Securing Real Estate: Wireless Integration and Device Security

Marcus Thuvesen
Abstract

For decades, wired systems have been utilized when connecting operational technology devices to internal real estate systems. With the advancement of new technologies, there is a growing trend toward wireless communication in this domain, necessitating further research and exploration. This thesis examines the security considerations of integrating wireless technologies into operational technology systems within the context of real estate smart properties. It addresses the challenges and opportunities associated with the adoption of wireless communication by examining the built-in security features of Operational Technology devices and the wireless communication techniques LoRaWAN and private 5G networks. Additionally, potential vulnerabilities that may arise with the adoption of wireless communication are examined. The thesis provides a set of recommendations for effective and secure wireless integration relating to network security measures. Another contribution of this study is the type assessment of Operational Technology devices, based on device performance requirements, influencing the choice of network technologies. A categorization of Operational Technology devices into high-security, medium-security, and basic-security levels aids in determining the appropriate security measures for each device. These contributions aim to guide the development of secure, efficient, and sustainable smart properties in the evolving real estate sector.
# Table of Contents

**List of Tables**

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>III</td>
</tr>
</tbody>
</table>

**List of Figures**

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV</td>
</tr>
</tbody>
</table>

**List of Acronyms**

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>V</td>
</tr>
</tbody>
</table>

**1 Introduction**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Introduction</td>
<td>1</td>
</tr>
</tbody>
</table>

**2 Related Work**

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
</tr>
</tbody>
</table>

**3 Smart Properties**

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

**4 Cyber Security in Real Estate**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Encryption</td>
<td>7</td>
</tr>
<tr>
<td>4.2 Error Control</td>
<td>7</td>
</tr>
<tr>
<td>4.3 Monitoring</td>
<td>8</td>
</tr>
<tr>
<td>4.4 Network Segmentation</td>
<td>8</td>
</tr>
<tr>
<td>4.5 Operational Technology (OT) Risk Assessment</td>
<td>8</td>
</tr>
<tr>
<td>4.6 Incident Response</td>
<td>9</td>
</tr>
<tr>
<td>4.7 Built-in Security in OT Devices</td>
<td>9</td>
</tr>
</tbody>
</table>

**5 Wireless Communication Techniques**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 LoRa</td>
<td>12</td>
</tr>
<tr>
<td>5.1.1 Long Range Wide Area Network (LoRaWAN)</td>
<td>13</td>
</tr>
<tr>
<td>5.2 Private 5G Networks</td>
<td>14</td>
</tr>
<tr>
<td>5.3 Vulnerabilities and Threats</td>
<td>15</td>
</tr>
<tr>
<td>5.4 Financial and Sustainability Considerations</td>
<td>15</td>
</tr>
</tbody>
</table>

**6 Methodology**

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
</tr>
</tbody>
</table>

**7 Transitioning to Wireless: A Study of Uppsalahem**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 OT Equipment Types</td>
<td>18</td>
</tr>
</tbody>
</table>

**8 OT Security Categorization and Security Requirements**

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
</tr>
</tbody>
</table>

**9 Security for Wireless Integration of LoRaWAN and Private 5G Networks**

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
</tr>
</tbody>
</table>
Table of Contents

10 Discussion 30
  10.1 Limitations .......................... 31
  10.2 Future Work .......................... 31

11 Conclusion 32

Literature 33
List of Tables

Table 8.1: OT security requirements checklist with security features listed to the left and security categories listed on top. 22
Table 8.2: OT equipment types in relation to OT security categorization. 24
Table 9.1: Implementation guidelines for secure integration of LoRaWAN and Private 5G Networks. 29
List of Figures

Figure 5.1: LoRaWAN Classes ........................................... 13
Figure 8.1: OT Categories ............................................. 21
Figure 9.1: Wireless Protocol Consideration .................... 27
## List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
</tr>
<tr>
<td>LoRaWAN</td>
<td>Long Range Wide Area Network</td>
</tr>
<tr>
<td>LoRa</td>
<td>Long Range</td>
</tr>
<tr>
<td>CSS</td>
<td>Chirp Spread Spectrum</td>
</tr>
<tr>
<td>SF</td>
<td>Spreading Factor</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
</tr>
<tr>
<td>PETs</td>
<td>Privacy-Enhancing Technologies</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation, and Air Conditioning</td>
</tr>
<tr>
<td>BAC</td>
<td>Building Automation and Control</td>
</tr>
<tr>
<td>BAS</td>
<td>Building Automation Systems</td>
</tr>
<tr>
<td>BMS</td>
<td>Building Management Systems</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed-Denial-of-Service</td>
</tr>
<tr>
<td>MITM</td>
<td>Man-in-The-Middle</td>
</tr>
<tr>
<td>NB-IoT</td>
<td>Narrowband Internet of Things</td>
</tr>
</tbody>
</table>
1 Introduction

Operational Technology (OT) [1] refers to software or hardware systems that monitor, detect, or cause changes in physical processes or devices, with a primary focus on control and management of control systems. In the context of real estate, OT can be used to optimize building operations and increase energy efficiency, comfort, and safety for tenants.

The field of OT has been gaining attention in the last decades due to improvements in several technologies like embedded systems, ubiquitous computing, and machine learning [2] [3] [4]. Internet of Things (IoT) refers to physical devices connected to the internet and other devices. In contrast to OT, IoT is focused on collecting and exchanging data between devices over a network, whereas OT is more concerned with the control and management of physical processes and devices. There is an increased focus on the integration of OT systems with other technologies, such as the IoT, to create more intelligent and interconnected systems that can further improve operational efficiency and effectiveness within homes and buildings.

As real estate companies seek to provide high-quality living experiences for their residents and to be able to streamline and enhance the management of their properties, they often resort to wired technology to manage their properties. However, the growing demand for smarter and more efficient properties necessitates a shift towards more advanced solutions, including the integration of OT for monitoring and managing various property functions [1]. More OT devices in the buildings result in an increasing amount of wires needed, hence a wireless solution is suitable to facilitate scale-up and flexibility when it comes to the integration of new OT in the properties. In this context, LoRaWAN, a network protocol designed for IoT applications [5], along with private 5G networks, emerges as a promising solution to enhance connectivity and ensure secure communication in real estate settings.

