SR/ITS CDAs. This and future research efforts on the implementation of wireless technologies in SR/ITS systems would help future instrumentation and controls designers select secure wireless systems for nuclear facilities.

6. REFERENCES

[1] Electric Power Research Institute (EPRI), "Guidelines for Wireless Technology in Power Plants Volume 1: Benefits and Considerations," EPRI, Palo Alto, CA, 2002.

[2] Electric Power Research Institute (EPRI), "Guidelines for Wireless Technology in Power Plants Volume 2: Implementation and Regulatory Issues," EPRI, Palo Alto, CA, 2002.

[3] Electric Power Research Institute (EPRI), "Implementation Guideline for Wireless Networks and Wireless Equipment Condition Monitoring," EPRI, Palo Alto, CA, 2009.

[4] Electric Power Research Institute (EPRI), "Initial Requirements for Wireless Sensors in Power Plant Applications," EPRI, Palo Alto, CA, 2002.

[5] Electric Power Research Institute (EPRI), "Wireless Technology Power Plant Applications, 1004905," EPRI, Palo Alto, CA, 2003.

[6] International Atomic Energy Agency (IAEA), "Application of Wireless Technologies in Nuclear Power Plant Instrumentation and Control Systems NR-T-3.29," IAEA, Vienna AU, 2020.

[7] V. K. Nassa, "Wireless Communications: Past, Present and Future," *Dronacharya Research Journal,* vol. III, no. II, pp. 50-54, 2011.

[8] K. Sharma and N. Dhir, "A Study of Wireless Networks: WLANs, WPANs, WMANs, and WWANs with Comparison," *International Journal of Computer Science and Information Technologies,* vol. 5, no. 6, pp. 7810-7813, 2014.

[9] Electric Power Research Institute (EPRI), "Demonstration of Wireless Technology for Equipment Condition Assessment: Application at TXU Comanche Peak Steam Electric Station, 1011826," EPRI, Palo Alto, CA, 2005.

[10] V. Yadav, H. Zhang, C. P. Chwasz, A. V. Gribok, C. Ritter, N. J. Lybeck, R. D. Hays, T. C. Trask, P. K. Jain, V. Badalassi, P. Ramuhalli, D. Eskins, R. L. Gascot, D. Ju and Iyen, "The State of Technology of Application of Digital Twins," Idaho National Laboratory, Idaho Falls, ID, June 2021.

[11] Department of Energy-Nuclear Energy (DoE-NE), "Advanced Sensors and Instrumentation Project Summaries," Office of Nuclear Energy, 2020.

[12] T. McIntyre, "Wireless Sensors for Nuclear Energy Applications," 30 October 2019. [Online]. Available: https://www.energy.gov/sites/default/files/2019/12/f69/ne-25-2019-Direct-Digital-Printing-Passive-Wireless-Sensors.pdf. [Accessed 10 February 2022].

[13] US Nuclear Regulatory Commission, *Title 10 CFR Part 73 Physical Protection of Plants and Materials,* Washington, DC: NRC, January 1, 2019.

[14] National Archives, "Title 6 CFR Chapter I Part 27 Chemical Facility Anti-Terrorism Standards," 9 April 2007. [Online]. Available: https://www.ecfr.gov/current/title-6/chapter-I/part-27?toc=1. [Accessed 2022].

[15] DHS, CISA, " Chemical Facility Anti-Terrorism Standards (CFATS)," 2007. [Online]. Available: https://www.cisa.gov/chemical-facility-anti-terrorism-standards. [Accessed 2022].

[16] DHS, CISA, "Chemical Facility Anti-Terrorism Standards (CFATS) Program Overview," 2006. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/fs_cfats-overview-508.pdf. [Accessed 2022].

[17] OPCW, "Chemical Safety and Security Management Programme," 2022. [Online]. Available: https://www.opcw.org/resources/capacity-building/international-cooperation-programmes/chemical-safety-and-security. [Accessed 2022].

[18] Electric Power Research Institute (EPRI), "Use of Cellular Network and Distributed Antenna Systems to Improve Connectivity and Increase Data Transfer," EPRI, Palo Alto, CA, 2017.

[19] Electric Power Research Institute (EPRI), "Wireless Sensor Application Guideline," EPRI, Palo Alto, CA, 2002.

[20] Cybersecurity and Infrastructure Security Agency (CISA), "About CISA," 1 January 2022. [Online]. Available: https://www.cisa.gov/about-cisa. [Accessed 2022].

[21] National Archives, "Title 6 CFR Chapter 1 Part 27 Appendix A," 20 November 2007. [Online]. Available: https://www.ecfr.gov/current/title-6/chapter-I/part-27/appendix-Appendix%20A%20to%20Part%2027. [Accessed 2022].

[22] National Institute of Standards and Technology (NIST), "Guidelines for Securing Wireless Local Area Networks (WLANs) SP 800-153," NIST, Gaithersburg, MD, 2012.

[23] National Institute of Standards and Technology (NIST) , "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i," NIST, Gaithersburg, MD, 2007.

[24] National Institute of Standards and Technology (NIST) , "Guide to Bluetooth Security, SP 800-121 Rev. 2," NIST, Gaithersburg, MD, 2022.

[25] National Institute of Standards and Technology (NIST) , "Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5," NIST, Gaithersburg, MD, 2020.

[26] The Chlorine Institute, "May's Member Spotlight – Matt Fridley (Brenntag)," 1 May 2022. [Online]. Available: https://www.chlorineinstitute.org/about-us/ci-member-spotlight/may-s-member-spotlight-matt-fridley-brenntag/. [Accessed 2022].

[27] L. Abrams, "Chemical distributor pays $4.4 million to DarkSide ransomware," BleepingComputer, 13 May 2021. [Online]. Available:

https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/. [Accessed 2022].

[28] J. Bergal, "Florida Hack Exposes Danger to Water Systems," PEW, 10 March 2021. [Online]. Available: https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems. [Accessed 2022].

[29] A. H. Tullo, "C&EN's Global Top 50 chemical firms for 2021," Chemical and Engineering News (C&EN(, 26 July 2021. [Online]. Available: https://cen.acs.org/business/finance/CENs-Global-Top-50-2021/99/i27. [Accessed 2022].

[30] Cybersecurity and Infrastructure Security Agency's (CISA), "CYBER STORM: SECURING CYBER SPACE," CISA, 2022. [Online]. Available: https://www.cisa.gov/cyber-storm-securing-cyber-space. [Accessed 2022].

[31] NATA, "Safety vs. Security: Is there a difference?," 25 July 2018. [Online]. Available: https://info.natacs.aero/blog/safety-vs.-security-is-there-a-difference. [Accessed 2022].

[32] FAA, "Aviation Cyber Initiative (ACI)," 01 July 2021. [Online]. Available: https://www.faa.gov/air_traffic/technology/cas/aci/. [Accessed 2022].

[33] FAA, "Air Traffic Organization Wireless Policy," 30 September 2015. [Online]. Available: https://www.faa.gov/documentLibrary/media/Order/JO_1370.118.pdf. [Accessed 2022].

[34] RF Wirless World, "Home of RF and Wireless Vendors and Resources," 2012. [Online]. Available: https://www.rfwireless-world.com/Terminology/Air-Traffic-Management.html. [Accessed 2022].

[35] GlobalNewswire, "Aviation Cyber Security Market is projected to be Worth USD 5.87 Billion in 2030: Visiongain Research Inc," 18 October 2021. [Online]. Available: https://www.globenewswire.com/news-release/2021/10/18/2315726/0/en/Aviation-Cyber-Security-Market-is-projected-to-be-Worth-USD-5-87-Billion-in-2030-Visiongain-Research-Inc.html. [Accessed 2022].

[36] Ally Bank, "Serious Security: How Online Banks Keep Your Money Safe," 04 December 2017. [Online]. Available: https://www.ally.com/do-it-right/banking/online-banking-security/. [Accessed 2022].

[37] Wikipedia, "TEMPEST (codename)," 2022. [Online]. Available: https://en.wikipedia.org/wiki/Tempest_(codename). [Accessed 2022].

[38] Wikipedia, "The Thing (listening device)," 2022. [Online]. Available: https://en.wikipedia.org/wiki/The_Thing_(listening_device). [Accessed 2022].

[39] A. Weinand, M. Karrenbauer and H. Schotten, "Security Solutions for Local Wireless Networks in Control Applications based on Physical Layer Security," in *Proceedings of*

the 3rd IFAC Conference on Embedded Systems, Computational Intelligence and Telematics in Control, Oxford, UK, 2018.

[40] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao and K. Zeng, "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8169-8181, 10 2019.

[41] D. Wang, B. Bai, W. Zhao and Z. Han, "A Survey of Optimization Approaches for Wireless Physical Layer Security," *IEEE Communications Surveys Tutorials,* vol. 21, no. 2, pp. 1878-1911, 2019.

[42] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Communications,* vol. 14, no. 12, pp. 1-14, 12 2017.

[43] P. Singh, P. Pawar and A. Trivedi, "Physical Layer Security Approaches in 5G Wireless Communication Networks," in *First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, Jalandhar, India, 2018.

[44] A. Sanenga, G. A. Mapunda, T. M. Jacob, L. Marata, B. Basutli and J. M. Chuma, "An Overview of Key Technologies in Physical Layer Security," *entropy,* vol. 22, no. 11, pp. 1-34, 06 11 2020.

[45] E. Khorov, A. Kiryanov, A. Lyakhov and G. Bianchi, "A tutorial on IEEE 802.11 ax highefficiency WLANs," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 1, pp. 197-216, 2018.

[46] Wi-Fi Alliance, "WPA3 (TM) Specification Version 3.0," Wi-Fi Alliance, 2020.

[47] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," in *2020 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2020.

[48] F. L. Coman, K. M. Malarski, M. N. Petersen and S. Ruepp, "Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT," in *2019 Global IoT Summit (GIoTS)*, Aarhus, Denmark, 2019.

[49] A. Levi, E. Çetintas, M. Aydos, C. Koc and M. Çağlayan, "Relay Attacks on Bluetooth Authentication and Solutions," in *Computer and Information Sciences - ISCIS 2004, 19th International Symposium*, Kemer-Antalya, Turkey, 2004.

[50] S. Raza, A. Slabbert, T. Voigt and K. Landernas, " Security considerations for the WirelessHART protocol," in *14th International IEEE Conference on Emerging Technologies and Factory Automation*, Palma de Mallorca, Spain, 2009.

[51] EMVCo, LLC, *A Guide to EMV Chip Technology,* Foster City, California, 2014.

[52] A. Kamerman and L. Monteban, "WaveLANR-II: a high-performance wireless LAN for the unlicensed band," *Bell Labs technical journal,* vol. 2, no. 3, pp. 118-133, 1997.

[53] CISCO, "IEEE 802.11ax: The Sixth Generation of Wi-Fi White Paper," 3 April 2020. [Online]. Available:

https://www.cisco.com/c/dam/en/us/products/collateral/wireless/white-paper-c11-740788.pdf. [Accessed 2022].

[54] Aruba, "802.11AX White Paper," 30 May 2018. [Online]. Available: https://www.arubanetworks.com/assets/wp/WP_802.11AX.pdf. [Accessed 2022].

[55] Quantenna, "quantenna.com," January 2018. [Online]. Available: http://www.quantenna.com/wp-content/uploads/2018/01/WP-Dual-Band-11ax.pdf. [Accessed 2022].

[56] F. Adelantado and et al., "Understanding the limits of LoRaWAN," *IEEE Communications Magazine,* vol. 55, no. 9, pp. 34-40, 2017.

[57] J. deCarvalho Silva and et al., "LoRaWAN—A low power WAN protocol for Internet of Things: A review and opportunities," in *2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, Split, Croatia, 2017.

