# The New Work of Building Operations in the Digital Age:

# The Impact of IoT on Facility Management and Operational Practices

## Report 2 of 2: New Practices to Ensure Technological Feasibility


CENTER FOR EDUCATION + RESEARCH IN CONSTRUCTION
DEPARTMENT OF CONSTRUCTION MANAGEMENT

Daniel Dimitrov, Ph.D. Candidate
University of Washington, Department of Construction Management



7/5/2024

## Table of Contents

**Acknowledgements**

I would like to extend my sincere gratitude to all those who contributed to this research study.

First and foremost, I would like to thank our research team members for their valuable contributions to this study. Dr. Carrie Dossick's expertise, leadership, and insightful guidance and feedback were instrumental to this study. In addition, I would like to thank our research assistant on this project, Miriam Ccarita Cruz, who aided in data collection, participant recruitment, and case study development. Both Dr. Dossick and Miriam's contributions were critical to the success of this research study and the outcomes presented in this report.

I would also like to extend my gratitude to the University of Washington (UW) Facilities for their collaboration and support in this research as well as the UW Campus Sustainability Fund for funding this study. Their willingness to share insights and experiences has been invaluable in helping us understand the impact of technological transition within the organization. We also thank all the operators, engineers, managers, and technicians who participated in our interviews, providing us with the practical perspectives that shaped the findings of this study.

**Report 2 of 2 - New Practices to Ensure the Technological Feasibility of IoT Systems**

## Introduction

Introducing new technology into an organization for sustainable and operational improvements often presents significant challenges, as staff need time to familiarize themselves with the systems and work through the obstacles that come with change. However, the Industry 4.0 has led to change in almost all industries, including the facility management and operations industries. The integration of Internet of Things (IoT) devices and systems in facilities management (FM) represents a significant shift from traditional building management practices to a more data-driven and integrated approach. This research was done in collaboration with the University of Washington Facilities, examining the new technical practices that IoT brings to the FM landscape within the management of the University of Washington (UW) campus. By interviewing a diverse range of facilities personnel, we aimed to capture the real-world challenges and experiences associated with technical IoT implementation, including sensor configuration, network communication, middleware device management, leveraging IoT capabilities, lifecycle maintenance, and managing IoT access control and security. Through this qualitative analysis, we seek to provide insights that can inform future practices and reflect the current state of work using IoT and Direct Digital Control (DDC) technologies.

This report presents the new practices that support the technological feasibility of IoT systems at UW. The findings are categorized into six primary areas:

**Sensor Configuration:** The initial stage of configuring IoT devices involves managing diverse vendor-specific software tools and developing the programming skills to handle unique configuration requirements for different devices. This necessitates a high level of adaptability from facilities staff.

**Establishing Network Communication:** Assigning unique identifiers to devices, standardizing communication protocols, converting existing buildings to IoT control systems, and integrating third-party devices are essential practices in establishing a network communication infrastructure. These tasks require attention to detail and collaboration with various stakeholders.

**Middleware/Supervisory Device Configuration:** Implementing logic in supervisory devices for message routing and processing is a new critical practice for FM personnel. Facilities personnel must develop rule-based algorithms to capture and process relevant data correctly.

**Leveraging the Capabilities of IoT Systems:** IoT systems enable enhanced system performance monitoring, data analytics, troubleshooting, and fault detection. Facilities personnel

must create and maintain alerts, navigate diverse user interfaces, and develop data visualizations to manage building operations effectively.

**IoT Device/System Lifecycle Management:** Regular updates of software and servers and sensor lifecycle maintenance are critical for ensuring continuous compatibility and effectiveness of IoT systems. This requires a systematic approach to managing updates and replacements.

**Managing IoT Access Control and Security:** Implementing access control permissions and maintaining firewall and intrusion detection systems are vital for protecting IoT devices from potential threats. Facilities personnel must collaborate with IT professionals to establish and manage security protocols.

By addressing these areas, this report outlines the evolving role of facilities management in the era of IoT, highlighting the need for continuous learning, collaboration, and adaptation to leverage the benefits of IoT technologies effectively. The insights and recommendations provided aim to reflect the current practices needed to maintain IoT technological feasibility and guide future efforts in enhancing the efficiency and effectiveness of facilities management practices at the University of Washington and beyond.