With the new uprising of OT and the convergence of OT and IoT, prioritizing security considerations becomes important, especially when previously isolated systems are connected to networks. Although OT devices are simple, they are often connected to a company or a private network. If security does not maintain a high standard, this can be an entry point for intruders [6]. Security breaches can result in malfunctioning systems which can affect the physical safety of tenants. Moreover, the data transmitted
may contain sensitive information that can be maliciously exploited, for instance, to access private information or forge data.

To address the main challenges related to the development of next-generation smart properties using wireless technology for OT devices. The following questions will be addressed:

- How can OT devices in the real estate sector be categorized based on their security requirements?

- What are the essential components of a cyber security checklist for different categories of OT devices in smart properties?

- What are the necessary security measures to be included in an implementation guideline for the integration of LoRaWAN and private 5G networks in smart properties?

This study is divided into an investigation phase and a design phase. In the investigation phase, LoRaWAN and private 5G networks will be explored to gain insight into their cyber security functions mapped to real estate companies’ needs. Building upon the investigation phase, a categorization of OT equipment will be made along with the design of an OT security requirements checklist that can be utilized as a part of the procurement process for real estate companies. Additionally, a security review will assess the necessary measures for integrating LoRaWAN and private 5G networks, ensuring robust protection of data and communications.
2 Related Work

According to a report by the accounting firm Ernst & Young, the COVID-19 pandemic sparked a significant digital transformation in the real estate industry [7]. The shift was primarily driven by the need to maintain operations during the pandemic. Nonetheless, real estate companies recognized the potential for technology to build more value in the changed economic landscape. As a result, the industry has rapidly been adopting tech strategies such as data analytics and system integration.

Ernst & Young performed a survey showing that 69% of real estate owners identified technology adoption as a high strategic priority. Moreover, 64% of them cited increased efficiency and reduced costs as the number one reason to adopt new technologies. 87% states that collecting large-scale data and performing analytics is a significant challenge in the industry. This suggests that real estate companies are now open to new technologies which can help solve their data and analytics challenges.

In the report, the author describes that the adoption of technology previously has been a challenge in the real estate sector and that companies have been slow with the integration of new technology. This was due to skepticism, underinvestment, and not seeing the value of new tools. Despite this, industry attitudes have shifted, and real estate companies are now open to deploying technology solutions. However, many companies are unsure about which technologies are best for them. Additionally, he further explains the lack of property technology solutions, making the burden of integrating new systems and platforms fall in the hands of the real estate companies themselves.

Finally, the Ernst & Young report suggests that corporate board decisions can play a crucial role in improving operational efficiencies, creating new products and services, and entering untapped markets through the use of leading tech approaches. To encourage digital transformation in the real estate sector, the report ends with a list of questions intended to aid corporate boards in adopting new technology.

The University of Oulu in Finland conducted a study on the implementation of a wireless LoRaWAN communication system to monitor and regulate the Heating, Ventilation, and Air Conditioning (HVAC) system within their facility [8]. The LoRaWAN technology used in this study was based on the ALOHA protocol [9], which allowed for low-power, long-range communication between nodes. ALOHA is a random access protocol used
for communication in wireless networks. It allows nodes to transmit data whenever they have it, without waiting for permission from a central authority.

The university study concluded that the deployed network was successful in implementing an IoT-enabled use case for monitoring and regulating the HVAC system within the University of Oulu’s facility. Temperature, humidity, CO2 levels, light intensity, and motion data were received from all 331 nodes over a 4-week period, with less than 25% of packets lost for each sensor. However, the study noted that some nodes had a higher packet delivery rate, with less than 0.5% of packets lost. This was due to the strength of wireless signals for nodes located closer to the gateway. Because the signal had to travel a shorter distance, it allowed for better communication. Nodes that were further away from the gateway had a lower rate of successful data packet delivery on average. The study suggests that other factors could be causing this as well, such as a malfunction of the device, interference from other systems, or temporary obstructions affecting radio wave transmission. The findings relating to the variability in successful data delivery imply that signal strength and distance to the gateway should be considered in the implementation of a LoRaWAN network indoors.

Based on the implementation of LoRaWAN technology for monitoring and regulating HVAC systems within a university facility, it can be inferred that this technology has the potential to be applied in the real estate industry for similar purposes. Continuous monitoring and controlling capabilities can preempt inappropriate occurrences before being noticed by humans, while real-time monitoring can enhance internal security. Additionally, external information, such as weather and outdoor environmental conditions, can be utilized to increase performance further.
3 Smart Properties

Smart properties are real estate buildings equipped with automated systems and tools to optimize various functions within buildings [10]. The technologies typically include devices and sensors that can collect, analyze and act upon real-time data. This can improve efficiency, reduce costs and enhance the tenant experience. Building Management Systems (BMS) or Building Automation Systems (BAS) are typical examples of smart property technology which automate the regulation of various building systems [11], including lighting, locking mechanisms, information screens, security cameras, and HVAC which regulates temperature, humidity, and air quality inside buildings [12].

Traditionally, real estate companies have relied on wired OT systems to manage and control various functions within their properties [13]. These systems, while reliable, often lack the flexibility and scalability needed to keep up with the evolving needs of tenants and the rapid pace of technological innovation. As real estate companies expand their property portfolios or accommodate new tenants, scalable solutions that can adapt and grow to increased demands are needed. Wired setups require extensive rewiring, resulting in higher costs and longer implementation times compared to flexible wireless solutions.

Wireless OT technology offers a solution to the flexibility and scalability challenges faced by real estate companies relying on wired OT systems. Wireless systems can be installed and updated more easily and cost-effectively by eliminating the need for physical wiring [14]. They also provide greater flexibility, allowing for the integration of a wider range of devices and systems. This is particularly beneficial in the context of smart properties. Wireless OT technology can also facilitate the collection and analysis of real-time data from various systems and devices within a property.

The transition to wireless OT technology is not without challenges. One of the key concerns is security. As OT systems become more interconnected and accessible over networks, they also become more vulnerable to cyber threats. Therefore, real estate companies must prioritize the implementation of robust security measures to protect their wireless OT systems [15]. Given the essential role that OT plays in ensuring the safe and efficient operation of physical processes, the reliability and availability of these systems are of utmost importance. OT systems are designed to operate continuously and with a very low failure rate over a sustained period of time [16]. High uptime of the
system is a top priority in order for the system to always be accessible and available to users and operators.

