INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

Emerging Threats and Technology Investigation

Industrial Internet of Things - Risk and Mitigation for Nuclear Infrastructure

July 2022

Office of International Nuclear Security

National Nuclear Security Administration

INDUSTRIAL INTERNET OF THINGS RISK AND MITIGATION FOR NUCLEAR INFRASTRUCTURE

July 2022

Prepared by
Jeff Preston, PhD, Y-12 National Security Complex
Mik Bertolli, PhD, Avrio Analytics
Shannon Eggers, PhD, Idaho National Laboratory
Penny L. McKenzie, PhD, Pacific Northwest National Laboratory
Darlene Thorsen, Pacific Northwest National Laboratory
Jereme Haack, Pacific Northwest National Laboratory
Kenneth Thomas, Pacific Northwest National Laboratory
Lee M. Burke, Pacific Northwest National Laboratory
Dan A. Rosa De Jesus, Pacific Northwest National Laboratory

Managed by
Consolidated Nuclear Security, LLC
Management & Operating Contractor
for the
Pantex Plant and Y-12 National Security Complex
under Contract No. DE-NA0001942
with the
U.S. Department of Energy
National Nuclear Security Administration

CONTENTS

Abbreviations, Acronyms, and Initialisms v
1. Introduction 1
2. Background 3
2.1 IoT landscape for U.S. Federal Facilities 5
2.2 Nuclear System Requirements 6
2.2.1 NRC Power Reactor Cybersecurity Requirements 6
2.2.2 NNSA Requirements 7
2.2.3 Other Requirements and Guidance 7
3. Infrastructure 9
3.1 Communications 9
3.1.1 Wired Communication 9
3.1.2 Wireless Communications 10
3.1.3 Hybrid Communications 12
3.2 Device Hardware Design 13
3.2.1 Operational Characteristics 14
3.2.2 Hardware Security 14
3.2.3 Electrical Safety 15
3.3 Software Design 15
3.4 Algorithms 16
4. Risk Assessment 18
4.1.1 Cyber Risk Analysis 18
4.1.2 Vulnerabilities 18
4.1.3 Threats 18
4.1.4 Consequences 20
4.2 Cyber-Informed Engineering throughout the System's Engineering Life Cycle 21
4.2.1 CIE Design Principles 21
4.2.2 CIE Organizational Principles 22
5. Conclusions 24
APPENDIX A – Case Studies A.1
SolarWinds (U.S. GAO 2021) A.1
German Steel Mill Attack (de Maiziere 2014) A.1
Casino Fish Tank Hack (Townsend 2017) A.3
Oldsmar Water Treatment Facility (Cybersecurity and Infrastructure Security Agency 2021) A.4
Mirai Botnet (Cybersecurity and Infrastructure Security Agency 2017) A.5
Colonial Pipeline A.6
Log4shell A.8

APPENDIX B –References B.1
6. Works Cited B.1

FIGURES

Figure 1. Examples of IIoT opportunities in the nuclear security regime 3
Figure 2. Industrial Internet of Things 4
Figure 3. Basic IIoT framework 9
Figure 4. Example IIoT architecture 13
Figure 5. Example of condition-based monitoring 17
Figure 6. Example of AI/ML algorithm attacks 20
Figure 7. CIE principles (Eggers and Anderson, Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control 2022) 21

TABLES

Table 1. Wired Communications 10
Table 2. Wireless Communications 11
Table 3. Taxonomy of supply chain cyberattack types (Eggers and Rowland, Deconstructing the nuclear supply chain cyber-attack surface 2020). 19

ABBREVIATIONS, ACRONYMS, AND INITIALISMS

AI	artificial intelligence
BSI	German Federal Office for Information Security
CAN	Controller Area Network
CIE	Cyber-Informed Engineering
CISA	Cybersecurity and Infrastructure Security Agency
COTS	commercial-off-the-shelf
DDoS	Distributed Denial of Service
DNS	domain naming service
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
FTC	Federal Trade Commission
GAO	U.S. Government Accountability Office
I&C	Instrumentation and Control
ICS	industrial control system
ICT	information and communication technology
IIoT	Industrial Internet of Things
INS	Office of International Nuclear Security
IoT	Internet of Things
IP	intellectual property
IrDA	Infrared Data Association
ISM	Industrial, Scientific, and Medical
IT	information technology
LPWAN	Low-Power Wide Area Network
ML	machine learning
NaOH	Sodium Hydroxide
NIST	National Institute of Standards and Technology
NMAC	nuclear material accounting and control
NNSA	National Nuclear Security Administration
NOC	Network Operations Center
NRC	Nuclear Regulatory Commission
OT	operational technology
QoS	quality of service
RFID	radio frequency identification
SCADA	Supervisory Control and Data Acquisition
USB	Universal Serial Bus
VPN	virtual private network

CHAPTER 1

1. INTRODUCTION

Industries supporting the global nuclear infrastructure striving for cost savings, expansions in efficiency, and convenience are likely to adopt components (e.g., hardware, software) that comprise the Internet of Things (IoT) and Industrial Internet of Things (IIoT). These devices offer potential improvements along with security challenges. Modern conveniences achieved through application of technology have propagated through society in the form of interconnected devices, from doorbells to microwave ovens, commonly referred to as IoT. IoT devices are often Internet-connected devices that are designed to send data back to a cloud-based server, where a smart phone application then presents device status and control options. Home-based IoT applications carry a different set of risks when compared to a business or security environment, where there is also a history of convenience and interconnection. Industrial settings have long relied on specifically designed Supervisory Control and Data Acquisition (SCADA) systems for process control where IIoT devices are intended to inform business decisions and augment traditional processes. A recent National Institute of Standards and Technology (NIST) report provides a distinction between process control and IIoT in that traditional process control is not replaced by IIoT, but rather IIoT devices are intended to enhance industrial processes through additional monitoring of various sensors and application of data analytics models using artificial intelligence (AI) and machine learning (ML) (Fagan, Marron, et al. 2021) (Ross, et al. 2021).

The collection of physical sensor data (e.g., temperature, humidity, light density, radiation levels, and proximity) and actionable interpretation of this data is invaluable to ensuring the safety and security of personnel in nuclear facilities. These sensors can generate very large amounts of data that can be used to boost productivity, ensure safety of physical and environmental components, location and tracking services, and geographical information of tracked materials. IIoT can also be used to effectively monitor changes to working conditions, identify environmental changes that may affect materials, perform radiation detection, or provide alerts in an early warning system.

As the nuclear sector interconnects more control systems and associated devices, the industry struggles with developing a consistent set of verifiable security requirements (Fagan, Megas, et al. 2020). Sector-specific regulations, laws, or contractual obligations can require integration, system, or device standards. However, visibility of the integration of these various systems or the adequacy of applied cybersecurity controls largely remain a black box to the system owners or maintainers. This highlights another risk in that currently, there is no industry-accepted, efficient mechanism for tracking the usage characteristics of IIoT systems and devices whether they be cloud-connected or locally connected devices.

The effective management of IIoT in an operational environment and the efficient collection of information needs to be addressed to facilitate integration of future technology, sufficient protection of the entire system, and the reduction of harm caused by inadvertent or nefarious actions upon the system. Properly applying robust security controls based on industry standards protects the device, the data, and the system(s) it supports. Organizations using standards compliance as a means to maintain the security of these systems will help identify potential critical security flaws in the software and hardware as well as identify inappropriate or unapproved alterations. Clear requirements applied during design, along with continuous monitoring of IIoT devices, is fundamental in ensuring secure systems.

Determining how to use the information and best represent the data in a meaningful and productive way is crucial to the security design of the deployed IIoT into critical systems at nuclear facilities, including nuclear power plants, research and test reactors, and other radiological facilities. Once critical nuclear facility information is defined and the security of the devices are better understood, nuclear facilities will have to identify risks, mitigate these risks, and derive plans to maintain these systems to mitigate future risks as they arise. There are risks associated with individual devices, the security configuration used to connect to those devices, the physical access to the device, and the insecure firmware or software used to integrate these devices into a nuclear facility's system architecture.

As IIoT devices provide discrete functions within a complex system architecture for nuclear facilities, longevity of the system requires attention to the life cycle of security aspects. Systems containing IIoT devices present connection points that introduce additional potential attack surfaces of a system that may not be static. Evaluation of a device's security is a 'point in time' assessment that has a time stamp as new attack or analysis capabilities evolve. Thus, security personnel must periodically review security assessments to ensure that measures and approaches are effective in the concurrent threat landscape. As with many systems in the nuclear industry, a more robust and long-term digital security strategy depends on understanding the device and the system life cycle for the following aspects of IIoT:

- Adding new devices and decommissioning others
- Onboarding new cloud platforms
- Running secure software updates
- Implementing regular security key renewals
- Maintaining large fleets of devices

Integration of IIoT into automated processes can increase the ease of collecting relevant information about programs, operations, and policies, thereby providing data to address nuclear mission challenges in real-time and situation-specific conditions. IIoT optimization can enhance processes and operations by making the exchange of mission-critical information faster, more precise, and more reliable. IIoT can offer nuclear facilities efficiency gains across a myriad of hardware applications, from facility sensors to monitor power, radiation levels, environmental, or more discrete system-level processes. In addition, new technology from IIoT device manufacturers also maximize data captured with the use of autonomous devices or systems. With this information, IIoT can enhance the predictive maintenance processes of equipment by improving efficiency of resource allocation, maximizing working time of equipment, and reduction of waste.

Hyper-connectivity of IIoT and processing capabilities can influence decision-making processes specific to the nuclear domain. This includes the use of IIoT in ground-based vehicles (e.g., trucks, vans, and cars) and manned or unmanned aircrafts. Each has several advantages such as performing high-risk tasks (e.g., high radiation, contaminated areas, danger of explosion), more cost effective, and a lengthy time survey and monitoring capability. Depending on the degree of human intervention with the autonomous vehicle, they can be fully tele-operated (e.g., remote-operated vehicle), semi-autonomous (e.g., supervisory control), or fully autonomous. Search and rescue robots have the most similar domain applicable to the radiation measurements that are normally tele-operated or semi-autonomous. Potential applications of IIoT within nuclear security include:

- IIoT sensors may conduct and support radiation monitoring in the perimeter of the facility
- Dosimeter monitoring inside the facility

- Augmented reality and virtual reality applications for maintenance
- Moveable temporary measurement systems for selected sensors and equipment
- Fixed, short-range measurements to demanding places
- Moveable wireless cameras
- Visual drone inspections
- Drone inspections with carry-on sensors
- Remotely operated robots with carry-on sensors

This report aims to provide information on the emerging field of IIoT in regard to issues specific to nuclear security. Information provided from references is readily available through online resources. The volume of referenced material is such that this report provides summary information that may assist in generating awareness of IIoT concepts and challenges, while providing sufficient insight that may aid in planning or evaluating IIoT deployments.

2. BACKGROUND

The Office of International Nuclear Security (INS) within the National Nuclear Security Administration (NNSA) promotes the peaceful use of nuclear energy by collaborating with international partners to enhance global capabilities in prevention of theft or sabotage of nuclear material and facilities. INS maintains nine functional areas to improve and sustain effective nuclear security, including: Physical Protection, Nuclear Material Accounting and Control (NMAC), Transport Security, Response Force, Sabotage Mitigation, Insider Threat Mitigation, Cybersecurity, Performance Evaluation, and Regulations and Inspections. While there are numerous opportunities for using IIoT within power reactors and research and test reactors, IIoT may also benefit NMAC and other radiological facilities. Figure 1 provides examples of potential IIoT applications within the nuclear security regime.

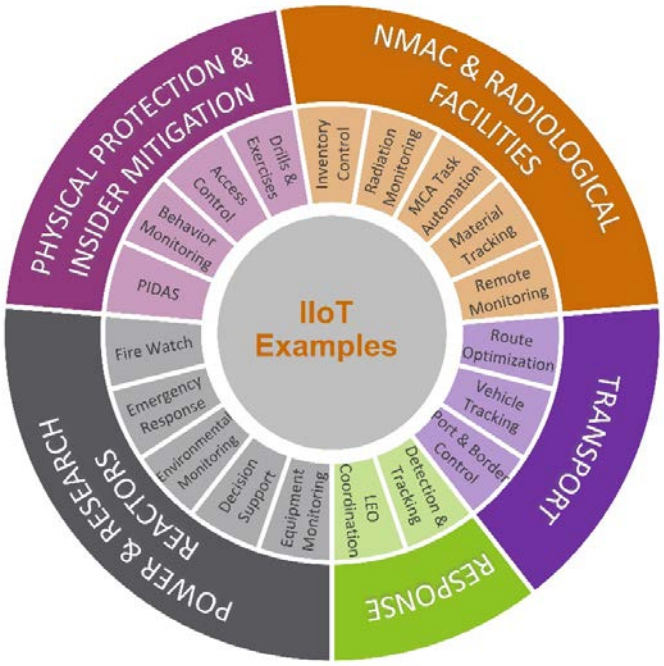


Figure 1. Examples of IIoT opportunities in the nuclear security regime

As technological advancement and modernization continues in the nuclear security regime, the prevalence of IIoT systems and devices will continue to expand, likely keeping slightly behind the pace of non-nuclear industries. To clarify the difference between similar terms, NIST defines IoT as the interconnection of consumer-level digital devices (e.g., smart appliances, home security systems, wearables, and cellular devices) in applications such as smart homes (Fagan, Megas, et al. 2020); whereas, IIoT is defined as the interconnection of digital devices (e.g., sensors, instruments, and machines) in industrial, manufacturing and business processes (Figure 2). IIoT is a transformational technology which integrates with information and communication technology (ICT) to bring enhancements to operational technology (OT) systems. OT systems are defined by NIST as "programmable systems or devices that interact with the physical environment" (ITL n.d.). These two areas of technology combine to bring enhancements to traditional OT systems, such as instrumentation and control (I&C) systems, SCADA systems, and distributed control systems, by providing additional monitoring and data analytic capabilities.