**Document Structure**

The findings of this research study are listed in Table 2 below. Following this table, each one of these findings will be discussed individually. Within each finding, a quote collected from our interviews with UW Facilities personnel that encapsulates the main topic of each finding will be shared. Following this, a brief description of the findings based on a robust literature review about this topic, as well as the fieldwork we conducted on-site with UW Facilities, will be provided.

***Findings Table 2:*** *UW FM Study - New Technical Practices*

| Category: | Findings: |
|---|---|
| **1. Sensor Configuration** | 1.1: Managing diverse vendor specific software tools |
| | 1.2: Programming/Coding Responsibilities in Device Configuration |
| **2. Establishing Network Communication** | 2.1 Sensor Configuration - Creating Unique Identifier/Instance Numbers |
| | 2.2: Communication Protocol Standardization for Device Communication |
| | 2.3: Network Wiring Requirements - Converting Existing Buildings to IoT Control |
| | 2.4: Third Party Device Integration and Ensuring Compatibility with Existing Systems |
| **3. Middleware/Supervisory Device Configuration** | 3.1: Establishing and Implementing Logic in Supervisory Devices - Message Routing and Processing |
| **4. Leveraging the Capabilities of IoT Systems** | 4.1: System Performance Monitoring |
| | 4.2: Data Analytics |
| | 4.3: Troubleshooting, Fault Detection, and Diagnostics |
| | 4.4: Creating, Maintaining and Responding to Alerts and Notifications |
| | 4.5: Managing and Navigating Diverse Vendor Specific User Interfaces and Applications |
| | 4.6: Creating, Understanding, and Maintaining Data Visualizations |
| **5. IoT Device/System Lifecycle Management** | 5.1: Updating Software and Servers |
| | 5.2: Sensor Lifecycle Maintenance |
| **6. Managing IoT Access Control and Security** | 6.1: Managing Access Control |
| | 6.2: Maintaining Firewall and Intrusion Detection Systems for IoT Devices and Controls |

## Findings

## 1. Sensor Configuration

In this section, the new required practices for FM personnel in initial sensor configuration for IoT devices will be discussed in detail. IoT device configuration involves programming devices in the field for their intended functionality so that they collect the data needed by the FM group. The integrated IoT sensors can come from various vendors and manufacturers, leading to a diversity of configuration requirements and specific software tools. In this section, the following topics will be discussed:

1.1. Managing diverse vendor-specific software tools

1.2. Programming/coding responsibilities in device configuration

### 1.1. Managing diverse vendor-specific software tools

*"All the vendor does for us is provide us with a package. They say these are the software tools needed to install physical devices and put them on a network".*

*"Every manufacturer of a piece of, per se, HVAC equipment has a proprietary control protocol…Carrier has CCN, Carrier Comfort Network. Mitsubishi has the M-NET. There's just a smattering of them across the industry."*

As the first stage of configuring IoT devices, facility personnel must use the tools and software provided by the vendor of the IoT system to establish the initial device configuration. However, the process of doing so varies depending on the package provided by the vendor. Once the software package is provided, it becomes the responsibility of the facility staff to understand the unique vendor and device-specific processes necessary to install the device hardware and its software correctly, configure the device, and ensure proper network communication. Facility personnel must become comfortable with a variety of different software packages and control protocols that are unique to the manufacturers. This necessitates new work to establish proficiency in installing, configuring, and maintaining these systems effectively. As the diversity of devices increases, so must the proficiency and adaptability of facility staff in correctly configuring devices.

### 1.2. Programming/Coding Responsibilities in Device Configuration

*"You have to be versed in each one of those specifically because there's a lot of detail and nuance that you have to know that only experience gives you to be able to configure them correctly to work right."*

*"When I first started learning building automation systems, like I said, every single one was different. Every building you went to had a different version of that same control system, and they all acted a little bit differently… it was just a disaster."*

As part of the above discussion on the diversity of vendor-provided devices that come with unique configuration requirements, new work appears for facility personnel in properly programming the devices during the configuration phase. This leads to facility technicians and personnel needing to learn and develop a diverse set of programming skills to effectively configure devices. Each manufacturer's programming requirements differ, demanding a nuanced understanding of various programming requirements and coding techniques. This highlights the shift in skill set for facility personnel necessary to properly manage a facility and the learning curve that emerges for new and existing personnel.