Despite the security risks associated with the transition to wireless OT technology, the benefits of wireless OT technology make it a compelling choice for real estate companies looking to enhance their properties and stay competitive in the digital age. An example is Uppsalahem, a prominent Swedish real estate company. Uppsalahem has recognized that the integration of wireless solutions with high levels of IT security and standardized protocols is a critical step in the development of next-generation smart properties. Uppsalahem operates over 17,000 residential units in and around Uppsala City [17], one of the more populated cities in Sweden. In the context of Uppsalahem, the need for additional sensors and better monitoring of the facilities has grown. Hence, a wireless solution is to be integrated with the current wired solution, aiming at a cost-beneficial and effective operation of the properties.
4 Cyber Security in Real Estate

With the increasing adoption of OT in managing and controlling real estate assets, there comes a great need for robust cyber security measures to protect assets. Several mechanisms are involved in real estate cyber security [18]. Each plays a contributing role when ensuring the confidentiality, integrity, and availability of systems and facilitating secure communication among devices and networks.

4.1 Encryption

With the advancements of modern connected OT, the need for built-in encryption in devices is becoming increasingly essential to ensure data confidentiality and integrity to mitigate the risk of cyber threats [19]. Encryption transforms data into an unreadable format, ensuring that only authorized parties with access to decryption keys can read it [20]. Both LoRaWAN and 5G networks incorporate built-in encryption protocols to ensure data security [21] [22].

While having encryption in the communication channels is essential for securing data in real estate OT systems, it is worth noting that some OT devices lack built-in encryption capabilities [23] [24]. Building Automation and Control (BAC) systems, typically used for managing and monitoring different building systems including lighting, elevators, and HVAC, are examples of legacy OT systems that may lack proper encryption [25]. This can be due to factors such as cost savings or the fact that older OT equipment was not designed for wireless connections and networks, reducing the risk of intrusions and making device-level encryption unnecessary.

4.2 Error Control

Error control is essential to maintain the accuracy and reliability of data transmitted between different devices and systems in real estate OT [26]. Error control uses mechanisms such as parity checking, checksums, and error-correcting codes to detect and correct errors during data transmission. This helps to ensure that data is received accurately and in order, reducing the risk of system failures that could arise from data corruption. However, error control mechanisms are not completely immune to cyber...
attacks, and malicious actors can intentionally introduce errors to compromise data integrity and disrupt the system’s functionality. Therefore, it’s important to implement monitoring protocols in addition to error control mechanisms to cover a wider range of errors.

4.3 Monitoring

Monitoring allows continuous observation of system behavior to detect and respond to anomalies that may indicate potential cyber threats, misuse of the system, or malfunctions [27]. The use of real-time alerts, system logging, and network traffic analysis can help identify security breaches, enabling security personnel to take appropriate action in a timely fashion. Monitoring real estate OT systems can be challenging due to the distributed nature of the systems and the number of sensors and devices used in buildings. Centralized management systems, automated monitoring, and threat detection tools can help overcome these challenges.

4.4 Network Segmentation

Network segmentation involves dividing a network into several subnets that function as individual entities within the larger network [28]. By creating isolated subnets with separate security policies, network segmentation offers several advantages, such as improving network performance, addressing network issues, and enhancing monitoring capabilities. Companies employing subnets can control access to sensitive data and applications, making it more challenging for unauthorized individuals to gain access. Additionally, network segmentation can help limit the spread of security threats by containing them within specific subnets and reducing the damage caused by a security breach.

4.5 OT Risk Assessment

In real estate, risk assessments for OT systems are used for identifying potential vulnerabilities and protecting against cyber attacks [29]. These assessments evaluate the components and operational processes of the system, identify potential threats, and suggest ways to mitigate them. Identifying assets, defining risk scenarios, assessing likelihood and impact, and implementing control measures are key steps in the process. In addition, it’s important to consider the devices, systems accessed, data, network infrastructure, and potential impact on occupants and overall functionality. Conducting a thorough risk assessment enables real estate organizations to understand vulnerabilities.
and implement effective security measures to safeguard their assets from potential cyber threats.

4.6 Incident Response

Having an incident response plan is needed to reduce the impact of cyber attacks targeting OT or networks [30]. These plans involve a coordinated approach to identify, contain, eradicate, and recover from a security incident. Real estate companies should have a well-defined incident response plan that outlines roles and responsibilities, communication channels, and escalation procedures to minimize the impact of a security breach. In case of an incident, a rapid response can help minimize asset damage, prevent data loss, and maintain the trust of tenants.

4.7 Built-in Security in OT Devices

In addition to securing communication channels from OT equipment to the network, one should also consider the security of each individual end device. Therefore, when evaluating the security of a specific end device, the following security features should be taken into account.

Secure Boot Process: One potential security concern is the possibility that a malicious actor could install an unauthorized operating system or boot software on a device [31]. To address this threat, it is important to implement a secure boot process that verifies the integrity of the device’s firmware before allowing it to start up. This can be achieved by incorporating a pre-installed authenticator code into the device’s hardware, which authenticates the system code against the hardware. By taking these steps, the device can be better protected against unauthorized modifications that could compromise its security or functionality.

Secure Firmware Updates: Firmware updates are essential for maintaining operational technology OT equipment, as they allow manufacturers to address existing bugs, vulnerabilities, and enhance overall performance [32]. Nevertheless, unsecured updates can leave devices vulnerable to adversaries who may exploit the process and inject malicious code. To minimize this risk, implementing code signing is both beneficial and necessary. By adopting code signing, manufacturers ensure that any new update for the OT device includes a signature generated by a trusted key holder. While this signature cannot be forged, it can be verified by the OT asset, providing an additional layer of security against potential threats.
Encryption and Error Control: As mentioned earlier in this section, encryption is the backbone of the security of OT devices [20] [33]. All data on the device should be properly handled and encrypted before it is transmitted onto the network. This not only ensures the confidentiality of sensitive data but also helps maintain the integrity and availability of the device. Error control is another great advantage in the context OT devices [26]. By implementing error control mechanisms in the encryption process, data transmission errors can be detected and corrected.

Tamper-resistance: One of the first layers of security of a OT device involves placing them in hard-to-reach locations and ensuring that the device is designed to withstand tampering, even if unauthorized individuals gain physical access. To accomplish this, several strategies can be implemented:

- Incorporate tamper-resistant materials and designs: Employing materials and designs that necessitate specialized equipment or tools for access can substantially impede unauthorized efforts to tamper with the device [34]. This could involve using secure enclosures, tamper-evident seals, or designs that either self-destruct or erase sensitive data upon detecting tampering. One example is the use of specialized fasteners. By integrating screws with distinctive, custom drives, unauthorized individuals attempting to open the device with standard tools will find it difficult, thus deterring tampering attempts [35].