[58] LoRa Alliance, "LoRa Alliance resource HUB," November 2015. [Online]. Available: https://lora-alliance.org/resource_hub/what-is-lorawan/. [Accessed 2022].

[59] M. Luvisotto, F. Tramarin, L. Vangelist and S. Vitturi, "On the use of LoRaWAN for indoor industrial IoT applications," *Wireless Communications and Mobile Computing,* vol. 2018, no. Article ID 3982646, pp. 1-11, 17 May 2018.

[60] Rohde & Schwarz, "From cable replacement to the IoT Bluetooth 5 White Paper," 2016. [Online]. Available: https://www.rohde-schwarz.com/. [Accessed 2022].

[61] M. Woolley, "Bluetooth Core Specification Version 5.0 Feature Enhancements," 9 December 2021. [Online]. Available: https://www.bluetooth.com/wp-content/uploads/2019/03/Bluetooth_5-FINAL.pdf. [Accessed 2022].

[62] J.-r. Lin, T. Talty and O. K. Tonguz, "On the potential of bluetooth low energy technology for vehicular applications," *IEEE Communications Magazine,* vol. 53, no. 1, pp. 267-275, 2015.

[63] M. Wedd, "Bluetooth IoT Applications: From BLE to Mesh," 25 June 2020. [Online]. Available: https://www.iotforall.com/bluetooth-iot-applications. [Accessed 2022].

[64] M. Woolley, "BLUETOOTH BLOG How Bluetooth Mesh Puts the ‘Large’ in Large-Scale Wireless Device Networks," Bluetooth.com, 26 June 2018. [Online]. Available: https://www.bluetooth.com/blog/mesh-in-large-scale-networks/. [Accessed 2022].

[65] Y. Zhuang, J. Yang, L. You, Q. Longning and N. El-Sheimy, "Smartphone-Based Indoor Localization with Bluetooth Low Energy Beacons," *Sensors,* vol. April, no. 26, p. 596, 2016.

[66] J. A. Afonso, A. J. F. Maio and R. Simoes, "Performance Evaluation of Bluetooth Low Energy for High Data Rate Body Area Networks," *Wireless Personal Communications,* vol. 90, no. 1, pp. 121-141, 2016.

[67] Link Labs, "Bluetooth Mesh - Protocol for Industrial IOT," 14 February 2017. [Online]. Available: https://www.link-labs.com/blog/bluetooth-mesh-protocol-for-industrial-iot. [Accessed 2022].

[68] S. Petersen and S. Carlsen, "WirelessHART versus ISA100. 11a: The format war hits the factory floor.," *IEEE Industrial Electronics Magazine 5.4,* vol. 4, pp. 23-24, 2011.

[69] A. N. Kim, F. Hekland, S. Petersen and P. Doyle, "When HART Goes Wireless: Understanding and Implementing the WirelessHART Standard," in *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, 2008.

[70] Daintree Networks , "Getting Started with ZigBee and IEEE 802.15.4," http://www.science.smith.edu/~jcardell/Courses/EGR328/Readings/Zigbee%20Getting Started.pdf, 2008.

[71] Q. Wang and J. Jiang, "Comparative examination on architecture and protocol of industrial wireless sensor network standards," *IEEE Communications Surveys & Tutorials ,* vol. 18, no. 3, pp. 2197-2219, 2016.

[72] ISA100 Wireless Compliance Institute, " ISA100 Wireless Applications, Technology, and Systems A Tutorial White Paper," November 2014. [Online]. Available: https://isa100wci.org/en-US/Documents/White-Papers/White-Paper-ISA100-Applications-Technology-and-Sys.aspx. [Accessed 2022].

[73] T. P. Raptix, A. Passarella and M. Conti, "A survey on industrial Internet with ISA100 wireless," *IEEE Access ,* vol. 8, pp. 157177-157196, 2020.

[74] D. A McFarlane, S. Sarma, J. L. A Chirn, C. A Wong and K. A Ashton, "Auto ID systems and intelligent manufacturing control," *J Engineering Applications of Artificial Intelligence,* vol. 16, no. Elsevier, pp. 365-376, 2003.

[75] Areva NP, Inc., "U.S. EPR Final Safety Analysis Report," U.S. Nuclear Regulatory Commission, Washington DC, 2013.

[76] Framatome, "Teleperm XS-Based Modular Safety Instrumentation and Control," Framatome, [Online]. Available: https://www.framatome.com/scripts/customer/publigen/content/templates/show.asp?P=1324&L=EN&SYNC=Y. [Accessed 15 February 2022].

[77] Areva, "Teleperm XS System Overview," Areva, [Online]. Available: http://de.areva.com/customer/liblocal/docs/KUNDENPORTAL/PRODUKTBROSCHUEREN/Brosch%FCren%20ohne%20Nummer%20-%20ToDo/UN0355A%20ANP%20DS%20Systembrosch_US%20BEL.indd.pdf. [Accessed 15 February 2022].

[78] I. Rouf, Miller, Rob, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe and I. Seskar, "Security and Privacy Vulnerabilities of {In-Car} Wireless Networks: A Tire Pressure Monitoring System Case Study," *19th USENIX Security Symposium,* 2010.

[79] The International Society of Automation, "ProSoft Technology Introduces PROFIBUS DP High Speed Wireless Communication Gateways," 15 3 2006. [Online]. Available: https://www.automation.com/en-us/products/product21/prosoft-technology-introduces-profibus-dp-high-spe.

[80] Siemens AG, "PROFIBUS According To IEC 61158/EN 501705," Siemens AG, 2005.

[81] V. Watson, X. Lou and Y. Gao, "A Review of PROFIBUS Protocol Vulnerabilities," in Proceedings of the 14th International Joint Conference on e-Business and Telecommunications, 2017.

[82] C. Cerrudo, E. Martinez Fayo and M. Sequeira, "LoRaWAN Networks Susceptible to Hacking: Common Cyber Security Problems, How to Detect and Prevent Them," IOActive, 2020.

[83] X. Yang, E. Karampatzakis, C. Doerr and F. Kuipers, "Security Vulnerabilities in LoRaWAN," in *EEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI) IEEE*, 2018.

[84] J. Wang, F. Hu, Y. Zhou, Y. Liu and H. Zhang, "BlueDoor: Breaking the Secure Information Flowvia BLE Vulnerability," in *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, 2020.

[85] K. Kitano and s. Yamamoto, "Strong security measures implemented in isa100," Yokogawa, 2014.

[86] Z. Zhang, M. Wei, P. Wang and Y. Kim, "Research and Implementation of Security Mechanism in ISA100.11a Networks," in *2009 9th International Conference on Electronic Measurement & Instruments*, 2009.

[87] A. Lashkari, M. Danesh and B. Samadi, "Lashkari, Arash Habibi, Mir Mohammad Seyed Danesh, and Behrang Samadi. "A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i)," in *2nd IEEE international conference on computer science and information technology*, 2009.

[88] J. Dion, M. Mowlader and P. Ewing, "Wireless Network Security in Nuclear Facilities," in Proceedings of the 7th International Topical Meeting on Nuclear Plant Instrumenation, Control and Human-Machine Interface Technologies , Las Vegas, NV, 2010.

[89] D. F. V. H. Dae-Ki Kang, "Learning Classifiers for Misuse and Anomaly Detection Using a Bag of System Calls Representation," in *IEEE Workshop on Information Assurance and Security*, West Point, NY, 2005.

[90] T. Panse and P. Panse, "A Survey on Security Threats and Vulnerability attacks on Bluetooth Communication," *International Journal of Computer Science and Information Technologies,* vol. 4, pp. 741-746, 2013.

[91] A. Agarwal, "Types of Wireless Networks," 13 May 2010. [Online]. Available: https://www.labnol.org/tech/types-of-wireless-networks/13667/. [Accessed 31 January 2022].

[92] T. Ali-Yahiya, "Chapter 4: LTE Phyiscal Layer," in *Understanding LTE and its Performance*, 1 ed., New York, NY: Springer-Verlag New York, 2011, pp. 55-73.

[93] H. Bao, H. Zhang and K. Thomas, "An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants," DOE-NE, Idaho Falls, ID, 2019.

[94] CISCO, Demystifying 5G in Industrial IoT, Cisco, 2019.

[95] R. Castillo, "Wireless Monitoring Improves Power Plant Operations," 1 June 2019. [Online]. Available: https://www.powermag.com/wireless-monitoring-improves-power-plant-operations/?printmode=1. [Accessed 1 September 2021].

[96] J. V. Cordaro, D. Shull, M. Farrar and G. Reeves, "Ultra Secure High Reliability Wireless Radiation Monitoring System," *Instrumentation & Measurement Magazine,* pp. 14-18, 1 December 2011.

[97] L. L. Dhirani, E. Armstrong and T. Newe, "Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap," *Sensors,* vol. 21, no. 11, p. 30, 05 06 2021.

[98] Dragos, "WhitePaper: Pipedream: Chernovite's Emerging Malware Targeting Industrial Control Systems," Dragos, Hanover, MD, 2022.

[99] A. C. d. S. Frederico Mendes Macias, " Achieving a Zero Trust Architecture in an industrial environment with multiple facilities," Deloitte, 2021. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/pt/Documents/risk/Case-Study-Zero-Trust-Architecture-for-Industrial-Environments.pdf. [Accessed 2022].

[100] A. Goldsmith, Wireless Communications, 1 ed., New York, NY: Cambridge Press, 2005, pp. 1-674.

[101] N. Gopal, "Application of Wireless Instrumentation in Heavy Power Plant," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,* vol. 4, no. 10, pp. 8301-8307, October 2015.

[102] H. Hashemian, C. Kiger, G. Morton and B. Shumaker, "Wireless Sensor Applications in Nuclear Power Plants," *Nuclear Technology,* vol. 173, no. 1, pp. 8-16, 2011.

[103] M. K. Howlader and P. D. Ewing.

[104] Q. P. D. S. S. C. H. Hung Le, "URLNet: Learning a URL Representation with Deep Learning for Malicious URL Detection," in *Conference'17*, Washington, DC, USA, 2017.

[105] Honeywell, "Wireless Solutions for the Power Industry," Honeywell, Phonenix, AZ, 2008.

[106] G. Johnston MIET, Wireles Instrumentation for Process Industries, ABB, 2007.

[107] B. Kaldenbach, M. Moore, P. Ewing, W. Manges, C. Dillard, K. Korsah and R. Kisner, "NUREG/CR-6882, Assessment of Wireless Technologies and Their Application at Nuclear Facilities," 07 2006. [Online]. Available: https://www.nrc.gov/docs/ML0621/ML062140045.pdf. [Accessed 15 09 2021].

[108] Keithley Instruments, An Introduction to Orthogonal Frequency Division Multiplex Technology, www.keithley.com, 2004.

[109] K. Korsah, D. Holcomb, M. Muhlheim, J. Mullens, A. Loebl, M. Bobrek, M. Howlader, S. Killough, M. Moore, P. Ewing, M. Sharpe, A. Shourbaji, S. Cetiner, T. Wilson, Jr. and R. Kisner, "USNRC," 12 2008. [Online]. Available: https://www.nrc.gov/docs/ML0929/ML092950511.pdf. [Accessed 09 2021].

[110] A. Laikari, J. Flak, A. Koskinen and H. Janne, "Wireless in Nuclear," Energiforsk AB, Stockholm, 2018:513.

[111] J. Li, J. Meng, K. Xiaojing, Z. Long and X. Huang, "Using Wireless Sensor Networks to Achieve Intelligent Monitoring for High-Temperature Gas-Cooled Reactor," *Science and Technology of Nuclear Installations,* vol. 2017, no. 3721578, p. 8, 30 May 2017.

[112] R. Lin, Z. Wang and Y. Sun, "Wireless Sensor Networks Solutions for Real Time Monitoring of Nuclear Power Plant," in *Proceedings of the 5th World Congress on intelligent Control and Automation*, Hangzhou, P.R. China, 2004.

