PROJECT DESCRIPTION

SECURITY FOR IOT SENSOR NETWORKS

Building Management Systems Case Study

Jeffrey Cichonski
Jeffrey Marron
Nelson Hastings

National Institute of Standards and Technology

Jason Ajmo
Rahmira Rufus

The MITRE Corporation

DRAFT

February 2019

sensor-security-nccoe@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology. To learn more about the NCCoE, visit http://www.nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a Community of Interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

ABSTRACT

This document explores common components of sensor networks and the associated requirements for the secure functioning of the sensor network. For each component, the document lists exposed interfaces, applicable threats, and technologies that may be utilized to help ensure the security requirements. A mapping to relevant Categories and Subcategories of the Cybersecurity Framework is also included. Additionally, the document considers various scenarios applying the components of a sensor network and associated security requirements to a building management system.

KEYWORDS

building management sensors; data integrity; device integrity; internet of things; IoT; networked sensors; sensors; sensor data; sensor security

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

All registered trademarks or trademarks belong to their respective organizations.

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://www.nccoe.nist.gov.

Comments on this publication may be submitted to: sensor-security-nccoe@nist.gov

Public comment period: February 1, 2019 to March 18, 2019

TABLE OF CONTENTS

1 Executive Summary..1
Purpose 1
Scope.. 2
Assumptions/Challenges.. 2
Background 2
2 High-Level Architecture...4
Component List 4
Temperature, Humidity, and Motion Sensors 5
Base Station/Aggregator.. 5
Controller 6
Communications Channels 7
Security Requirements.. 8
3 Scenarios 9
Scenario 1: Integrity of Sensor Data 9
Scenario 2: Unauthorized Sensor.. 10
Scenario 3: Wireless Sensor Communications Channel Security.................. 11
Scenario 4: Latency Considerations in Sensor Networks.............................. 12
Scenario 5: Security Considerations of Sensor Network Aggregators 12
Scenario 6: Trustworthiness of Sensor Components – Microcontrollers and Firmware........ 13
Scenario 7: Sensor Network Data Leakage 14
Scenario 8: Secure Update of Devices 14
4 Relevant Standards and Guidance 15
5 Security Control Map 17
Appendix A References...24
Appendix B Acronyms and Abbreviations...25

1 Executive Summary

Purpose

At their essence, sensor networks monitor the physical characteristics of an environment and translate those physical readings to electrical impulses. Sensor networks commonly measure characteristics such as temperature, pollution, electrical usage, or a patient's vital signs, among others. In many cases, the network is designed to not only sense the environment but also act on the physical environment based on the sensed data. Logic may be programmed into controllers to make a physical change to the environment based on the sensed data. For example, a smart building management system might be programmed to open air vents when the outdoor temperature drops below a certain temperature or to stop all air pulled into the facility when the humidity reaches a predetermined threshold.

Sensor networks are integral parts of many modern industries and critical infrastructure, including the electric grid, healthcare, environmental protection, and manufacturing. For example, in the electric grid, sensor networks may monitor and control the power generation of distributed resources, such as photoelectric systems (solar cells) owned by consumers. Sensor networks are also increasingly used in implanted medical devices, which monitor a patient's applicable health conditions. The implanted device may make changes to the patient's dosage of medicine based on the blood chemistry reported by a sensor network. Sensor networks may also monitor the properties of critical water supplies, measuring for the presence of minerals or toxins. In many of these use cases, the accuracy, integrity, and availability of the data being reported and monitored by a sensor network can be safety critical.

This document explores common components of sensor networks and the associated requirements for the secure functioning of the sensor network. For each component, this document lists exposed interfaces, applicable threats, and technologies that may be utilized to help ensure the security requirements. A mapping to relevant Categories and Subcategories of the Cybersecurity Framework is also included. Additionally, this document considers various scenarios applying the components of a sensor network and the associated security requirements to a building management system. These sensor network scenarios, although written for a building management system, may be applicable to multiple industry sectors and are listed for consideration for inclusion as future National Cybersecurity Center of Excellence (NCCoE) use cases.

These are the goals and objectives of the project:

- Understand the cybersecurity considerations (including the threats, threat vectors, vulnerabilities, risks, and organizational considerations for those risks) for a building management system sensor network, specifically
- Serve as a building block for sensor networks in general, future Internet of Things (IoT) projects, or specific sensor network use cases
- Establish a security architecture to protect a building management system sensor network by using standards and best practices, including the communications channel/network used to transmit sensor data to the back-end building control systems (hosts) for processing

- Explore the cybersecurity controls to promote the reliability, integrity, and availability of building management system sensor networks
- Exercise/test the cybersecurity controls of the building management system sensor network to verify that they mitigate the identified cybersecurity concerns/risks, and understand the performance implications of adding these controls to the building management system sensor network

Scope

This section details the scope of the project:

- Explore the components of a sensor network and their associated cybersecurity considerations
- Collaborate with NCCoE partners to integrate commercial off-the-shelf (COTS) cybersecurity solutions to mitigate sensor network risks

Detailed explorations of other considerations (e.g., physical access to the sensor network components), while important, are outside the scope of this project.