- Implement chip-level data encryption: Encrypting data within individual chips inside the device makes it challenging for adversaries to access sensitive information, even if they manage to breach the device [36].

Minimal Functionality: The OT device should only provide the necessary functionality to perform its intended task and not allow any other operations [16]. This reduces the surface of vulnerability. A single-function OT device is less susceptible to attacks than a multi-purpose device. Ideally, the device should be designed to only be able to serve a specific intended purpose.

Access Control: Access control within OT assets and networks helps to ensure that only authorized individuals or systems can access specific resources [37]. For example, various building systems may have access control features to limit access to sensitive system settings based on user roles and permissions. In addition to the improved security of the resources, access control also helps to monitor access to these resources. This is important for detecting potential security breaches, unauthorized access attempts, and necessary actions that can be taken based on these warnings.
Endpoint Protection Platform: By installing an endpoint protection platform, real estate companies can monitor network traffic to identify suspicious activity within the devices [38]. The traffic can be analyzed for certain patterns to detect anomalies or compare the activity to known attack signatures. This helps in detecting and responding to security incidents promptly, mitigating potential damages caused by cyber threats.

Redundancy: To enhance reliability, the introduction of redundancy in devices is helpful [39]. This entails duplicating critical components or functions within a device. By implementing redundancy, if one component or function fails, backup components or redundant systems can take over, ensuring uninterrupted operation and minimizing downtime. This creates a fail-safe environment that allows devices to continue functioning without any disruptions, thereby increasing the reliability and resilience of OT systems.
5 Wireless Communication Techniques

Several wireless communication options are available when transitioning from wired to wireless OT in real estate [40]. These alternatives include technologies such as Narrowband Internet of Things (NB-IoT) [41], Zigbee [42], and Z-wave [43], each offering its own unique benefits and use cases. LoRaWAN and private 5G networks stand out as particularly compelling options [44]. Their unique strengths, including LoRaWAN’s long-range, low-power communication capabilities, and 5G’s high data rate and low latency, can be leveraged to build an all-encompassing wireless OT solution. Both protocols also ensure high-security standards during data transmission. These factors make LoRaWAN and 5G particularly suitable for diverse wireless OT applications in real estate, where security, extended range, efficient power usage, and high-performance communication are essential requirements.

5.1 LoRa

Long Range (LoRa) is a radio communication technique designed by the LoRa Alliance [5]. It targets devices that require the ability to send small amounts of data over long distances, using minimal power. Its long-range, low-power characteristics make it ideal for use in OT applications where devices are spread across a wide area in challenging environments with obstacles like buildings and trees.

LoRa uses Chirp Spread Spectrum (CSS) [5] to modulate symbols over a defined license-free frequency spectrum. One of the key features of LoRa is its ability to adjust data load and transmission time based on the specific requirements of the use case. This is made possible through a parameter known as Spreading Factor (SF), which dictates the bits sent per symbol, thus making the data load and transmission time adjustable for its intended purpose. A higher SF results in slower communication but has a longer range, whereas a lower SF achieves a lower range but increases data rate and has lower energy consumption [8]. While the maximum distance for LoRa communication is up to over 830 km [45], the practical range is often reduced due to the presence of obstacles such as buildings, trees, and other materials [46]. Under practical conditions, the maximal range for LoRa communication in dense rural areas is estimated to be approximately 2 kilometers. However, when the antenna is installed in less dense areas, the maximum range can be extended up to 5 kilometers [5].
5.1.1 LoRaWAN

LoRaWAN [5] defines a network layer that can be used on top of the physical layer of LoRa. LoRaWAN acts as a communication protocol between end devices and gateways. One of the more important aspects of the protocol, as established by the LoRa Alliance, is the three different device classes.

- **Class A** is implemented by all end devices and enables them to initiate a transmission. This is typically used by sensors or measurement devices such as heartbeat monitors.

- **Class B** is used for beaconing. The network sends a beacon at fixed intervals via the gateway, which is then received by the end device, causing it to wake up and receive the message.

- **Class C** provides continuous downlink capability, whereby the end device actively listens for incoming messages. This consumes more battery power, making this solution temporary, or the end device may need to be connected to a power source.

Figure 5.1 demonstrates that both Class A and Class B have Rx2 receiver windows scheduled for specific intervals when devices wake up to receive data. Outside of these windows, the devices enter a low-power sleep mode, effectively reducing energy consumption. Class C devices have an active receiver window, continuously listening for incoming data, reducing latency but also increasing energy consumption.

LoRaWAN provides end-to-end data encryption [5]. The security is mainly provided by the network and application layer. LoRaWAN also uses two Advanced Encryption Standard (AES) 128-bit session keys, the AppSKey and NwkSKey. The AppSKey is a symmetric key used for encryption, which is shared by the application owner and the
end device. The key is used to encrypt the message before it is transmitted over the air. The NwkSKey, on the other hand, is used to calculate message integrity by comparing the previous payload to the network header of the current message.

5.2 Private 5G Networks

Private 5G networks refer to wireless communication networks that utilize 5G technology within an organization or company. These networks are owned and managed by the organization itself, offering enhanced reliability, manageability, and flexibility that can be tailored to meet specific business needs. In contrast, public 5G networks are operated by telecommunications companies and offered to compatible customers [48]. 5G technology represents the latest generation of cellular networks and serves as the successor to the widely used 4G network. Instead of relying on lower frequency bands, 5G operates in the higher frequency spectrum leveraging higher bandwidth and millimeter waves, to facilitate communication between end devices and the telephone network [49]. While millimeter waves offer superior throughput and capacity, they can be drastically weakened when attempting to pass through buildings and walls and thereby limit the range of the network [50].

5G networks rely on wireless communication and can therefore be vulnerable to security threats, such as interception, eavesdropping, and data tampering. The 5G communication protocol has built-in security mechanisms which offer Authentication, Access Control, Network Slicing, and Privacy.

- **Authentication** is typically provided by user authentication protocols, such as Extensible Authentication Protocol (EAP), requiring a user to have valid credentials to access the network.

- **Access Control** regulates and restricts access within the network based on the user type, device, and type of traffic. This can be achieved by Network Access Control (NAC) and firewalls.

- **Network Slicing** is a technique that partitions the network into separate virtual networks. Each network can then have its own set of security rules and policies.

- **Privacy** is achieved through built in encryption and Privacy-Enhancing Technologies (PETs) to protect the communication from interception and eavesdropping [51].