## 2. Establishing Network Communication

In this section, the new requirements for establishing IoT network connectivity will be discussed in detail. For IoT devices and sensors to communicate with each other and transmit data in real-time to management applications for analytical purposes or improvements in decision-making, establishing proper network communication between all devices and the network is crucial. In this section, the following topics will be discussed:

2.1. Sensor configuration- creating unique identifier/instance numbers and device inventory

2.2. Communication protocol standardization for device communication

2.3. Network wiring requirements- converting existing buildings to IoT control

2.4. Third-party device integration and ensuring compatibility with existing systems

### 2.1. Sensor Configuration - Creating Unique Identifier/Instance Numbers and Device Inventory

*"You need the instance number, which is a unique identifier that each one of the devices have. And if two of them have the same, then you have a communication problem."*

In IoT sensor configuration, assigning unique identifiers or instance numbers to individual devices is important in facilitating data communication. Unique device identifiers serve as distinct labels for each sensor, allowing for identification, communication, and tracking within the network. The necessity for implementing nomenclature standards exists on multiple levels within the organization, from ensuring device communication on the network to ensuring proper device identification on management platforms. However, this task is more complicated than it seems, as the number of unique and individual devices ranges in the hundreds or thousands,

leading to the necessity to create and maintain an updated and accurate device inventory that tracks this growing number of devices and their nomenclature.

### 2.2. Communication Protocol Standardization for Device Communication

*"We have to bring in all of these different vendors into a cohesive network."*

*"BACnet is kind of what most everybody uses now. And it's an ASHRAE standard."*

In establishing network communication for IoT devices comes the need to ensure communication protocol standardization across communicating devices on campus. This is done so that devices from a diverse range of manufacturers can communicate with each other and relay data through a shared communication network. At the UW, devices utilize the BACnet communication protocol. Standardizing communication protocols is critical to device connectivity amongst the entire IoT ecosystem, leading to new required practices in this arena for FM personnel.

### 2.3. Network Wiring Requirements - Converting Existing Buildings to IoT Control

*"We're pulling all the pneumatics out, and we're putting in brand new controls; it's almost like a brand new job to a certain degree."*

*"We've kind of separated into a smaller team solely focused on upgrading older analog buildings to digital controls, and with that, integration of BACnet or Modbus or LonWorks or whatever they have."*

*"Communication is always key. And with that comes the physical wiring standards."*

As more buildings are converted from existing pneumatic control systems to IoT or DDC-based management systems, new work forms for facility personnel in establishing the communication infrastructure on which IoT systems rely in order to operate effectively. Establishing network communication involves installing the proper cabling onto the RS-485 network communication system used by the University Facilities division. However, converting buildings from pneumatic control to IoT control often requires restructuring the building's wired infrastructure. Although this work is collaborative with university electricians, it still becomes labor-intensive for facility personnel. This has led to establishing a separate team within UW Facilities dedicated to managing such building transitions and retrofits.

### 2.4. Third-Party Device Integration and Ensuring Compatibility with Existing Systems

*"If a third-party system does not abide by the BACnet standard, you have to go through and find out what each point is physically relaying or, even worse, sometimes third-party devices are literally just hard outputs, dry outputs. And from there, you have to program our system to take it in, use it as needed, and then spit out a usable piece of information."*

In many instances, devices produced by manufacturers outside the typical state-sponsored vendors at the University (Johnson, Allerton, Siemens) require integration into the existing IoT infrastructure. This is often done when devices are acquired to solve specific and unique problems on campus. This responsibility falls upon facility personnel to ensure the device is securely connected and can communicate seamlessly within existing protocols, even when it does not come from sponsored manufacturers. Sometimes, such third-party devices are BACnet native, which allows for a more simple integration process. However, in other circumstances, third-party devices may not be BACnet native and, therefore, require a more intricate procedure to foster communication within the existing network. When this occurs, FM personnel must have the skills to connect non-compatible devices to the network and maintain them over time.