Assumptions/Challenges

This document focuses on the functional security requirements associated with sensor networks and their components. Additionally, the security issues arising within sensor networks are explored.

Many general network security practices are outside the scope of this effort but may be essential for the security of building management system sensor networks. For reference, these network security practices should be reviewed for your unique needs and may include the following practices:

- network perimeter protection (e.g., intrusion prevention system (IPS), firewall)
- network policy violation detection (e.g., intrusion detection system (IDS), sniffer)
- logging (e.g., event activity, system, procedural, respond/recovery) and log processing/analysis
- incident recording/reporting
- response procedures during/after incident
- incident containment/mitigation procedures
- optimization scheme (system/process improvements from incident)
- recovery procedures during/after incident
- optimization scheme execution/implementation procedure

In general, network security best practices adhere to guidance from National Institute of Standards and Technology (NIST) Special Publications (SPs) applying the principles and practices to securing information technology (IT) systems.

Background

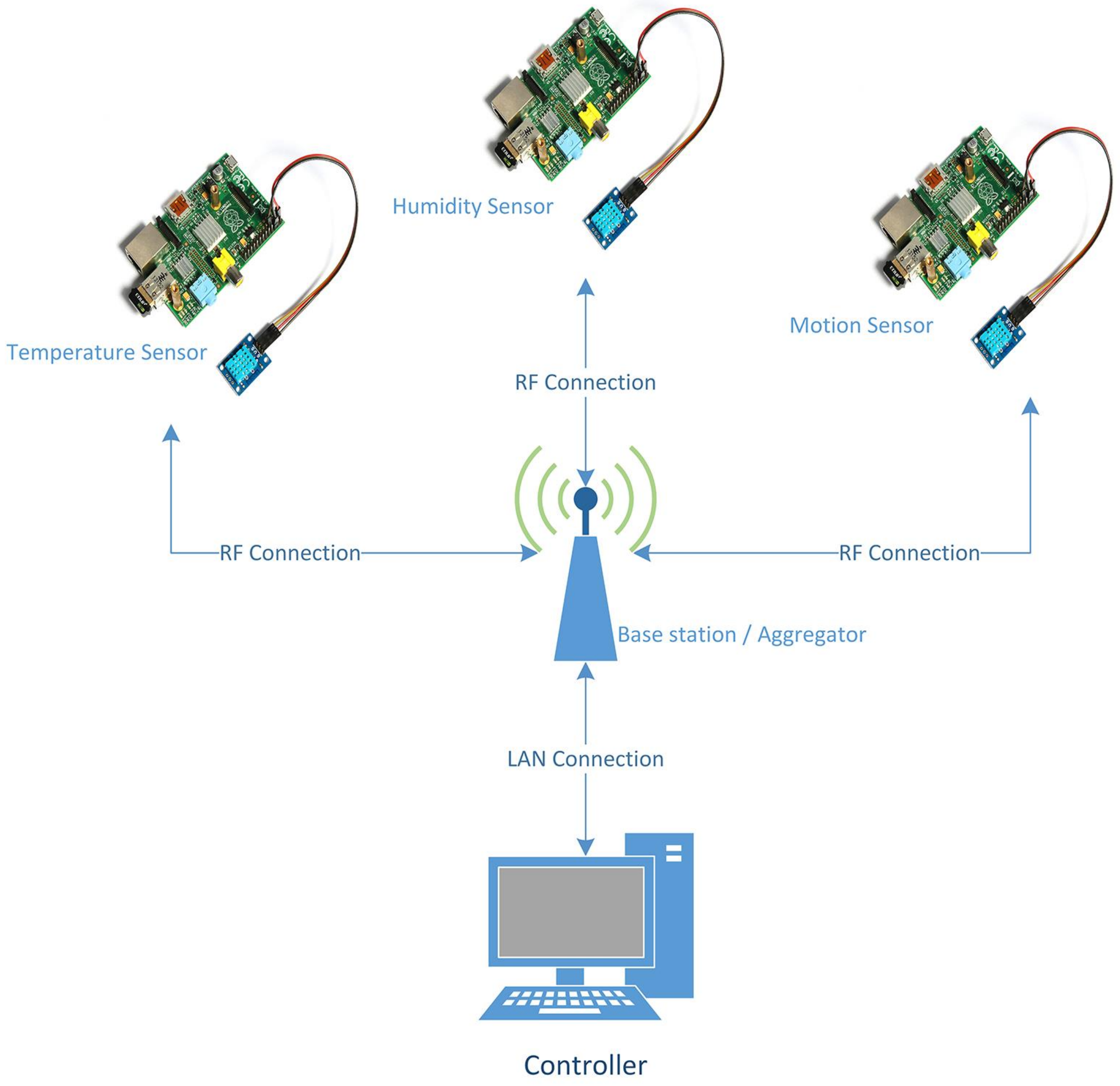
The wireless sensor network market was valued at $573 million in 2016 and is projected to increase to at least $1.2 billion by 2023, growing at a compound annual growth rate of 11% from 2017 to 2023 [1]. The growth of this sector is being propelled by the development of cheaper, smaller sensors; an expanding market for smart and wearable devices; an increased need for real-time applications; and a surge in demand for IoT sensors for various applications, such as measurement, recognition, and interpretation.