One of the major advantages of having a non-public 5G network is that the organization can control, adjust and further build upon the built-in security measures to accommodate the specific needs of the industry or regulatory environment in which the organization is in [52].
5.3 Vulnerabilities and Threats

Despite the built-in security features of both LoRaWAN and 5G, the communication protocols may still be susceptible to specific vulnerabilities and threats. Some of these threats include Distributed-Denial-of-Service (DDoS), Unauthorized Access, Man-in-The-Middle (MITM) and Firmware vulnerabilities.

DDoS attacks occur when a malicious actor overwhelms the networks with traffic, rendering it unusable or unavailable [27]. This attack is seen as a relatively unsophisticated attack but the consequences of a successful attack can often be highly noticeable to end users. Unauthorized Access poses a threat to systems when cybercriminals attempt to gain access to the networks by exploiting weaknesses in credentials or authentication mechanisms [53]. MITM is another method to intercept and manipulate communication between devices and networks [54]. The risk of this threat can increase when going from wired systems to wireless systems and can be very harmful in the context of real estate as it could compromise the integrity of data from IoT and OT devices. Firmware vulnerabilities can be present, implying that devices and sensors may be susceptible to firmware-level attacks, which exploit weaknesses in the underlying software operating on these devices [55]. This threat is particularly crucial to consider when converging OT with IT, as numerous OT devices were not designed with security in mind, often assuming they would operate within an air-gapped environment [6].

5.4 Financial and Sustainability Considerations

When it comes to costs regarding the implementation of LoRaWAN and 5G networks, several factors have to be taken into account. These include initial investment, ongoing operational expenses, maintenance, and cost savings.

The upfront costs for implementing LoRaWAN and private 5G networks involve the expenses related to procuring hardware such as gateways, base stations, and access points, as well as the costs of licensing fees and labor for installation [56]. LoRaWAN is generally viewed as more cost-effective due to its simpler infrastructure and the utilization of an unlicensed spectrum, which reduces expenses [57].

Regarding operational expenses, both LoRaWAN and private 5G networks entail ongoing costs, encompassing network management, monitoring, and support. LoRaWAN’s energy-efficient design may result in lower operational costs than private 5G networks [58]. Additionally, since 5G networks operate in a licensed spectrum, there are associated costs, and they might require more sophisticated support and maintenance [56]. Scalability is another factor to consider. LoRaWAN is often perceived as easier to scale by simply adding more gateways, whereas private 5G networks may need further investments in
infrastructure, such as additional base stations and small cells, to ensure comprehensive coverage and capacity [59].

Another aspect to be considered is the low environmental impact of using LoRaWAN. LoRaWAN’s low energy consumption offers real estate companies a significant environmental advantage [60]. Firstly, LoRaWAN devices operate with minimal energy consumption, allowing them to run on batteries for extended periods without frequent replacements [61]. This reduces resource consumption energy consumption. Also, LoRaWAN’s technology enables wide coverage with fewer gateways, resulting in lower energy consumption during installation, operation, and maintenance [5]. Additionally, LoRaWAN devices spend most of their time in a low-power sleep mode. This operation significantly reduces energy consumption. [60]
6 Methodology

In order to address the challenges associated with the transition from isolated OT environments to wireless solutions and investigate the security measures for OT devices, a two-phase methodology consisting of an investigation phase and a design phase was used. In the investigation phase, interviews were conducted with a Swedish real estate company to gain valuable insights into their practices in the field. This was followed by a literature review, which aimed to gather additional insights into the standards of OT security and the security aspects related to the integration of wireless OT. The design phase built upon these findings to categorize OT devices and to propose effective security measures for wireless OT integration in the real estate sector.

In the investigation phase, interviews with the information security coordinator at Uppsalahem were conducted. Uppsalahem is a real estate company, operating in Uppsala, a city located in Sweden. With over 17 000 residential units in and around Uppsala, Uppsalahem makes a significant contribution to the city’s housing infrastructure. The interviews provided knowledge of their current wired OT infrastructure, relevant OT types, and wireless technologies. This was important to gain knowledge into the current state of real estate companies in their integration of wireless OT in a real-life scenario. In light of the new knowledge obtained from the interviews, a literature study was carried out to evaluate the suitability of utilizing LoRaWAN and private 5G networks for OT applications in the real estate industry with a strong focus on security.

In the design phase, based on the information gathered during the investigation phase, OT devices were categorized according to their security needs. This categorization allowed for an understanding of the security requirements of different types of OT devices used in the real estate sector. By categorizing the devices, it became possible to design a security checklist for built-in security in OT, to ensure the protection of devices in each category. Building upon the insights from Uppsalahem relating to wireless security along with the literature study on LoRaWAN, 5G networks, an implementation guideline for secure wireless integration was established.
7 Transitioning to Wireless: A Study of Uppsalahem

Uppsalahem [62], a Swedish real estate company located in Uppsala, has been leveraging OT in its properties for several decades. The OT systems monitor and manage a variety of functions, including ventilation, heating, water, and access systems. These systems are interconnected through Uppsalahem’s wired property technology network, which has demonstrated its practicality and reliability over the years. However, as Uppsalahem strives to modernize its properties and incorporate more advanced technology, the existing wired solution has started to show its limitations. The company is looking to add new features and capabilities to its properties, reduce the costs associated with implementing these upgrades, and gain more understanding of its property operations. To achieve these goals, Uppsalahem recognizes the need to integrate wireless solutions that offer high levels of IT security and use standardized protocols with its existing systems.

Uppsalahem finds wireless technologies such as LoRaWAN and private 5G networks particularly suitable for their purpose. These technologies offer the necessary range, bandwidth, and security features that make them ideal for large-scale real estate applications. They can support a wide variety of OT devices and sensors, enabling Uppsalahem to implement a diverse range of smart building applications.

In essence, Uppsalahem is seeking a transition from a wired to a wireless infrastructure for its OT systems. This transition is aimed at not only enhancing the functionality and efficiency of the properties but also keeping the security and standardization of the technology solutions.

7.1 OT Equipment Types

During discussions with IT personnel at Uppsalahem, the trade-off between device speed and range became apparent. This trade-off is relevant to the OT equipment used by real estate companies due to the impact it has on the effectiveness and functionality of the OT employed. Such equipment can be categorized into two main types based on their applications and characteristics: High-Speed, Low-Latency OT and Long-Range, Low-Power OT.
**High-Speed, Low-Latency OT:** These are devices that require low latency, high throughput, and real-time monitoring. Relevant systems include surveillance cameras and smart locks [63].