## 3. Middleware/Supervisory Device Configuration

This section will discuss the new requirements for managing middleware/supervisory devices, specifically for establishing and implementing logic in supervisory devices. This is necessary to ensure that data is routed and processed correctly. For data to get where it needs to go for analytics or storage, implementing logic in transitory devices as middleware within the IoT system architecture is a new practice required for FM personnel in IoT management.

### 3.1. Establishing and Implementing Logic in Supervisory Devices - Message Routing and Processing

*"It really depends on what data we choose to capture. Obviously, there is a large amount of information passing these industrial computers. All we're choosing to capture is pertinent information. So, sometimes, that's temperatures, pressures, operating hours, kilowatts, and energy consumed."*

*"There's business logic in that you can choose to pull every piece of data from a device, but that's a lot of data. So, we go through and write small pieces of code saying if parameters are between this and this, then report. If it goes through a change of value, then report. Sample times, buffer sizes, etc."*

In IoT system architecture, the supervisory (or middleware) devices are the central hub for collecting data from various sensors and devices within the established network. For data to be processed appropriately so that important information can be collected and sent to the server

level for historicization or later analytics, facility personnel must implement logic within these devices for message routing and processing. Such logic includes the implementation of rule-based algorithms so that the supervisory devices can process incoming data, identify relevant data patterns, and use implemented logic to route data accordingly. These duties fall upon facility personnel. With the vast diversity of IoT devices implemented throughout campus comes the necessity to implement different and unique logic within each supervisory device to ensure that the desired information is collected and processed.

## 4. Leveraging the Capabilities of IoT Systems

In this section, the new requirements for leveraging the capabilities of IoT systems will be discussed. This means that FM personnel can use implemented IoT devices and systems to improve building operations by leveraging their functional capabilities. Many of these new practices fall within the application layer of IoT system architecture. If IoT devices are implemented but not leveraged properly, their full potential cannot be reached. In this section, the following topics will be discussed:

4.1. System performance monitoring

4.2. Data analytics

4.3. Troubleshooting, fault detection, and diagnostics

4.4. Creating, maintaining, and responding to alerts and notifications

4.5. Managing and navigating diverse vendor-specific user interfaces and applications

4.6. Creating, understanding, and maintaining data visualizations

### 4.1. System Performance Monitoring

*"Device activity on the network is monitored; offline devices generate email alerts and other notifications. Devices are also monitored for unexpected data outputs or status updates to address issues within the built environment."*

IoT systems allow for much greater detail in system performance monitoring, which creates new work for facility personnel in maintaining procedures for daily/frequent monitoring. This enables the organization to move away from reactive maintenance and into a more predictive maintenance strategy. Through leveraging IoT sensors and devices, facility managers can continuously collect and analyze real-time data about various aspects of system performance, such as temperature, humidity, energy consumption, and equipment status. Facility operators must actively check dashboards and management applications and ensure that systems are operating within norms daily. In addition, to receive notifications of anomalies or deviations

from typical system performance, facility operators must create rules for the system to follow for it to detect the anomaly and inform the proper personnel to respond accordingly. The new abundance of data that systems can generate with the use of IoT devices also leads to new work in performance reporting.

### 4.2. Data Analytics

*"The trending and some of the other information like that enables us to compile a lot of information and we can layer the information on top of each other. Say, if we have a piece of equipment that we want to put five different trends on, then we put them on one graph, and then you're able to see all of how each one of those pieces interacts with each other, and you're better able to troubleshoot what's wrong with the equipment."*

The use of IoT systems that continuously collect and process data opens the door to a new era of enhanced insights and opportunities for operational efficiency. With IoT devices deployed throughout buildings to collect building performance information in real-time, facility personnel now have access to an abundance of data across various metrics such as equipment status, temperature, humidity, energy consumption, occupancy information, and more. This influx of data presents an opportunity for FM by enabling the implementation of data analytics techniques to not only drive better-informed decision-making but also allow systems to take autonomous action when corrective responses are necessary. However, the introduction of data analytics opportunities creates new technical work for facility personnel which is separate from the traditional arsenal of responsibilities within the realm of building operations and maintenance. Facility managers must now leverage data analytics to identify patterns, trends, and anomalies within building operations, allowing for proactive interventions. Gaining the skills to achieve these tasks comes with experience and training, as the power of the data is only useful if it can be manipulated in meaningful ways.