The increased use of IoT sensor data for decision-making, process control, and other functions within an organization has increased the potential impact of confidentiality, integrity, and availability threats. Examples of security issues include ensuring that sensor data is accessible only to authorized parties, that the sensor network is available during an attack, and that sensor data is not altered in transit.

The nature of sensor networks presents unique risks and challenges to the components, such as the ease of physical access, limited processing power, and limited ability for security monitoring and maintenance. Detecting and preventing these attacks has historically been a problem, primarily due to very limited processing power on the components.

2 HIGH-LEVEL ARCHITECTURE

Figure 1: Example Sensor Network Architecture



Component List

This project description utilizes a simplified sensor network to explore the cybersecurity considerations of a building management system. In the following subsections, each component of the sensor network is described, organized by the following topic areas:

- exposed interfaces
- possible attack vectors
- security requirements/outcomes of the component to ensure the secure operation of the sensor network
- specific technologies that can help achieve the security requirements/outcomes
- mappings to relevant Subcategory outcomes of the Cybersecurity Framework

Temperature, Humidity, and Motion Sensors

The sensors in this project will be composed of a computing device (e.g., microcontroller) with an attached sensor (e.g., thermocouple). These sensors will be able to interface with the base station by using a radio frequency (RF) connection. The configuration for these sensors will be managed through a wired connection.

- Interfaces:
    - RF interface to the base station used for the communication of sensor data, device health, and over-the-air management
    - physical connection to the sensor used for out-of-band management and configuration
- Possible attack vectors:
    - The sensor is physically manipulated (e.g., mirror in front of a motion sensor)
    - The sensor is spoofed, and fraudulent information is transmitted
    - The sensor RF communications channel is jammed or intercepted by a man-in-the-middle attack
- Security requirements/outcomes:
    - The integrity of sensor data can be verified
    - The integrity of the sensor firmware and configuration can be verified
    - The identity of the physical sensor can be verified
- Specific technologies:
    - A root of trust is utilized to ensure the integrity of the sensors' firmware and configuration
    - Public/private key pairs (or pre-shared keys) are utilized to verify the identity of sensor network components
    - Security features on the RF technologies are enabled and configured
    - Physical security is addressed
- Cybersecurity Framework Subcategory mappings:
    - PR.AC-1
    - PR.AC-4
    - PR.AC-7
    - PR.DS-6
    - PR.DS-8
    - PR.IP-3
    - PR.PT-4

Base Station/Aggregator

The base station will be a wireless radio configured to receive and aggregate signals from the sensors. The base station will forward signals to the controller for processing. Similarly, the base station may receive command and control information from the controller to send to the appropriate sensor.

- Interfaces:
    - RF interface to the sensors used for the reception of sensor data, sensor health, and over-the-air management
    - physical connection to the controller used for management and configuration
- Possible attack vectors:
    - modification of received sensor data
    - modification of the algorithms used by the aggregator to combine and weigh data received from the sensors
    - modification of the base station firmware and configuration via a serial connection from the controller
    - controller transmitting malicious command and control information to the sensors and base station/aggregator
- Security requirements/outcomes:
    - The integrity of received sensor data can be verified.
    - The integrity of the base station firmware and configuration can be verified.
    - The identity of the base station can be verified.
    - The integrity of the algorithms used to aggregate sensor data can be verified.
    - Authentication to the aggregator from the controller can be enforced.
    - The authentication of sensors can be enforced.
- Specific technologies:
    - Hashing algorithms are utilized to ensure the integrity of sensor data and algorithms.
    - A root of trust is utilized to ensure the integrity of the components' firmware and configuration.
    - Public/private key pairs (or pre-shared keys) are utilized to verify the identity of sensor network components.
    - Authentication protocols are utilized to enforce access rights to the base station.
- Cybersecurity Framework Subcategory mappings:
    - PR.AC-1
    - PR.AC-4
    - PR.AC-7
    - PR.DS-6
    - PR.DS-8
    - PR.IP-3
    - PR.PT-4

Controller

The controller will be software installed on a connected computer to receive and process sensor data and to provide command and control information to the sensors. Alternatively, a Raspberry Pi or a BeagleBone Black could function as the controller.