[113] X. Lu, D. Niyato, N. Privault, H. Jiang and P. Wang, "Managing Physical Layer Security in Wireless Cellular Networks: A Cyber Insurance Approach," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS,,* vol. 36, no. 7, pp. 1648-1661, 07 2018.

[114] K. Manjunatha and V. Agarwal, "ISM band Integrated Distributed Antenna Systems for Industry 4.0: A Techno-Economic Analysis," IEEE, Taipei, Taiwan, 2020.

[115] L. Morris, "Wireless at Power Plants," 1 September 2011. [Online]. Available: https://www.power-eng.com/coal/wireless-at-power-plants/#gref. [Accessed 1 September 2021].

[116] E. J. Panama, "Wireless Technology Modernizes Power Plant Performance Monitoring," 6 January 2020. [Online]. Available: https://www.process-heating.com/articles/93258-wireless-technology-modernizes-power-plant-performance-monitoring. [Accessed 1 September 2021].

[117] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," in *Proceedings of the National Academy of Sciences*, 2017.

[118] Qualcomm Technologies, Inc., *5G Waveform & Multiple Access Techniques,* Qualcomm Technologies, Inc., 2015.

[119] Rantec Microwave Systems, "The Different Types of Wireless Communication," [Online]. Available: https://www.rantecantennas.com/blog/the-different-types-of-wireless-communication/. [Accessed 31 January 2022].

[120] P. Sereiko and J. Werb, "Industrial Wireless Instrumentation Adoption Considerations," in *Process Control and Safety Symposium*, Houston, TX, 2014.

[121] R. Sparks, "Reduce Costs with Wireless Instrumentation," *Power,* vol. 153, p. 22, 03 2009.

[122] R. Teja, "Wireless Communication: Introduction, Types and Applications," Electronics Hub, 3 April 2021. [Online]. Available: https://www.electronicshub.org/wireless-communication-introduction-types-applications/#Global_Positioning_System_GPS. [Accessed 31 January 2022].

[123] US Nuclear Regulatory Commission, "Basic References Glossary Safety Related," 09 March 2021. [Online]. Available: https://www.nrc.gov/reading-rm/basic-ref/glossary/safety-related.html. [Accessed 2022].

[124] US Nuclear Regulatory Commission, "General Provisions §73.1 Purpose and Scope," [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html. [Accessed 2022].

[125] US Nuclear Regulatory Commission, "Generic Letter No. 84-01," 5 January 1984. [Online]. Available: https://www.nrc.gov/docs/ML0311/ML031150515.pdf. [Accessed 2022].

[126] US Nuclear Regulatory Commission, *Title 10 CFR Part 100 Reactor Site Criteria,* Washington DC: NRC, January 1, 2019.

[127] US Nuclear Regulatory Commission, Title 10 CFR Part 50 Domestic Licensing of Production and Utilization of Facilities, Washington DC: NRC, January 1, 2019.

[128] N. Ahmed, H. Rahman and M. Hussain, "A comparison of 802.11ah and 802.15.4 for IoT," *ICT Express,* vol. 2, no. 3, pp. 100-102, 2016.

[129] IEEE , IEEE Standard 802.11ax Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE, 2021.

[130] CISCO, Demystifying 5G in Industrial IOT - White Paper, CISCO, 2019.

[131] T. P. Raptis, A. Passarella and M. Conti, *A Survey on Industrial Internet With ISA100 Wireless,* IEEEAccess, 2020.

[132] R. Matalucci, *Risk Assessment Methodology for Dams (RAM-D(sm)),* Albuquerque: Sandia National Laboratories, 2005.

[133] S.-H. Ye, Y.-S. Kim, H.-S. Lyou, M.-S. Ki and J. Lyou, "The applications of wireless technology for operating Nuclear Power Plants," in *2014 14th International Conference on Control, Automation and Systems (ICCAS 2014)*, Seol, South Korea, 2014.

[134] J. Garcia-Hernandez and C. Garcia-Hernandez, "An Analysis of Implementing Wireless LAN Technology in Nuclear Power Plants," in *2008 Electronics, Robotics and Automotive Mechanics Conference (CERMA '08)*, Cuernavaca, Mexico, 2008.

[135] US Nuclear Regulatory Commission, "Regulatory Guide 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," US Nuclear Regulatory Commission, 2003.

[136] US Nuclear Regulatory Commission, "Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities," US Nuclear Regulatory Commission, 2010.

[137] International Electrotechnical Commission, "IEC TR 62918:2014 - Nuclear power plants - Instrumentation and control important to safety - Use and selection of wireless devices to be integrated in systems important to safety," International Electrotechnical Commission, 2014.

[138] International Electrotechnical Commission, "IEC 61158-1:2019 - Industrial communication networks - Fieldbus specifications - Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series," International Electrotechnical Commission, 2014.

[139] C. E. P. K. B. e. a. Dillard, "Assessment of wireless technologies and their application at nuclear facilities," 2006.

[140] J. K. Y. Hwang, "visiting random key pre-distribution schemes for wireless sensor networks," ACM Workshop on Security of Ad Hoc & Sensor Networks , 2004.

[141] S. Jayaweera, "Machine Learning in Cognitive Radios, in Signal Processing for Cognitive Radios," *Wiley Telecom,* pp. 768-770, 2015.

[142] S. X. Z. S. C. e. a. Junfeng, "Analysis of the structure and characteristics of wireless sensor networks," vol. 28, no. 2, pp. 16-19, 2005.

[143] C.-H. R. C. Kao, "An improved Link-16/JTIDS receiver in pulse-noise interference," *IEEE MilCom,* p. 341–346, 2011.

[144] C. S. B. Kiger, "Managing the electromagnetic compatibility and wireless coexistence concerns for the implementation of existing and future wireless technologies in nuclear power plants," *IEEE, Future of Instrumentation International Workshop,* 2012.

[145] S. L. H. L. S. S. I. Kim, "Study on cyber security assessment for wireless network at nuclear facilities," *2018 6th International Symposium on Digital Forensic and Security (ISDFS),* pp. 1-5, 2018.

[146] D. Li, "Analysis of wireless network security of AP1000 nuclear power plant. Instrum," *USERS,* vol. 26, no. 06, pp. 66-68, 2019.

[147] F. Nekoogar, "A robust wireless communication system for harsh environments including nuclear facilities," 2017.

[148] L. Ning, "Research on hotspots of wireless sensor networks," *Comput. Dev. Appl,* vol. 24, no. 9, pp. 1-3, 2011.

[149] Z. Xinbo, "Tianwan nuclear power station wireless monitoring case," *China Public Safety (Market Edition) ,* vol. 01, pp. 118-119, 2007.

[150] S. Xinghong, "search on Some Key Technologies of Wireless Sensor Networks. Nanjing University of Technolo," 2013.

[151] W. Q. L. X. Z. B. X. S. W. X. Deng Z., "Application Analysis of Wireless Sensor Networks in Nuclear Power Plant," *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems,* 2020.

[152] FieldComm Group, "WirelessHART Technology Modernizes Power Plant Performance Monitoring," *Control,* 2019.

[153] Rohde & Schwarz, "White Paper: From cable replacement to the IoT Bluetooth 5.1".

[154] F. Duran and R. Waymire, "Computer Security for Commercial Nuclear Power Plants – Literature Review for Korea Hydro Nuclear Power Central Research Institute," Sandia National Laboratories, Albuquerque, NM, USA, 2013.

[155] R. S. B. R. J. Wagner, "Performance Comparison of Wireless Sensor Network Standard Protocols in an Aerospace Environment: ISA100.11a and ZigBee Pro," IEEE, 2012.

[156] R. Kumar, "Achieving Ultra-High Reliability and Low-latency in Future Wireless Networks," New York University, New York, 2020.

[157] US Nuclear Regulator Commission, "NUREG/CR-6992: Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update," NRC, 2008.

[158] US Nuclear Regulator Commission, "NUREG/CR-6939: Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment," NRC, 2007.

[159] US Nuclear Regulator Commission, "NUREG/CR-6882: Assessment of Wireless Technologies and Their Application at Nuclear Facilities," NRC, 2005.

[160] US Nuclear Regulator Commission, "TLR/RES-DE-REB-2021-01: THE STATE OF TECHNOLOGY OF APPLICATION OF DIGITAL TWINS," NRC, 2021.

[161] LoRa® Alliance Technical Marketing Workgro, "LoRaWAN™ What is it?: A technical overview of LoRa® and LoRaWAN™," LoRa Alliance, 2015.

[162] J. -M. L. a. D. -S. K. A. Moallim, "Wireless control and monitoring using Programmable Logic Controller (PLC)," in *2017 17th International Conference on Control, Automation and Systems (ICCAS)*, Jeju, Korea (South), 2017.

APPENDIX A. CYBER SECURITY CONSIDERATIONS OF SELECT WIRELESS TECHNOLOGIES

This information in this section is intended to give insight into the vulnerabilities of some, but not all, of the wireless technologies discussed in this report. The information contained here is not specifically endorsed by the NRC in any way.

As with wired technology and communication many of the cyber security Common Vulnerabilities and Exposures (CVEs) of wireless technology depend on several factors, what technology is being used, the location of the wireless sensors (i.e., in a building with 12-inch concrete walls or one with windows, how far away from public access to the building, etc.), other wireless networks, technical settings of the network, signal strength, etc. As such, the mitigations for these vulneraries are just as varied and complex.

Table 3 lists different wireless technologies, any CVEs published in Mitre's CVE® Program's database. "The CVE Program partners with community members worldwide to grow CVE content and expand its usage." Additional vulnerabilities associated with wireless technologies, not listed here, can be found in MITRE's CVE database.[3] For supplemental detailed information about the wireless technologies listed in Table 3 see Appendix B.

In addition, it is worth mentioning that security measures to defend against a cyber attack depend on myriad factors, such as technology used, where the wireless network or technology is implemented, how it is implemented, etc. Because of this, listing security measures for wireless is outside the scope of this body of work. Each type of technology has its own standards and security mitigations, depending on the implementation. There are numerous standards and guidelines, many listed previously, that do address individual technologies and security measures for each. See each of the following References in Section 6 [24] [22] [23] [25] [39] [40] [41] [42] [43] [44] [45].

Bottom line, there is no replacement for a seasoned cyber security professional with experience with implementing and securing wireless networks.

[3] https://www.cve.org

This page left blank

Table 3 Cyber Security Considerations of Select Wireless Technologies

Technology	CVEs	Additional Comments/Information
WLAN	Because WLAN is widely used it should come as no surprise that there are over two hundred[4] listed CVEs. The most recent listing pertains to smartphones and WLAN denial of service if the vulnerability is exploited. Another vulnerability pertains specifically to the CISCO Aironet Access Point and if exploited, allows attackers to conduct a denial of service attack or create a buffer leak.	In approximately 2018 the Wi-Fi alliance (wi-fi.org) launched WPA3 which improved security over WPA2. [46] There are still questions about whether WPA3 is a sufficient improvement over WPA2, as the Wi-Fi alliance determined that WPA3 has yet to meet modern security protocol standards after they conducted a series of cyber attacks. This was expressed in the conclusion of a 2020 paper by Vanhoef and Ronen, "In light of our attacks, we believe that WPA3 does not meet the standards of a modern security protocol." [47] If the network is implemented with a weak password, no password, password written in the breakroom on the fridge, etc. gaining access to the WLAN is trivial. Alternatively, in WPA2, an attacker can easily capture a handshake for a device joining the network and bring the hash offsite to be cracked. Depending on the attacker's access to computational power and the password strength it could take anywhere from seconds to years to recover the password. By nature of being a wireless network, WLAN is vulnerable to eavesdropping. The information should be encrypted, but if the attacker is on the network, they will be able to eavesdrop on all the packets that are being sent. An additional layer of security like SSL helps but doesn't hide all information. For example, if you visit a website without SSL the attacker sees the entire body of the website and form data etc.; with SSL you still see the destination website, but not the contents. Likely in an NPP environment there is going to be a lot of information that is not encrypted, e.g., Modbus/TCP has no protections. Another issue with WLANs is Denial of Service attacks. These are very simple to implement. An attacker can basically just send a packet that says "disconnect device X from access point Y."