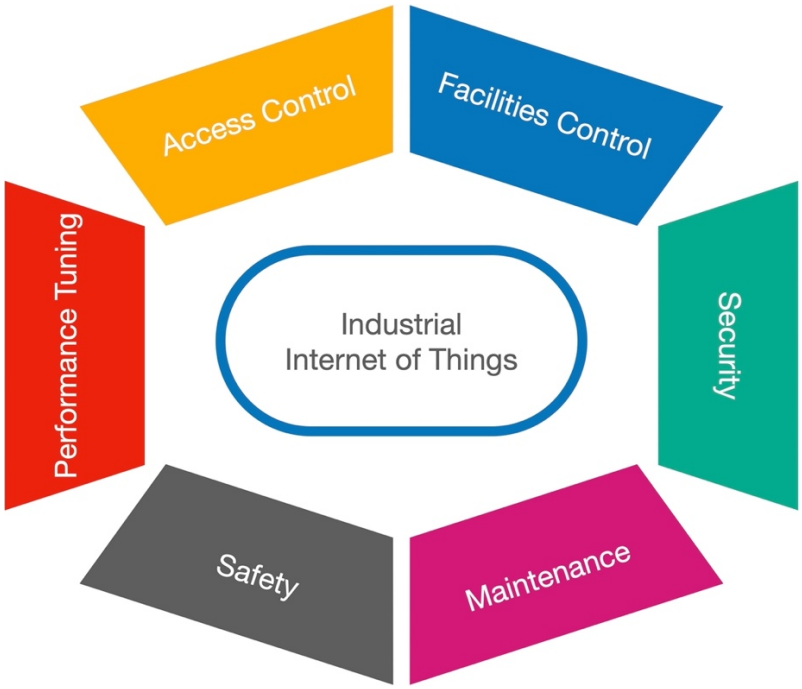


Figure 2. Industrial Internet of Things

While traditional OT often interconnects via wired networks, a benefit of IIoT is that it can be connected using wireless technology for wide area coverage, such as Wi-Fi, cellular, satellite, Bluetooth, Low-Power Wide Area Network (LPWAN), or radio frequency identification. This expanded network potentially enables broad distribution of data outside the traditional nuclear facility. Furthermore, tailored deployments of AI and ML applications can take advantage of these connectivity options to enhance automation and improve real-time insights into processes. These enhancements can lead to improved efficiencies, safety, and quality while reducing human errors, costs, maintenance, and downtime.

Although extensive wireless networks and Internet-based applications can potentially connect more dispersed devices than traditional wired networks, they are more likely to experience outages or can be expensive to deploy. Required system uptime necessary for nuclear facilities must be carefully balanced with system design to ensure a wireless connection is appropriate. Since wireless can experience interruptions due to wireless interference or physical barriers that limit or reduce signal between devices, specific architecture decisions will need to take intermittent connectivity or

physical placement into account. In addition, depending on design, IIoT can have high initial investment costs, especially if integrating new IIoT with legacy infrastructure. Interoperability of I&C devices with IIoT devices can be challenging and development of custom AI/ML applications to fit the specific need may be difficult, if not unfeasible.

An additional concern is that the security of IIoT systems is often overlooked. IIoT devices are often comprised of commercial-off-the-shelf (COTS) devices that may not include intrinsic security features in consideration nor be manufactured in secure factory environments. The motto "move fast and break things," encouraged by many technology companies, promoted new technologies without completing the necessary security or vulnerability assessments that were often pushed to later releases, often resulting in a partially finished product (Satell 2019). Not only are devices potentially insecure, there may be limited information about the digital bill of material (e.g., hardware, software, firmware) that may depend on insecure upstream suppliers or utilize outdated software codebases. This lack of knowledge can lead to improper configuration and insufficient mitigation of cyber risk. Further, AI/ML and IIoT applications are also vulnerable to cyberattacks; data corruption attacks can skew model learning or cause misclassification while AI model attacks can alter the learning process compromising model accuracy. Adequate preparation in the design process can help mitigate many of these risks.

2.1 IOT LANDSCAPE FOR U.S. FEDERAL FACILITIES

The United States Government Accountability Office (GAO) conducted a study in September 2020 to better understand the adoption and use of IoT devices in the federal government. The study included surveys that were sent to 90 government agencies and the results were mixed. Not all of the respondents answered each of the questions posed by the GAO. The report highlights that out of the 90 agencies that were sent the survey, 56 agencies report that they have adopted the use of some form of IoT technology. Broadly, many of the IoT devices the agencies are using are incorporated in control or monitoring equipment, access control systems, physical tracking sensors, and various other sensors. Many devices have a disperse number of functions, (e.g., air quality monitoring, occupancy monitoring, water quality monitoring, physical security applications, lighting sensors). Most of the data collected is used to increase operational efficiency and quick decision making which frees up personnel to focus on more pertinent tasks (Government Accountability Office 2020).

The Cybersecurity and Infrastructure Security Agency (CISA) published a paper on the "Internet of Things Security Acquisition Guidance" (CISA 2020). The paper provides an overview of cybersecurity considerations for the acquisition and deployment of IoT devices in federal facilities. CISA outlines the life cycle considerations that should be met to align with security recommendations for IoT (e.g., assessments, analysis, selection process, obtainment, support). There are associated risks with any new technology, and the paper outlines many examples of the security concerns related to the devices, systems, and services provided by IoT. Many of the guidelines provided are centered around the use of the NIST Cybersecurity Framework. The framework is designed to help organizations with security best practices and practical applications of security in their information technology (IT) enterprise systems. Some of the baseline security information suggested include NISTIR 8259, "Foundational Cybersecurity Activities for IoT Device Manufacturers," "Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers," and the "C2 Consensus on IoT Security Baseline Capabilities," developed and published by the Counsel to Secure the Digital Economy (Fagan, Megas, et al. 2020) (CDSE 2019).

The U.S. State Department has suggested using IoT as a mechanism to improve safety and operations at diplomatic facilities. IoT devices are an opportunity to give U.S. embassies in 190 countries a snapshot of their air quality, provide better energy efficiency with their building

management systems, and sensors deployed on the generators. The State Department has outlined its resilience strategy that includes using sensors for bigger picture projects, such as measuring and tracking seismic and floodplain data to ensure embassies remain safe from natural disasters. The State Department already leverages satellite and geospatial information to gain insights on the integrity and longevity of buildings. Also included are sensors for its global fleet of more than 14,000 vehicles. All data from the IIoT devices provide the State Department with facility analytics that they otherwise would not have (Heckman 2019).

The U.S. General Services Administration is working on a Smart Building Strategy to modernize existing buildings and establish new standards for design and construction to achieve their goals of energy efficiency and sustainability (General Services Administration 2021). The IoT adoption will include adding smart systems to building systems, occupancy sensors, environmental controls, and smart energy resources (e.g., solar, wind), all designed to maintain lower operating expenses, reduce energy costs, and decrease operational inefficiencies.

In a study conducted by the Center for Data Innovation in 2016, it was found that IoT devices are already being used in government facilities to help improve efficiency and reduce overall operational costs (New 2016). Many of the IoT devices include thousands of low-cost, connected sensors in high-energy use government buildings to help identify and help reduce overall operational costs.

The challenges that federal agencies are facing with IoT technology programs include widespread cybersecurity implications. There are fragmented standards, devices, and services for many IoT systems that can deter or hinder the additional use of smart systems including Wi-Fi power requirements and range constraints that can limit the suitability of IoT for long-range systems. There are inherently weak security applications that include lack of hardware security capabilities and security best practices, such as digital certificates. Many IoT devices have low computing and processing power that limits the use of encryption as well no encryption at all. The dispersed number of differing protocols makes managing these devices difficult in an IoT ecosystem. Many IT and OT professionals lack the knowledge or understanding of IoT aspects because of the varying communication and network pathways where knowledge may be uncommon or very specific to a particular system. The lack of standards can elevate the possibility of a widespread cyberattack using lateral movements from the base IoT devices to internal network infrastructures. IoT devices pose risks to assets across the entire network. The increased security risks from each of these endpoints can create an easy pathway for adversaries to compromise otherwise secure systems. The cascading effects of a cyberattack could be devastating to critical internal systems that manage the health and wellbeing of personnel, not just the building systems. IoT deployments also bring insurmountable amounts of data that could cause performance issues in traditional operational and management systems.

2.2 NUCLEAR SYSTEM REQUIREMENTS

2.2.1 NRC POWER REACTOR CYBERSECURITY REQUIREMENTS

The U.S. Nuclear Regulatory Commission (NRC) published regulations in 10 CFR 73.54, "Protection of Digital Computer and Computer Systems and Networks," that require NRC power reactor license holders to provide "high assurance" that the license holders provide "adequate protection" against cyberattacks for digital computer and communications systems and networks. The protection must address attacks up to, and including, design basis threats.

NRC power reactor license holders must protect critical digital assets that perform:

- Safety-related and important-to-safety functions

- Physical, personnel, and cybersecurity functions
- Emergency management and preparedness functions and off-site communication capabilities
- Support systems and equipment, that if the capabilities were degraded, would negatively affect safety, security, or emergency management and preparedness functions

NRC RG 5.71, "Cyber Security Programs for Nuclear Facilities," does not specifically address IIoT or IoT devices as a unique category; however, all digital assets (including IIoT devices) that are identified as critical digital assets must be adequately protected in accordance with 10 CFR 73.54. Since wireless connectivity of critical digital assets is generally not approved by the NRC and interference from wireless communications is often a concern, IIoT devices are not yet widely deployed in U.S. nuclear power reactors.

2.2.2 NNSA REQUIREMENTS

NNSA implements its cybersecurity program under SD 205.1, "Baseline Cybersecurity Program," and DOE O 205.1C, "Department of Energy Cybersecurity Program." These documents describe an integrated approach to managing risks associated with networked computer systems that interact or use connections to the Internet to conduct vital NNSA and DOE missions while fulfilling federal cybersecurity requirements.

2.2.3 OTHER REQUIREMENTS AND GUIDANCE

The President of the United States issued EO 14028, Improving the Nation's Cybersecurity, on May 21, 2021 that directs multiple agencies to enhance cybersecurity through initiatives related to the security and integrity of the software supply chain. It also directed the director of NIST to initiate pilot programs to educate the public on the security capabilities of IoT devices and software development practices, and to identify IoT cybersecurity criteria for a consumer-labeling program to reflect increasingly comprehensive levels of testing and assessment that a product may have undergone (Biden 2021).

NIST published NISTIR 8228, Considerations for Managing IoT Cybersecurity and Privacy Risks, to assist federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their individual IoT devices throughout the devices' life cycles and introduces a foundation for a planned series of publications. Specifically, the document:

- Identifies unique characteristics that separate IoT from other IT and OT systems
  - Physical computing and the ability to affect the environment in which the device monitors
  - Device access challenges
  - Privacy concerns
- Provides unique aspects for cybersecurity and privacy risk considerations
  - Device interactions with the physical world
  - Device access, management, and monitoring features
  - Cybersecurity and privacy capability availability, efficiency, and effectiveness
- Outlines high-level cybersecurity and privacy risk mitigation goals
  - Protect device security
  - Protect data security

- Protect individuals' (organizational) privacy
- Recommends actions to address cybersecurity and privacy risk mitigation challenges
- Organizational policies and processes
- Update risk mitigation practices

The NIST series of documents provides manufacturers, users, system designers, and third-party support personnel core baseline device cybersecurity capabilities for new IIoT devices for integration into information and operation systems.

- NISTIR 8259:
  - Manufacturer activities impacting the IoT device pre-market phase
    - Identify expected customers and define expected use cases
    - Research customer cybersecurity needs and goals
    - Determine how to address customer needs and goals
    - Plan for adequate support of customer needs and goals
  - Manufacturer activities impacting the IoT device post-market phase
    - Define approaches for communicating with customers
    - Decide what to communicate to customers and how to communicate it
- NISTIR 8259A:
  - Device identification
  - Device configuration
  - Data protection
  - Logical access to interfaces
  - Software update
  - Cybersecurity state awareness
- NISTIR 8259B:
  - Documentation
  - Information and query reception
  - Information dissemination
  - Education and awareness

NIST published "Secure Software Development Framework Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities" in February 2022. The document provides security software development practices without being prescriptive in the implementation of the practices. The practices may be implemented in IoT. For example, it suggests that software teams maintain secure development tools in environments separated from standard IT networks, where limited connectivity and access provide additional confidence during the development process. This guidance is applicable to systems of any scale, setting, and function, not just to IoT.

3. INFRASTRUCTURE

As shown in Figure 3, IIoT is comprised of a wide array of edge sensors streaming data over networks, to data acquisition systems that store and interpret the data, ultimately presenting the data to a person or other system to initiate an action. IIoT application designs will vary, but they generally include a selection of relevant sensors designed to monitor a specific system or process, a means for communication of acquired data, data processing algorithms suitable to develop operational conclusions, and a means of presenting these results as possible actions to a user. In the nuclear security domain, this also includes a strict adherence to safety and security, where the design must meet various criteria that other industries may not.