- Interfaces:
  - graphical user interface of controller software via the local system
  - physical connection to the base station for reception of aggregated data and for transmission of control signals to the sensors and the base station
- Possible attack vectors:
  - modification of controller software
  - modification of controller's kernel and/or configuration settings
  - access controller software via the compromised base station
- Security requirements/outcomes:
  - The integrity of the controller's kernel and configuration settings can be verified.
  - The integrity of the controller software can be verified.
  - The identity of the controller can be enforced.
  - Authentication to the controller software can be enforced by the local system.
- Specific technologies:
  - A root of trust is utilized to ensure the integrity of the controller's kernel and configuration settings.
  - Hashing algorithms are utilized to ensure the integrity of the controller's software.
  - Public/private key pairs (or pre-shared keys) are utilized to verify the identity of sensor network components.
  - Authentication protocols are utilized to enforce access rights to the controller.
- Cybersecurity Framework Subcategory mappings:
  - PR.AC-1
  - PR.AC-4
  - PR.AC-7
  - PR.DS-6
  - PR.DS-8
  - PR.IP-3
  - PR.PT-4

Communications Channels

The communications channels in the sensor network will be critical in transmitting sensor data to the controller via the base station. Communications channels may also utilize the base station to send control signals from the controller to the sensors. The controller may be connected to the base station via an RF or physical connection.

- Interfaces:
  - RF interface to the base station and the sensors used for communication of sensor data, device health, and over-the-air management
  - physical interface between the controller and the base station
- Possible attack vectors:

    - interception or dropping of RF data in transit
    - modification of RF data in transit
    - denial of service (DoS) on wireless communications channels
- Security requirements/outcomes:
    - The integrity of transmitted sensor data can be verified
    - The integrity of control signals from the base station to the sensors can be verified
    - The integrity of the communications channels can be verified
    - The availability of the communications channels is ensured
- Specific technologies:
    - Hashing algorithms are utilized to ensure the integrity of sensor data and control signals.
    - Public/private key pairs and/or certificate pinning may be utilized to verify the integrity of the communications channels.
    - Redundancy can be utilized to ensure the availability of the communications channels.
    - RF technologies:
        - Wi-Fi
        - ZigBee
        - Bluetooth/Bluetooth Low Energy (BLE)
    - Ethernet
    - Message Queuing Telemetry Transport (MQTT)/message protocols
- Cybersecurity Framework Subcategory mappings:
    - PR.AC-5
    - PR.DS-2
    - PR.DS-6
    - PR.PT-4

Security Requirements

Based upon the security requirements/outcomes for the network components mentioned in the previous sections, all components (with the exception of the communications channel) require the core protection capabilities from the following Cybersecurity Framework Subcategories:

- PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
- PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
- PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
- PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.

- PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.
- PR.IP-3: Configuration change control processes are in place.
- PR.PT-4: Communications and control networks are protected.

Many of the sensor network components have the same security requirements. Table 1 consolidates the various security requirements of the components into a single list. The identifier (ID) in the left column will be referenced in the security control map in Section 5.

Table 1: Security Requirements

ID	Security Requirement
1	The integrity of sensor network data can be verified.
2	The integrity of the sensor network components' software and configuration can be verified.
3	The identity of the sensor network components can be verified.
4	The integrity of the algorithms used to aggregate sensor data can be verified.
5	Authentication to the sensor network components can be enforced.
6	The integrity of control signals from the base station to the sensors can be verified.
7	The integrity of the communications channels can be verified.
8	The availability of the communications channels is ensured.

3 Scenarios

The specific scenarios included in this section explore sensor networks related to building management systems. These systems may include environment sensors, such as temperature, humidity, motion detection, and carbon monoxide (CO).

The example scenarios described below illustrate some of the challenges that this project may address. Each of the subsections below lists the relevant Cybersecurity Framework Functions and Categories that can be employed to mitigate the events throughout the attack. The specific Cybersecurity Framework Subcategories are listed in parentheses within each colored text box.

Scenario 1: Integrity of Sensor Data

The integrity of sensor data can be critical to sensor networks. Incorrect or manipulated data from sensors can negatively impact the network's logic decisions and can influence the subsequent actuation. In a building management system, the actuation may be the activation of an alarm in response to detected movement. This scenario can explore data integrity considerations in sensor networks that have data being provided by a large or even small number of sensors.

In this scenario, a malicious actor has modified data from motion-detection sensors to make it appear as if there is no physical activity in a restricted-access area of a building. However, the malicious actor is able to infiltrate the restricted-access area to acquire proprietary information.

This scenario addresses the following Cybersecurity Framework Categories and Subcategories:

- Malicious actor locally modifies the data from motion-detection sensors:
    - Protect: Integrity-checking mechanisms are used to verify software, firmware, and information integrity (PR.DS-6).
    - Protect: Integrity-checking mechanisms are used to verify hardware integrity (PR.DS-8).

This scenario does not address the following Cybersecurity Framework Categories and Subcategories:

- Malicious actor physically accesses the sensor:
    - Protect: Physical access to assets is managed and protected (PR.AC-2).
    - Detect: The physical environment is monitored to detect potential cybersecurity events (DE.CM-2).

Scenario 2: Unauthorized Sensor

In sensor networks, rogue sensors can be introduced to provide false data and to affect logic decisions and the subsequent actuation. This scenario can explore sensor network considerations for authentication of sensors. How are unauthorized sensors detected?

In this scenario, a malicious actor has added an unauthorized temperature-measurement sensor in the data center to a building management system. This sensor is providing preprogrammed low temperature readings to an aggregator. With this false data, the heating, ventilation, and air conditioning system turns up the temperature in the data center to a dangerous level, causing the computers to overheat.