**Long-Range, Low-Power OT:** These are devices that should be able to communicate and operate over longer distances and do not require high data rates or low latency [64]. Relevant systems include HVAC, energy and water consumption sensors, info-graphic screens, smart lighting, waste management, and parking management.
8 OT Security Categorization and Security Requirements

As the majority of OT are connected to a company network, security is of high importance for all types of OT. The specific nature of the OT device and the sensitivity of its stored data often demand enhanced cyber security measures, beyond standard protocols, to effectively counter potential data breaches. Based on the work presented in Section 4 of this thesis, a real estate OT device categorization has been devised. This categorization divides the devices into High-security, Medium-security, and Basic-security.

The assignment of the three categories is determined by considering the overall security importance of the devices and the corresponding level of security measures required. The device’s importance is determined by to what degree of confidential and sensitive data it handles. This data could include sensitive tenant details or building operational information. The potential fallout from a security breach also determines the required security level. The greater the possible impact, the more robust the necessary security measures. The three categories reflect the varying degrees of sensitivity and criticality of the devices within the real estate environment.

**High-security:** This category consists of OT devices that demand the utmost level of security measures due to their critical nature and sensitivity. These devices are involved in handling highly confidential and sensitive data. Devices in this category include devices that handle information that is of significant importance to the organization and potential unauthorized access, loss, or modification of this information could cause substantial harm to the organization or tenants. Examples of such devices are surveillance cameras, access control systems, smart locks, elevators, and BAC. The protection of these devices is crucial to safeguard the integrity and privacy of the real estate.

**Medium-security:** While the OT in this category handle important data and contribute to the overall security of the real estate, their criticality is not as high as the devices in the high-security category. Examples of devices in this category may include environmental sensors, info-graphic screens, and smart lighting. Smart lighting may play a role in enhancing security by allowing scheduled or remote control of lighting. The direct impact on physical security makes the device more critical than Basic-security devices.
OT Security Categorization and Security Requirements

Figure 8.1: Categories of OT devices in real estate based on required security.

**Basic-security:** The basic-security category includes OT devices that require fundamental security measures. These devices handle non-sensitive or non-critical data, but it is still important to implement basic security considerations to ensure the overall security of the real estate. Examples of devices in this category could be simple environmental sensors and straightforward monitoring devices such as waste management, and parking management sensors.

A visual representation of the categorization of OT based on their security requirements is shown in Figure 8.1. The three categories: High-security, Medium-security, and Basic-security, are each accompanied by examples of real estate OT devices that align with the specific security level. Comprehending these categories and identifying the group to which each device belongs can enable real estate companies to apply appropriate security measures in a cost-efficient manner within their buildings. High-security OT devices often entail higher costs, so deploying them where they are most needed can result in substantial cost savings. Medium and basic-security devices can often be effectively safeguarded with less costly measures, further contributing to cost reduction.

Understanding the security importance of each device helps in risk management. Especially the high-security devices, if compromised, could cause a lot of damage, affect the availability of the services and potentially leak private data. Thus harming the reputation of the company. By putting extra security focus on these devices, real estate companies can manage their risk and prevent major security incidents.

The cyber security requirements for OT devices vary depending on the device category. High-security, devices such as surveillance cameras require extra security measures to prevent unauthorized access, while basic-security devices like environmental sensors need more emphasis on data encryption and minimal functionality. Thus, it should be noted that it is important to assess the cyber security needs for each category of
Table 8.1: OT security requirements checklist with security features listed to the left and security categories listed on top.

<table>
<thead>
<tr>
<th>Security Category</th>
<th>Basic-security</th>
<th>Medium-security</th>
<th>High-security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Minimal Functionality</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Secure Protocol Support</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access Control</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Secure Boot Process</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Secure Firmware Updates</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Error Control</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Tamper Resistance</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Endpoint Protection Platform</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Redundancy</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

OT equipment, considering their specific applications, characteristics, and associated risks.

Table 8.1 presents an OT security requirements checklist based on the investigation phase. The checklist is intended to act as a hands-on guideline when it comes to what requirements are needed for what security category. To avoid having devices with inadequate security acting as a gateway into the network, even the Basic-security category has a relatively high security threshold. The checklist is designed to be flexible and adaptable to different scenarios, budgets, and environments. It serves as a guideline, and the specific security measures implemented may vary depending on the specific circumstances and needs of the real estate company.

The security categories in the OT security requirements checklist represented in Table 8.1 are designed in a cumulative manner, where each category incorporates and builds upon the security measures of the preceding category.
**Basic-security:** These devices require fundamental security measures such as encryption, limited functionality, secure protocol support, access control, and if possible, secure boot process. These measures form a foundation of device protection, designed to protect the device and its data from basic threats and unauthorized access.

- **Encryption:** Ensures secure protection of transmitted data, safeguarding the confidentiality of sensitive information.
- **Minimal Functionality:** Reduces attack surface by restricting device functionality to essential operations, minimizing vulnerabilities.
- **Secure Protocol Support:** Implements secure communication protocols to establish encrypted and authenticated connections, ensuring data security during transmission.
- **Access Control:** Prevents unauthorized access to device functionalities and sensitive information through strong authentication and authorization processes.
- **Secure Boot Process:** Verifies the integrity and authenticity of the device’s firmware during the boot-up process, preventing the execution of unauthorized or modified firmware.

**Medium-security:** In addition to the basic security measures, these devices also require secure error control and secure firmware updates. Error control ensures that the data keeps its integrity, avoiding data corruption or manipulation. Secure firmware updates add an extra layer of protection against firmware attacks.

- **Error Control:** Essential for medium-security devices, error control mechanisms detect and correct transmission errors during data transfer. They safeguard the integrity of operations and data, providing protection against data corruption or manipulation.
- **Secure Firmware Updates:** Addresses vulnerabilities and enhances device performance, regular and secure firmware updates ensure trusted and untampered updates from the manufacturer. Secure firmware updates can combined with a secure boot process mitigate firmware attacks. The implementation of secure firmware updates often relies on an established secure boot process. Also, only a limited number of manufacturers for simpler OT devices and sensors offer these secure updates. These two factors largely contribute to the placement in the Medium-security category.
Table 8.2: OT equipment types in relation to OT security categorization.