### 4.3. Troubleshooting, Fault Detection, and Diagnostics

*"We do the first pass at it up and down. Can we determine any kind of IT issue? Is it a meter issue? Then we will go to site to troubleshoot the meter."*

*"You start out at the server level typically and you see something is wrong where it's not reacting the way that you feel like it should be. Then you go down farther, and then you directly plugin, figure out if there's something wrong with the configuration."*

The integration of IoT systems in facility management is revolutionizing the nature of troubleshooting processes, which leads to changes in practices. Traditionally, facility managers relied heavily on reactive measures to address issues as they arose and mainly implemented physical maintenance measures to troubleshoot errors and address malfunctions. However, with the integration of IoT technology, troubleshooting has become increasingly proactive and data-driven. Many device and system troubleshooting processes are now primarily driven by software investigation and technical analysis of systems and their network connectivity. This transition to

more technical rather than physical troubleshooting does not eliminate the need for physical investigation and fieldwork; it simply changes the order of operations and shifts physical on-site troubleshooting to a later point when technical troubleshooting measures have already been attempted. Device and system troubleshooting is additionally shifting in form, allowing for remote work and offsite response to issues when they occur in real-time. This shift is due to the technical nature of errors and the reduced need for on-site maintenance, as described above. This allows facility personnel to be more responsive to issues and address problems more efficiently.

Furthermore, the implementation of rule-based algorithms during the configuration phase of IoT system deployment has led to automated fault detection, swiftly notifying facility personnel of device malfunctions. While this enhances efficiency, it also results in a higher frequency of issues requiring attention from facility personnel. This contrasts sharply with pneumatic systems, where faults often went undetected until damage occurred and became noticeable.

### 4.4. Creating, Maintaining, and Responding to Alerts and Notifications

*"If it's critical enough, then you're going to set up an alarm that will alert somebody that there is a situation happening. Then I can immediately interface with that situation within five minutes."*

Facility personnel have access to a new abundance of data that can be used to respond to system faults and irregularities in real-time with the use of IoT. Therefore, creating, maintaining, and responding to system alerts and notifications is critical to FM practices when operating IoT-integrated buildings. Creating alerts means that FM personnel must define conditions within the IoT system that dictate system responses to specific parameters. More specifically, this means that when a set parameter is met or exceeded, it automatically triggers alerts that inform facility personnel of the abnormality in the performance of that device or system. Once such alerts are created, maintaining them requires regular review and adjustment to ensure they remain relevant and effective in identifying potential issues or abnormalities as systems, their function, and the context change. However, due to the size of the campus and the limited number of staff available at any given time to respond to system alerts, the facility team has to develop and establish protocols for promptly responding to these alerts by creating automated responses or establishing a priority hierarchy to deem the criticality of immediate response.

### 4.5. Managing and Navigating Diverse Vendor-Specific User Interfaces and Applications

*"Every other Tuesday, they seem to have changed their entire system. And with that comes the growing pains of a new system."*

*"They changed the entire architecture of how the entire system worked. And so, doing something as simple as just adding an input, like a sensor input, to a field device now became a challenge, because the way you did it was entirely different."*

Each manufacturer of IoT devices develops their control application/platform for device control, manipulation, and data access. As more IoT devices are acquired from diverse vendors, the challenge of continually adding new control platforms to the existing IoT ecosystem means that FM personnel must continuously learn the nuances of specific applications and adapt to a plethora of diverse control systems. In addition, these individual platforms regularly update and change their software requirements and user interface based on manufacturer updates, which again requires FM staff to evolve their skill sets within them continuously. Each management application is often subject to regular updates and changes in software requirements and interfaces, which calls for FM personnel to be able to adapt to new platforms and user interfaces regularly.