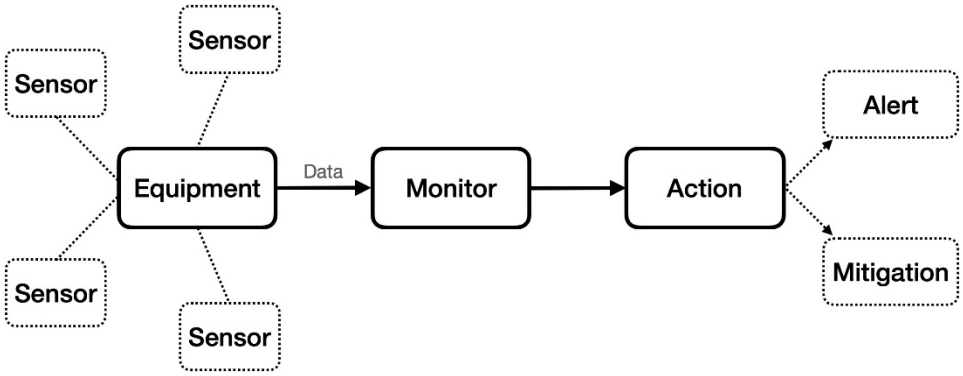


Figure 3. Basic IIoT framework

3.1 COMMUNICATIONS

Communication methods are critical in networked systems and are likely to be selected according to a variety of factors: initial and recurring cost of operation, available bandwidth, distance of operation, quality of service (QoS), compatibility with non-communications features, and security. Design of an IIoT system begins with selection of wired or wireless communication or a combination thereof. Wired offers some advantages to nuclear security, where directly wired systems (e.g., Ethernet) may expose fewer attack surfaces. Some wireless options may have more advantageous capabilities than others, depending on whether transport is long distance radio (e.g., cellular or long range), medium distance using Wi-Fi or ZigBee, or short distance using Bluetooth or RFID. Each wireless transport case offers trade-offs between device cost, convenience of operation, and security enhancements necessary for operation. Consideration should also be given to QoS, encryption, authentication, and available bandwidth. This report will not address satellite or fiber optic connections to regional communications systems as these will be similar to Ethernet and cellular communications.

3.1.1 WIRED COMMUNICATION

Communications using directly connected wires offers many solutions that may be adapted toward various IIoT designs where selections often vary on bandwidth, length of runs, number of devices, and other factors. These options generally include Ethernet, serial (e.g., RS-232 or RS-485), Controller Area Network (CAN), and Universal Serial Bus (USB), as shown in Table 1 (Pramberger 2022) (Texas Instruments 2016). Each option may serve a role in a specific type of design or may be combined for a specific topography, as will be discussed in Section 3.1.3, Hybrid Communications. This section only discusses the physical layer implementation, not any specific communication protocol as that may be similar across several types. Also, this section only discusses potential communications for wide areas, where in-device busses (e.g., I2C or SPI) are omitted.

Table 1. Wired Communications

Method	CAN (Texas Instruments 2016)	Ethernet	Serial EIA		USB (Forum n.d.)
			RS-232 (Maxim Integrated 2001)	RS-485 (Integrated 2001)	
Maximum cable length		~1km	~150ft	4000ft	15ft
Cable type	Twisted pair	Twisted pair	Twisted pair		Twisted pair
Maximum number of devices	128	Many	2	256	128
Standardization	ISO 11898-2	IEEE 802.3	EIA-232	EIA-485	USB-IF
Topology	Bus	Bus, Star, ring	Line	Bus	Bus
Maximum transmission speed	1Mbps at 40m 50kbps at 1km	>1km	<350kbps	<10Mbps	1.5Mbps (1.0) 12Mbps(1.1) 480Mbps(2.0) 5Gbps (3.0)

Each wired method described requires physical wire to transmit the electronic signals between two or more devices. Signals in this case often utilize a differential method to send and receive bits at a time, where error correction may also be included. Some cases use as few as two wires for serial busses and up to eight for Ethernet, where additional wires result in increased maximum bandwidth. In every case, as the wire length increases, the maximum speed decreases as the capacitive load on the wires is such that transmitted bits lose sharpness to the point that the binary states are indistinguishable to the hardware. Thus, each modality has a maximum working distance for a given data transmission rate that must match the deployment scenario where a specific optimum may exist as a balance between installation costs and requirements. Similarly, in some cases, wired solutions may be preferred as it is feasible to power the sensor using the communications wires, as in the case of Power over Ethernet (Microsemi 2011).

As cable traverse a facility, running wires through metal conduit is common practice according to electrical codes and is a good physical security practice. Wired communications typically require physical access to read or inject a signal using a 'man-in-the-middle' attack, whereby an attacker could insert a device and sniff or corrupt the transmission between sensors and the data acquisition system. To protect against this, access to the wires needs to be restricted as a graded approach depending on the risk associated with a given sensor or system.

3.1.2 WIRELESS COMMUNICATIONS

Radio transmission offers a set of advantages over wired operations that enable several additional deployment strategies, but also comes with security challenges. Wireless enables mobile systems, communications over very long distances, and provides localization methods through triangulation. Wireless networks exist in many forms and cover many frequencies that may vary across the world. In most locations, high frequency Industrial, Scientific, and Medical (ISM) bands are readily available bands for unlicensed communications, which include the 2.4GHz ranges common for Bluetooth and Wi-Fi. ISM bands cover different frequencies and can vary regionally, where commonly used frequencies include 915MHz, 868MHz, and 433MHz (LoRa Alliance 2021).

Table 2. Wireless Communications

Method	Bluetooth (Di Marco, et al. 2017)	Cellular (1NCE n.d.)	Wi-Fi (Ethernet) (Certification 2009)	LoRa (Alliance n.d.)	ZigBee (Wojciechowicz 2018)	Z-Wave
Frequency	ISM	Licensed	2.4GHz or 5GHz	ISM	ISM	908MHz
Maximum number of devices	32,767	Up to 50k devices per NB-IoT cell	Varies	100s	65,000 as mesh	232
Standardization	IEEE 802.15.1 (Bluetooth SIIG)	Various: CDMA, GSM, 4G LTE EDGE, 5G, NB-IoT	IEEE 802.11	IEEE 802.15.4g	IEEE 802.15.4	Silicon Labs
Topology	Star, Mesh	Star	Star, Mesh	Mesh	Mesh	Mesh
Transmission distance	Up to 100m	Long distance km	Up to 200ft	100m to km	10-20m (915MHz) 100m (2.4GHz)	30-65m
Maximum Transmission Speed	Up to 2Mbps	Up to 300MBps (4G LTE) 1Gbps (5G)	Up to 7Gbps	0.3 to 50kbps	250kb/s	40kb/s

Choice of wireless network is often related to a few key parameters: required bandwidth, coverage area indoors and outdoors, and QoS. For IIoT sensors that transmit a small data packet periodically (e.g., temperature or barometric pressure), bandwidth can be limited and a mesh solution or other low bandwidth mode without a high QoS might suffice. Accelerometers with high speed sensing, common to vibration monitoring systems, would require a high QoS as lost packets inhibit algorithm performance, but a modest bandwidth. Full motion video for analytics requires high speed connection using a wireless Ethernet or possibly cellular, where cost and coverage might prefer the local infrastructure over a cellular solution. Wide area mobile IIoT solutions preclude the short area coverage and would opt for the LPWAN solutions similar to long range or cellular.

Low-power wireless often uses the ISM bands, which have varied coverage for indoor use depending on operating frequency and choice of building materials. In concrete facilities, 2.4GHz common to Bluetooth and Wi-Fi do not traverse walls or floors easily, where an infrastructure of repeaters would be necessary for operation of a Wi-Fi network. Bluetooth in a direct link connection would not be able to broadcast around corners easily, where a Bluetooth mesh may be preferred. In the case of nuclear security, this drawback is a benefit in that physical access should be denied in the broadcast range of wireless equipment that may affect facility or material security; thus, a Faraday cage is preferred, followed closely by significantly attenuating walls such that perimeter security does not have to cover as much ground area.

Where mesh networks are feasible, collaboration between each IIoT device on the network is required, as each acts as a repeater until a message reaches its end of life. A single IIoT device transmits a packet to the entire network with the intention of reaching the hub that collects and

forwards the data as an uplink. Nodes within the range of the original receiver will pass the message to all nodes within the range of that node, ad infinitum. Each node receiving the packet increments a lifetime counter by one in the packet header, such that packets are not infinitely repeated, and nodes that already received and broadcasted will not retransmit the same message. A mesh system does not necessarily remember the pathway a packet may take, but it is self-adjusting; mesh nodes that are mobile within an area will maintain connection. An additional benefit is that mesh systems allow networks to saturate areas in buildings constructed with materials that inhibit radio transmission. Meshes offer useful features, but also create seemingly random delays in message receipt times and provide an indeterminate QoS in the event packets reach their end of life before the hub.

Cellular systems are rapidly becoming a cost-effective means for mobile or geographically diverse IIoT installations. Narrowband IoT is a rapidly evolving IIoT platform that enables cellular communications for devices with similar coverage to cellular phones (1NCE n.d.). Cellular communications are often security concerns at nuclear facilities as the transmission distance is quite far; thus, cellular and LPWAN solutions may be preferred for some limited scenarios.

Also of note are some non-radio wave-based wireless systems that utilize optics for data transmission. The Infrared Data Association (IrDA) is an industry group that developed a series of protocols in the mid-1990s where light in the infrared range (>800nm) carried data between a transmitter and receiver. As sensor speeds improved, the latest revision is capable of speeds up to 1Gbit/s over distances of up to a few meters (IRDAJP n.d.). Line-of-sight communications are very secure but have historically shown difficulty adapting to large deployments and are ergonomically difficult. While IrDA was primarily a direct connection only, another effort using visible light communications through standard LED lighting is being promoted by the Li-Fi consortia (LiFi n.d.). Li-Fi allows speeds up to 100MB/s over standard Ethernet protocols, can broadcast to a wider area, and maintains the physical security advantages of IrDA. For most applications, Li-Fi versus Wi-Fi would be indistinguishable to the end user unless transmission speed was a priority.

In summary, several options exist for wireless communications, where industry trends driving faster speeds and longer transmission distances may sometimes be at odds with nuclear security. Similarly, industry standard encryption methods may not provide the security needed over time as demonstrated by the difficulties with the original Wired Equivalent Privacy and subsequent versions of Wi-Fi Protected Access. In these cases, mitigations through encrypted transport are feasible and strongly encouraged to protect data attribution and integrity in transit. Lastly, while optical methods may not be as common, the security models do pose some distinct advantages.

3.1.3 HYBRID COMMUNICATIONS

Network architectures do not necessarily fall within a single method on a large scale. Often, hybrid networks offer benefits in sensor selection, cost, and graded approaches to security. In many cases, hybrid networks are embodied as a mix of high bandwidth backbones that connect a central operations center with various routers that fan out to lower bandwidth lines that then fan out to individual pieces of equipment or types of sensors, as illustrated in Figure 4. In this case, selection of the physical layer will be suited to each leg according to required bandwidth, QoS, and cost for components attached to it. From a security perspective, each leg would need to follow a graded approach to security regarding encryption and sensor complexity, where it is preferred to enable specific choke points to limit lateral movement in the case of a breach. More importantly, each selection also entails the entire suite of potential attack vectors and security requirements associated with the individual methods, where the sum may require more complex network security.

Consider a large organization spread across a single geographical region, but spatially separate, where a single Network Operations Center (NOC) is preferred for health and security monitoring of the entire enterprise. In this case, a star topology would exist from this NOC, where it may be most cost effective to connect to each site through a Virtual Private Network (VPN) using fiber service from one or more communications providers. Cellular-connected IIoT devices may monitor movements of materials between sites. At each site, a single point of communication up to the NOC would collect all information, where another star topology may exist. A series of Ethernet routers would fan out to the various areas of a facility providing a backbone on site. Wireless access points may be connected to these routers to provide wireless Ethernet communications as a star topology. Ethernet switches providing localized power over Ethernet may provide power and Ethernet communications to particular sensors (Microsemi 2011). A single, large piece of equipment may contain multiple sensors connected through a CAN bus or Z-wave network where a single data acquisition system collects and forwards data up to the NOC. In this example, several physical options for communications comprised a single network where each modality was selected for specific purposes. This also presented several locations where data may be converted from one physical method to another.

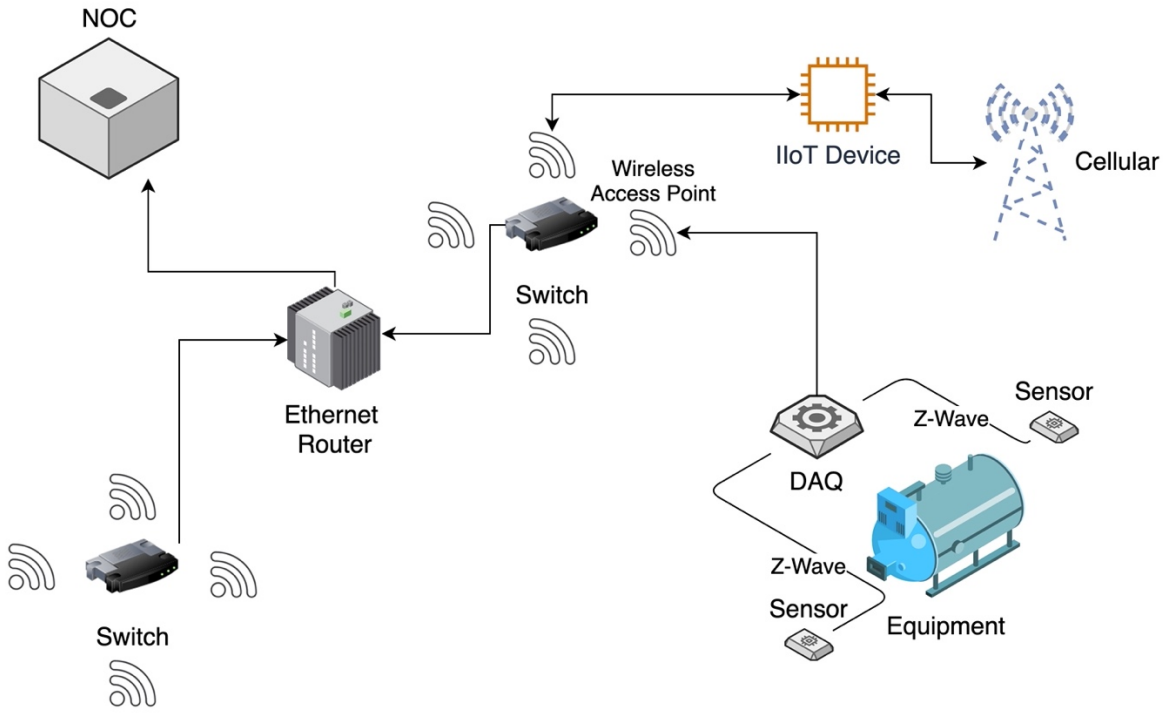


Figure 4. Example IIoT architecture

3.2 DEVICE HARDWARE DESIGN

Hardware selection includes review of operational characteristics of the sensors to meet a specific use case, but also includes considerations for security of the hardware as well as electrical safety specific to the facility requirements. Certain applicable industry standards and certifications from testing agencies (e.g., PSA Certified and Connectivity Standards Alliance) provide good selection criteria as a starting point for due diligence in designing an IIoT system (Connectivity Standards Alliance n.d.) (PSA Certified n.d.). While low-level design expertise should not be required in order to select suitable equipment, a good understanding of the current common attack methods and security countermeasures provides a good base of questions to ask of a solution provider.