This scenario addresses the following Cybersecurity Framework Categories and Subcategories:

- Malicious actor adds an unauthorized sensor to the sensor network:
    - Protect: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes (PR.AC-1).
    - Protect: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) (PR.AC-7).
    - Detect: Monitoring for unauthorized personnel, connections, devices, and software is performed (DE.CM-7).

This scenario does not address the following Cybersecurity Framework Categories and Subcategories:

- Malicious actor adds an unauthorized sensor to the sensor network:
    - Identify: Physical devices and systems within the organization are inventoried (ID.AM-1).
    - Detect: The physical environment is monitored to detect potential cybersecurity events (DE.CM-2).
    - Detect: A baseline of network operations and expected data flows for users and systems is established and managed (DE.AE-1).

Scenario 3: Wireless Sensor Communications Channel Security

Many sensor networks transmit data through wireless protocols, such as Bluetooth, Wi-Fi, or Zigbee. These wireless communication protocols provide many security features to protect sensor data in transit. This scenario can explore the trustworthiness of these wireless communications channels as well as the impact that these protocols' security features can have on the reliability and resiliency of sensors.

In this scenario, a malicious actor has intercepted wireless communications between a humidity sensor and a base station. Positioned between the sensor and the base station, the malicious actor modifies the humidity sensor data before transmitting it to the base station. The modified data results in increased humidity, leading to condensation and corrosion inside computing equipment. Alternatively, the malicious actor can stop the data transmission, making it appear that the sensor is failing.

This scenario addresses the following Cybersecurity Framework Categories and Subcategories:

- Malicious actor intercepts wireless communications in the sensor network:
    - Protect: Network integrity is protected (e.g., network segregation, network segmentation) (PR.AC-5).
    - Protect: Data in transit is protected (PR.DS-2).
    - Protect: Integrity-checking mechanisms are used to verify software, firmware, and information integrity (PR.DS-6).
    - Protect: Communications and control networks are protected (PR.PT-4).

This scenario does not address the following Cybersecurity Framework Categories and Subcategories:

- Before the malicious actor intercepts wireless communications in the sensor network:
    - Identify: Organizational communication and data flows are mapped (ID.AM-3).

Scenario 4: Latency Considerations in Sensor Networks

Many sensor networks depend on the timely transmission of sensor data to aggregators or other controllers. Any delay of sensor data — especially in time-critical applications such as CO alarms — due to latency can have serious consequences or can render the sensor data useless. Security solutions (e.g., device authentication, encryption) applied to sensor networks may introduce latency. This scenario can explore any negative impacts that these security solutions have on sensor networks due to latency.

In this scenario, a manufacturing organization has implemented capabilities for sensors in its building management system to authenticate to aggregators before the sensor data will be accepted. The organization has also employed mechanisms to ensure the integrity of data transmitted from sensors to aggregators. These capabilities have unintentionally introduced significant latency into the sensor network. Unfortunately, CO sensor data was delayed in notifying the alarm system of a critical level of CO in the plant.

This scenario addresses the following Cybersecurity Framework Categories and Subcategories:

- Timely transmission of sensor data to aggregators or other logic controllers:
    - Detect: Anomalous activity is detected in a timely manner, and the potential impact of events is understood (DE.AE).
    - Respond: Response plan is executed during or after an incident (RS.RP-1).

Scenario 5: Security Considerations of Sensor Network Aggregators

In many sensor networks, sensors transmit data to aggregators that integrate multiple copies and sources of sensor data into one copy for processing or actuation. Aggregators may utilize algorithms to weigh the importance of data from sensors, to combine data from multiple sensors, or to disregard data from sensors. Aggregators may take the form of more traditional computing devices or software implementations and do not necessarily have the same processing constraints as the sensors themselves. This scenario can explore the security concerns of aggregators, particularly how aggregator operating systems, software implementations, and algorithms can be attacked and manipulated to impact the integrity of the sensor network's data or to improperly weigh the data from the sensors.

In this scenario, a malicious actor has infected the operating system controlling the logic utilized by an aggregator in a building management system. This malware enabled the actor to assign more value to a rogue sensor that has been introduced into the sensor network.

This scenario addresses the following Cybersecurity Framework Categories and Subcategories:

- Sensors transmit data to aggregators to integrate multiple copies and multiple sources of sensor data into one copy for processing or actuation:
  - Detect: Event data is aggregated and correlated from multiple sources and sensors (DE.AE-3).
- Aggregators can be leveraged to compromise the integrity of the sensor network's data:
  - Protect: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities (PR.PT-3).
  - Protect: Communications and control networks are protected (PR.PT-4).

Scenario 6: Trustworthiness of Sensor Components – Microcontrollers and Firmware

In sensor networks, the trustworthiness of the sensors and the data they provide is critical. Logic decisions and actuating are based upon the data received from sensors. The reliable sensing of the physical world as well as the transformation of that information into electric signals depend in large part on the integrity of the physical sensors — particularly the microcontroller and the resident firmware. This scenario can explore how the reliability of the sensor's data can be affected by alterations to the sensor node's firmware.