<table>
<thead>
<tr>
<th>OT Type</th>
<th>Security Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Basic-security</td>
</tr>
<tr>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>-</td>
</tr>
<tr>
<td>Range</td>
<td>Simple environmental sensors</td>
</tr>
<tr>
<td></td>
<td>Waste management sensors</td>
</tr>
<tr>
<td></td>
<td>Parking management sensors</td>
</tr>
</tbody>
</table>

**High-security:** These devices require all the security measures of the previous categories, plus error control and tamper resistance. Error control is crucial for these devices as it ensures the integrity of their operations and data. Tamper resistance provides physical protection to the device, preventing unauthorized modifications.

- Tamper Resistance: High-security devices employ tamper resistance mechanisms, such as secure enclosures, special screws, seals, or tamper detection sensors, to prevent unauthorized access or modifications. These measures maintain device integrity and promptly detect and report any unauthorized tampering.

- Endpoint Protection Platform: Entails installed security software at the device level. Includes extra monitoring for high-security devices and enhances the chances of detecting malicious activity or intrusions within the device’s traffic.

- Redundancy: Adds a duplicate of critical components or functions in a device. This increases the reliability of the device and creates a fail-safe environment where vital devices can continue to function even if one component fails, ensuring uninterrupted availability of services or functionality.

It’s important to note that while this checklist provides a good foundation, real estate companies should conduct a thorough risk assessment and consider their specific needs and constraints when deciding on the appropriate security measures for their OT devices. For instance, secure firmware updates and secure boot processes are effective mitigation measures for firmware attacks. Both measures when installed, tend to result in more overhead and increased device costs. In some cases, they may be limited to high-security devices based on risk tolerance, budget considerations, and the availability of devices conforming to these measures in the market.

_Uppsala University_
In order to have a functional operating smart property, the efficiency, provided by the network protocol, and the security, provided by security measures listed in Figure 8.1, need to harmonize. Table 8.2 illustrates the relationship between OT equipment types (Section 8.2) and security categories.

The relationship between underlines the balance between efficiency and security within smart properties. High-speed equipment, such as surveillance cameras, smart locks, and elevators, require the High-security measures due to the criticality of their functionalities. Equipment that operates over a longer range, such as simple environmental sensors, waste management sensors, and parking management sensors, typically necessitates lower-tier security measures.

The pattern evolving from Table 8.2 indicates a potential correlation between the operational requirements of OT equipment (speed contra range) and their security categorization. Specifically, equipment demanding high-speed performance also seems to necessitate higher levels of security, potentially suggesting a connection between the critical nature of their functions and high-speed requirements. This can be explained by the fact that devices that require high speed often do so because of their critical nature, which also classifies them in the high security category. In contrast, equipment with a broader operational range tends to have lower security requirements, due to their generally less critical roles.
9 Security for Wireless Integration of LoRaWAN and Private 5G Networks

Based on the investigation and vulnerability assessment of LoRaWAN and private 5G networks, a set of security recommendations and measures have been formulated regarding wireless integration. These recommendations address the specific security challenges associated with the integration of wireless networks in smart properties. To ensure a secure integration, it is important to consider the specific OT equipment types previously discussed: High-Speed, Low-Latency, and Long-Range, Low-Power. Deciding which network to utilize after assessing which type the specific device belongs to, is straightforward. For High-Speed, Low-Latency OT devices, 5G networks can provide the necessary low-latency communication. For Long-Range, Low-Power OT devices, LoRaWAN networks offer long-range connectivity and low-power operation. Both solutions offer built-in security features for safe data transmissions.

As shown in Figure 9.1, by filtering the OT type based on its requirements for speed and range, real estate companies can make informed decisions about the suitable wireless technology (5G or LoRaWAN) for each device type. This approach ensures that the integration of wireless networks and security measures is tailored to the specific needs of the devices, promoting a secure, cost-effective, and efficient environment within smart properties.

For LoRaWAN, the key security features include end-to-end data encryption, device classes, and AES 128-bit session keys. Enabling encryption with AES 128-bit session keys ensures secure communication between devices and gateways.

Private 5G networks offer a range of security features such as authentication, access control, network slicing, and privacy enhancements. Robust authentication mechanisms should be implemented to verify the identity of devices and users accessing the network. Access control policies need to be defined to determine authorized access and modification of network resources. Network slicing enables the creation of isolated virtual networks with dedicated resources and security measures for different applications or tenants. Privacy enhancements, including techniques to protect sensitive information and mitigate unauthorized access, should also be implemented.

Based on the analysis and vulnerability assessment conducted in the first phase, a set of security recommendations and measures have been formulated when integrating...
Figure 9.1: The process of choosing LoRaWAN or Private 5G Networks based on the type of OT equipment.
wireless networks. To make the integration end-to-end encrypted from OT device via the wireless network and into the company network, security measures are needed at the receiving end of the data transmission inside the company network. The implementation guideline in Table 9.1 outlines these measures, providing strategies for secure integration.

The security measures outlined provide strategies for addressing vulnerabilities when integrating LoRaWAN and private 5G networks. Network configurations are a key factor in securing these integrations. By creating distinct network segments and employing zoning and firewalls, real estate companies can better manage traffic and limit unauthorized access. Also, using secure communication protocols for data encryption within the network helps maintain data integrity and confidentiality.

Authentication mechanisms form another important part of these security measures. Effective authentication is necessary to confirm the identity of devices and users accessing the networks. In addition, enforcing unique, strong passwords and considering the use of multi-factor authentication can considerably reinforce the overall security of these network systems.

Encryption protocols, with end-to-end encryption for data between devices and gateways, add an extra layer of data protection. The use of strong encryption algorithms, like AES, along with regular updates of encryption keys helps reduce the risk of unauthorized decryption and potential data breaches.

Access control policies are also key to managing access and modification privileges within the network. Role-based access control allows for specific access rights based on the roles and responsibilities of different users, providing a level of control and reducing the risk of unauthorized access or modifications.

Lastly, having a well-defined incident response plan is necessary for effectively handling security incidents. This plan ensures that when an incident occurs, the response is quick, efficient, and minimizes potential damage to the network and devices connected to it.

When these measures are properly implemented, they will greatly improve the security of integrating LoRaWAN and private 5G networks in the context of smart properties.
Table 9.1: Implementation guidelines for secure integration of LoRaWAN and Private 5G Networks.