[4] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=WLAN

Technology	CVEs	Additional Comments/Information
LoRaWan	As of May 2022, there are no recorded CVEs.[5]	LoRaWAN has a small payload and devices in the plant communicate a finite number of commands/responses. This opens the door for an attacker eavesdropping and seeing only encrypted data to perform a statistical analysis and make an educated guess about the payload's contents. Coman, et.al.'s paper, from the 2019 Global IoT Summit, expresses, "In the case of a node or gateway takeover, security keys could be extracted, forged messages could be sent as though originating from the node, every message passing through it can be intercepted, or the device could be destroyed." [48] For example, if a plant takes regular measurements of a coolant pool, after gathering enough samples, an attacker could make an educated guess as to which encrypted payloads correspond to information such as temperature. LoRaWAN has a relatively small bandwidth meaning some jamming hardware could be used to essentially fill the communications channel and stop communications (DoS attack). Since LoRaWAN networks generally have a very large footprint (miles) it would be difficult, but it would not be too hard to jam the signal across a NPP for all their devices. Finally, the 128-bit AES key that LoRaWAN uses is sufficient currently, but probably not the case a decade from now, and NPP tech tends to stick around for time periods upwards of a decade once implemented.
802.11ax	Like WLAN, because 802.11 is widely used there are numbers of CVE records associated with this technology[6] and it shares many similar vulnerabilities with WLAN. An example of an 802.11 vulnerability was listed in 2020 and is associated with an Alfa Network USB adapter where the vulnerability ultimately grants attackers the ability to decrypt packets in either WPA or WPA2 networks supporting the TKIP data-confidentiality protocol.	

[5] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=LoRaWan
[6] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=802.11

Technology	CVEs	Additional Comments/Information
Bluetooth	Based on the number of CVEs listed[7], Bluetooth technology is one of the more susceptible wireless technologies to attack. The more recent CVEs listed for Bluetooth is a vulnerability which allows for privilege escalations without user interactions due to a missing permission check. There are, fortunately, numerous patches for the discovered vulnerabilities.	Bluetooth can be implemented in a device in 3 modes: 1. connect to anyone, 2. connect to anyone in whitelist, 3. connect to no one. This poses a bit of an issue being that option 2 is the only one usable and secure, but it's difficult to maintain a whitelist of devices in an operational environment, and time spent dealing with that is potential money lost. This is usually implemented like in a car radio by both devices prompting a user to verify that they intend for the connection to be allowed, but a lot of devices in NPPs do not have an interface that would allow for a user to do that. Bluetooth low range and encryption makes eavesdropping and data injection not impossible, but relatively unlikely. Bluetooth implements many channels for communications which can be victim to a DoS attack (https://ieeexplore.ieee.org/document/8780851). There is also the possibility of a relay attack in instead of obtaining some secret between to victim devices to impersonate one, the attacker relays information between the victim to make them both think they are next to each other. [49]
Wireless HART	There are a few CVEs listed for HART protocol, different results, based on the search text.[8,9,10]	WirelessHART is vulnerable to traffic analysis in a similar manner to LoRaWAN. Even though portions of the packets are encrypted, there is still some which is sent in "cleartext." An attacker can use traffic analysis to find new devices by analyzing join requests, work peak hours, device usage that can help to make other attacks more effective, etc. WirelessHART can be DoS attacked somewhat trivially. Flooding the network with join requests or advertisements could result in a denial of service. An adversary could place a device to send advertisements to a new device attempting to join the network. If the attacker device is closer, the new device will attempt to join its network. WirelessHART uses AES 128 bit key; this may not be suitable for long term usage. The network key is also known to all devices on the network, which will have varying levels of security. Gaining access to one of these devices allows the adversary to recover the network key and therefore gain access to the network. [50]

[7] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=bluetooth
[8] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wirelesshart
[9] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22wireless+hart%22
[10] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=hart

Technology	CVEs	Additional Comments/Information
ZigBee	There are 24 CVE Records as of May 2022[11]. The most recent is a vulnerability (CVE-2020-7476) which exists in the ZigBee Installation Kit (versions released prior to 1.0.1) which enables the execution of a malicious code what a malicious file is in the search path. In 2019, another CVE recorded that an insecure key transport vulnerability, attackers could gain sensitive information and conduct denial of service attacks.	Like all wireless networks ZigBee is also potentially vulnerable to jamming and DoS attacks. Zigbee communications are encrypted with an AES 128 bit key; this may not be suitable for a long term implementation, see above. Zigbee assumes the safekeeping of a symmetric key. Devices in a ZigBee network are normally IoT or OT devices with a wide array of security. If an attacker gains access to one of these devices, they could obtain the key and gain unfettered access to the network for data injection and eavesdropping.
ISA100	As of May 2022, there was one recorded CVE[12] associated specifically with ISA100.	ISA100 shares essentially the same security concerns with Zigbee and WirelessHART. It improves slightly on the former because it uses asymmetric keys during the joining phase, which authorizes devices upon joining. After that it uses symmetric AES-128 encryption. Channels could be jammed, or networks could be flooded to bring the network down.
RFID	There are numerous CVE records listed for RFID[13], and NFC[14] technology. Many of the vulnerabilities associated with this technology are related to weakness which, if exploited, allow attackers network access, full read access of RFID security data, access to user lists, information disclosure, and the ability to execute malicious code.	Radio-frequency identification (RFID)'s security information could fill volumes because of the term's myriad uses, e.g., the term is used interchangeably with NFC (Near Field Communication). At its core, the definition of RFID is a way of providing an identifier over a radio frequency. In that context there are quite literally no security measures. There are custom off the shelf (COTS) devices which anyone can buy that will read the identifier from a tag (potentially up to meters away) and clone it onto a new tag. Alternatively, this can be implemented in very secure manner, like what your credit card does, which is probably adherent to the EMV standard (Europay, Mastercard, and Visa). [51] This involves a challenge, response, and tamper resistant chip card that contains a private key that is held nowhere other than the secure storage on the chip. The chip also can be verified by a certificate signed by some trusted third party.

[11] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ZigBee
[12] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ISA+100
[13] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=rfid
[14] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=nfc

APPENDIX B. TECHNICAL DESCRIPTION OF WIRELESS PROTOCOLS

This section provides an overview of several of the prevalent wireless technology protocols that may be used in a NPPs safety/security critical networks. The intent of this section is not to imply that the wireless technologies discussed herein are deemed technically acceptable by the NRC or that NRC licensees are planning to adopt them in the future.

As mentioned in Section 2.1 Types of Wireless, there are two types of wireless network protocols which will be reviewed and analyzed in this report, WLAN and WPAN.

B.1. WLAN

Wireless Local Area Networks (WLAN) [52] are low coverage, limited capacity access points, operating at an unlicensed spectrum of 2.4 and 5 GHz capable of providing high data rate wireless connection to any cellular technology. Now the most established way for devices to access the internet whether at home or at work, WLANs consists of components such as authentication servers, access controllers, and Access Points (APs). An access controller assigns an IP address to users, which allows users to communicate with a WLAN's AP to transmit and receive data. The network capacity of WLAN is controlled by distributing wireless APs with limited frequencies, similar in principle to cellular networks, to fulfill the coverage and capacity requirements. Since WLANs operate at unlicensed bands, there will be interference from neighboring APs, and it is necessary to have proper distribution of APs with appropriate transmit power control.

B.1.1. 802.11ax Technical Features

The sixth generation Wi-Fi standard 802.11ax [53], also called Wi-Fi-6, is the latest step in the WLAN advancement aimed at high flexibility and scalability, making way for new and existing networks to power next-generation applications. A brief comparison of 802.11 legacy versions [54] with Wi-Fi-6 is shown in Table 4.

Table 4 Comparison of 802.11 legacy versions with Wi-Fi-6E

Specifications	Legacy feature (11ac,11n)	802.11ax (Wi-Fi-6E)
Frequency band	5GHz	2.4GHz, 5GHz, 6GHz
Subcarrier Spacing	312.5 KHz	78.125 KHz
OFDMA	Not Available	Available
Channel bandwidths	20, 40, 80+80, 160 MHz	20,40,80,80+80,160 MHz
MU-MIMO	Only Downlink	Downlink and Uplink
Modulation Scheme (highest)	256 QAM	1024 QAM
OFDM Symbol duration	3.2μS	12.8μS
Basic Channel Access	CSMA/CA	OFDMA on top of CSMA/CA
Random Channel Access	DCF, EDCA	UL OFDMA on top of CSMA/CA
Multiuser Technology	MU-MIMO	MU-MIMO, OFDMA
Fragmentation	Static	Dynamic
Interference Mitigation	NAV, RTS/CTS	Two NAVs, Quiet period

Specifications	Legacy feature (11ac,11n)	802.11ax (Wi-Fi-6E)
Spatial Reuse	Sectorization (11ah)	Adaptive Power and Sensitivity threshold
Power Management	Many	Enhance TWT, Enhanced Microsleep
Maximal Data Rate	≈ 7Gbps	≈ 9.6 Gbps

B.1.1.1. OFDM to OFDMA

The basic building block of Wi-Fi transmission is OFDM. An OFDM symbol is a small-time segment of the modulated waveform of a subcarrier that carries information. Downlink and uplink Orthogonal Frequency-Division Multiple Access (OFDMA) is one of the most complex features in 802.11ax. 1024-QAM [55]offers gigabit data rates in low-density enterprise environments. However, when the user density increases, the likelihood of achieving higher throughput diminishes due to contention or increase in air-time usage (also called as co-channel interference [CCI]) from all the users in the same AP. Introduced to combat co-channel interference (CCI), OFDMA is a new channel access technique like, but distinct from cellular/LTE radio networks. It maintains the robustness of Wi-Fi in an unlicensed spectrum.

In 802.11ax, the subcarrier spacing is reduced by a factor of 4x, while OFDM [54] symbol duration is increased by 4x. Reduced subcarrier spacing allows OFDM to extend to small sub-channels with a channel bandwidth of 2MHz, which can accommodate low power and low bit-rate-driven applications. In the downlink, the AP alone transmits to different clients by splitting the channel by frequency, such that different frames intended for different client devices use a group of subcarriers. Uplink OFDMA is like downlink, but in this case multiple client devices transmit simultaneously on a different group of subcarriers within a channel. In uplink, multiple client devices coordinate and synchronize transmission. [54]

On the other hand, increased OFDM symbol duration allows increased cyclic prefix length without sacrificing spectral efficiency. This enables increased immunity toward long delay spread effects due to multipath conditions. Figure 1 shows the subcarrier spacing and OFDM symbol duration in 802.11ax as compared to 802.11ac.