3.2.1 OPERATIONAL CHARACTERISTICS

An IIoT device is more than a single component, as devices are comprised of several subsystems and components that share purpose in an integrated package often fusing the mechanical and hardware design aspects. These may include:

- Communications – Ethernet, radio, serial, USB
- Environmental – ESD suppression, magnetic shielding, radiofrequency shielding
- External sensors – accelerometer, barometer, positioning system, temperature
- Power supplies – conditioners, DC-DC voltage converters, switching AC/DC adapters
- Processing units – Encrypted root trust, trusted platform module
- User interface – Buttons, display, LED indicators

Vendors choose each component in a system according to several criteria, typically based on size, weight, power, and cost, where security has often been an afterthought, but is now becoming an important consideration during the conceptual design phase. Mechanically, a device should prohibit physical access to internal electronics as this is the source of many attacks (e.g., side channel and "glitching") (Quast 2018) (Franklin 2019). Tamper indicating, through either electronic or physical means, can inhibit system operation after opening or applying various voltages, frequencies, or temperatures, where a non-resettable fuse or other method can block system start up, restrict access to cryptographic storage to disallow the device to access the network, or alerting the NOC of the intrusion. Tamper-indicating devices common in nuclear safeguards applications are similarly applicable to IT/OT/IIoT infrastructure where periodic physical checks may indicate tampering or unknown changes.

As devices are often specific to a task, processors driving these systems will be general-purpose parts suitable for many different applications, which will likely include many unused features that require disabling, ideally by the manufacturer, to limit attack surfaces. For example, if an IIoT device was performing video analytics for change detection of a storage area, where the instrument contains a microphone that is not used in the application, an attacker might be able to make use of the microphone capability for other purposes. Being able to physically disable the microphone would entirely block the capability.

3.2.2 HARDWARE SECURITY

Microprocessors have evolved greatly in terms of capability and power; small systems suitable for IIoT are incredibly complex compared to where low-power microcontrollers were in the early 2000s. Microcontrollers are often used for small tasks with a minimal memory footprint, making them ideal to read out a single sensor and transmit data; however, this restricted capability has historically limited the security features, where compromised networked systems offer a foothold for lateral movements. Modern systems include a variety of security features on die, where a few key aspects have been highlighted as integral: hardware root of trust, secure boot, attestation, and anti-rollback prevention (Hunt, Letey and Nightengale 2020) (IoT Security n.d.). While these are common in the industry, vendors often offer additional security features beyond this set.

- A root of trust is defined here as the cryptographic engine within a processor that contains encryption certificates that are inaccessible to software. By partitioning this from software, the certificates cannot be modified with a software vulnerability.

- The secure boot is a means by which the firmware is validated through cryptographic signatures to match the vendor, inhibiting booting from tampered firmware.
- Attestation is similar to a birth certificate of the device as a cryptographic key that exists in the hardware such that the instrument cannot be duplicated or copied, which enables network awareness software to positively identify a device connected to the network.
- Anti-rollback blocks a common attack vector where an older firmware version is loaded onto a device that carries an exploitable vulnerability, where anti-rollback mechanisms block this capability.

3.2.3 ELECTRICAL SAFETY

Nuclear facilities have significantly stricter electrical safety requirements for safety-related equipment and potentially higher requirements for non-safety-related equipment than commercial facilities, which may pose some issue with IIoT adoption, especially for safety-related applications. In many cases, commercial offerings will meet most criteria in terms of specifications of form and function of a device; however, additional requirements for electrical safety through a Nationally Recognized Testing Laboratory, or NRTL (e.g., UL and TUV), intrinsic safety (e.g., UL-913 or ATEX), and possibly government-mandated restrictions on potential suppliers will limit potential hardware choices (Aloxy.io 2022) (IFM Electronic GmbH 2020). Hardware should be selected in coordination with relevant engineering personnel to ensure that sensors and required wiring meet facility design criteria. From a nuclear security perspective, compromised IIoT devices can have a potential to cause physical damage if they control power supplies, heaters, or other components.

3.3 SOFTWARE DESIGN

Software covers a very wide range from development environments to automated systems to user interfaces, where the aspects of security far exceed the scope of this report; however, a few key aspects specific to IIoT require consideration. As IIoT is a collection of sensors, software is the glue that enables a system to combine this data and enable an algorithm to perform some interpretive task. Software may be split into two categories: back end and front end. Back end refers to anything within the system that a user does not directly interface with including network stacks or databases, while front end includes what a user may directly control, particularly graphical user interfaces. Software attacks are possible at both levels, but the back end is typically where events occur.

IIoT systems generally include transport of data from one point to another through a network medium, described previously, where a sensor transmits data to a server. This data packaging and transportation operation requires data assurance, integrity, and security as key concerns otherwise the resulting algorithm may not operate with confidence. At a low level, this includes choice of protocol, where designers may opt for a User Datagram Protocol operation where individual packets have some tolerance for loss, while a Transmission Control Protocol may be necessary for data assurance.

In many instances, the concept of trust on a network precludes allowing two systems to operate on the same network, where isolating certain systems from others is a form of security. Duplicating network hardware infrastructure for an isolated system is expensive, where technologies including Software Defined Networks and Virtual Local Area Networks are similar in approach while using the same hardware. In these cases, network hardware creates partitioned subnetworks by specifying physical ports or MAC addresses that are connected in the same subnet, while excluding all others. This allows IIoT hardware to coexist on the same hardware network, while being entirely separate from any network transport.

In nuclear security, data transmitted may not be individually sensitive, but may be compiled with other transmitted sources where data encryption is necessary between the sensor and data acquisition system. Encrypted connections also provide a level of protection against data poisoning and spoofing. In many cases, this requires system administrators to manage a trusted certificate authority within the confines of their own network that can issue certificates for various devices.

Computer systems include many general-purpose capabilities that may include unused network ports, application server connections, or other potential attack surfaces, where an administrator should filter, close, or restrict these to specific users according to the least access principle. Tailoring specific users to specific applications limits the ability of an attacker to cross boundaries quietly and easily. Authentication requirements for user privilege escalation (e.g., from a basic user to a user with database administrator rights) will generate a log history that may include some logic that alerts a NOC administrator of a potential attack. The Zero Trust Architecture includes this as a fundamental design aspect.

Modern cloud computing operations built around containerized server applications provide some additional security. System administrators may deploy containers in a secured state as tested by a vendor rather than requiring specific expertise locally. These lab-tested containers will have undergone significant quality assurance tests, including penetration testing, that may require excessive cost and time for a single customer to perform. Several big data platforms specific to IoT and IIoT provide containerized servers for this type of architecture, where Security-as-a-Service is produced.

3.4 ALGORITHMS

Data acquisition systems are often designed as either centralized or distributed services that process data and forward it onto another system or human for determination of an action. In many cases, these include Network Attached Storage systems with large amounts of memory that provide means to access and select specific data. Algorithms using AI/ML approaches are often used for developing data models and interpretation, where upstream software for these algorithms are often built on open-source software that should be vetted and acquired from a reputable source. In nuclear security, these algorithms may affect safety or security of nuclear material and need to be rigorously tested for vulnerabilities, particularly areas where the algorithm may not generalize as expected to data values outside of training boundaries.

Algorithms using AI/ML approaches are often applied to condition-based monitoring, where some level of automation supports operations and maintenance of equipment. The data used is typically gathered in real-time from various sensors distributed strategically across a facility, system, or component, where sensor types may include thermocouples for temperature monitoring or accelerometers for vibration and shock analysis. Algorithmic approaches then process this data for trends or key indicators that aid in predicting equipment failures, operational safety concerns, or remaining useful life of a component. An example laboratory system, shown in Figure 5, labels various sensors common to condition-based monitoring. Within an IIoT-enabled facility, conditioned-based monitoring may be integrated with facility OT and access controls. For example, real-time identification of critical failures or deteriorating safety conditions can trigger safety lights or alter access controls to support the appropriate response.

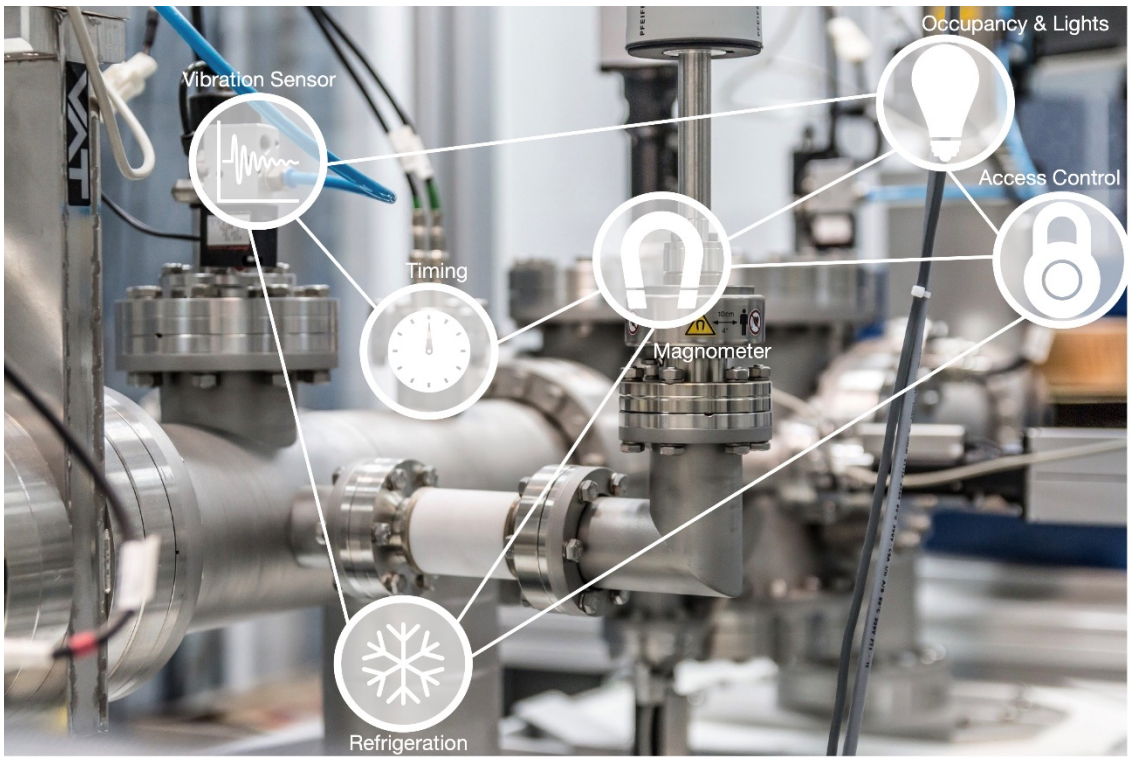


Figure 5. Example of condition-based monitoring

Several AI/ML techniques are applicable to the type of sensor data collected with IIoT devices. While the specific algorithm chosen is highly dependent on both the data and the use case, there are a wide variety of approaches related to classification and time-series modeling that are broadly applicable to IIoT. Gaussian process models and deep learning sequence models are well suited for analysis of time-series data, such as temperature and vibrational data. Gaussian processes can determine key change points that indicate upcoming repair needs and can generate critical trends that can serve as a baseline in anomaly detection for safety and security concerns. Similarly, support vector or restricted Boltzmann machines can provide sequence classification analysis of electromagnetic sensor data to generate strongly predictive features correlated to circuit failure.

However, the use of data by AI/ML algorithms to inform any decision-making introduces the potential for a new threat vector. Particularly where open-source software is used, the algorithms can be compromised to intentionally produce false results, such fabricating both false positives and false negatives. For example, a compromised algorithm may perform as expected for condition-based monitoring except for when a particular equipment failure mode is detected that is desired by a malicious actor. The algorithm may be intentionally designed to neglect that failure mode in an effort to sabotage the equipment in a particular manner.

Furthermore, because maintenance and safety indicators are, in general, obscured by high amounts of noise within the data, stages of data cleaning and filtering prior to use is required in an AI/ML algorithm. These stages of an analysis pipeline introduce additional vulnerabilities. The data pipeline can be poisoned, providing training and inference data to algorithms that have been manipulated in unknown and potentially malicious ways. For example, corrupted training data may be passed in the pipeline to a time-series analysis algorithm, such as a Gaussian Process, in order to alter the true baseline that is used for anomaly detection. Even with a secure and well-implemented algorithm, the corrupted data input would result in false negatives that are tailored by the poisoning attack.

4. RISK ASSESSMENT

4.1.1 CYBER RISK ANALYSIS

Traditionally, risk is defined as the complete set of triplets considering scenarios (or undesired events), likelihood (or probability of the scenario successfully occurring), and consequence (or impact of the scenario) (Kaplan and Garrick 1981). Techniques such as probabilistic risk assessment have been used to estimate public risks by using historical data to quantitatively identify the probability that a severe accident or failure scenario will occur and result in adverse consequences. When considering cyber risk, however, this probabilistic analysis technique is ineffective. Cyber incidents, both unintentional and malicious, are largely a function of device vulnerabilities and threats, both of which are often unknown and dynamically changing, making it difficult, if not impossible, to quantitatively calculate risk. Thus, cyber risk is often evaluated by considering the triplet of threats, vulnerabilities, and consequences, where consequences are conditionally dependent on both the threats and vulnerabilities. Additionally, it is important to remember that cyber risk includes both unintentional incidents, such as device failure or human performance errors, as well as intentional, malicious actions by adversaries.