<table>
<thead>
<tr>
<th>Security Measure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Configurations</td>
<td>Establish clear network segments and boundaries to isolate components.</td>
</tr>
<tr>
<td></td>
<td>Utilize network zoning and firewalls to regulate traffic flow and restrict unauthorized access.</td>
</tr>
<tr>
<td></td>
<td>Configure secure communication protocols for data encryption within the network.</td>
</tr>
<tr>
<td>Authentication Mechanisms</td>
<td>Implement robust authentication mechanisms for devices and users accessing OT systems.</td>
</tr>
<tr>
<td></td>
<td>Enforce the use of unique and strong passwords for each device and user account. Enhance security with complex and unique passwords.</td>
</tr>
<tr>
<td></td>
<td>Consider implementing multi-factor authentication for stronger access credentials.</td>
</tr>
<tr>
<td>Encryption Protocols</td>
<td>Enable end-to-end encryption for data between devices and gateways.</td>
</tr>
<tr>
<td></td>
<td>Utilize robust encryption algorithms (e.g., AES) for data protection. Ensure strong encryption for data security.</td>
</tr>
<tr>
<td></td>
<td>Regularly update encryption keys to minimize the risk of unauthorized decryption.</td>
</tr>
<tr>
<td>Access Control Policies</td>
<td>Define comprehensive access control policies for authorized access and modification privileges.</td>
</tr>
<tr>
<td></td>
<td>Implement role-based access control for appropriate access rights based on roles and responsibilities.</td>
</tr>
<tr>
<td>Incident Response Plan</td>
<td>Develop a well-defined incident response plan for effective handling of security incidents.</td>
</tr>
</tbody>
</table>
10 Discussion

The study relating to built-in security features of OT equipment revealed that some legacy systems are still in use, especially in older buildings. While these systems might be secure while connected by wire, they are likely not to have sufficient security if they were to be integrated with wireless technology. The OT would need greater built-in security features as the attack surface increases with the wireless connection.

The categorization of OT security significantly simplifies the process of determining necessary security features for each device. This method aids in directing resources effectively toward devices that demand strong built-in security. Although it would be ideal for all devices to adhere to the High-security standard, real-world constraints like budget limitations often call for compromises. In these instances, the checklist can be utilized as a valuable tool, assisting organizations in upholding a secure OT environment while staying within their financial boundaries.

The simplification of OT types also raised questions about some devices that don’t easily fit into either High-Speed, Low-Latency, or Long-Range, Low-Power. Some devices may land somewhere in between, requiring a balance between speed and range. In such instances, the organization is faced with a decision that necessitates careful consideration of various factors, including cost and speed. From a cost perspective, it is recommended to consider LoRaWAN as the preferred option whenever feasible, especially for Long-Range, Low-Power OT applications. It is generally advisable to avoid private 5G networks in cases where LoRaWAN can adequately meet the requirements, as it offers a more cost-effective solution. If speed is more of an essential factor for the specific device, the device should be integrated with the 5G network.

Another consideration relating to deciding which network to use is the sustainability aspect. As more companies and organizations seek to reduce their climate impact, lower power consumption from the internal networks can be a way to achieve this goal. The use of energy-efficient technologies like LoRaWAN can significantly reduce the overall power consumption of a smart property’s internal network systems. This contributes to the organization’s broader sustainability efforts. Additionally, incorporating renewable energy sources for powering these networks could further enhance their eco-friendliness.

In the context of a real estate company, the categorization of OT devices into High-security, Medium-security, and Basic-security is not a one-size-fits-all approach. It
should be tailored to the unique characteristics of the building, the devices used, and the specific requirements of the company. For instance, a high-rise office building might have more high-security devices, such as surveillance cameras or access control systems, compared to a small residential building. Moreover, an individual company’s risk tolerance, budget, and security policies would further influence the assignment of devices into these categories.

10.1 Limitations

An inherent limitation in any study dealing with security is that the advancement and increasing sophistication of artificial intelligence (AI) poses both opportunities and challenges for cyber security. AI can significantly enhance cyber security measures by automating threat detection and response, predicting potential vulnerabilities, and improving the overall efficiency of security systems. AI also presents new threats to cyber security. Cyber criminals are increasingly leveraging AI to carry out more sophisticated and targeted attacks. This includes using AI to automate hacking attempts and exploit vulnerabilities in security systems. These emerging threats were not addressed in this study, which could limit the completeness of the findings in the upcoming cyber security landscape.

10.2 Future Work

Based on this work, a study could be conducted to analyze the performance, cost-effectiveness, and security of network technologies other than LoRaWAN and private 5G networks. Additionally, future work could investigate how the choice of network technology impacts the development and performance of smart properties. This could include aspects like functionality, user experience, and maintenance costs. Furthermore, given the increasing role of AI in cyber security, the impact of AI on the cyber security landscape should also be explored. This could involve studying how AI can be leveraged to enhance cyber security measures, as well as how to mitigate the new threats posed by AI. Such research could provide valuable insights into how to navigate the evolving cyber security landscape and ensure the security of smart properties in the face of emerging AI threats.
11 Conclusion

With a new real estate security landscape relating to a transition from wired OT systems to wireless OT systems, the aim of the thesis is to provide a guideline for secure integration of a new wireless system from end-device via wireless communication into the company network. To answer the problems related to new security considerations, a literature review was carried out in the investigation phase, with the initial focus on the security features of OT equipment. The subsequent phase of the review centered on the cyber security capabilities of LoRaWAN and private 5G networks, with the objective of gathering knowledge of how these technologies could align with real estate companies, such as Uppsalahem, in their pursuit of smarter properties without compromising on security. During the investigation phase, valuable and significant insights were obtained regarding the cyber security standards and OT equipment security in the real estate sector.

The security review of the integration measures for LoRaWAN and private 5G networks highlighted the strong built-in security in both networks. LoRaWAN provides end-to-end encryption and unique network keys for secure data transmission, while private 5G networks provide authentication and traffic isolation features. For extra layers of security in the receiving end of the company network, additional measures were suggested in the Implementation Guideline in Table 9.1.

The thesis also introduced an OT Security Categorization in Figure 8.1, dividing devices based on criticality. To highlight the appropriate security measures, a corresponding Security Requirements Checklist in Figure 8.1 was developed to aid real estate companies in strategically applying these measures. A correlation between OT equipment’s operational requirements and their security categorization was observed in Section 8. Specifically, OT devices demanding high speed typically necessitate elevated security standards. Devices designed for long-range operation with lower power consumption are predominantly found within the basic or medium security categories. These contributions serve as a foundation for managing OT security in the evolving real estate landscape.
Literature