### 4.6. Creating, Understanding, and Maintaining Data Visualizations

*"There are basically two sets of visualization tools, one for the UW customer – the kind of summary or final report views, and that's in Tableau… and there is a web visualization tool called PI Vision that is accessible directly."*

To make collected IoT data easy to comprehend and distribute to stakeholders, facility teams need to create data visualizations to represent trends and performance in a way that is easy to digest and simpler to understand by non-directly involved parties. Creating visualizations to represent data can also make it easier for internal facility personnel to analyze and comprehend data by creating things such as data graphs, tables, and 3D visualizations to represent the data or the building sections themselves. This introduces new responsibilities for facility personnel in using visualization software to represent collected IoT data. Leveraging data visualization tools entails not only learning software like Tableau and PI Vision but also leveraging them to create different forms of visual representations like code-required reports or interactive dashboards and 3D models of building spaces to make the IoT data more comprehensible.

## 5. IoT Device/System Lifecycle Management

In this section, the new requirements for IoT lifecycle management will be discussed in detail. This is an essential attribute to ensuring the operational capabilities of IoT systems over time, especially due to their contrasting maintenance requirements and reduced lifespan compared to traditional building elements, which often require less attention and demand much less frequent maintenance. The following topics will be discussed in this section:

5.1. Updating Software and Servers

5.2. Sensor Lifecycle Maintenance

### 5.1. Updating Software and Servers

*"This [upgrading software] is a challenge both in terms of funding and staff availability. Historically devices have run to failure and software updates were, with some exceptions, only applied through an ad hoc process"*

*"The IT world doesn't wait for us. They keep moving forward...so we have to keep upgrading our stuff to keep up with them at times too, both with server and with the local interface"*

As IoT systems evolve and manufacturers continuously release new versions of software, facility personnel must stay ahead of the curve on updating software and servers in addition to keeping track of the status of their systems to ensure continuous compatibility. An "ad hoc" updating process is no longer viable with IoT systems. They can quickly become outdated if the correct updates are not regularly performed, requiring an organized approach to managing system updates. Such an organized approach would include tracking and documenting the status of existing systems through inventory efforts. Further complexity is added to this process because various integrated IoT technologies are updated on different cycles based on the release of new software versions from their coinciding vendors. The continuous release of new software versions requires increased attention to update requirements and an organized tracking effort from the FM side. Falling behind the curve with updates creates compatibility issues, which have cascading effects as newer upgrades become available over time.

### 5.2. Sensor Lifecycle Maintenance

*"Some of those meters are now 15 years old, and they're starting to wear out and break. So [facility manager] is needing to order spares and make sure that there's parts stocked so that when meters die they could be replaced in a reasonable amount of time so you're not losing all the data"*

Over the lifecycle of IoT devices and as system updates/upgrades become available, measures need to be taken by facility personnel to maintain the end device sensor hardware and device configuration to account for continual compatibility and effectiveness with system updates. Sometimes, this involves performing hardware maintenance, changing configurations, rewiring devices, or replacing entire controllers when they are no longer compatible with systems. In certain circumstances, changes to the system software and the rapid pace of technological development for IoT require total device replacements when the hardware is no longer viable to support new software versions. This additionally can occur when communication protocols are changed or updated, and the existing hardware no longer supports the ability to interchange data. This can require the rewiring of entire systems or, in some scenarios, the total replacement of the sensor or end device for it to maintain its communication abilities with the network and other devices. The fast-changing IoT landscape calls for timely 134 replacement of end devices and enhanced attention to the lifecycle of IoT systems, which is significantly reduced compared to static building elements that FM teams are used to maintaining.