4.1.2 VULNERABILITIES

Digital footprints of IIoT implementations vary based on application. While some IIoT systems may include many geographically dispersed devices connected by multiple communication methods, others may be standalone with limited connectivity. As outlined, this IIoT infrastructure may include OT devices, such as sensors, data acquisition, monitors, processors, and controllers as well as ICT devices for networking and wireless communication. Since each device in an IIoT system is comprised of hardware, firmware, and software, as the IIoT digital footprint expands, the number of vulnerabilities and access points also expands.

Vulnerabilities are known or unknown weaknesses. Since many IIoT devices are COTS components used in a variety of industries and applications, they are often not designed to meet the same strict requirements necessary in critical SCADA or industrial control systems (ICSs). Thus, vulnerabilities, such as programming bugs or manufacturing defects, may be introduced into devices due to lack of proper design or quality assurance standards. Additionally, security may not even be considered as part of the design. This lack of security may leave the IIoT devices and systems exploitable, enabling adversaries to extract information or insert compromises leading to unauthorized access and/or malicious activity.

Vulnerabilities are often identified by facility personnel, manufacturers, or other users. While many ICS manufacturers or vendors often supply vulnerability notifications once discovered, this service is often not available for IIoT devices. However, several vulnerability tracking databases are available which can provide awareness into known vulnerabilities (MITRE n.d.) (MITRE n.d.) (FIRST n.d.) (CISA n.d.).

4.1.3 THREATS

As the digital footprint expands, not only does the possibility for unintentional actions increase but this expanded cyberattack surface can provide adversaries with many opportunities for gaining access into the IIoT system. Similar to ICS in nuclear facilities, threat vectors into IIoT systems include wired and wireless communication networks or connections, portable media and maintenance devices, insiders, and the supply chain. As discussed in Section 3.1, many options exist for IIoT communication pathways. Improperly designed IIoT networks may not only allow

unauthorized access to the IIoT system, but could also inadvertently interconnect IIoT systems with other systems, such as ICS or business networks, thereby creating additional insecure data pathways for exploitation or compromise of all connected systems.

Even if IIoT system architectures are securely designed or air-gapped, malware or other compromises can be introduced during maintenance or configuration activities when USB drives or maintenance equipment (e.g., laptops) are connected to the IIoT or network devices. Additionally, witting or unwitting insiders can compromise IIoT systems by directly accessing the components. This direct access may result in unintentional actions through human performance errors, such as misconfiguration, improper testing, or improper procedure adherence, or it may result in deliberate, malicious actions by an adversary intent on causing harm or system malfunction.

Even if the other threat vectors are secured, compromises can still be introduced on IIoT systems through the supply chain. Hardware, firmware, software, and system information are all vulnerable to attack throughout the supply chain life cycle. Table 3 provides a taxonomy of supply chain cyberattack types. As many IIoT devices are ubiquitous and often designed without security as a priority, there are many opportunities for adversaries to compromise components throughout the global, complex supply chain network.

Table 3. Taxonomy of supply chain cyberattack types (Eggers and Rowland, Deconstructing the nuclear supply chain cyber-attack surface 2020).

Supply Chain Attack Type	Description
Theft of intellectual property (IP), design, or data	Unauthorized disclosure of information from a stakeholder who has a trust relationship with the end target, enabling future attacks and/or causing economic loss. This may include but is not limited to IP, design information, operational/configuration data, or stored secrets (i.e., private key, digital certificates).
Malicious substitution	Complete replacement of digital technology, including hardware, firmware, and/or software. Hardware clones or counterfeits may not impact all end users depending on the distribution, whereas a substituted software package may compromise all end users even if only a few were targeted.
Design, specification, or requirements alteration	Unauthorized modification of design, specifications, or requirements that compromises the design stages and results in the purposeful inclusion of latent design deficiencies (e.g., requirements that result in vulnerabilities) or built-in backdoors.
Development, build, or programming tool alteration	Unauthorized modification of the development environment, including platform, build, and programming tools, with the intent to corrupt the device under development.
Malicious insertion	Addition or modification of information, code, or functionality directly into a device to cause malicious intent, such as impairing or altering device operation or function.
Tampering and configuration manipulation	Unauthorized alteration or fabrication of configuration, non-executable data, or sending of unauthorized commands with the goal of impacting device operation or function.

Appendix A of this report includes examples that comprise one or most aspects of the aforementioned attack types.

- The SolarWinds incident provides a description of where a vulnerability discovered in a software supplier caused a large number of remote access attacks.
- The German Steel Mill Attack provides an example of unwitting insider threats posed from spear-phishing campaigns.

- The Casino Fish Tank Hack shows a vulnerability in a hardware vendor's software.
- The Oldsmar Water Treatment Facility details an attack on a SCADA system.
- The Miari Botnet attack describes consequences of unsecured systems.
- The Colonial Pipeline event describes a ransomware attack.

4.1.4 CONSEQUENCES

Consequence is often determined by evaluating the adverse impacts from a loss of confidentiality, integrity, or availability on the system. For example, a loss of confidentiality may result in a loss of sensitive information that can then be used by adversaries to design future attacks against an IIoT system. Specific to AI/ML IIoT algorithms, this loss of information could be the model design itself. A loss of integrity through modification of data, logic, or commands could impact the truthfulness of an IIoT system leading to improper operation or decision making. For instance, as shown in Figure 6, data poisoning or evasion attacks in AI/ML models or model tampering can lead to erroneous algorithm outputs or actions. And finally, a loss of availability (e.g., denial of service attack) may adversely affect IIoT operation by impacting data or communication flows.

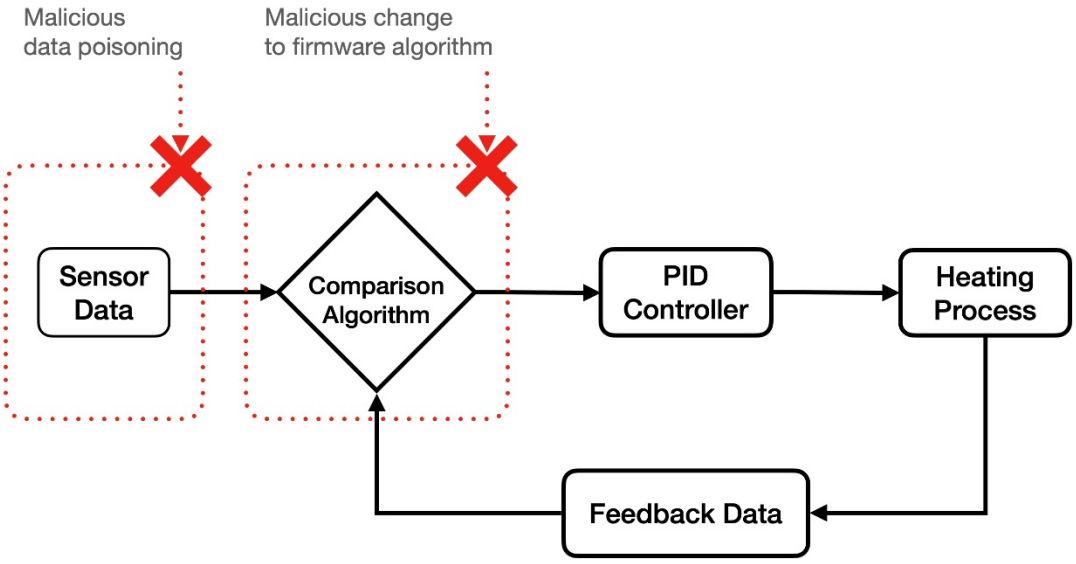


Figure 6. Example of AI/ML algorithm attacks

Often, the first step in cyber-risk analysis is identifying the top-level consequences of a cyber incident. At a nuclear facility, this might be determined by evaluating the facility's design basis accidents with potential for radiological release. The consequence or impact of a cyber incident on an IIoT system, however, is wholly dependent on the purpose of the application. For instance, a cyberattack on an isolated equipment condition monitoring system that uses various sensors or devices to monitor vibrations, temperatures, and other characteristics may have limited impact on critical facility functions, especially if the IIoT system does not directly interconnect with the equipment or ICS components. On the other hand, a cyberattack on an IIoT system for an NMAC system may enable theft or sabotage of nuclear or radiological material.

4.2 CYBER-INFORMED ENGINEERING THROUGHOUT THE SYSTEM'S ENGINEERING LIFE CYCLE

The Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response established the Cyber-Informed Engineering (CIE) national strategy in June 2022 (DOE Office of Cybersecurity 2022). CIE is a multidisciplinary approach that advocates the use of CIE principles throughout the system's engineering life cycle. This approach ensures that cyber considerations are included in every aspect of design, testing, implementation, operation, maintenance, and disposal or retirement (Anderson, et al. 2017) (Eggers and Anderson, Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control 2022). The five pillars of the National CIE Strategy are illustrated by Figure 7. The objective of the strategy is to enable the body of knowledge, the diverse and expanded workforce and the engineering and manufacturing capacity to apply CIE to today's energy infrastructure and to engineer future systems to eliminate or reduce the ability of a cyber-enabled attack to generate significant impact. (DOE Office of Cybersecurity 2022)

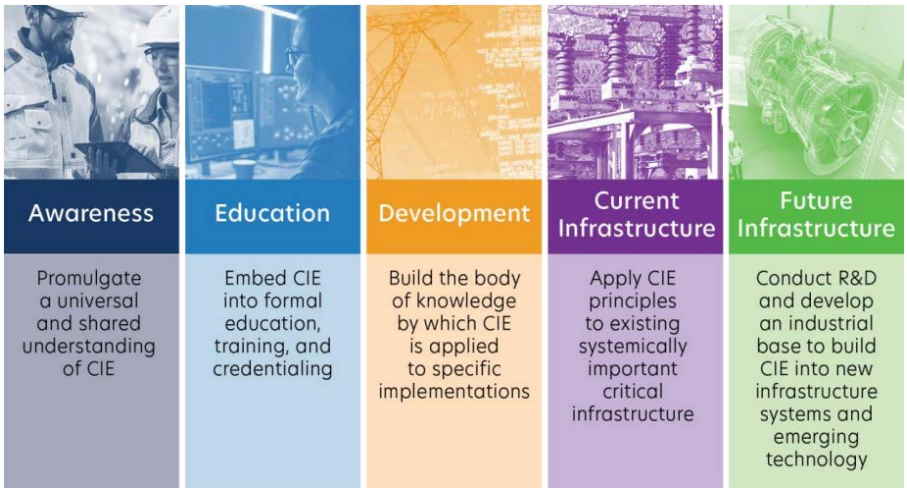


Figure 7. Strategic Pillars (DOE Office of Cybersecurity 2022)

4.2.1 CIE DESIGN PRINCIPLES

4.2.1.1 ENGINEERING RISK TREATMENT

Upon completion of a cyber-risk analysis for an IIoT application, the risks should be evaluated and prioritized based on the organization's risk tolerance. Similar to other risk management processes, the IIoT project team has several engineering risk treatment options for responding to the risk:

1. Eliminate the risk (e.g., alter the IIoT design to remove the risk)
2. Transfer the risk (e.g., transfer ownership of the IIoT application to another entity)
3. Mitigate the risk (e.g., design in security controls to reduce risk)
4. Accept the risk (e.g., make no design changes)

4.2.1.2 Secure Architecture

The principles of secure architecture, design simplification, resilient design, and active defense are elements of risk treatment. The goal of secure architecture in IIoT systems is to establish networks and architectures such that data flows are segregated and limited to trusted devices and other

subsystems or systems. This architecture must be carefully considered with IIoT applications because, while the ability to use wired, wireless, and hybrid communication pathways is a benefit of IIoT, it is also an increased risk.

4.2.1.3 DESIGN SIMPLIFICATION

The goal of design simplification is to reduce the complexity of the IIoT system, including components and architecture, while maintaining the intended function of the system. As mentioned, reducing the IIoT digital footprint reduces the overall cyberattack surface. Additionally, hardening IIoT components by eliminating, limiting, or disabling unnecessary features or capabilities will lessen opportunities for unintentional or malicious actions.

4.2.1.4 RESILIENT DESIGN

The goal of resilient design is to develop an IIoT system that can withstand external and internal disruptions. Depending on the criticality of the IIoT system, it may be necessary to add in separation, redundancy, diversity, and defense in depth to ensure the same failure (e.g., software common cause failure) or compromise (e.g., denial of service attack) does not cause the entire application to fail. Often there is tradeoff between design simplicity and resiliency.

4.2.1.5 ACTIVE DEFENSE

The goal of active defense is to build in capabilities, such as security information event monitoring and real-time anomaly detection and response tools, to preemptively prevent, detect, and respond to cyber incidents on IIoT systems. Active defenses can proactively defend against attacks originating from all four threat vectors (e.g., wired and wireless networks, portable media and maintenance devices, insiders, and supply chain).

4.2.2 CIE ORGANIZATIONAL PRINCIPLES

CIE organizational principles are intended to enable holistic integration of cybersecurity into other programs within organizations throughout the system's life cycle. There are two goals for the interdisciplinary principle: a multidisciplinary approach to ensure all stakeholders (e.g., engineering, maintenance, operations, emergency response) involved in an IIoT project understand the linkage between cybersecurity and other disciplines, and a systems and system of systems understanding of how a cyber incident may impact other interconnected IIoT functions.

4.2.2.1 Digital Asset Inventory

The goal of the digital asset inventory is to maintain a complete, accurate listing of all hardware, firmware, and software components used in an IIoT application, including make, model, version, configuration, and restoration instructions. This entire digital bill of materials is necessary to ensure adequate protections are in place. While this may be challenging for a geographically dispersed IIoT application, it is impossible to ensure security for unknown components. Additionally, as new threats and vulnerabilities arise, this listing provides a useful reference for continuous risk management.

4.2.2.2 SUPPLY CHAIN AND SYSTEM INFORMATION CONTROL

The goal of the supply chain and system information controls principle is to develop supply chain controls that prevent malicious or inadvertent compromise of hardware, firmware, software, and system information throughout the procurement and acquisition process. In most industries, there is a reliance on one or more outside suppliers. Depending on the IIoT application, this supply chain may

be very complex with multiple tiers of suppliers. As technology for nuclear and nuclear security-related IIoT applications may have more stringent requirements than other industries, it is imperative to maintain authenticity, integrity, confidentiality, and exclusivity throughout the life cycle (Eggers, The nuclear digital I&C system supply chain cyber-attack surface 2020). In addition to the cyber supply chain attacks listed in Table 3, there may be unknown or hidden insecure upstream software dependencies and unexpected vulnerabilities introduced while connecting various technologies.

Supply chain assurance focuses on eliminating these risks prior to purchasing and detecting anomalies during receiving activities. For nuclear ICS components, this often results in a formalized vetting process through adherence to recognized quality programs including ISO 9001 or Nuclear Quality Assurance (NQA-1), proof of historical performance, and site visits for technology demonstrations prior to signing procurement contracts. Unfortunately, standalone IIoT applications that are installed outside the nuclear sector may not have this same vetting requirement, especially when considering the potential for IIoT applications within the nuclear security regime as illustrated in Figure 1. In the case of COTS items from standard retailers, Internet searches and consulting vulnerability databases can be used to gauge vendor reputation prior to purchase.

While reviewing an IIoT device or system, flaws and compromises can occur with software, hardware, and firmware. Aside from design flaws, complete substitution of an integrated circuit via counterfeits or clones can occur as indicated in Table 3. Malicious insertion or tampering of hardware, while uncommon, is also possible. Often, hardware clones or counterfeits appear visibly correct and may initially operate correctly but begin to fail at a later date due to external factors, such as after prolonged operational periods or operation outside of room temperature. Software may exist at a high level on the network as data acquisition and interpretation from sensors or as an embedded operating system on the device itself. Often software includes several layers of dependencies and open-source libraries where one or more vulnerabilities may be found. Reviewing a supplier's history of involvement with, and attention to, vulnerability databases can indicate whether a potential software bug or flaw is likely to be found and remedied quickly. Additionally, similar to hardware, software and firmware is also susceptible to malicious substitution, malicious insertion, and tampering throughout the supply chain. In all cases, a compromise may be an advanced persistent threat that lies in wait until a specific trigger condition is met thereby launching the attack.

The nuclear ICS industry is a small market that often benefits from advancements in other markets, where system integrators will perform customizations necessary for nuclear sector requirements. This may include creating dashboards of multiple sensors specific to a task or developing algorithms that influence decisions requiring some knowledge of nuclear operations. System integrators may not necessarily be large contracting firms nor have a noticeable footprint in common vulnerability databases; thus, nuclear ICS products from integrators should stand for design and engineering reviews during development and maintain sufficient documentation of the design in case the integrator leaves the field. Quality standards, including ISO 9001 and NQA-1, have defined processes for new product development that specify design reviews and design documentation. Cybersecurity and IT professionals should attend these design reviews to provide relevant domain expertise as a quality check.

However, since IIoT applications in the nuclear security regime are so varied and generally may not be associated with critical nuclear reactor ICS functions, these quality standards may not apply. In all cases, procurement contracts should include cybersecurity requirements, such as those provided by the Department of Homeland Security, the Energy Sector Control Systems Working Group, or Electric Power Research Institute (Department of Homeland Security 2009) (Energy Sector Control Systems Working Group (ESCSWG) 2014) (EPRI 2018). CISA has also developed a vendor questionnaire template for ICT suppliers and a report on mitigating supply chain risks with qualified bidder and manufacturer lists (National Risk Management Center 2021) (CISA 2021). To the extent possible,

acquirers should also require the vendor to provide a complete software bill of material for the components and systems purchased.

4.2.2.3 Incident Response Planning

In conjunction with the digital asset inventory and resilient design principles, the goal for incident response planning is to ensure that there are adequate procedures, current backups, and accurate configurations for responding to and recovering from a deliberate or inadvertent cyber incident on the IIoT system. It is important to have a plan in place for each stage of the life cycle, as an incident or attack could occur at any time. For instance, what are the procedures or contingency plans if system information detailing the design of an NMAC IIoT system is stolen during the high-level design stage?

4.2.2.4 CYBERSECURITY CULTURE AND TRAINING

The final CIE principle is cybersecurity culture and training. The goal for this principle is to ensure that all stakeholders involved have the necessary cyber knowledge, skills, and abilities commensurate with their role in the IIoT project. The intent is not to develop everyone into cybersecurity specialists, but to develop cyber-informed engineers and personnel who are aware of the cyber implications and cross-functional dependencies within the IIoT project. Similar to a safety culture, organizations need to develop a cybersecurity culture to raise cyber awareness and help guard against cyber incidents that may reduce the overall security of the global nuclear security regime.

5. CONCLUSIONS

As advanced technologies expand throughout industries in the nuclear supply chain and society in general, it is inevitable that similar technologies similarly expand throughout the nuclear industries. Given the risks of nuclear security, a strong degree of conservatism exists for adoption of new technology where a slow and deliberate pace often lags other industries. In many instances, this aids in allowing time for private industry to reach maturity prior to deploying new technologies that may introduce unknown security holes. IIoT will follow this same route, where gradual adoption will enable less critical industries to uncover security issues.

This report provides several topical areas surrounding IIoT design and deployment from a nuclear security perspective. Several recently released policy documents from NIST, CISA, and other agencies show that the regulatory landscape is maturing rapidly, as are industry standards with the addition of PSA's and other manufacturer consortia's certifications. Multiple lessons learned provide high-level overviews of where attacks occurred in industrial settings, and what steps may have prevented these attacks.

Lastly, this paper provides one potential path of the design process for an IIoT system. Fundamentally, the process includes, but is not limited to, the following:

- Defining requirements
  - What does the system do?
  - What data does the system need?
  - What regulatory requirements exist?
- Design

  - What network architecture is appropriate?
  - How does one choose hardware that will be secure?
  - What software design aspects should be followed?
  - How do these algorithms interface with a user?
- Risk assessment
  - What is the consequence if the IIoT system or device is compromised?
  - What credible threats exist that need to be addressed?
  - How does one identify potential vulnerabilities?
- Lessons learned
  - What attack patterns need to be mitigated?
  - How might a contingency plan be established for an unforeseen event?

While each of the headings are important contributors to a successful and secure system, the concept of iterating during the design process is an underlying rule. Iteration of design prior to deployment allows a security team to assess detailed plans critically at all levels, revise, and improve the final product. This careful and deliberate design process is of high importance when weighing the risks of nuclear security.

APPENDIX A – CASE STUDIES

Even well designed systems may introduce vulnerabilities into industrial operations. Observing the case studies of comparable industrial systems may inform the future designs of systems deployed in nuclear security operations. This appendix includes several such cases with diverse attack methods that hobbled large systems and entire industries, where the methods employed by the attackers are not necessarily inventive, but were incredibly effective at the time. Lastly, this provides specific lessons learned to consider when contemplating new designs.

SOLARWINDS (U.S. GAO 2021)

Event: In September 2019, SolarWinds, a Texas network management company, was breached by a sophisticated and widespread hacking campaign. The attackers used trojanized malware that was hidden in the code of software updates for SolarWinds Orion that provided a backdoor into infected computers. The threat actors were able to exploit the networks and systems of SolarWinds customers that used the compromised software updates.

Impact: SolarWinds is widely used by the U.S. government to monitor activities in their federal networks. The incident allowed the threat actors to breach federal systems using the compromised system updates. SolarWinds has estimated that nearly 18,000 customers had downloaded the compromised software, although a small subset of the customers was specifically targeted for espionage.

Specifics: SolarWinds has more than 320,000 customers in 190 countries and provides large-scale infrastructure management software and services to businesses and government agencies. The threat actors conducted dry runs injecting code into the SolarWinds network management and monitoring suite of products. FireEye, a cybersecurity consulting firm, was the first to discover the breach in December 2020. The attackers used the malicious software that was embedded in updates for the management software and network platform to traverse their way through all compromised systems. Since February 2020 when the malware was deployed, the attackers moved within targeted systems, reading emails, and other documents. They were very good at covering their tracks and took extreme measures to remain undiscovered. Government agencies confirmed to have been affected by the malware include the Department of Commerce, Defense, Energy, Homeland Security, Justice, Labor, State, and Treasury, as well as the National Institutes of Health.

Lessons learned:

- Better manage supply chain risk
- Review the Cybersecurity and Infrastructure Security Agency (CISA) authorities and resources
- Increase sharing and analysis of threat intelligence between the public and private sectors
- Strengthen and establish international rules and norms in cyberspace
- Hold countries accountable for cyberattacks

GERMAN STEEL MILL ATTACK (DE MAIZIERE 2014)

Event: In December 2014, the German government's Federal Office for Information Security (BSI) described a malicious attack on an unnamed German steel mill in their annual findings report. Attackers used advanced social engineering and spear-phishing tactics to get into the mill's networks. According to the report, the attackers leveraged their extensive knowledge of industrial

control system (ICS) networks to disrupt multiple control systems and cause individual components to fail.

Impact: As systems and components began to fail, plant operators lost the ability to properly shut down a large blast furnace which resulted in massive damage to the furnace and other infrastructure. Although the attacker's identity and motivations are unclear, the BSI specifically mentioned that the attackers showed advanced technical capabilities in both classical information technology (IT) systems as well as in industrial controls systems and production processes. These factors have led some investigators to speculate that the attackers were possibly part of an advanced persistent threat group and that causing physical damage to the furnace may have been an unintended side effect—with espionage or sabotage possibly being the main motivation. This attack was noteworthy because, at the time it was reported, it was only the second confirmed cyberattack that resulted in physical damage to equipment following the Stuxnet incident in 2007.

Specifics: According to the BSI report, the attack began with a spear-phishing campaign that targeted industrial operators at the steel mill. The phishing emails likely looked legitimate and appeared to come from a trusted source (e.g., company employee, industrial supplier, etc.). It is also highly likely that these emails contained an attached document that contained some malicious code. When the operators opened the document, the malicious code would have triggered and targeted application vulnerabilities on the victim's system. Once an application vulnerability was discovered and exploited, the victim's system would have opened a remote connection point creating a path for the attackers to access to the corporate network.

Next the attackers would have likely worked to establish a foothold in the corporate network; scanned for valuable target devices, credentials, and unsecured systems; and searched for opportunities to move laterally to other networks. Although the BSI report did not give any specific details, it did indicate the attackers were able to leverage a trusted connection between the corporate network and the production network.

Once in the production network, the attackers compromised the industrial control systems and individual mill components. Eventually, the attackers discovered a way to control the shutdown sequence for one of the blast furnaces at the mill. These blast furnaces house molten steel at very high temperatures (>1500°C). The attackers overrode the shutdown sequence so operators could not shut it down and the consequence was terrible damage to the furnace and other mill infrastructure. Fortunately, no loss of life occurred.

Lessons learned:

- Thoroughly educate employees on phishing and other security risks, so they can detect attempts and identify suspicious emails/content
- Periodically test employees to determine the effectiveness of training
- Segment networks based on function and eliminate two-way communication between IT and operational technology (OT) networks
- Ensure critical computers do not have Internet access
- Implement tools that increase network visibility
- Keep operating systems and application software up to date

CASINO FISH TANK HACK (TOWNSEND 2017)

Event: In 2017, a North American casino was hacked through an Internet-connected fish tank. Once inside the casino's internal network, the attackers were able to locate a valuable database and exfiltrate a large volume of data.

Impact: The database information that was stolen may have included information about some of the casino's biggest spenders along with other private information. The integrity of the security of the casino was damaged due to this oversite that hackers were able to exploit.

Specifics: Sometime in 2017, a British cybersecurity company, Darktrace, installed their software on the network of a North American casino to conduct an assessment. The casino had recently added a high-tech fish tank as a new attraction in their lobby. The fish tank was equipped with an Internet-connected thermostat and advanced sensors that worked together to help the tank automatically regulate temperature, salinity, and feeding schedules. For security, the tank was configured to communicate its data via a Virtual Private Network (VPN) connection to the casino's corporate network.

However, the connected thermostat was also configured to send its data to a location in the cloud. Almost immediately after they installed their assessment software, Darktrace discovered anomalous data transfers from the connected fish tank to an unexpected external destination. The Internet Protocol address belonged to a cloud server located in Finland.

Since Darktrace's report on the incident did not contain many technical details, readers were left to speculate on things such as how the attackers were able to hack the wireless thermostat, the logical makeup of the casino's network, and the specific nature of the data that was stolen.

It is possible the attackers used default credentials or exploited a vulnerability found in common communication protocols used for audio and video to gain access to the thermometer. Then, they possibly watched for and stole VPN credentials to enter through the VPN and into the corporate network.

It is not definitively known how the attackers were able to gain access to the Internet-enabled tank, but once inside, the attackers were able to move freely throughout the network until they found a valuable target. Darktrace CEO, Nicole Eagan, recounted the attack at a subsequent conference and stated that the attackers were able to gain access to a database housing sensitive information on a number of the casino's most valuable and wealthy patrons or "high rollers."

The attackers then transferred the database data back across the network, out through the VPN and connected thermostat, and out to the cloud server in Finland. Darktrace determined, in total, that nearly 10GB of data was exfiltrated from the casino's network.

Lessons learned:

- VPNs can be an excellent security feature, but cannot protect against legitimate account use
- Proper network segmentation would have restricted the attackers' ability to move freely across the network
- Reduce attack surface by ensuring default credentials on all devices connected to the network have been updated
- Ensure the right people have the appropriate access to data and know exactly what assets are connected to the network

- Monitor network activity and respond to anomalous network activity in a timely manner

OLDSMAR WATER TREATMENT FACILITY (CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY 2021)

Event: In 2021, a hacker attempted to add a dangerous level of chemicals to the water treatment plant in Oldsmar, Florida. The event was detected when a plant operator at the Oldsmar Water Treatment Facility "noticed that someone remotely accessed the computer system that he was monitoring," which controls the chemicals at the plant.

Impact: According to Pinellas County Sheriff Bob Gualtieri, the unidentified hacker responsible had remotely accessed the system for three to five minutes, opening various functions on the screen. "One of the functions opened by the person hacking into the system was one that controls the amount of sodium hydroxide in the water. The hacker changed the sodium hydroxide from about 100 ppm to 11,100 ppm. This is obviously a significant and potentially dangerous increase."

"Did this come from down the street or outside the country? No idea."
Bob Gualtieri, Pinellas County Sheriff

Temporarily adjusting sodium hydroxide levels to dangerous amounts could have made the population sick had the chemicals been introduced into the water supply. While city officials caught the action and reversed it within minutes, further reporting has shown the plant had an austere cybersecurity profile that is sadly familiar for public-sector organizations—use of outdated operating systems, disregard for best practices, and lack of a budget to support any real upgrade or staff additions. Actors in the cybercriminal underground understand that profile fits thousands of enterprises around the world, which gives them rich targets to set their sights on.

Specifics: On Friday, February 5, 2021, an individual accessed a water treatment system in Oldsmar, Florida and increased the levels of sodium hydroxide to potentially dangerous levels. Oldsmar is 17 miles west of Tampa and has a population of 15,000 people. The individual gained access through the TeamViewer remote access software in use. This was not an advanced attack, and this is not a new or uncommon problem.

Since the early reports of this event, it has been publicly acknowledged that an operator machine had a remote access software package, TeamViewer, installed and accessible to the Internet. This led to manipulation of control set points for the dosing rate of sodium hydroxide (NaOH) into the water. NaOH is a chemical often used in drinking water treatment used to adjust pH and alkalinity. Although an important component of the drinking water treatment process, NaOH can be a hazardous chemical to water consumers if concentrations exist in excess of safe operating parameters.

Typically, water systems are engineered with many safeguards to keep parameters within acceptable limits, not the least of which is trained and licensed drinking water treatment operators. In this incident, the adversary raised the NaOH dose set point from its normal setting of 100 ppm to 11,100 ppm, thereby temporarily increasing the amount of chemical being added to the water. It was reported that the water treatment operator on duty observed the mouse moving on the operating screen, making changes, and then exiting the system. It was also reported that the operator identified the incident and restored the normal operating parameters fast enough so pH monitoring alarms did not detect a level beyond acceptable parameters.

Had the operator not observed the attacker actively manipulating the screen, it is possible that several other mechanisms in the water treatment plant control and monitoring system would have alerted plant staff to the condition. However, it is also entirely possible that this action could have resulted in people getting sick or potentially even death. The control systems in modern water treatment plants use process instrumentation that continuously monitor water quality parameters (e.g., pH) to carefully control the addition of chemicals and provide real-time alerts when those parameters go outside acceptable limits; these critical parameters are typically monitored at multiple points throughout the treatment process and in the transmission and distribution systems.

TeamViewer is a legitimate software package that is directly installed on a Windows host that allows for easy connectivity from anywhere. Its ease of use has allowed it to increasingly be used in industrial environments and, while legitimate software, may be unauthorized or rogue software.

Remote access to industrial facilities can be architected safely, but the best architecture can also be circumvented with unapproved software such as TeamViewer. This shows where visibility into what software, vulnerabilities, and behaviors is necessary in industrial environments.

Lessons learned:

- Be aware of any remote access software (such as TeamViewer) in the environment. These programs reduce the need for employees on site and streamline access, from anywhere in the world. Remote access software is also the most vulnerable to cybersecurity breaches.
- Mitigate potential security breaches through apps, using strong passwords, two factor authentication strategies and by whitelisting (i.e., only allowing authorized sites access to IT networks).
- Information technology and operational technology teams should evaluate the security of OT devices integrated with other data networks, including IT systems. Segmenting OT from IT may be the best solution.
- A best practice is to have a third party, dedicated Security Operations Center (SOC), continuously monitoring for any incidents. Just as important as cyber hardness is the ability to step in and mitigate the effects of breaches in real-time.

MIRAI BOTNET (CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY 2017)

Event: In 2016, a massive Distributed Denial of Service (DDoS) attack was launched against a DNS, Dyn, by using more than 100,000 infected IoT devices.

Impact: The Mirai Botnet DDoS attack reached up to 10 TBps during the attack. It brought down DNS services hosted by Dyn that manages major Internet services for Xbox, Netflix, Twitter, and many others in Europe and the U.S.

Specifics: In October 2016, a massive DDoS was launched against a major Internet service provider affecting e-commerce, access to multiple websites and services. The Mirai Botnet is a sophisticated malware that scanned the Internet to find vulnerabilities in many IoT devices (e.g., cameras, DVRs, routers) that were hijacked to flood Dyn systems with unwanted requests.

The botnet used an estimated 100,000 Internet connected devices that used default usernames and passwords easily found in an Internet search or the manufactures' websites. The traffic that was generated by the devices was up to 10TB worth of data per second, leading to the largest DDoS

attack to date. This attack has led researchers to believe that this type of DDoS attack is just the beginning of a more widespread problem.

The low cost and low hygiene of IoT devices on the Internet can lead to unforeseen consequences to other organizations and other Internet services needed for healthcare and major critical infrastructure need for the world (e.g., oil and gas, power, water). IoT devices that manage the very nature of how we live can have dire consequences in the future if basic security measures are not realized.

In a coordinated effort, government agencies are addressing the need for stricter security applications for newly developed IoT devices. This include guidelines drafted by NIST in NISTR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers, and additional European standards from the European Union Agency for Cybersecurity Baseline Security Recommendations for IoT.

Lessons learned:

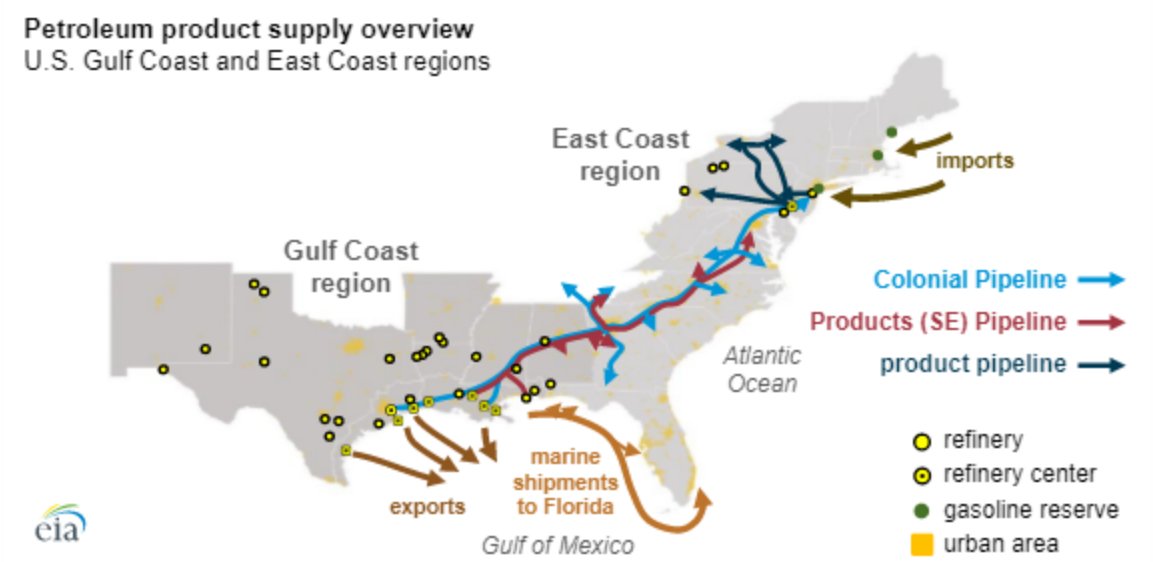
- Change default passwords and usernames of connected devices
- Disable Universal Plug-and-Play
- Disable remote management through telnet
- Check for software updates and patches
- Proper network segmentation would have restricted the attackers' ability to move freely

COLONIAL PIPELINE

Event: In 2021, a ransomware attack was launched against Colonial Pipeline business systems by DarkSide affecting more than 5,500 miles of petroleum pipelines.

Impact: Immediately following the attack, Colonial Pipeline initiated a remediation response to contain the ransomware affects which resulted in the shutdown of all 5,500 miles of pipeline for the transportation of fuels for the East Coast. This shutdown affected the entire length of the pipeline from the refineries in Houston, Texas up to Linden, New Jersey which affected 45% of the fuel used on the East Coast (U.S. Department of State 2021) (U.S. Energy Information Administration 2021). The loss of this supply chain required the sector to rely on alternative sources of fuel to include imports from the global market using deep water ports in the southeast U.S. and a smaller pipeline that carries petroleum products from the U.S. Gulf Coast to Washington, D.C (U.S. Energy Information Administration 2021).

The depth of this loss can be visually appreciated with the petroleum product supply overview (U.S. Department of State 2021). Both upstream and downstream supply chain components were affected by this cyberattack, including refineries across the south and product pipelines in the northeast.



Note: Map updated to reflect changes in U.S. refineries since initial report.

Figure A-1. Petroleum product supply overview (Cybersecurity and Infrastructure Security Agency 2021)

In addition to the physical restrictions of petroleum products, the long-term effects of this attack resulted in numerous federal and regulatory updates to mitigate future attacks to our critical infrastructure, including the Biden administration's EO 14028, Improving the Nation's Cybersecurity, and the request of lawmakers to enact a threat-hunting program on vendors' networks (Maggie Smith and Jonathon Monken 2021) (The White House 2021).

Specifics: On May 7, 2021, Colonial Pipeline's corporate information systems were affected by a ransomware attack initiated by the cyber group DarkSide. In this event, DarkSide was able to enter Colonial's network through a legacy VPN profile that was not "intended to be in use" (Joseph Blount 2021). DarkSide then initiated the ransomware attack which encrypted critical information affecting the corporate business and accounting systems on the information technology networks and held the systems hostage until a ransom was paid (Maggie Smith and Jonathon Monken 2021).

Figure A-2 demonstrates two entry points for a cyberattack. In the Colonial Pipeline case, DarkSide entered through a VPN connected to the business systems, as defined on the top right-hand side of the diagram. To contain the effect of the attack, the OT systems that control and safely oversee the delivery of petroleum products across the company's 5,500-mile pipeline, were shut down by the company (U.S. Energy Information Administration 2021).

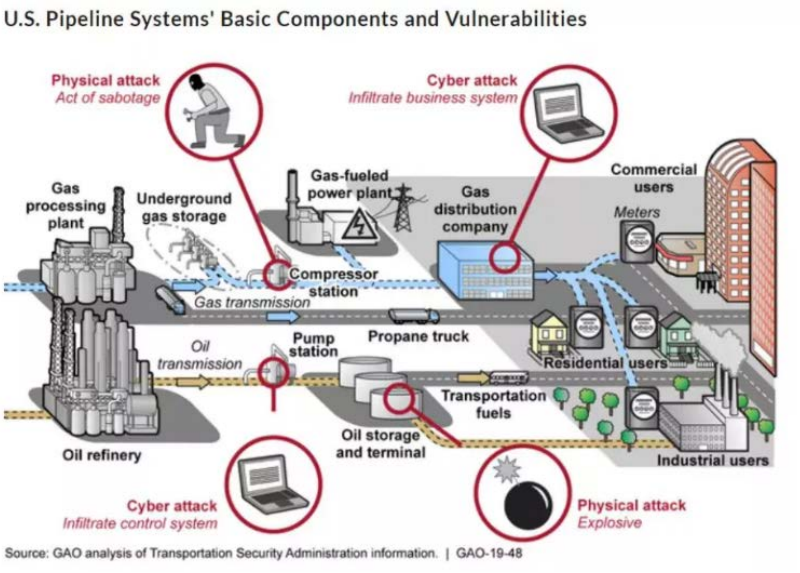


Figure A-2. U.S. Pipeline Systems Basic Components and Vulnerabilities (U.S. Government Accountabilty Office Watchblog 2021)

On the night of the attack, May 7, 2021, Colonial Pipeline chose to pay 75 bitcoins which equated to an approximately $4.3M ransom to release their systems. DarkSide responded the following day with an encryption tool that "helped to some degree." However, it took five days for Colonial to resume pipeline operations with assistance of consultants to assess the damage and improve cybersecurity (Joseph Blount 2021). Following the attack, the Department of Justice (DOJ) formed the Ransomware and Digital Extortion Task Force which seized only 63 of the 75 bitcoins paid to DarkSide by Colonial Pipeline (The Honorable Joe R. Reeder 2021).

In addition to the actions by Colonial Pipeline and the DOJ, the Biden and State administrations enacted a series of waivers to boost the availability of supply; however, it was reported that the population reacted with panic and social disruption as they experienced the adverse effects of a limited fuel supply (The Honorable Joe R. Reeder 2021). In addition to the social aspects of a devastating cyberattack, this attack demonstrates the cyber risks of converging IIoT systems and the business systems that integrate with them (U.S. Department of State 2021) (U.S. Energy Information Administration 2021).