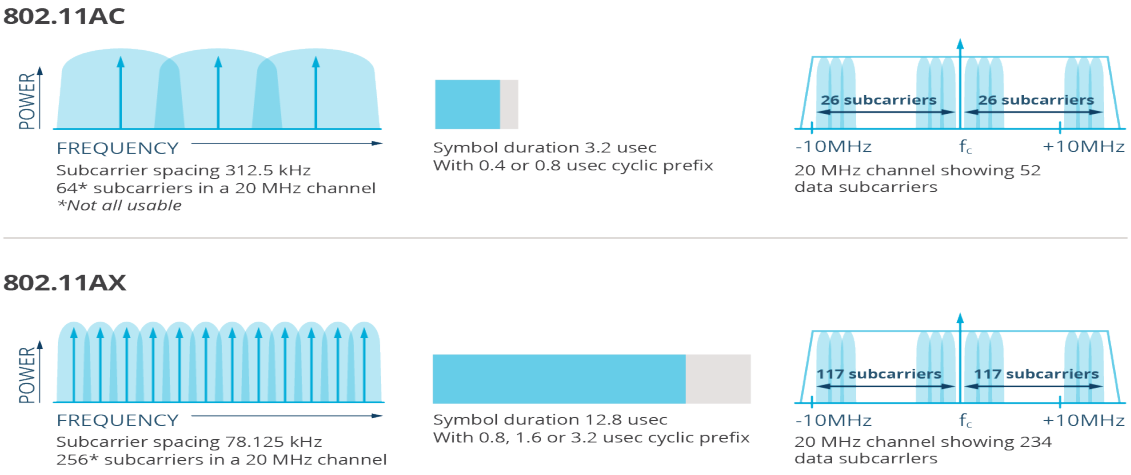

Figure 1 Comparison of 802.11ac and 802.11ax Subcarrier Spacing and Symbol duration

With OFDMA transmission across the frequency dimension is divided with pairs of users assigned to transmit and receive in sub-channels of the main RF channel in a single timeslot. Moreover, the addition of multiuser Enhanced Distributed Channel Access (EDCA) to UL-OFDMA allows APs to affect the relative channel access priority of the users. An AP can then bundle (for downlink) several frames together in different subchannels in a single transmission opportunity while users tune to their respective sub-channels to receive their respective frames. This scheme is not only more efficient, but also less prone to packet loss and errors due to air-time contention. Figure 2 depicts the difference between OFDM and OFDMA principle which accommodate multiple users in parallel.

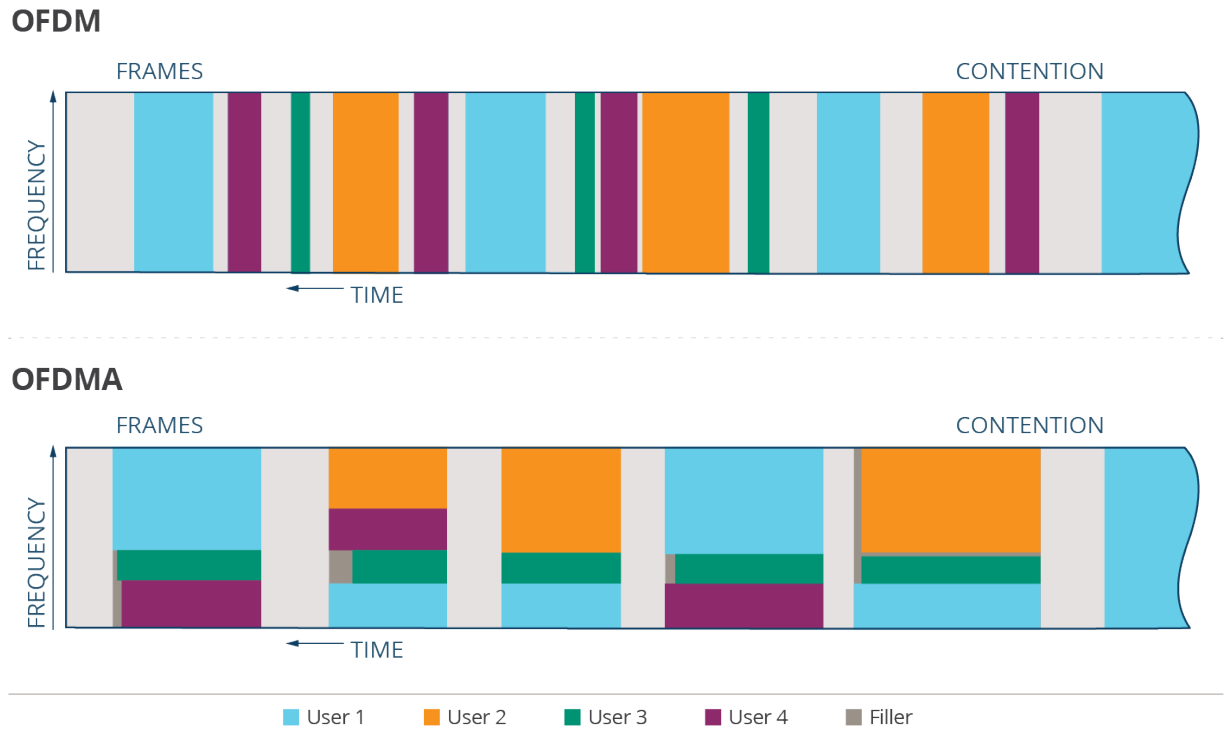

Figure 2. OFDM vs. OFDMA principle.

B.1.1.2. MU-MIMO

Downlink and uplink Multi-user, Multi-input, Multi-output (MU-MIMO) makes use of the multipath effect of the surrounding environment to send frames to different client devices in a single time interval. The number of downlink MU-MIMO groups is increased in 802.11ax, allowing more efficient operation. Uplink MU-MIMO is a new addition to 802.11ax. Like the uplink OFDMA, the AP coordinates the simultaneous transmission of multiple client devices. [54]

Extending the concept of spatial diversity and beamforming, MU-MIMO extends the concept to support simultaneous transmission and reception between AP and number of users. This is possible where the transmission to one user or group of clients will not be heard at a significant signal level by another user, and vice versa. **Error! Reference source not found.** shows the MU-MIMO in uplink and downlink transmissions.

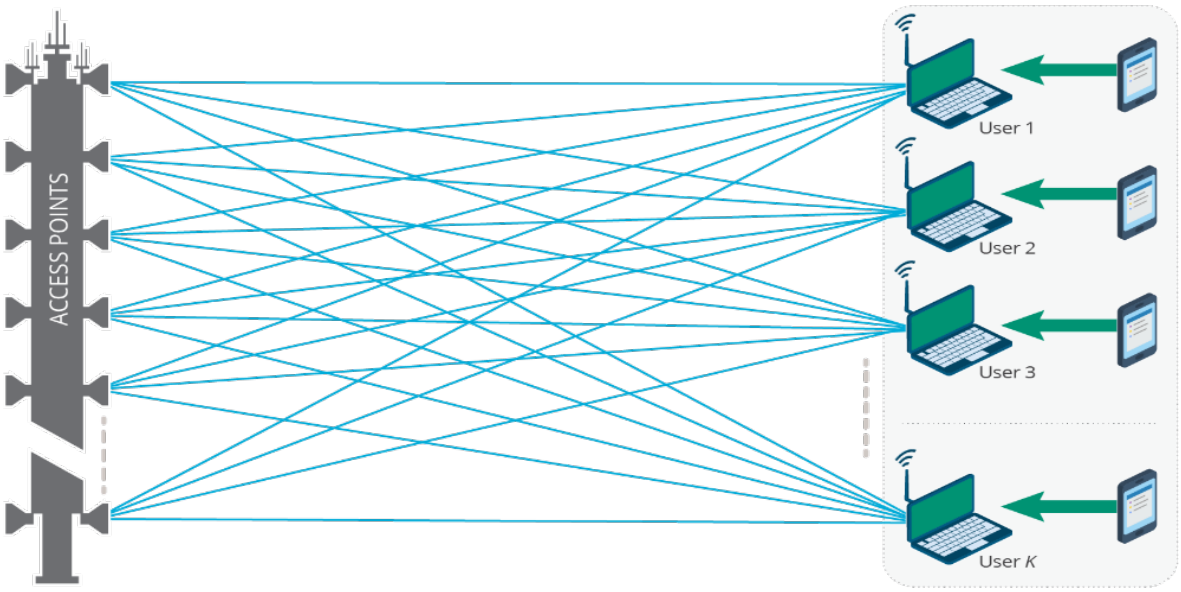

Figure 3. MU-MIMO in Downlink (DL) and Uplink (UL).

B.1.1.3. Flexible low-power device scheduling

OFDMA scheduling capability has a new power saving mode called Target-Wakeup Time (TWT) [55] [45]. With TWT the user can request a schedule to wake up at any time in the future using AP's beacon signals. The TWT can also be used as an uplink scheduling which puts a user to sleep with a predetermined wake-up time, helping to reduce contention and address delay sensitive applications. More importantly, IoT devices that only transmit occasionally can be in sleep mode for extended periods, resulting in better battery life for IoT applications. **Error! R eference source not found.** shows the TWT operation using beacon signals.

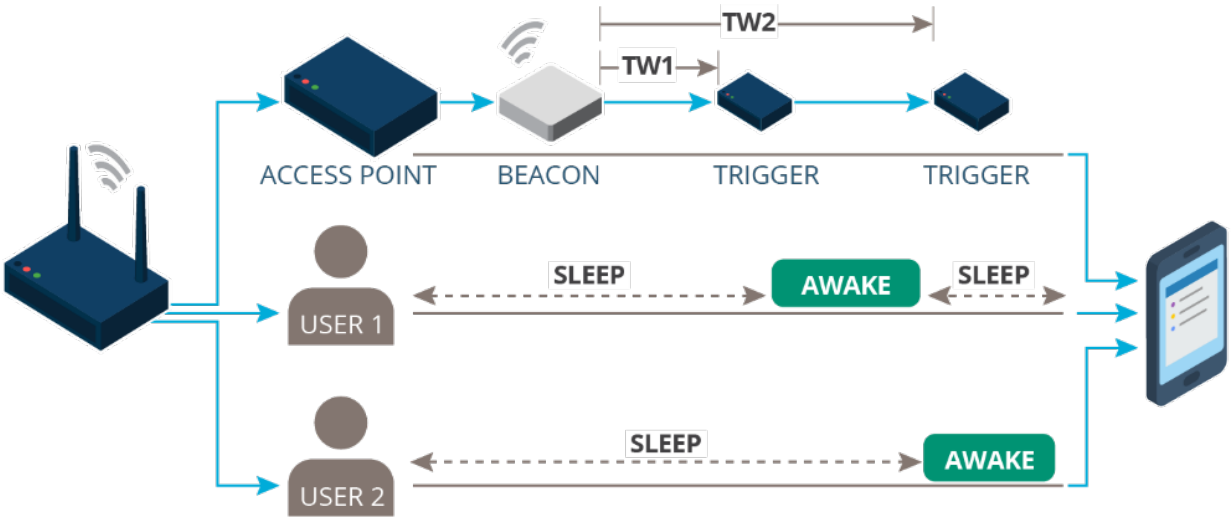

Figure 4. TWT operation using beacon signals.

B.1.1.4. Transmit Beamforming

Transmit Beamforming allows an AP to use several transmit antennas to focus a local maximum signal on a receiver antenna (client devices). It improves data rates and extends the range by reducing the signal interference. [54]

B.1.1.5. Higher Order Modulation

Higher order modulation is extended up to 1024 quadrature amplitude modulation increasing good channel condition (high signal-to-noise ratio) peak data-rates. Lower-order modulations such as BPSK, QPSK, 64-QAM, etc., are used when the channel conditions are not conducive. In addition, according to channel condition, the OFDM symbols, subcarrier spacing and FFT size are changed to allow efficient operation of small OFDMA sun-channels under poor channel conditions. [54]

B.1.1.6. Outdoor Operation

There are several improvements to Outdoor operation. A new packet format was added, where the most sensitive fields are repeated for robustness along with long guard intervals between OFDM symbols and modes, adding redundancy which allows error recovery in received data. [54]

B.1.1.7. Reduced Power Consumption

Power-save modes are introduced which reduce power consumption, allowing longer sleep intervals and scheduled wake times. The 20 MHz channel only mode is introduced for IoT devices, allowing simpler, less powerful chips which support low bandwidth. [54]

B.1.1.8. Spatial Reuse

Spatial Reuse is introduced with the use of OFDMA and MU-MIMO. This provides an increase in the transmission capacity, allowing more simultaneous transmissions in a geographical area. [54]

B.1.1.9. Rate at Range

In addition to offering higher data rates, 802.11ax also supports great range for lower effective data rates through the minimal resource allocation (2MHz). The low bandwidth allows concentrating the transmit energy into a narrower bandwidth, providing a link budget boost of up to 8 dB. The low bandwidth also enables simple and cost-effective radios, supporting only simple Binary Phase Shift Keying, BPSK modulation.