In this scenario, a malicious actor has obtained physical access to the sensor and has loaded a recompiled kernel and/or kernel modules to impact the sensor's ability to correctly process and transmit data within the building management system.

This scenario addresses the following Cybersecurity Framework Categories and Subcategories:

- Malicious actor has modified the sensor kernel:
  - Protect: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes (PR.AC-1).
  - Protect: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties (PR.AC-4).
  - Protect: Integrity-checking mechanisms are used to verify software, firmware, and information integrity (PR.DS-6).
  - Protect: Integrity-checking mechanisms are used to verify hardware integrity (PR-DS-8).

This scenario does not address the following Cybersecurity Framework Categories and Subcategories:

- Malicious actor has obtained physical access to the sensor:
  - Protect: Physical access to assets is managed and protected (PR.AC-2).

Scenario 7: Sensor Network Data Leakage

Some sensors have been known to transmit data to the original equipment manufacturer (OEM) or other third parties without the user's knowledge. This data may include information about the sensed environment or other metadata generated by the sensor. This scenario can explore the considerations of "data leakage" in sensor networks and the related privacy considerations.

In this scenario, an organization is using sensors to measure the humidity and temperature in critical areas of the facility. Unknown to the organization, the sensors are transmitting this sensed data — as well as metadata, such as the precise sensor location and power usage — to the OEM. The OEM uses this data to market other heating and cooling products and services to the organization. The OEM also sells this data to other parties in the organization's geographic region.

This scenario addresses the following Cybersecurity Framework Categories and Subcategories:

- Transmit data to the OEM or other third parties without knowledge of the user:
  - Protect: Data in transit is protected (PR.DS-2).
  - Protect: Protections against data leaks are implemented (PR.DS-5).

Scenario 8: Secure Update of Devices

Sensors and their supporting devices are often expected to perform simple repetitive tasks. The code that is deployed on these devices to support these simple operations is often written without the expectation of being changed. This scenario will explore the appropriate measures that need to be taken to successfully update the code running on these devices.

In this scenario, an organization is using a sensor network to measure and control the humidity and temperature in areas around the facility. It is brought to the attention of the organization that the devices installed are vulnerable to an attack that would cause the entire system to malfunction. All of these installed devices need a software update provided by the OEM via an internet download. The scenario will explore possible ways to securely update sensors and their corresponding components. The update will take into account the security of the communications channel, the integrity of the update package, and the integrity of the device.

This scenario addresses the following Cybersecurity Framework Categories and Subcategories:

- The OEM is required to update the sensor network components' software:
  - Protect: Remote access is managed (PR.AC-3).
- Sensor network components' software is updated:
  - Protect: Integrity-checking mechanisms are used to verify software, firmware, and information integrity (PR.DS-6).
  - Detect: Detection processes are continuously improved (DE.DP-5).

4 Relevant Standards and Guidance

- NIST Cybersecurity Framework

  https://www.nist.gov/programs-projects/cybersecurity-framework

  The NIST Cybersecurity Framework outlines the best cybersecurity practices to minimize risk to critical infrastructure.

- NIST Framework for Cyber-Physical Systems (CPSes)

  https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

  The NIST CPS framework is intended to provide guidance in designing, building, and verifying CPSes. It also acts as a tool for analyzing complex CPSes.

- National Institute of Standards and Technology Internal/Interagency Report (NISTIR) 8114: Report on Lightweight Cryptography

  https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf

  This NISTIR provides information about the lightweight cryptography project at NIST. It also describes plans for the standardization of lightweight cryptography algorithms.

- NIST SP 500-325: Fog Computing Conceptual Model

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf

  This publication describes fog and mist cloud-computing models. These models are better suited for large amounts of heterogenous data that require minimal network latency.

- NIST SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations

  https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

  This publication provides a catalog of security and privacy controls for federal information systems and organizations. The catalog is aimed at protecting operations and assets, individuals, other organizations, and the nation from a diverse set of threats.

- NIST SP 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

  This publication provides guidance on how to secure ICS.

- NIST SP 800-98: Guidelines for Securing Radio Frequency Identification (RFID) Systems

  https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-98.pdf

  This publication goes into detail about mitigating security and privacy risks in RFID systems through management, operational, and technical controls.

- NIST SP 800-121 Revision 2: Guide to Bluetooth Security

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

  This publication outlines the security capabilities of Bluetooth and BLE. It also provides information on how these protocols can be secured in a corporate environment.

- NIST SP 800-183: Networks of ‘Things’

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

  This publication provides important definitions of things used for describing and building IoT networks.

- NIST SP 800-193: Platform Firmware Resiliency Guidelines

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

  This publication provides guidelines and recommendations for ensuring firmware and data resiliency against potentially destructive attacks.

- American National Standards Institute (ANSI)/American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) Standard 135-2016: BACNet A Data Communication Protocol for Building Automation and Control Network

  This standard defines BACNet, a universal protocol that applies to computerized systems wishing to exchange arbitrary types of data.