LOG4SHELL

Event: A critical zero-day security flaw was noted in the National Vulnerability Database on December 10, 2021, for the open-source Log4J library used within Apache Software Foundation's library Java software. This flaw allows a remote attacker to use code within Log4J to execute arbitrary code or perform denial of service attacks on targeted servers (National Institute of Standards and Technology 2021).

Impact: Java and its library, Log4J, is used extensively across the world both for online and local software solutions. It is a common component, and this vulnerability is relatively easy to exploit (National Cyber Security Centre 2021). The extensive nature of this vulnerability puts untold systems at risk across all critical infrastructure sectors and across the world. Documentation of the software and systems affected by this vulnerability is maintained on the CISA GitHub repository and is crowd sourced (CISA 2021).

Specifics: Software development incorporates numerous sources of code, one of which includes the Apache Software Foundation's Log4J library which manages the collection and storage of records or activity during software use. The Apache software is publicly accessible, and it is maintained by many volunteers who maintain and update the libraries including Log4J. The vulnerabilities for Log4J include Log4JShell among others and are documented on the CISA webpage for Mitigating Log4Shell and Other Log4j-Related Vulnerabilities (CISA 2021).

Since this vulnerability is so pervasive and so easily used in an attack, the federal government has applied numerous significant efforts to encourage organizations to mitigate this vulnerability. They include warnings from CISA to organizations across the globe, as well as across multiple critical infrastructures sectors, and from the U.S. Food and Drug Administration which has sent out warnings to medical device manufactures (CISA 2021) (U.S. Food and Drug Administration 2022). In addition, the Federal Trade Commission (FTC) is reminding companies and their venders to take reasonable steps to mitigate this vulnerability to avoid legal actions by the FTC and the Gramm Leach Bliley Act (Federal Trade Commission 2022).

APPENDIX B –REFERENCES

6. WORKS CITED

1NCE. n.d. *Overview of cellular mobile network standards.* 1NCE. Accessed January 12, 2022. https://1nce.com/en/blog/cellular-mobile-standards/.

Alliance, LoRaWAN. n.d. "What is LoRaWAN Specification." *LoRa Alliance.* Accessed January 21, 2022. https://lora-alliance.org/about-lorawan/.

Aloxy.io. 2022. *Aloxy End-to-End Industrial IoT Solutions.* January 22. https://www.aloxy.io.

Anderson, R S, J Benjamin, V L Wright, L Quinones, and J Paz. 2017. *Cyber-Informed Engineering.* Idaho Falls: Idaho National Laboratory.

Biden, President Joseph. 2021. "Executive Order 14028: Improving the Nation's Cybersecurity." Washington, DC: Federal Register, May 17. https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

CDSE. 2019. *The C2 Consensus on IoT Device Security Baseline Capabilities.* Council to Secure the Digital Economy. https://securingdigitaleconomy.org/projects/c2- consensus/.

Certification, Pearson IT. 2009. "Pearson IT Certification." *802.11 Wireless Standards.* June 9. Accessed January 21, 2022. https://www.pearsonitcertification.com/articles/article.aspx?p=1329709&seqNum=4.

CISA. 202. *cisagov/log4j-affected-db.* Accessed 2022. https://github.com/cisagov/log4j-affected-db.

—. 2021. "Cybersecurity & Infrastructure Security Agency." April. https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf.

—. n.d. *ICS-CERT Alerts.* Cybersecurity & Infrastructure Security Agency. Accessed September 29, 2020. https://us-cert.cisa.gov/ics/alerts.

CISA. 2020. *Internet of Things Security Acquisition Guidance: Information Technology Sector.* Washington, DC: CISA. https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_0.pdf.

CISA. 2021. "Mitigating Log4Shell and Other Log4j-Related." Washington D.C. https://www.cisa.gov/uscert/sites/default/files/publications/AA21-356A_Joint_CSA_Mitigating_Log4Shell_and_Other_Log4j-Related_Vulnerabilities.pdf.

—. 2021. *Mitigating Log4Shell and Other Log4j-Related Vulnerabilities.* December 21. Accessed 2022. https://www.cisa.gov/uscert/ncas/alerts/aa21-356a.

n.d. *Connectivity Standards Alliance.* Connectivity Standards Alliance. Accessed January 21, 2022. https://csa-iot.org/.

Cybersecurity and Infrastructure Security Agency. 2021. *National Cyber Awareness System.* CISA. February 12. https://www.cisa.gov/uscert/ncas/alerts/aa21-042a.

—. 2017. *National Cyber Awareness System.* CISA. October 17. https://www.cisa.gov/uscert/ncas/alerts/TA16-288A.

de Maiziere, T. 2014. "The State of IT Security in Germany 2014." https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3.

Department of Homeland Security. 2009. *Department of Homeland Security: Cyber Security Procurement Lanugage for Control Systems.* Washington, DC: DHS.

Di Marco, Piergiuseppe, Per Skillermark, Anna Larmo, and Pontus Arvidson. 2017. "Bluetooth mesh networking." Ericsson AB.

DOE Office of Cybersecurity, Energy Security, and Emergency Response. 2022. *Cyber-Informed Engineering (CIE).* June 15. https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document.

Eggers, S. 2020. "The nuclear digital I&C system supply chain cyber-attack surface." *Transactions of the American Nuclear Society.* Virtual.

Eggers, S, and M Rowland. 2020. "Deconstructing the nuclear supply chain cyber-attack surface." *Proceedings of the INMM 61st Annual Meeting.* Virtual.

Eggers, S, and R Anderson. 2022. "Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control." In *Nuclear Reactors*. London, UK: IntechOpen.

Energy Sector Control Systems Working Group (ESCSWG). 2014. *Cybersecurity Procurement Language for Energy Delivery Systems.* Washington, DC: DOE.

EPRI. 2018. *Cyber Security in the Supply Chain: Cyber Security Procurement Methodology, Red. 2.* Electric Power Research Institute.

Fagan, Michael, Jeffrey Marron, Kevin G Brady, Barbara B Cuthill, Katerina N Megaas, Rebecca Herold, David Lemire, and Brad Hoehn. 2021. *SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements.* Gaithersburg: NIST. doi:https://doi.org/10.6028/NIST.SP.800-213.

Fagan, Michael, Katerina N Megas, Karen Scarfone, and Matthew Smith. 2020. *NISTIR 8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers.* Gaithersburg: NIST. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

Federal Trade Commission. 2022. *FTC warns companies to remediate Log4j security vulnerability.* January 4. Accessed March 2022. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability.

FIRST. n.d. *Common Vulnerability Scoring System (CVSS).* Forum of Incident Response and Security Teams. Accessed September 29, 2020. https://www.first.org/cvss/.

Forum, USB Industry. n.d. *Document Library.* Accessed January 21, 2022. https://usb.org/documents.

Franklin, Curtis. 2019. *The Edge - Glitching: The Hardware Attack That Can Disript Secure Software.* Dark Reading. October 18. Accessed January 21, 2022. https://www.darkreading.com/edge-articles/glitching-the-hardware-attack-that-can-disrupt-secure-software.

General Services Administration. 2021. *GSA Smart Buildings.* U.S. General Services Administration. December 16. https://www.gsa.gov/directive/gsa-smart-buildings.

Government Accountability Office. 2020. *Internet of Things: Information on Use by Federal Agencies (GAO-20-577).* Washington, DC: Government Accountability Office. https://www.gao.gov/assets/gao-20-577.pdf.

Heckman, Jory. 2019. *Federal News Network.* September 9. https://federalnewsnetwork.com/technology-main/2019/09/state-dept-using-iot-sensors-for-more-resilient-embassies/.

Hunt, Galen, George Letey, and Edmund B Nightengale. 2020. *The Seven Properties of Highly Secured Devices (2ed).* Seattle: Microsoft. https://www.microsoft.com/en-us/research/uploads/prod/2020/11/Seven-Properties-of-Highly-Secured-Devices-2nd-Edition-R1.pdf.

IFM Electronic GmbH. 2020. *On the safe side: capacitive IIoT sensors for hazardous dust areas.* Accessed January 21, 2022. https://www.ifm.com/de/en/shared/product-news/2020/sps/capacitive-iiot-sensors-for-hazardous-dust-areas.

Integrated, Maxim. 2001. "APP 763: Guidelines for Proper Wiring of an RS-485 (TIA/EIA-485-A) Network." November 19. https://pdfserv.maximintegrated.com/en/an/Guidelines_Proper_Wiring_Rs485_Network.pdf .

n.d. *IoT Security.* Silicon Labs. Accessed January 21, 2022. https://www.silabs.com/security.

IRDAJP. n.d. *Multi-Gigabit Communications Using Infrared Technology.* Accessed March 31, 2022. https://www.irdajp.org/gigair.

ITL. n.d. *Computer Security Resource Center.* NIST. Accessed February 27, 2022. https://csrc.nist.gov/glossary/term/operational_technology.

Joseph Blount. 2021. "President and Chief Executive Officer of Colonial Pipeline Company." *Hearing Before the United States Senate Committe on Homeland Security & Governmental Affairs.* Washington D.C. https://www.hsgac.senate.

Kaplan, S., and B. J. Garrick. 1981. "On the Quantitative Definition of Risk." *Risk Analysis* 1 (1): 11-27. https://www.nrc.gov/docs/ML1216/ML12167A133.pdf.

LiFi. n.d. *What is LiFi? .* LiFi.co. Accessed March 31, 2022. https://lifi.co/what-is-lifi/.

LoRa Alliance. 2021. *A Digital Revolution for Oil and Gas from SCADA to Industrial IOT.* LoRa Alliance. https://lora-alliance.org/wp-content/uploads/2021/04/FINAL_A-DIGITAL-REVOLUTION-FOR-OIL-GAS-FROM-SCADA-TO-INDUSTRIAL-IOT.pdf.

Maggie Smith and Jonathon Monken. 2021. "The Colonial Pipeline hack shows we need a better Federal cybersecurity ecosystem." *Modern War Institite at West Point*, 06 01. https://mwi.usma.edu/the-colonial-pipeline-hack-shows-we-need-a-better-federal-cybersecurity-ecosystem/.

Maxim Integrated. 2001. "Fundamentals of RS-232 Serial Communications." March 29.

Microsemi. 2011. *Understanding 802.3at: PoE Plus Standard Increases Available Power.* Irvine: Microsemi. https://www.microsemi.com/documents/powerdsine/whitepapers/Understanding_802_3at_PowerDsine.pdf.

MITRE. n.d. *Common Vulnerabilities and Exposures (CVE).* The MITRE Corporation. Accessed September 29, 2020. https://cve.mitre.org.

—. n.d. *Common Weakness Enumeration (CWE).* The MITRE Corporation. Accessed September 29, 2020. https://cwe.mitre.org.

National Cyber Security Centre. 2021. *Log4j vulnerability - what everyone needs to know.* December 14. Accessed 2022. https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know.

National Institute of Standards and Technology. 2021. *National Vulnerabilty Database .* December 21. Accessed March 2022. https://nvd.nist.gov/vuln/detail/CVE-2021-44228.

National Risk Management Center. 2021. "Cybersecurity & Infrastructure Security Agency." April. https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Vendor-SCRM-Template_508.pdf.

New, Joshua. 2016. *Comments to the NTIA on the Benefits, Challenges, and Potential Roles for Government in Fostering Advancement of the Internet of Things*, June 16, 2016, https://datainnovation.org

Pramberger, Roman. 2022. *Physical Layer.* January 19. https://osi-model.com/physical-layer/.

PSA Certified. n.d. *Our Approach to IoT Security.* Platform Security Architecture. Accessed January 20, 2022. https://www.psacertified.org/what-is-psa-certified/our-approach/.

Quast, Christina. 2018 . "Common attacks on IoT devices." Edinburgh. https://elinux.org/images/f/f8/Common-Attacks-on-IoT-Devices-Christina-Quast.pdf.

Ross, Ron, Victoria Pillitteri, Kelley Dempsey, Mark Riddle, and Gary Guissanie. 2021. *SP 800-171 rev2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* Gaithersberg: NIST. doi:https://doi.org/10.6028/NIST.SP.800-171r2.

Satell, Greg. 2019. *Harvard Business Review.* December 10. https://hbr.org/2019/12/why-move-fast-and-break-things-doesnt-work-anymore.

Texas Instruments. 2016. *Introduction to the Controller Area Network (CAN).* Texas Instruments. https://www.ti.com/lit/an/sloa101b/sloa101b.pdf.

The Honorable Joe R. Reeder, Cadet Tommy Hall. 2021. "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack." *The Cyberdefense Review West Point* (Army Cyber Institute West Point) 6 (3): 15-39. https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf?ver=6qlw1l02DXt1A_1n5KrL4g%3D%3D.

The White House. 2021. *Executive Order 14028, Improving the Nation's Cybersecurity.* May 12. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Townsend, K. 2017. *Security Week.* July 26. https://www.securityweek.com/hacked-smart-fish-tank-exfiltrated-data-rare-external-destination.

U.S. Department of State. 2021. *Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice.* November 4. Accessed 2022. https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/.

U.S. Energy Information Administration. 2021. *Cyberattack halts fuel movement on Colonial petroleum pipeline.* May 11. Accessed 3 2022. https://www.eia.gov/todayinenergy/detail.php?id=47917.

U.S. Food and Drug Administration. 2022. *Cybersecurity Alert: Vulnerabilities identified in medical device software components: PTC Axeda agent and Axeda Desktop Server.* March 8. Accessed 03 2022. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

U.S. GAO. 2021. *WatchBlog: SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic).* U.S. Government Accountability Office. April 22. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

U.S. Government Accountabilty Office Watchblog. 2021. *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic).* May 18. Accessed March 2022. https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic.

Wojciechowicz, T. 2018. "ZigBee vs Z-Wave: What's the Difference? Everything You Need To Know." *Symmetry Electronics.* November 18. Accessed January 21, 2022. https://www.symmetryelectronics.com/blog/zigbee-vs-z-wave-what-s-the-difference-everything-you-need-to-know-symmetry-blog/.