B.1.1.10. Coexistence With Other Technologies

In 2.4GHz band, 20MHz bandwidth can be divided into nine 2MHz channels. Any of these can be left blank (i.e., no 802.11ax) to coexist with other IoT technologies such as Bluetooth, ZigBee, etc. as shown in **Error! Reference source not found.**.

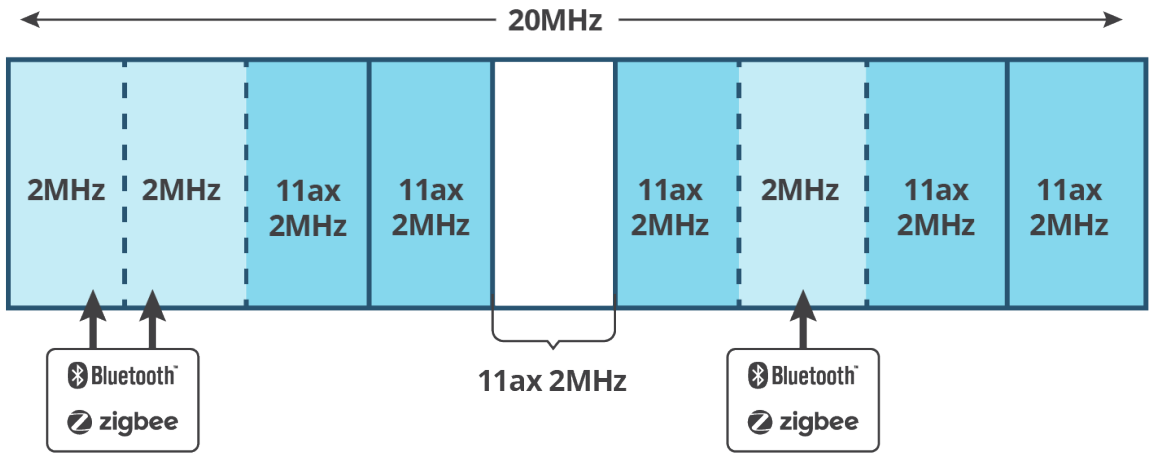

Figure 5. 802.11ax 20MHz Bandwidth Division

B.1.1.11. Built-In Security

The fundamental security of IoT devices is an ongoing and legitimate concern. Many smart devices are unproven in the field and are not designed with security in mind. With 802.11ax, organizations can build customized security strategies to mitigate the risk.

B.1.2. Long Range Wide-Area Network (LoRaWAN)

LoRaWAN is a MAC layer protocol that stands for Long Range Wide-Area Network with a "star of stars" network topology [56] [57] available on licensed as well as unlicensed bands, with extremely long battery life and limited throughput. LoRaWAN has mainly four components:

1. The end-devices send out information;
2. the gateways dispatch the information from the end-devices to the network server;
3. the network server decodes the packets received from the gateways and sends the information to the appropriate application server; and
4. the application server uses the information received from a network server to decide what action to perform [57].

The end-devices are not assigned to any specific gateway, so the same uplink message can be received by several gateways with different signal qualities. It is up to the network server to filter out the redundant information. This also means there is no handover needed when a node moves to a different location [58].

The following sections outline technical features and limitations of LoRaWAN.

B.1.2.1. Operating band and bandwidth

LoRaWAN specifications vary based on regional spectrum allocation in the unlicensed industrial, scientific, and medical (ISM) bands. The ISM band for the U.S. is 902-928 MHz and for Europe it is 863-870 MHz, with operating bandwidths of 64,125 KHz with 200 KHz increments, or 500 KHz with 1.6 MHz increments.

B.1.2.2. Transmit power and duty cycle

LoRaWAN devices must limit their maximum transmit power to 14 dBm (27 dBm in 869.4-869.65 sub-band and +30dBm for 902-928 MHz band) and can either adopt a duty cycled

transmission (0.1%, 1%, or 10% according to the sub-band), or a listen-before talk scheme. In either case, the dwell time per channel should not exceed 400msec [58].

B.1.2.3. Modulation

LoRa is a proprietary physical layer, or the wireless modulation derived from the chirp spread spectrum (CSS) modulation scheme [59]. CSS spreads each symbol in a fixed bandwidth with varied symbol duration according to the Spread Factor (SF) index, which is somewhat orthogonal to other SFs. The spreading technique reduces the complexity of the receiver design which enables long range, and high robustness to interference at the cost of a reduced data rate [58].

B.1.2.4. MAC layer protocol

MAC layer protocol is completely open, enabling the modification and building of customized protocols which best fit user applications and operating environments. LoRaWAN has three classes of operation, namely Classes A, B, and C, with the first one being mandatory for all LoRaWAN end devices [59]. Class-A devices access the channel in a random fashion, following an ALOHA-like scheme. An end device transmits in a time slot, then opens two reception windows at predefined slots in time and frequency to receive any data from the gateway. For the rest of the time, they remain in sleep mode making them the most energy efficient option, but with the highest latency. Class-B devices are still energy efficient, but they open receive windows at regular time intervals. They are time synchronized with their network server by means of beacon message sent by gateways. Class-C devices are bidirectional with continually open receive windows, sacrificing energy efficiency for low latency.

B.1.2.5. Low energy consumption

The long battery lives of end-devices are due to LoRaWAN's operating modes and simple circuit structure making it ideal for connecting devices to the internet in open spaces with low energy consumption [59].

B.1.2.6. Long range

Supports long range of up to 5 Km with low energy and low bit rate between devices.

B.1.2.7. Low bandwidth

Makes it ideal for IoT deployments with less data and/or with data transmissions.

B.1.2.8. Security

Supports a layer of security for the network and one for the application with AES encryption. It also allows adding/modifying custom security algorithms. **Error! Reference source not found.** shows the visual representation of the LoRaWAN in industrial IoT with different sensors.

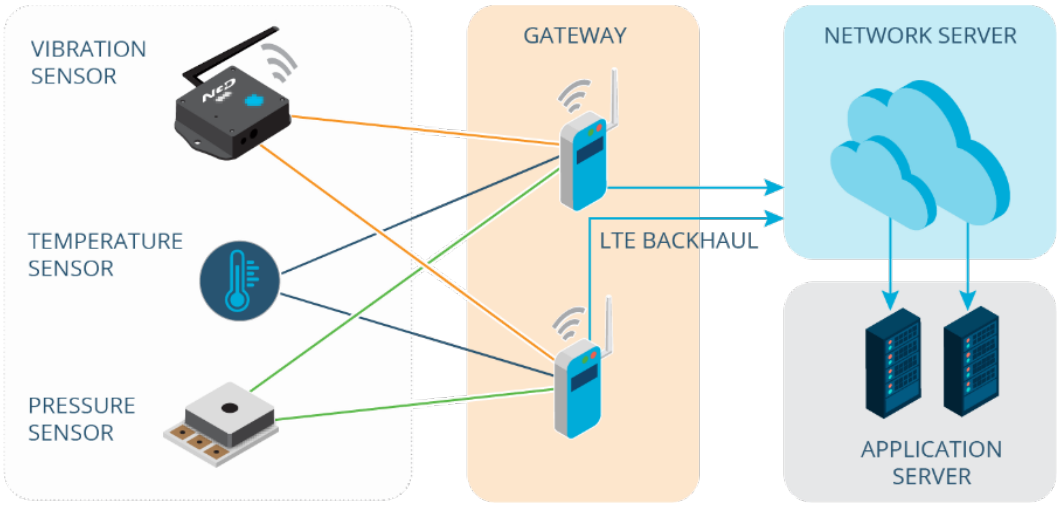

Figure 6. LoRaWAN architecture for Industrial IoT.

B.1.2.9. Duty Cycle Limitations

The capacity of the network is reduced by the On-Off periods (duty cycles) following their transmissions [56].

B.1.2.10. Coordinate Applications Limitations

A LoRaWAN network deployment follows a cellular network model by making gateways base stations and covering large areas. The increase in the number of end devices with different applications over the same shared infrastructure poses new challenges for coordinating applications.

B.2. WPAN

B.2.1. Bluetooth

After WLAN, Bluetooth is the second most popular wireless technology that was meant to replace physical cables [60] in short-range communications. Bluetooth Low Energy (BLE) is the state-of-the-art version featuring increased range, speed, and data broadcasting capacity [60]. A Bluetooth device is comprised of two main parts, a host, and a Bluetooth controller. The Bluetooth controller runs the Bluetooth stack and the actual application, and the Host-to-Controller-Interface (HCI) is a standard interface between the Bluetooth controller subsystem and the Bluetooth host [61]. BLE has different classes based on the maximum transmit power, as shown in **Error! Reference source not found.**.

Table 5. Transmit power classes in BLE

Class	Max Output Power (dBm)
1	+20
1.5	+10
2	+4
3	0

Profiles are used by BLE to transfer data from one device to another. Some profiles are universal, but if two devices want to exchange data, they must both use the same profile. Bluetooth supports:

- piconet, where a master device communicates with several slave nodes using different channels [62] and,
- a broadcast network, where an advertiser node sends messages using one of the advertising channels, and the scanner nodes scan those channels for messages.

Bluetooth also supports mesh networking [63] [64] where all the nodes can transmit and receive data. Any node transmits data omnidirectionally in a flooding technique to send data between two ends of network.

Operating in the 2.4 GHz unlicensed band, BLE has spectrum range of 2.402GHz to 2.4880 GHz supporting 40 channels of 2MHz bandwidth [65]. Out of 40 channels, three of them are used for advertisement messages and data is transmitted in the other 37 channels using Frequency Hopping Spread Spectrum and Gaussian Frequency Shift Keying modulation [62] [66]. The Time Division Multiple Access (TDMA) [66] technique is used by the BLE MAC protocol.

The following sections outline technical features and limitations of BLE.

B.2.1.1. BLE Mesh Network

Bluetooth transmits at low power (0 dBm or lower) with a high data rate (up to 2 Mbps), so the time-on-air is very short. This makes BLE a great choice for low-powered devices, which can be connected to a gateway device using a BLE Mesh network as shown in **Error! Reference s ource not found.**. Bluetooth mesh architecture allows well-distributed, low-cost, battery-powered devices to connect in industrial settings.

B.2.1.2. BLE to LTE-Cellular/Wi-Fi

Bluetooth can connect to the internet through LTE-Cellular or Wi-Fi directly and those networks can act as gateways for BLE. A group of BLE sensors can be connected to one reader device placed near the BLE sensors and powered by AC in a simple outlet [67].