- ANSI/Consumer Electronics Association Standard 709.1-B: LonWorks

  This standard defines LonWorks, a popular communications protocol for local-area building automation system (BAS) networks.

- ANSI/International Society of Automation Standard 62443-2-1: Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program

  This standard is part of a multipart series that addresses the issue of security for industrial automation and control systems.

- ASHRAE Guideline 13-2015: Specifying Building Automation Systems

  This guideline provides guidelines on BASes.

- MODBUS Application Protocol Specification V1.1b3

  http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

  This document describes MODBUS, a protocol used for client/server communication between devices connected on different types of buses or networks.

- ZigBee Specification 053474r20

  http://www.zigbee.org/wp-content/uploads/2014/11/docs-05-3474-20-0csg-zigbee-specification.pdf

  This document provides a specification for the ZigBee communications protocol.

- Institute of Electrical and Electronics Engineers (IEEE) Standard 802.15.4-2015: IEEE Standards for Low-Rate Wireless Networks

  https://ieeexplore.ieee.org/document/7460875/

  This document provides standards for low-data-rate, low-power, and low-complexity short-range RF transmissions in a wireless personal area network.

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Standard 14908-1:2012: LonTalk – Network Control Protocol

  This document describes LonTalk, a control protocol for local area networks (LANs). LonTalk is commonly used as a control protocol in BASes.

- ISO/IEC Standard 14908-2:2012: Control Network Protocol – Part 2: Twisted pair communication

  This standard specifies the control network protocol (CNP) free-topology twisted-pair channel for networked control systems in LANs. It is used in conjunction with ISO/IEC 14908-1:2012.
- ISO/IEC Standard 14908-4: Control Network Protocol – Part 4: IP Communication

  This standard describes how to encapsulate CNP packets for commercial LANs in Internet Protocol (IP) packets and how to transmit them over an IP tunnel.
- ISO Standard 16484-5:2017: Building Automation and Control Systems – Part 5: Data Communications Protocol

  This standard defines data communications and protocols used in BASes.
- ISO/IEC Standard 19637:2016: Information technology – Sensor network testing framework

  This document provides a framework for testing sensor networks.
- Request for Comments (RFC) 1157: Simple Network Management Protocol (SNMP)

  https://www.ietf.org/rfc/rfc1157.txt

  This RFC describes SNMP, which can be implemented to support legacy "cyberlightweight" systems and devices.
- Konnex

  This is an open standard for commercial and domestic building automation. It evolved from three earlier standards and supports many different types of links and topologies.
- Message Queuing Telemetry Transport

  http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.pdf

  This standard describes MQTT, a lightweight protocol designed for collecting data from many devices and transporting it back to the IT infrastructure.
- PROFINET (Process Field Net)

  This standard describes industrial Ethernet standards, designed for collecting data from and controlling equipment in industrial systems.

5 Security Control Map

Table 2 maps the characteristics of the commercial technologies that the NCCoE may apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), and to the scenarios, components, and security outcomes/requirements of the previous sections. This exercise is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Table 2: Security Control Map

Cybersecurity Framework v1.1			Applicable Scenarios	Applicable Components	Security Outcomes	Applicable Technologies
Function	**Category**	**Subcategory**				
Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Scenario 2 Scenario 6	sensor base station/aggregator controller	3 5	Identity Access Management (IdAM) Solutions: - Lightweight Directory Access Protocol (LDAP) - multifactor authentication
		PR.AC-3 Remote access is managed	Scenario 8	not applicable (N/A)	N/A	Remote Access Technologies: - Secure Shell (SSH) - remote desktop IdAM Solutions: - LDAP - multifactor authentication
		PR.AC-4 Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Scenario 6	sensor base station/aggregator controller	5	N/A

Cybersecurity Framework v1.1			Applicable Scenarios	Applicable Components	Security Outcomes	Applicable Technologies
Function	Category	Subcategory				
		PR.AC-5 Network integrity is protected (e.g., network segregation, network segmentation)	Scenario 3	communications channels	3 7 8	Encryption Technologies: • Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Security Controls: • firewall • network access control • anti-virus
		PR.AC-7 Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Scenario 2	sensor base station/aggregator controller	3 5	Authentication Solutions: • user certificate • device certificate • username and password • personal identification number (PIN) • multifactor authentication

Cybersecurity Framework v1.1			Applicable Scenarios	Applicable Components	Security Outcomes	Applicable Technologies
Function	Category	Subcategory				
	Data Security (PR.DS)	PR.DS-2 Data in transit is protected	Scenario 3 Scenario 7	communications channels	1 6 7	Encryption Technologies: • SSL/TLS Security Controls: • firewall • network access control • network intrusion detection system (NIDS)
		PR.DS-5 Protections against data leaks are implemented	Scenario 7	sensor	N/A	Data Loss Prevention (DLP) Solutions: • firewall • NIDS • host-based intrusion detection system (HIDS)
		PR.DS-6 Integrity-checking mechanisms are used to verify software, firmware, and information integrity	Scenario 1 Scenario 3 Scenario 6 Scenario 8	sensor base station/aggregator controller communications channels	1 2 4 6 7	Software Integrity Solutions: • Unified Extensible Firmware Interface (UEFI) • Secure Boot • file integrity monitoring • checksum validation • anti-virus
		PR.DS-8 Integrity-checking mechanisms are used to verify hardware integrity	Scenario 1 Scenario 6	sensor base station/aggregator controller	3	Hardware Integrity Solutions: • control flow integrity • Federal Information Processing Standard (FIPS) 140-2-certified hardware