## 6. Managing IoT Access Control and Security

In this section, the new requirements for managing IoT access control and overall system security with the growing number of IoT implementations on campus will be discussed. As more unique devices get integrated on campus, more system vulnerabilities may present themselves, and more precise access control to systems must be assigned. In this section, the following topics will be discussed:

6.1. Managing Access Control

6.2 Maintaining Firewall and Intrusion Detection Systems for IoT Devices and Controls

### 6.1. Managing Access Control

*"We grant engineers, data analysts, even just building coordinators with various permissions, what they can't change or what they can see… you can grant access to a smattering of people all across campus"*

*"Sometimes, we grant facilities a lot of permissions. Sometimes, we restrict it. It's a very case-to-case basis"*

With the increasing adoption of IoT devices in building automation systems for controlling building parameters such as HVAC, lighting, and energy, it becomes critical to implement security measures to protect against potential threats and unauthorized access. Therefore, the FM team needs to provide a diverse set of users with their appropriate level of system control and visibility. This creates new work for facility personnel in assigning access control permissions to users and controlling permission levels across the diverse university-wide organization. In an environment like an active research campus, assigning control permissions additionally goes beyond permission control for members of the facility division. Still, it can also include individual researchers and academic professionals who want higher space customization or specificity in their workspaces. The diversity in access control permissions reflects the complexity of this requirement, where permissions may range from basic monitoring capabilities to complete control over system settings, depending on individual circumstances. Therefore, the assignment of access controls is becoming an essential aspect of FM.

### 6.2. Maintaining Firewall and Intrusion Detection Systems for IoT Devices and Controls

*"The university manages all of the security devices, the firewalls, right. So we work with them to maintain the firewall rules and ensure that we have kind of that least privilege, basically block any and only allow traffic that's whitelisted"*

*"Even five years ago, it was just the Wild, Wild West out there. And then security has come front and center recently"*

Maintaining security systems such as firewalls aids in protecting interconnected IoT devices from possible security threats. In IoT management, facility operators work with IT professionals to monitor, manage, and update firewalls and intrusion detection systems to ensure that only authorized personnel and traffic can access device information. In this process, FM personnel work with IT groups to help establish permissions and rules to allow internal groups to bypass firewalls while blocking non-approved users. Although facility personnel are not the developers of security systems, as that task lies within the responsibilities of the University IT department, they are still critical in managing these systems and configuring their access rules and regulations. This creates an essential line of collaboration and communication between IT and FM, within which FM groups provide the logic behind how security systems operate and detect potential harm.

**Conclusion/Study Overview:**

Within the setting of the UW Facilities, this study aimed to understand what new practices are necessary for facility management teams to ensure the technological feasibility of IoT systems. Overall, the findings of this study fall into six categories, as seen in Table 2, including the following:

1. Sensor Configuration
2. Establishing Network Communication
3. Middleware/Supervisory Device Configuration
4. Leveraging the Capabilities of IoT Systems
5. IoT Device/System Lifecycle Management
6. Managing IoT Access Control and Security

Within Category 1, new practices to ensure the technological feasibility of integrated IoT systems include managing diverse vendor-specific software tools and programming/coding responsibilities in device configuration. In Category 2, new required practices include creating and maintaining unique identifier/instance numbers, standardizing communication protocols for device communication, converting existing buildings to IoT control, and integrating third-party devices. Within Category 3, new practices include establishing and implementing logic in supervisory devices for message routing and processing. In Category 4, new practices include system performance monitoring, responsibilities in data analytics, new work in troubleshooting and fault detection, creating and maintaining alerts and notifications, managing diverse vendor-specific user interfaces and applications, vendor management and collaboration, and creating and maintaining data visualizations. Within Category 5, new practices include updating software and sensor lifecycle management requirements. Lastly, in Category 6, new work forms in managing

IoT access control and maintaining firewalls and security for IoT devices and controls. These new practices described in this study serve as best practices to maintain the technological feasibility of integrated IoT systems.

Through interviews and qualitative analysis, we were able to speak with a variety of disciplinary professionals to understand the new challenges that are required to maintain IoT systems adequately. The findings of this report emphasize the importance of continuous learning, collaboration, and adaptability among facilities personnel. Technology develops rapidly, and keeping practice up to date is a difficult task. As IoT technologies continue to evolve, facilities management at UW and similar institutions must remain proactive in adopting these advancements. The insights provided in this report aim to reflect the new practices in maintaining IoT systems from a technical perspective to complement Report One, which analyzes the shifts in organizational practices required for organizations transitioning to IoT building management. In combination, these reports can help guide ongoing efforts in utilizing IoT, ensuring that facilities management practices keep pace with technological advancements and continue to meet the demands of modern building environments.