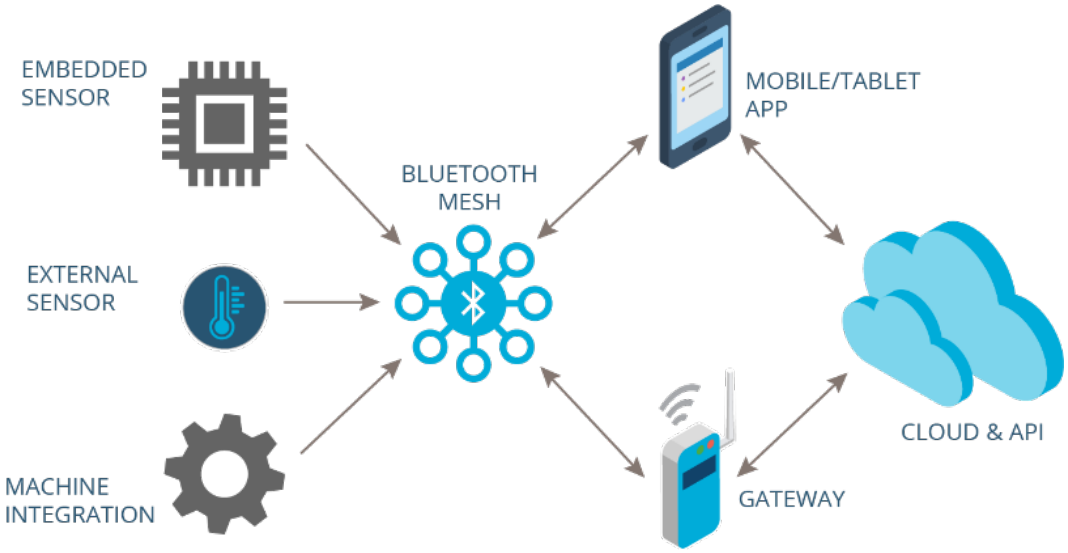

Figure 7. Bluetooth Mesh Network in Industrial IoT.

B.2.1.3. Range or Data Rate Limitations

Cannot achieve increased range and increased data rate together and is suitable only for one or the other.

B.2.1.4. Interference Limitations

Since Wi-Fi and BLE have the same operating frequencies of 2.4 GHz, channels should be carefully operated between Wi-Fi and BLE to avoid interferences.

B.2.1.5. Distribution and High Volume of Sensors Limitations

A BLE mesh network doesn't work if the sensors are not uniformly distributed throughout an area, and it will have throughput limitations if the mesh must relay more data.

B.2.2. WirelessHART

Highway Addressable Remote Transducer (HART) communication foundation introduced HART field communication protocol including wireless interface as WirelessHART [68]. The WirelessHART technology has been evolved with extensive features supporting security, unsolicited data transfers, event notifications, block mode transfers, and advanced diagnostics [69]. Diagnosis also includes information about the device such as sensors, the interface that the device is attached to, and the actual process being monitored. Thus, WirelessHART typically targets sensors and actuators which help in condition monitoring and maintenance. A generic WirelessHART network architecture [69] is shown in **Error! Reference source not found.**. The b asic network infrastructure includes:

1. field devices performing sensing or actuating functions,
2. routers routing packets in the wireless mesh,
3. adapters interfacing wired HART into wireless mesh,
4. access points connecting to wireless gateway,
5. handheld devices carried by plant operators and service engineers,
6. Plant Automation Host (PAH) connected to WirelessHART through core network, and
7. Network Manages (NM) and Security Manager (SM) connected to WirelessHART network through gateway.

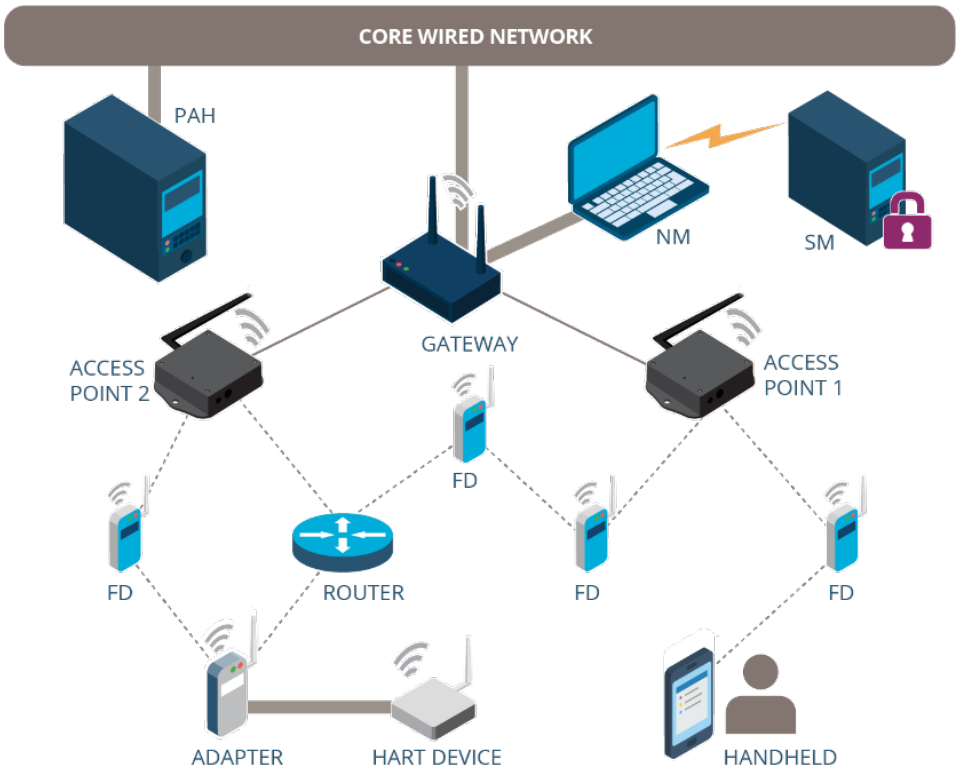

Figure 8. A generic WirelessHART Network Infrastructure

The communication is precisely scheduled based on TDMA and adopts a frequency hopping mechanism to maintain system data bandwidth and robustness. Scheduling is performed by a centralized network manager. The scheduling is translated into time slots and transferred from network manager to individual devices containing information about transmission slots. These communications are directed through single or multiple routes over one or more hops based on communication requirements. This network manager continuously adapts graphs and scheduling to changes in network topology and communication requirements. Using multiple gateways and AP, the WirelessHART network can be scaled to service large number of devices and high-data rates. The following sections outline technical features of WirelessHART. [69]

B.2.2.1. Physical layer

The WirelessHART physical layer is based on IEEE 802.15.4.-2006 2.4 GHz unlicensed band. It employs O-QPSK (Offset Quadrature Phase Shift Keying) with data rate up to 250 kbps in a 2MHz bandwidth. Direct-Sequency Spread Spectrum (DSSS) is utilized to resist interference and jamming. DSSS is combined with Frequency Hopping Spread Spectrum (FHSS) to further avoid interference and multipath fading. FHSS enables radio carrier to hop from one spectrum to another using a pseudo random sequence.

B.2.2.2. Data link layer

The datalink layer is also based on IEEE 802.15.4.-2006 MAC with TDMA to ensure contention free communication. With TDMA, the slots are typically divided into 10 msec duration to support transmit/receive data plus an acknowledgement. Collection of multiple slots forms superframe, which repeats at a fixed rate throughout the network lifetime. A transaction in a time

slot is described by a vector {frame id, index, type, source address, destination address, channel offset}, where frame id refers to specific superframe; index is the timeslot in superframe; type provides to transmit/receive/idle slot; source address is the source device address while destination address is the destination device address; and channel offset indicates logical channel to be used in communication.

B.2.2.3. Network layer

Network layer is responsible for routing and security within the mesh network. Network layer moves packets end-to-end within wireless network utilizing routing tables and timetables. Route tables ensure communication along graphs in which edge determines the link between two devices. Timetables provide communication bandwidth allocation intervals for specific services.

B.2.2.4. Transport layer

The unique feature of the WirelessHART transport layer is block data transfer. Transport layer provides reliable and connection-oriented communication link establishment between application host and field device. WirelessHART supports both acknowledged and unacknowledged transactions depending on type of data transmission. The data sent across the network are acknowledged like TCP/IP to facilitate retransmission of lost data. As an acknowledgement, Automatic Repeat Request (ARQ) can be utilized to ensure end-to-end data delivery.

B.2.2.5. Application layer

The application layer inherits from the wired HART enabling commands, responses, data types, and status reporting supported by the HART field communication protocol.

B.2.3. ZigBee

ZigBee is a standards-based protocol that provide network and application layer infrastructure required for wireless sensor network applications [70]. Zigbee was developed to support sensor needs, such as lower power consumption and low cost, and is secure, easy, and inexpensive to deploy. Thus, ZigBee addresses the unique needs of remote monitoring and sensor network applications. Typical architecture of ZigBee is shown in **Error! Reference source not found.**. Z igBee networks include coordinator, router, and end devices. Coordinator controls the network and acts as a trust center by storing network information. Router extends the network area coverage and dynamically provides backup routes in case of network congestion or failure. End devices typically execute applications and has neither a child node nor the ability to route messages. The ZigBee network supports star, tree, and mesh topologies [71].

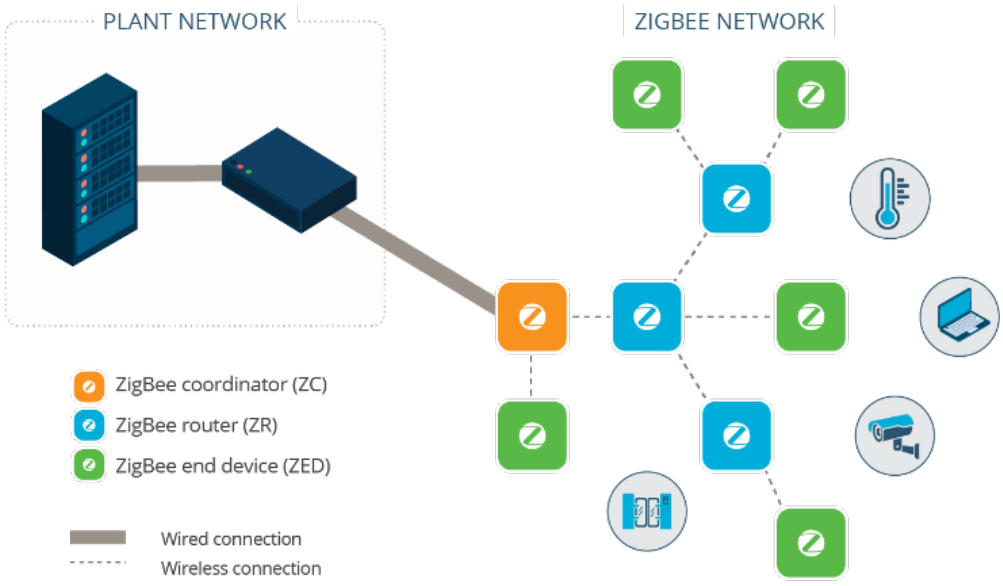

Figure 9. General Structure of Zigbee

The following sections outline the technical features of Zigbee. [70]

B.2.3.1. Physical layer

ZigBee supports two versions of the physical layer based on the frequency band they operate in. ZigBee can be operated in 868/915MHz with BPSK modulation and 2450MHz with O-QPSK modulation. 868MHz, 915MHz, and 2450MHz band supports date rate of 20KSymbols/sec, 40KSymbols/sec, and 62.5KSymbols/sec, respectively.

B.2.3.2. MAC layer

ZigBee MAC layer is built on CSMA/CA principle to enable collision free communication. ZigBee MAC layer frame composed of MAC header, MAC payload, and Frame Check Sequence (FCS). The ZigBee supports four frame structures such as, (i) beacon frame for time synchronization, (ii) data frame for data transmission, (iii) acknowledgement frame for successful frame recipient confirmation, and (iv) MAC command frame to set MAC layer parameters.

B.2.3.3. Network layer

Zigbee uses ad-hoc on-demand distance vector (AODV) routing protocol at the network layer. ZigBee specifies two address types, 16-bit addresses and 64-bit addresses. Sixteen-bit address are unique and assigned when the node joins the network. These addresses are not static and change under communication issue between end device and its parent or when the device type changes from end device to router. Whereas 64-bit addresses are unique and permanent.

B.2.3.4. Application layer

The data transmission and reception in ZigBee occurs using application profile. The ZigBee supports public profile IDs and manufacturer specific profile IDs in application layer. The public profile and manufacturer specific profile are assigned IDs of size 16 bits with value ranging from 0x0000 to 0x7fff and 0xbf00 to 0xffff, respectively. Public profile is used in enabling

interoperability between different Original Equipment Manager (OEM), whereas manufacturer specific profile is used by OEMs which do not require interoperability.

B.2.4. ISA100

The ISA100 standard has been developed and managed by International Society of Automation (ISA) to address all the aspects of monitoring and automation in the industrial manufacturing environment. ISA was built as an extension of the internet on top of Ipv6 “internet of things” standard and the standard is based on IEEE 802.15.4 protocol supporting coexistence with other wireless networks such as BLE and WLAN [72] [73]. A schematic depiction of ISA 100 network is shown in **Error! Reference source not found.**. The field devices and infrastructure/backbone d evices are the two classes of devices in an ISA network [71]. Field devices are fixed, portable, or mobile and are of three types:

1. I/O devices, which provide data to and/or collect data from other devices such as sensors and actuators;
2. routing devices, which route data/control signals between I/O devices and infrastructure devices; and
3. handheld devices, which are non-routing field devices. Infrastructure devices include gateway, backbone router, system manager, and security manager.

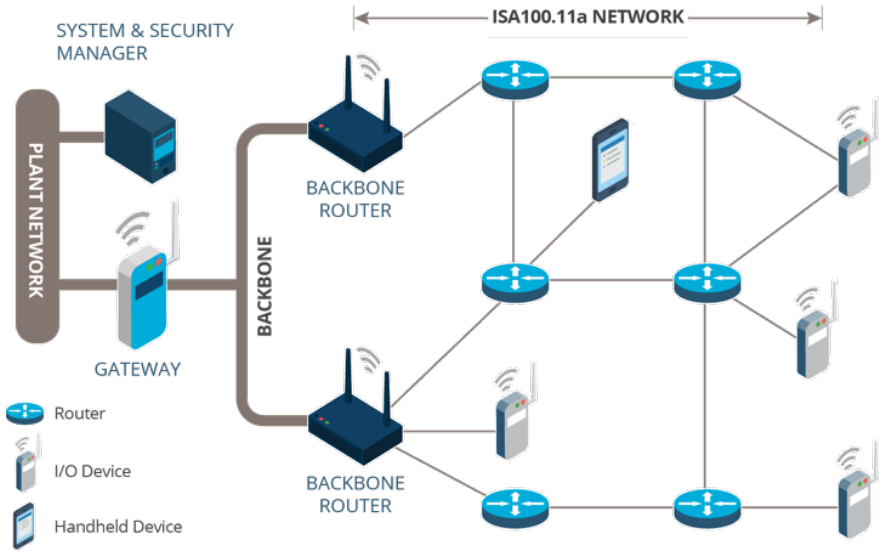

Figure 10. ISA100 Wireless Network Architecture

The following sections outline the technical features and limitations of ISA100. [71]

B.2.4.1. Physical layer

ISA100 is based on IEEE 802.15.4 standard, which uses 27 channels, number 0–26, at three different frequency bands [73]. Channels 11–26 are associated with 2.4GHz band with 5GHz channel spacing. ISA100 employs frequency hopping technique to avoid interference from other overlapping technologies such as WLAN and BLE. Additionally, ISA100 blacklists channels used by other wireless technologies achieve resilience against interference and achieve error free communication.

B.2.4.2. Data link layer

The ISA data link layer is unique to ISA100.11a and a non-compliant form of IEEE 802.15.4 MAC. The data link layer enables channel hopping, routing, and time-slotted time domain multiple access. It also establishes data packet structure, time synchronization, and packet error detection and forwarding. The time synchronized channel hopping provides accurate timing with improved utilization of all the channels to co-exist with other wireless technologies of the same spectrum. In addition, source, graph, and superframe routing are also supported at the data link layer [73].

B.2.4.3. Network and transport layer

The ISA100 network and transport layer utilize 6LoWPAN, which supports IPv6 (internet) packets in IEEE 802.15.4 to realize industrial internet requirements [73]. Moreover, the network layer supports packet fragmentation and reassembly to transmit large amount of data. The transport layer supports connectionless service based on UDP.

B.2.4.4. Application layer

Application layer supports object orientation to promote interoperability between diverse devices. Reference tunneling also further enables the wireless devices to encapsulate legacy protocols [73].

B.2.4.5. Communication optimization Limitations

Development of effective MAC mechanisms in internet-oriented wireless networked control systems is not trivial for critical control applications. MAC configurations and performance depends on the dynamics of the industrial environment. Thus, MAC configuration challenges can be technically addressed by optimizing the deployment and planning aspects of ISA100.

B.2.4.6. Routing mechanisms Limitations

The harsh and noisier industrial environments [73] require routing mechanisms to provide reliable transmission to meet end-to-end latency requirements and real-time decision-making.

B.2.4.7. Real-time control Limitations

Multiple support controls in a single wireless network would reduce cost and increase flexibility. But supporting such capabilities depends on meeting strict real-time wireless communication to avoid operational failures and accidents. Achieving such real-time control is challenging in the industrial set up consisting of unpredictable channel behaviors, physical obstacles, and interferences [73].

B.3. RFID

Radio Frequency Identification (RFID) is an automatic identification and data acquisition technology composed of three elements:

1. a tag formed by a chip with a connected antenna;
2. a reader sending a radio signal and receiving information from tags; and
3. a bridge connecting RFID hardware to an enterprise application [74]. Based on the distance between the system and the objects to which the tags are adhered, there exist different kinds of antennas and tags, as shown in **Error! Reference source not found.**.

Figure 11. A general architecture of RFID network.

Table 6. Operation bands for RFID technology.

Band	Frequency Range	Distance Range
125-150 Hz	Low Frequency (LF)	<2m
13.56 MHz	High Frequency (HF)	< 20 m
433-928 MHz	Ultra-High Frequency (UHF)	<100m and <2m
2.45-5.8 GHz	Microwave	<1m
3-10.5 GHz	Ultra-Wide Band (UWB)	<10 m

In an industrial environment, end users need to control and gather information related to both people and instruments, which are sparse in the environment with distances in the range of dozens of meters. In most cases, the UHF antennas are used for tracking materials or workers [74]. The information exchanged is stored in the RFID tags, which have two parts:

1. an integrated circuit, which stores and processes the information, modulates the signal, and collects the power from the transceiver if necessary, and
2. an antenna for transmitting and receiving the signal.

RFID has three types of tags active, passive, and semi-passive [74] . Active tags transmit the signal to the transceiver using power supply, whereas passive tags acquire the required energy from the RF wave created by readers to transmit signal. Finally, semi-passive tags transmit the

signal using a backscattering approach with tags being turned on by a signal. **Error! Reference s ource not found.** shows the comparison between different kinds of tags.

Table 7. Comparison of RFID types.

Metrics	Active Tags	Passive Tags	Semi-Passive Tags
Distance Range	Up to 100 m	Up to 15 m	Up to 60-80 m
Power	Battery	Inducted from readers	Turned on by a signal
Relative cost ($)	>30	1	>20
Data storage	Extendable	512 bytes to 4KB	Extendible
Data transfer rate	Up to 128 KB/s	Up to 1 KB/s	Up to 16 KB/s
Lifetime	Up to 10 years	Unlimited	Over 6 years

Each of the discussed industrial wireless sensor network standards has its own application, advantage, limitation, and more importantly, none of these technologies can be applied to all the applications. **Error! Reference source not found.** shows the comparison of different wireless t echnologies considering various parameters.

Table 8. Comparison of technical features.

Layer	Element	LoRaWAN	ISA100	WirelessHART	ZigBee
PHY	Number of channels	64 (902MHz)	16 (2.4GHz Band)	15 (2.4GHz Band)	27 (All Bands)
	Modulation	CSS	CSS	O-QPSK	BPSK/ O-QPSK
MAC/DLL	Beaconing	No	No	No	Yes/No
	Superframe Structure	Collection of Timeslots	Collection of Timeslots	Collection of Timeslots	IEEE802.15.4 Superframe
	Access Method	TDMA/ALOH A	TDMA/CSMA	TDMA/CSMA	Slotted and Unslotted CSMA
	Frequency Hopping	Slotted Hopping	Slotted/Slow/ Hybrid Hopping	Slotted Hopping	No (Frequency Agility)
	Timeslot Duration	Configurable	Flexible and configurable	10ms	Configurable
	Time Standard	Undefined	TAI	UTC	Undefined
	Cast Method	Unicast/Multic ast /Broadcast	Unicast/Broa dcast/ DuoCast/n-cast	Unicast/Broadcast	Unicast/Multica st /Broadcast
DLL/NET	Routing	One-hop	Superframe/ Source and	Superframe/Source and Graph Routing	Tree/Z-AODV

Layer	Element	LoRaWAN	ISA100	WirelessHART	ZigBee
			Graph Routing		
NET	Network Topology	Star	Star, Mesh	Star, Mesh	Tree, Star, Mesh
APP	Native APP Layer	LoRa	ISA100.11a	HART	ZigBee Profile
SYS	Clock Tolerance	Loose Requirement	10ppm or Loose requirement	10ppm	Loose Requirement
	Time Synchronization Mechanism	Advertisement/Pairwise Communication	Advertisement/Pairwise Communication	Advertisement + Pairwise communication	Beacon Frame
	Encryption	Symmetric (AES-128)	Symmetric AES-128	Symmetric (AES-128)	Symmetric (AES-128)
	Security Keys	Network key, Session key, Application key	Join key, Network key, and Session key	Join key, Network key, Session key	Link key, Network key, Master key
	Route Ability of Device	No	Non-routing field devices are allowed	All devices can operate router	RFD without Routing Ability
	Handheld device	Yes	Yes	Yes	No
	Peer to Peer Communication		Full	Full	Full/Limited
	Resource Allocation		Centralized	Centralized	Centralized + Decentralized

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Lon Dawson	08851	ladawso@sandia.gov
Alexandria Haddad	08851	alexhaddadnm@gmail.com
Chris Lamb	08851	cclamb@sandia.gov
Jenna DeCastro	08851	jdecast@sandia.gov
Mike Rowland	08851	mtrowla@sandia.gov
Shadya Maldonado	08851	sbmaldo@sandia.gov
Robert Bruneau	08851	rjbrune@sandia.gov
Doug Osborne	06812	dosborn@sandia.gov
Technical Library	01977	sanddocs@sandia.gov

Email—External (encrypt for OUO)

Name	Company Email Address	Company Name
Koushik Araseethota Manjunatha	koushik.araseethotamanjunatha@inl.gov	INL
Erick Martinez Rodriguez	erick.martinezrodriguez@nrc.gov	NRC
Anya Kim	anya.kim@nrc.gov	NRC
Eric Lee	eric.lee@nrc.gov	NRC
Christopher Cook	christopher.cook@nrc.gov	NRC
Dave Trask	dave.trask@cnl.ca	CNL
Richard Brown	richard.brown@cnl.ca	CNL
Mike Thow	mthow@epri.com	EPRI
Matt Gibson	mgibson@epri.com	EPRI
Jonathan Turner	turnerjp@zachrynuclear.com	Zachry NE
Stephen Lopez	slopez@epri.com	EPRI
Paul Martyak	pmartyak@epri.com	EPRI
Zeina Azar	zeina.azar@cisa.dhs.gov	CISA
Barry Hogan	barry.hogan@onr.gov.uk	ONR
Ian Begbie	ian.begbie@onr.gov.uk	ONR
Matt Fridley	mfridley@brenntag.com	Brenntag, NA
Scott Whelchel	swhelchel@dow.com	Dow
Sandra Parker	skparker@dow.com	Dow
Maulik Patel	mpatel@dow.com	Dow
Chad Kiger	chad@ams-corp.com	AMS
Michael Dack	michael.dack@exeloncorp.com	Constellation
David Olszewski	david.olszewski@constellation.com	Constellation
Kevin Deyette	kdeyette@nuscalepower.com	NuScale

This page left blank

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.