Cybersecurity Framework v1.1			Applicable Scenarios	Applicable Components	Security Outcomes	Applicable Technologies
Function	Category	Subcategory				
	Information Protection Processes and Procedures (PR.IP)	PR.IP-3 Configuration change control processes are in place	N/A	sensor base station/aggregator controller	2	configuration management solutions
	Protective Technology (PR.PT)	PR.PT-3 The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Scenario 5	N/A	N/A	configuration management solutions
		PR.PT-4 Communications and control networks are protected	Scenario 3 Scenario 5	sensor base station/aggregator controller communications channels	6 7 8	Security Controls: • firewall • NIDS • HIDS • network access control • anti-virus Encryption Technologies: • SSL/TLS

Cybersecurity Framework v1.1			Applicable Scenarios	Applicable Components	Security Outcomes	Applicable Technologies
Function	Category	Subcategory				
Detect (DE)	Anomalies and Events (DE.AE)	N/A	Scenario 4	sensor base station/aggregator controller communications channels	N/A	N/A
		DE.AE-3 Event data is collected and correlated from multiple sources and sensors	Scenario 5	base station/aggregator	4	N/A
	Security Continuous Monitoring (DE.CM)	DE.CM-7 Monitoring for unauthorized personnel, connections, devices, and software is performed	Scenario 2	N/A	3 5	Continuous Monitoring Solutions: • NIDS • HIDS
	Detection Processes (DE.DP)	DE.DP-5 Detection processes are continuously improved	Scenario 8	N/A	N/A	N/A

Cybersecurity Framework v1.1			Applicable Scenarios	Applicable Components	Security Outcomes	Applicable Technologies
Function	Category	Subcategory				
Respond (RS)	Response Planning (RS.RP)	RS.RP-1 Response plan is executed during or after an event	Scenario 4	N/A	N/A	N/A

Appendix A References

[1] C. Poddar and B. Supradip, “Industrial Wireless Sensor Network Market by Sensor (Pressure Sensor, Temperature Sensor, Level Sensor, Flow Sensor, Biosensor, and Others), Technology (Zigbee, Bluetooth, Wi-Fi, and Others), and Industry Vertical (Oil & Gas, Automotive, Manufacturing, Healthcare, and Others), Global Opportunity Analysis and Industry Forecast, 2017–2023,” Allied Market Research, Portland, OR, Feb. 2018. Available: https://www.alliedmarketresearch.com/industrial-wireless-sensor-network-market.

R. Faludi, *Building Wireless Sensor Networks*. Sebastapol, Ca: O'Reilly Media, Inc., 2011.

M. Frei, J. Hofer, A. Schlüter, and Z. Nagy, “An easily-deployable wireless sensor network for building energy performance assessment,” *Energy Procedia*, vol. 122, pp. 523-528, Sept. 2017.

L. Zhu, Z. Zhang, and C. Xu, “Secure Data Aggregation in Wireless Sensor Networks,” in *Secure and Privacy-Preserving Data Communication in Internet of Things*. Singapore: Springer, 2017, pp. 3-31.

S. Nikhade, “Wireless sensor network system using Raspberry Pi and zigbee for environmental monitoring applications,” in *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, Avadi, Chennai, India, 2015.

S. M. Ferdoush, “A Low-Cost Wireless Sensor Network System Using Raspberry PI and Arduino for Environmental Monitoring Applications,” M.S. thesis, Dept. Elect. Eng., Univ. North Texas, Denton, Tex., May 2014.
Available: https://digital.library.unt.edu/ark:/67531/metadc500182/m2/1/high_res_d/thesis.pdf.

Appendix B Acronyms and Abbreviations

ANSI	American National Standards Institute
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BAS	Building Automation System
BLE	Bluetooth Low Energy
CNP	Control Network Protocol
CO	Carbon Monoxide
COTS	Commercial Off-the-Shelf
CPS	Cyber-Physical System
DLP	Data Loss Prevention
DoS	Denial of Service
FIPS	Federal Information Processing Standard
HIDS	Host Intrusion Detection System
ICS	Industrial Control Systems
ID	Identifier
IDS	Intrusion Detection System
IdAM	Identity and Access Management
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MQTT	Message Queuing Telemetry Transport
N/A	Not Applicable
NCCoE	National Cybersecurity Center of Excellence
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal/Interagency Report

OEM	Original Equipment Manufacturer
PACS	Physical Access Control System
PIN	Personal Identification Number
PROFINET	Process Field Net
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
SNMP	Simple Network Management Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface