Security Controls for Smart Buildings with Shared Space

Tapio Frantti
University of Jyväskylä
Jyväskylä, Finland
Email: tapio.k.frantti@jvk.fi

Markku Korkiakoski
Netox Ltd.
Oulu, Finland
Email: markku.korkiakoski@netox.fi

***Abstract*—In this paper we consider cyber security requirements of the smart buildings. We identify cyber risks, threats, attack scenarios, security objectives and related security controls. The work was done as a part of a smart building design and construction work. From the controls identified we concluded security practices for engineering-in smart buildings security. The paper provides an idea toward which system security engineers can strive in the basic design and implementation of the most critical components of the smart buildings. The intent of the concept is to help practitioners to avoid ad hoc approaches in the development of security mechanisms for smart buildings with shared space.**

Keywords *smart building, security risks, security controls, IoT*

I. Introduction

Authors in [1] considers *Smart building* as an umbrella term that has come into use to describe a number of different technologies that are being integrated into buildings. They continue that there is no clear definition of what makes a building *smart*. Authors in [2] describe a progression of building technologies, from *primitive*, to *simple*, to *automated*, to *intelligent*, to *smart* buildings. The primitive buildings have four walls and a roof. The simple buildings have manually controlled technologies such as lighting and climate control. The automated buildings use timers and central controls. Systems in the intelligent buildings are still controlled automatically, but sensors allow the buildings to adjust to user needs in real time. The smart buildings go a step further and collect also data about how and when a building is being used and provide a real-time picture of the status of a building.

Authors in [3] state that the integrated network of a smart building is where the true benefits of a smart and converged infrastructure are realised by building owners and operators; however, this is also the point where extreme exposure to security vulnerabilities are manifest. They continue that "today smart buildings are increasingly enabled by Internet of Things (IoT) and made functional by the ongoing convergence of operational technology (OT) systems and information technology (IT) systems in buildings".

In paper [4] is noted that we are currently witnessing the steady invasion of IoT devices into buildings and their networks, and there is a growing security need to support this area. This has fundamentally changed how built environments are being used and operated, and have thrown open an otherwise closed-loop building architecture into one that necessitates the open access and control of many operators and service providers. This fundamental change also exposes buildings and all associated with them to susceptibilities and risks of cyber threats.

The susceptibility to the advanced cyber threats and risks is a main concern for smart buildings because these complex systems are inexorably linked to the economic and security interests of the actors in smart buildings. The dependence on the systems for technical and economical success, has set the actors vulnerable to hostile cyber actions and attacks, and other serious cyber threats. Adversaries may penetrate to the networks of smart buildings, disrupt or defeat the defence using exploits available on the Internet, hang on systems for a long time, and utilise data available on the systems. Unknown and adversary-created vulnerabilities are, for the most part, totally invisible to the most actors in the field. Vulnerability scanners, for example, almost solely search known vulnerabilities according to their vulnerability databases. However, unknown vulnerabilities can be addressed by well established security system engineering techniques, methodologies, processes, and practices that provides the trustworthiness to withstand and survive well-resourced, sophisticated cyber attacks as noted in [5].

It is obvious that a new approach of engineering-in information and cyber security to smart buildins is required. It has to be driven by knowledge of vulnerabilities, threats, assets, potential attack impacts, and the motives and targets of potential adversaries because the traditional reactive approach to information security strategy is no longer effective, nor is it defensible. In this paper we consider the first step of the approach, definition of cyber risks, threats, and controls of the smart buildings with shared spaces. We also consider different attack scenarios, security practices, and related design principles for engineering-in smart buildings security. The research assumption for the new approach is that *Setting up satisfactory security controls for smart buildings is a system design problem and it requires a combination of equipment, communications, physical, personnel, and administrative safeguards for comprehensive security*. The research question is the corollary of the assumption: *Can we identify security measures that form the foundation for engineering-in smart buildings security*?

The organisation of the rest of the paper is following.

The section II considers as a literature review cyber risks and threats of the smart buildings. The section III considers identified risks, objectives, and controls of the constructed smart building. Discussion and conclusions are drawn in sections IV and V, respectively.

II. Cyber risks for smart buildings

A. Security concerns of the IoT

Authors, like [3], note that investigation of cyber threats in smart buildings is timely and pertinent. They continue that avoidance may not be an option, but the ability to minimise the impact of cyber threats needs exploring and leaders and experts must collaborate to address various aspects of cybersecurity. In addition, evaluating the efficacy of technology solutions at an industry level is important and cyber threats demand the utmost recognition and intervention of administrators and regulators to implement industry-wide changes.

Paper [6] notes that IoT enables data-driven decisions for smart building but exposes it to cybersecurity risks, too. The emerging technologies, like smart sensors are used in smart buildings without appropriate security testing. Suppliers are paying more attention on ease-of-use and quick implementation of these technologies than focusing on security. They continue that integrated network of smart building is the main point of security vulnerabilities. The integrated network consist of the building automation, energy management and demand response, physical security, HVAC (Heating, Ventilation, Air Conditioning) and lighting, fire and life safety, elevator, monitoring and control, voice and data network, facility and asset management, parking and signage systems.

Authors in [3] define that dealing with cyber risks and threats for smart buildings consist of a systematic review and analysis of vulnerabilities of the IoT, cost of damages, scope and magnitude of cyber crimes, mitigation methods, and cybersecurity management strategy. Paper [7] notes that new operational and risk management processes, security practices and paradigms are essential to overcoming cyber challenges. It also mentions that these systems are often times not designed, configured or operated with security in mind [7].

Paper [8] underlines cybersecurity testing and considers information sharing of the IoT security incidents insufficient as CERT (Computer Emergency Response Team) merely does not exist. The European Union Agency for Network and Information Security notes that fragmented and slow adoption of standards and regulations to guide the adoption of IoT security measures and good practices is one of the issues that hinder the consolidation of secure IoT use [9]. They continue that for each IoT environment it is necessary to carry out a risk assessment to go through the threats that can affect the different assets, define the plausible attack scenarios, and put them in the context of the IoT service defined, working out which hazards are critical or not and which ones can be mitigated.

Paper [9] also addresses that ensuring security in IoT products and services is a fundamental priority. They note that one of the main concerns is the impact that the different threats may have since attacks on IoT deployments could dramatically jeopardise people security, privacy and safety, while additionally IoT in itself can be used as an attack vector against other critical infrastructures. Also, since IoT can drastically change the ways personal data is collected, analysed, used, and protected, privacy concerns have been raised. Therefore, the adoption of IoT has raised also many new legal, policy and regulatory challenges.

B. Security concerns of the BAS

Various authors, such as [10], have separately evaluated security threats to the BAS (Building Automation System)[1]. Threat modes, like direct manual interference by insiders and outsiders, phising, spear phising, external attacks, keystroke logging and botnet systems exposure risks. These include unplanned or unauthorized pathways, unauthorised access to systems, data loss, revealing occupants personal data to adversaries, route to physical damage, disrupting set points of physical quantity, and damaging transport functions such as lifts and escalators.

In paper [11] is stated that BAS are vulnerable for destructive attacks against smart building infrastructure and against users privacy and even pose a significant risk for people lives. Papers [3], [7], and [6] note, that attackers infiltrating BAS can potentially infiltrate the enterprise. The scale of damages can inflate more when BASs are overlayed with IoT (Internet of Things). These may imply security breaches that could render a smart building, its occupants, and service providers powerless over an adversary's damaging actions to corrupt networks, misuse critical information, and cause significant operational and financial loss.

C. IoT threats

The number of security threats targeting IoT devices and the occurrence of cybersecurity incidents have increased over the last years due to the ever wider penetration of IoT across the entire spectrum of daily activities and critical infrastructures.

Paper [9] presents threat taxonomy that is based on the various adverse impacts on the IoT devices. The main threat categories are *outages*, *physical attacks*, *disasters*, *damages and loss of assets*, *failures and malfunctions*, *nefarious activities and abuses*, and *eavesdropping, interception, and hijacking*. Authors in [12] classify security threats targeting IoT devices according to the four communication protocol layers: *application layer*, *middleware layer*, *network layer*, and *perception layer*. Authors in [13] consider taxonomy of the IoT threats as attacks according to the targeted layer and security goal and classify attacks into three classes: *attacks on the cyber-physical layer*, *attacks on the middleware layer*, and *attacks on the application layer*. Paper [14] categorises the IoT attacks to *physical*, *network*, *software* and *encryption* attacks. They emphasise that all of the security challenges and threats of each network technology are passed by default onto

[1]BAS is the centralized automated control of the building's Heating, Ventilation and Air-Conditioning (HVAC), lightning, electrical, access control, security and other interrelated systems.

the IoT system that utilises these technologies, and there is the possibility of additional security threats that arise from the coexistence and collaboration of the different technologies and the open standards and protocols created for the IoT. Paper [15] present IoT security taxonomy classes as *architecture and layers*, *threat vector*, *trust*, *compliance*, *domains*, and *access control*.

The presented classifications focus on intentional attacks from an adversary. All the classifications are good if they cover all the security challenges and threats. However, we prefer to use threat based classification presented in [9], because it presents threats as such without any implementational or architectural abstraction.

TABLE I
IOT ATTACK SCENARIOS.

Attack scenarios	**Importance level**
Against the connection between controller(s) and actuators	High - Crucial
Against sensors, modifying values read or settings	High - Crucial
Against actuators by modifying their settings	High - Crucial
Against the administration systems of IoT	High - Crucial
Exploiting protocol vulnerabilities	High
Exploiting control or operating system vulnerabilities	High
Creating backdoors during the manufacturing	High
Ransomware	Medium - Crucial
Injecting self-propagating malware	Medium - High
DDoS using an IoT botnet	Medium - High
Stepping stones attacks	Medium - High
Hardware additions	Medium - High
Power source manipulation	Medium - High

D. Asset criticality

Asset criticality refers to the relative risk of a cost arising from failure of that particular asset. Protection costs of the asset should be in line of the asset value and never exceed the value of the asset. Authors in [16] note that the value of some assets may change over time and should therefore be subject to review. They continue that different operational focuses, operational environments, and asset types may be indicative of the range of threats (intent to inflict harm), threat actors (hostile with malicious intent), and threat vectors (means to realise the threat) arrayed against organisations. They also state that all organisational assets and systems that are necessary for the delivery of effective operations or are of specific organisational value should be identified.

Paper [9] describes the criticality of the main assets based on the responses received by the subject matter experts in the interviews. The most critical IoT assets are the sensors, then the device and network management controls and thirdly the communication protocols, the gateways and the applications and services, all of them marked as critical by at least two thirds or more of the experts interviewed. Therefore, when addressing security, especially those assets should be prioritised. In asset protection, we should also keep in mind the holistic nature of the security challenges and note that the Internet is the foundation and core supporting IoT. Hence, almost all the security threats that lie within Internet propagate to IoT - and vice versa - and may endanger assets in any network.

E. Attack scenarios

Table I presents some typical IoT attack scenarios identified from the literature and from the authors experience [9], [11].

Attacks against the connection between controller(s) and actuators includes, *e.g.*, eavesdropping, replay, and man-in-the-middle intercepting actions. Attacks against sensors may analyse devices for weaknesses and manipulate devices while in use. Attacks against the administration systems of IoT are getting access and hiding presence, analysing IoT system for weaknesses, manipulation of system, and changing the system to attack vector type attacks, among others. Exploiting protocol, control or operating system vulnerabilities are often used to get into the system and hiding presence for information collection, espionage, and some adversary use in future. Embedded software of the product may also include backdoors either intentionally by legislation or manipulating software by adversaries or unintentionally as a consequence of the programming flaws. Ransomware is a type of malware designed to hijack computers so hackers can force victims to pay a ransom to regain access. Self-propagating malware are often the type of fileless malware that do not require human interaction. Computer exploits often involve an attacker being able to compromise a sequence of hosts, creating a chain of stepping stones from source to ultimate target. Adversaries may introduce computer accessories, computers, or networking hardware into a system or network that can be used as a vector to gain access. IoT devices often do not have strong security features built into them to prevent hackers from accessing them and the danger is that these connected devices can be harnessed by hackers to form a botnet, which is an interconnected network of computers infected with malware without the user's knowledge. In particular, Distributed Denyal of Service (DDoS) attacks are common because it is easy to purchase and launch a DDoS toolkits. Power source manipulation includes, *e.g.*, power deprivation attacks.

F. Mitigation methods for vulnerabilities

Paper [3] note that dealing with cyber risks and threats demands a sophisticated and robust approach for smart buildings, which essentially consists of a systematic review and analysis of aspects such as Industrial Control Systems (ICS) vulnerabilities, cost of damage, scope and magnitude of cyber crimes, technology initiatives and mitigation methods, and a cybersecurity management strategy.

In the review of the cyber security technology options, it is important to begin by looking at a building's critical vulnerability areas that gain top consideration. BAS tops the list, but shared networks, data management, and third-party services are equally impacted. In addition, open protocols and interoperable platforms have little cyber defence mechanisms. The smart buildings industry is currently adopting mitigation methods that are varied and they are somewhat specific to every organisation. However, several best practices and commonalities in techniques have emerged from these approaches.

For a successful cyber security strategy, the life-cycle approach to cybersecurity should essentially apply to the entire process, starting from conceptual planning, construction, operation, commissioning, and decommissioning of a smart building. Furthermore, cybersecurity requirements across the various stages of a smart building's life cycle need to be evaluated in conjunction with the resilience requirements that are fundamentally linked with each stage.

Authors in [3] state that the incidences and impact of cyber threats will only advance in severity and sophistication. Therefore, any counter initiatives undertaken by the smart buildings industry participants will have to incorporate predictive capabilities to combat such organised and orchestrated adversarial tactics. In order to respond this, we present here our approach for obtaining security measures for smart buildings.

TABLE II
RISKS FOR SMART BUILDINGS DERIVED FROM RISK ANALYSIS.

Prioritized risks	
Prioritized risk 1:	Convergence of OT and IT
Prioritized risk 2:	Personnel risks
2.1	Phishing/Spear phishing/Social engineering
2.2	Unaware personnel
Prioritized risk 3:	Remote attacks
3.1	Building protocol based exploits
3.2	Malware infection
3.3	Web page and API attacks
3.4	Vulnerabilities of the 3^{rd} office management applications
3.5	Ransomware
3.6	Low level exploits through device firmware
Prioritized risk 4:	Unauthorised access to BAS
4.1	Stepping stone attacks
Prioritized risk 5:	Unauthorized access to data
5.1	Corruption or modification of information/resources
5.2	Theft, loss or removal of information/resources
5.3	Disclosure of information
Prioritized risk 6:	Unauthorized access to real estate
6.1	Interruption and deterrence of the building services
6.2	E-locks breach
6.3	Surveillance camera breach
Prioritized risk 7:	Unavailability of services and infrastructure of the building
7.1	Congestions, crashes, radio jamming of the connections
7.2	Network traffic analysis attacks
7.3	Protocol deceive or violation attacks
7.4	Sybil and sinkhole attacks
Prioritized risk 8:	Exposure to physical attacks
8.1	Node capturing
8.2	Node injection
8.3	Node tampering
8.4	Location and/or topology changes
8.5	Generate a physical event monitored by the sensors
8.6	Malicious resource consumption
8.7	Visual observations
Prioritized risk 9:	No updates for connected devices or applications
Prioritized risk 10:	System delays
Prioritized risk 11:	Bogus denial of a transaction
Prioritized risk 12:	Bogus transaction claims
Prioritized risk 13:	High level of network distribution
13.1	Remote management unable to see physical tampering
13.2	Distributed management cause fragile organisation
Prioritized risk 14:	Marginal resiliency
Prioritized risk 15:	Risks endangering human lifes
Prioritized risk 16:	Building visitor procedure fails: unauthorized visitors

III. RISKS, OBJECTIVES, AND CONTROLS

For the risk-and-threat-identification-and-assessment, we propose to identify and prioritise risks, maintain risk register, follow-up risks, and do risk management. This is especially emphasised if the smart building includes legacy systems, such as building automation systems that may be unprotected. Risk analysis is also required whenever a 3^{rd} party offers any new application to the smart building and to identify also intended use of any networked device, and monitor and track anomalies on network traffic. It is also emphasised to conduct regular security audits to maintain the overall integrity of OT (Operational Technology) and IT systems and maintain up-to-date threat intelligence about the types of cyber threats. One option is to subscribe to a regular feed of threat data from a threat intelligence subscription service. Commercial example is Wapack Labs Cyber Threat Analysys Center[2]. Another useful source of threat intelligence is information sharing and analysis centers (ISACs)[3]. The third useful source of vulnerability information is Computer Emergency Response Team (CERT)[4].

The increasing digitization of the buildings increases cyber risks in the smart building development. BASs are incorporating more ITs, and they are moving away from the older proprietary systems of the past toward adopting edge-to-cloud computing architectures. In addition, there is a tendency to deploy more lower cost sensors to gather as much data as possible, but the building industry has a considerable installed base of legacy BAS, applications, devices, and networks that must be managed, maintained, and gradually modernized. The new cyber-attacks, many of which appear to be organized by nation states with almost unlimited resources, are sophisticated multistage attacks designed to gain control over IT and OT systems causing disruption, chaos, and potential loss of human life. A report from Kaspersky analyzed smart buildings worldwide that use the company's security products, and found that nearly 4 in 10 (37.8%) of these buildings had been affected by a malicious cyber attack, see [17]. In most cases, these cyber attacks were attempting to infect the computers that control smart building automation systems.

Another increasingly important category of cyber attacks is referred to as *non-malware attacks* that does not involve downloading any malware code onto target devices. The attacker may use existing software in target machines. The most common type of non-malware attack is the remote logins. An intrusion or another indicator of compromise requires both automated tools for recognition and human intervention for response. Ability of the legacy antivirus software to prevent non-malware attacks is pretty low.

Smart building technology creates a connected asset that introduces a new attack surface that needs protection. Research and experience have shown repeatedly, when things are connected to the Internet, they become a target for malicious hackers. Risks may due to, *e.g.*, weak password protection of older building automation systems and industrial control systems (ICS), embedded operating systems that are not ap-

[2]https://www.wapacklabs.com
[3]https://www.nationalisacs.org
[4]https://www.sel.cmu.edu/about/divisions/cert/index.cfm

TABLE III
SECURITY OBJECTIVES OF THE SMART BUILDINGS.

Security objective	Description	Related risks
Security objective 1:	Prevent the use of OT systems as entry point into IT networks and vice versa	Convergence of OT and IT
1.1	Isolate OT systems	
1.2	Replace legacy systems	Building protocol based exploits
Security objective 2:	Up-to-date security training	Personnel risks
2.1	Regular social engineering training	Phishing/Spear phishing/Social engineering
2.2	Regular threat landscape training	Unaware personnel
Security objective 3:	Detect anomalies and prevent attacks	Remote attacks
3.1	Intrusion prevention	Malware infection
3.2	Continuous threat intelligence	
3.3	Regular vulnerability scanning of networked systems	
3.4	Regular Web vulnerability scanning	Web page and API attacks
3.5	Vulnerability checks for apps	Vulnerabilities of the 3^{rd} office management applications
3.6	Intrusion prevention	Ransomware
3.7	Continuous threat intelligence	Low level exploits through device firmware
3.8	Backup process	
Security objective 4:	Restrict access and authorization to BAS	Unauthorised access to BAS
4.1	Prevent external connections to BAS	
4.2	Prevent priviledge escalation by AAA	Stepping stone attacks
Security objective 5:	Restrict access to data	Unauthorised access to data Corruption or modification of information/resources Theft, loss or removal of information/resources
5.1	Information handling process Privacy	Disclosure of information
Security objective 6:	Restrict access to real estate	Unauthorised access to real estate
6.1	Availability of services	Interruption and deterrence of the building services
6.2	Secure key exchange	E-locks breach
6.3	Regular scanning of malwares	
6.4	Regular scanning of surveillance system	Surveillance camera breach
Security objective 7:	Service and infrastructure availability	Unavailability of services and infrastructure of the building
7.1	Maintenance of services and infrastructure	Congestions, crashes, radio jamming of the connections
7.2	Conceal or distribute traffic	Network traffic analysis attacks
7.3	Preserve integrity, originality and timeliness	Protocol deceive or violation attacks
7.4	Detect trust-shaking attacks	Sybil and sinkhole attacks
Security objective 8:	Defend against physical attacks	Exposure to physical attacks
8.1	Node capturing prevention	Node capturing
8.2	Node injection prevention	Node injection
8.3	Node tampering prevention	Node tampering
8.4	Prevent visual line-of-sight	Location and/or topology changes
8.5	Anti-tampering solutions	Generate a physical event monitored by the sensors
8.6	Defend against malicious resource consumption	Malicious resource consumption
8.7	Conceal the physical location of nodes	Visual observations
Security objective 9:	Reliable nodes update mechanisms	No updates for connected devices or applications
Security objective 10:	Faster infomation handling	System delays
Security objective 11:	Prevent bogus denials	Bogus denial of a transaction
Security objective 12:	Prevent bogus claims	Bogus transaction claims
Security objective 13:	Centralised functions	High level of network distribution
Security objective 14:	Anti-tampering solutions	Remote management unable to see physical tampering
Security objective 15:	Centralize management	Distributed management cause fragile organisation
Security objective 16:	Recovery and remediation methods	Marginal resiliency
Security objective 17:	Keep critical systems always running	Risks endangering human lifes
Security objective 18:	Visitor authentication procedure	Building visitor procedure fails: unauthorized visitors

propriately patched or even supported anymore and compound security updates for multiple connected smart building devices and systems from different vendors.

Here, we consider a risk analysis as a part of the smart building system requirement analysis process to get security controls. The considered smart building was a modern multilayer office building with surveillance systems, multiple wireless and wireline networks, common office devices such as printers and scanners, BASs for HVAC, e-locks in indoors and outdoors, an application for the use of devices and services, conductive floor mats to detect peoples, proximity and motion detectors, and a monitoring and data collection systems. Physical spaces were decomposed to office, meeting room, general, service desk and refreshment spaces. All the spaces had different physical security requirements considered in the risk and threat identification process. Networks were decomposed to communication, surveillance and IoT networks. Communication networks were further distributed to company and visitor networks for each tenant of the smart building and only necessary ports are exposed. The building automation system was kept as a separate system with no access to and from the other networks. Surveillance system was operated by a dedicated network but it had a route to the Internet for remote monitoring and alerts. Services, such as printing, meeting room reservations, orders, and maintenance services were used by own applications.

For the definition of the smart building security requirements, different use case and attack scenarios were formed. Each use case scenario was literally described as narrative descriptions that were chopped to use cases to identify different actors, preconditions and assumptions. Use cases were divided to sequential steps in detail. In each step it was identified

required generic and specific functionalities that were grouped into classes. Risk survey and analysis focused on to the identified functionalities, see the method in [18]. Implementation methods and the related implementation specific cyber risks were evaluated for each functionality.

Various kind of attack scenarios including those listed in Table I were used to identify possible security holes and flaws in the system design phase. Actual vulnerability scanning was performed after the system implementation and it is recommended to be done regularly, *e.g.*, once a week. In addition to vulnerability scanning, it is recommended to do penetration testings for all the interfaces of the smart building after the implementation.

The most relevant cyber risks identified in the smart building project are presented in Table II. Risks with more probability and a bit low severity are prioritised over risks with a bit higher severity but low probability, *i.e.*, the *Level of risk* can be expressed as:

$$\frac{Probability\ of\ adverse\ event}{Mitigation\ factor}\ x\ Impact\ value \quad (1)$$

Table III presents the identified risks and the connected objectives to them. The most relevant security objectives and the related controls are presented in Table IV.

A. Identified risks

The risk analysis revealed 16 main risks and 28 subrisks. *Convergence of the Operational Technology and Information Technology* risk was prioritized to the top. Cyber security is a holistic issue and it is known that OT[5] systems, such as Building Automation Systems, may act as an entry point into IT systems and may enable malicious actions. *Personnel risks* were prioritized suprinsingly high. This may due to fact that remote attacks and malware injections are mostly done through social engineering. High prioritization reflect experts worries about the personnel unawareness of the cyber security pitholes. Sophisticated multistage attacks that are designed to gain control over OT systems causing disruption, chaos, and potential loss of human life increase risks and impacts that are seen as *remote attacks*, *unauthorized access to BAS*, *unauthorized access to data*, *unauthorized access to real estate* and *unavailability of services and infrastructure of the building*. They may also due malicious actions that are not targeted specifically to the smart buildings. *Exposure to physical attacks* and *no updates for connected devices or applications* risks are related especially to IoT devices and networks. *System delays* may due to DoS or DDoS attacks or they may be used to mislead Incident Response Team (IRT) from simultaneous malware delivery, installation and exploitation phases. *Bogus denial of transaction* and *bogus transaction claims* are related to the different kind of office space and service payments. *High level of network distribution* could open routes to the fraudulent misuse of the smart building systems. Security control cannot guarantee absolute security but malicious actions, data breaches, and malwares are possible despite of comprehensive security measures and emphasize the importance of remediation actions, *i.e.*, *resiliency*. *Endangering human life* risk is serious but it was estimated unprobable. However, its' probability may increase when the threat ecosystem grows. *Unauthorized visitors* or inadequate visitor procedures may expose building to malicious persons, but also persons not aiming to cyber crimes but more conventional crimes.

[5]Operational Technology can be defined as functions using hardware and software in real time to monitor, automate changes, and control various devices, processes and events in an enterprise.

B. Security objectives and controls

The security objective *Prevent the use of OT systems as an entry point into IT networks and vice versa* and the related subobjectives *Isolate OT systems* and *Replace legacy systems* are responded by the security controls *Conduct regular vulnerability analysis to maintain the overall integrity of OT and IT systems* and *Renew all the legacy systems with up to date solution*. After renewal of the legacy systems smart house enterprises need to regularly scan software, systems, and networks for vulnerabilities to proactively address to them before any exploitation emerges. The Center for Internet Security (CIS)[6] recommends to run automated vulnerability scanning tools against all systems on the network on a weekly or even more frequent basis. It is generally recommended to run specialized vulnerability scanning tools for different systems such as computers, networks, information systems, and Web applications to reveal as much vulnerabilities as possible. In addition, use of several vulnerability scanners for the same target is also required to cover extensive range of vulnerabilities.

The security objective *Up-to-date security training* and the related subojectives *Regular social engineering training* and *Regular threat landscape training* are responded by the security control *Education of the personnel*. Social engineering, like phishing and spear-phishing, have arouse to the main channel for malware delivery. However, there are advanced malware attacks, such as Pegasus, that do not require any user actions for the delivery and installation of the malware in the target system. For these kinds of malware are also needed highly sophisticated intrusion detection and prevention systems and education of the personnel.

The *Detect anomalies and prevent attacks* objective is responded by the control *Continuous proactive threat intelligence*. One aim of the threat intelligence is to transfer the detection point of malware from the action phase to the delivery phase in the cyber attack kill chain, [19]. Another aim is to recognize non-malware based attacks by trying to get and analyze log and operational data, identify security events and aggregate them in an effort to find cause-and-effect correlations to reveal potential attack.

The subobjective *Intrusion prevention* is responded by the controls *Establish an Incident Response Team (IRT)* and *Use*

[6]https://www.cisecurity.org

Intrusion Prevention Systems (IPS). Incident response team should have understanding of known threats, attack signatures, and vulnerabilities. They should also know enterprise network, security infrastructure and have experience in security response and troubleshooting techniques as well as remediation methods. It is also mandatory to understand regulations and laws as they pertain to privacy. In the smart building environment with multiple companies and own devices in a common shared space, the need for effective intrusion detection and prevention increases. Host-based and network based intrusion detection solutions range in scope from single computers to large networks. However, intrusion information may need to be collected centrally using a security information and event management (SIEM) system usually operated by a Security Operator Center (SOC) service provider.

The subobjectives *Continuous threat intelligence* is responded by the control *Do proactive threat intelligence*, which is already included as a countermeasure above. Similarly, the subobjectives *Regular vulnerability scanning of networked systems*, *Regular Web vulnerability scanning*, are responded by the controls *Do proactive threat intelligence*, *Do vulnerability scanning with several scanners*, *Do vulnerability scanning for Web pages with several scanners* that are also considered as the countermeasures above.

The subobjective *Vulnerability checks for apps* is mitigated by the control *Default deny app installation*. It allows to install only the acctepted 3^{rd} party applications. However, this is challenging to the smart buildings with multiple tenants, own devices, and shared space and service infrastructure. It requires a common security policy and agreements. Devices that are used outside the internal network(s) may be infected and contaminate other devices in internal network if not properly protected, monitored and updated for vulnerabilities.

The subobjectives *Intrusion prevention* is responded by the *IRT and IPS* which is also considered above. In the same way, the subobjective *Continuous threat intelligence* is responded by the controls *Establish an Incident Response Team (IRT)* and *Use IPS* that are included as the countermeasure above.

The subobjective *Backup process* is responded by the control *Organize backups and duplicate systems*. This is also challenging to the smart buildings with multiple tenants. Operator of the smart house should organize and test backup processes and duplicate common infrastructure systems. The backups must be validated before storing them to avoid, for example, storing contents encrypted by malware for ransomware.

For system safety and reliability, all the critical systems in the smart building should have policies and self-operations, such as diagnosis, repair and healing, to recover from failure, malfunction or a compromised state. Essential features should continue to work with a loss of communications and if necessary, *e.g.*, due to malicious actions, cut the connections and use back-up devices and connections by different communication systems.

The security controls *Authentication, authorization and accounting control to BAS*, *Prevent external connections to BAS* and *Prevent priviledge escalation by access control* were defined to respond to the objective *Restrict access and authorization to BAS*. BAS is a part of critical infrastructure and thus it needs Authentication Assurance Level (AAL) 2 or 3 authentication, see [20]. AAL2 is based on proof of possession and control of two distinct authentication factors through secure authentication protocols.

The security controls *Authentication, authorization and accounting*, *Resiliency: backups, duplicate systems*, *Encrypt data*, *Intrusion detection/prevention systems* and *Firewalls* are used for the objective *Restrict access to data*. The controls also make sure or improve the availability of data. As a specific access control method, an attribute-based access control (ABAC) based on attributes associated with subjects, object, targets, initiators, and resources is recommended, see more details in [19]. The ABAC express conditions of properties of both the resource and the subject. The strengths of the ABAC approach are its flexibility and expressive power that are needed in smart building type complex environment. It is also emphasized to ensure change of the default passwords and usernames during the initial setup, salt, hash and encrypt credentials.

The security objective *Privacy* is responded by the controls *Document confidential information handling process and arrange training* and *Personal information handling process*. General Data Protection Regulation (GDPR) requires to make privacy information removal an integral part of the system. Therefore, personal data must be collected and processed fairly and lawfully and it should be removable.

The objective *Restrict access to real estate* is responded by the control *Authentication and access control to real estate*. The subobjective *Availability of services* is responded by the control *Continuous surveillance and service monitoring*. The objective *secure e-lock key exchange* is handled by *out-of-band key exchange* procedure, *i.e.*, keys are not delivered by a shared radio link. The controls *Threat intelligence* and *Regular scanning and monitoring of IT and OT systems* are used to control delivery and installation of malwares (*regular scanning of malwares*).

Continuous monitoring of services and infrastructure control is used to guarantee *Service and infrastructure availability*. All the services are monitored and the related log files are analysed for unauthorized access attempts. For *Maintenance of services and infrastructure* the control *Duplicate critical connections and systems* is used. *Encrypt and distribute traffic* is used to *Conceal or distribute traffic* and *Protocols with message digests, nuance and time stamps* are used to *Preserve integrity, originality and timeliness* and thus to resist replay attacks. *Session keys for identification* are used for *Detection of trust-shaking attacks*.

In the trust control of the devices, it is advised to set together with product producers trust mechanism in the boot environment, *i.e.*, ensure that any device is not running tampered software by verifying its authenticity before execution. We also propose to control the installation of software and devices, prevent load of unauthenticated files, sign code cryptographically, verify users with multi-factor authentication, and avoid solutions from rogue countries.

TABLE IV
SECURITY CONTROLS IN SMART BUILDINGS.

Security control	**Description**	Related security objective
Security control 1:	Conduct regular vulnerability analysis to maintain the overall integrity of OT and IT systems	Prevent remote access to OT systems
		Isolate OT systems
1.1	Renew all the legacy systems with up to date solution	Replace legacy systems
Security control 2:	Education of the personnel	Up-to-date security training
		Regular social engineering training
		Regular threat landscape training
Security Control 3:	Continuous proactive threat intelligence	Detect anomalies and prevent attacks
3.1	Establish an Incident Response Team (IRT)	Intrusion prevention
	Use Incident Prevention Systems (IPS)	
3.2	Do proactive threat intelligence	Continuous threat intelligence
3.3	Do vulnerability scanning with more scanners	Regular vulnerability scanning of networked systems
3.4	Do vulnerability scanning for Web pages with more scanners	Regular Web vulnerability scanning
3.5	Default deny app installation	Vulnerability checks for apps
3.6	IRT and IPS	Intrusion prevention
3.7	Establish an Incident Response Team (IRT)	Continuous threat intelligence
	Use IPS	
3.8	Organize backups and duplicate systems	Backup process
Security control 4:	Authentication, authorization and accounting control to BAS	Restrict access and authorization to BAS
	Prevent external connections to BAS	
	Prevent priviledge escalation by access control	
Security control 5:	Authentication, authorization and accounting	Restrict access to data
	Resiliency: backups, duplicate systems	
	Encrypt data	
	Intrusion detection/prevention systems	
	Firewalls	
5.1	Document confidential information handling process and arrange training	Privacy
	Personal information handling process	
Security control 6:	Authentication and access control to real estate	Restrict access to real estate
6.1	Continuous surveillance and service monitoring	Availability of services
6.2	Out-of-band key exchange	Secure key exchange
6.3	Threat intelligence	Regular scanning of malwares
6.4	Regular scanning and monitoring of IT and OT systems	
Security control 7:	Continuous monitoring of services and infrastructure	Service and infrastructure availability
7.1	Duplicate critical connections and systems	Maintenance of services and infrastructure
7.2	Encrypt and distribute traffic	Conceal or distribute traffic
7.3	Use protocols with message digests, nuance and time stamps	Preserve integrity, originality and timeliness
7.4	Use session keys for identification	Detect trust-shaking attacks
Security control 8:	Surveillance and monitoring systems	Defend against physical attacks
8.1	Detection and notification of movement	Node capturing prevention
	Automatic and accurate location detection	
	Destruction of the test circuitry	
8.2	Network traffic monitoring	Node injection prevention
	Request-reply protocol transactions	
8.3	Invisibility/undetectability	Node tampering prevention/Anti-tampering solutions
	Track node movements	
	Secure location information	
	Self-destruction solutions	
8.4	Invisibility/undetectability	Prevent visual line-of-sight
	Windows coverage, design of offices, location of desks	
8.5	Set border and baseline values	Recognize frequent and abnormal events
	Physical constrictions of actuators	
8.6	Set border values	Defend against malicious resource consumption
	Restricted program counter	
	Limiting transaction with time	
8.7	Conceal the physical location of nodes	Conceal the physical location of nodes
8.7	Secure location information	
Security control 9:	Cryptographically signed update mechanisms	Reliable nodes update mechanisms
Security control 10:	Low latency protocols	Faster infomation handling
	More processing power	
Security control 11:	Multifactor authentication	Prevent bogus denials
Security control 12:	Use cryptographic functions	Prevent bogus claims
Security control 13:	Centralised network management	Centralize functions
Security control 14:	Clarify command chains	Centralize management
Security control 15:	Duplicate systems and do backups	Recovery and remediation methods
Security control 16:	Duplicate critical systems	Keep critical systems always running
	Use Uninterruptible Power Supply (UPS)	
Security control 17:	Authenticate visitors	Visitor authentication procedure

A *logging* system should be based on the risk analysis. It should record events relating to user authentication, management of accounts and access rights. The logging system should also record change of the authorisation and security rules, and the functioning of the system.

These controls are partly congruent but more dimensional than the controls of other offices and manufacturing buildings because technical differences arise only from the number and type of network interfaces and services that may be more numerous and more diverse in smart buildings. Each interface

is an attack surface and some short range IoT technologies have substantial cyber security deficiences that enable their use as an attack vector.

For the objective *Defend against physical attacks* are responded by the *Surveillance and monitoring systems*. *Node capturing prevention* is controlled by the *Detection and notification of movement* and *Automatic and accurate location detection*. *Destruction of the test circuitry* can be used to mitigate the effects of node capturing.

Node injection prevention is controlled by *Network traffic monitoring* and *Request-reply protocol transactions*. *Node tampering prevention/Anti-tampering solutions* objective is responded by node *Invisibility/undetectability*, *Securing location information* of the nodes and implementing *Self-destruction solutions*.

It is also important to ensure that unused interfaces are disabled, encryption is used on storage, and proven hardware antitampering solutions are used. Note that detection and reaction to hardware tampering should not rely on network connectivity but should work also offline.

For the objective *Prevent visual line-of-sight* is responded by *Invisibility/undetectability* solutions and *Window coverage, design of offices and location of desks* controls. *Recognize frequent and abnormal events* are reacted by *Set border and baseline values* control and *Physical constriction of actuators*. *Defend against malicious resource consumption* is controlled by *Set border values*, *Restricted program counter* and *Limiting transaction with time*. For default security of the devices we propose to enable all security features by default, disable insecure functionalities by default, disable access to resources until it is granted, and set strong, device-individual default passwords. Run-time protection and execution monitoring aid to make sure that malicious attacks do not overwrite code, and enable a system to return to a last known secure state, after a security breach has been occurred.

Conceal the physical location of nodes is responded by *Concealing the physical location of nodes* and *Secure location information*.

Devices, such as printers, e-locks, IoT gadgets, surveillance cameras, and network equipment used in smart buildings are usually provided by 3^{rd} parties. It is important to ensure that all the used devices are secure, located in a proper way, updated securely, and they are used in a secure way. Own devices should not be set without a system operator's permission.

Reliable nodes update mechanisms objective is responded by the control *Cryptographically signed update mechanisms*. The update server must be secured, the updates transmitted via a secure connection, and the updates should not contain sensitive data, such as hardcoded credentials. For secure software and firmware updates the IoT device software/firmware, its configuration and its applications is preferred to have the ability to update Over-The-Air (OTA).

For *Faster information handling* can be responded by *Low latency protocols* and especially *More processing power* solutions. The security objectives *Prevent bogus denials* and *Prevent bogus claims* are responded by the controls *Multifactor authentication* and *Use cryptographic functions*, respectively.

The objective *Centralize functions* is responded by the control *Centralized network management*. The objective *Centralize management* is reacted by the control *Clarify command chain*. The objective *Recovery and remediation methods* is responded by the control *Duplicate systems and do backups*. The objective *Keep critical systems always running* is responded by the controls *Duplicate critical systems* and *Use uninterruptible power supply (UPS)*.

Secure failure and recovery principle defines that neither a failure in a system function or mechanism nor any recovery action in response to failure should lead to a violation of security policy. Together with the *principle of continuous protection*, a system should be capable of detecting actual and impending failure at any stage of its operation [5]. The system should also be capable of recovering from impending or actual failure to resume normal, degraded, or alternative secure operation. Paper [21] states that a system should fail in a secure way. Failure should not give the user additional privileges, and it should not show sensitive information. The objective *Visitor authentication procedure* is responded by the control *Authenticate visitors*.

IV. Discussion

In order to answer to the research question *Can we identify security measures that form the foundation for engineering-in smart buildings security?*, we approached it through risk analysis to get up-to-date intelligence about the types of cyber risks, threats and related security objectives in smart buildings. Security controls or measures have to be implemented before security event management (SEM) process can be set up and operative use of the building is initiated. This is especially true for critical functionalities. The *level of risk* we expressed earlier in Section III changes to *Residual risk level, RRL* that is

$$\frac{probability\ of\ adverse\ event}{mitigation\ factor}\ x\ impact\ value \quad (2)$$

The *mitigation factor* reflects the effect of security controls to the probability of the risk. We identified main security measures and related submeasures that cover all the identified risks. However, we cannot guarantee that the use case and attack scenarios we used cover all the functionalities of the smart building. It is also possible to inadvertently omit risks or misconfigure security objectives. Therefore, we emphasize SEM process as a mean to keep security measures up to date. We believe that the presented approach identified comprehensively security controls for the smart buildings and the security controls derived form the foundation for engineering-in complex systems security.

V. Conclusions

The presented security measures/practices provide an idea toward which system security engineers can strive in the basic design and implementation of the most critical components

of smart buildings, given practical constraints and limitations. Those constraints and limitations translate to risks that are managed through analyses and decisions applied to the architecture and design of the implementation. The presented concept is an abstract security model. It does not refer to any particular policy to be enforced by a system, nor does it address any particular implementation. Instead, the intent of this concept is to help practitioners avoid ad hoc approaches in the development of security mechanisms to provide assurance that the proper security measures are taken into consideration.

ACKNOWLEDGEMENT

The research was supported by Netox Ltd., Finnish Research and Engineering, anf Business Finland (KEKO project).

REFERENCES

[1] M. B. Hoy and T. J. Brigham, "Smart buildings: An introduction to the library of the future," *Medical Reference Services Quaterly*, vol. 35, no. 3, pp. 326–331, 2016.

[2] A. Buckman, M. Mayfield, and S. Beck, "What is a smart building," *Smart and Sustainable Built Environment*, vol. 3, no. 2, pp. 92–109, 2014.

[3] K. Khaund, M. Pyle, M. M. Duszynski, D. Noller, and M. Petock, "Cybersecurity in smart buildings: Inaction is not an option any more," Frost & Sullivan, Tech. Rep., 2019.

[4] B. Russell, D. Purves, E. Boakes, E. Salveggio, J. Willison, J. Moor, M. Richardson, N. Ghadiminia, P. Gupta, P. Mary, P. Dorey, P. Kearney, S. Shukla, and S. Sembhi, "Can you trust your smart building?, understanding the security issues and why they are important to you," Internet of Things Security Foundation (IoTSF), Tech. Rep., 2019.

[5] R. Ross, M. McEvilley, and J. C. Oren, "Systems Security Engineering: A Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," *Special Publication 800-160, NIST*, vol. 1, 2018.

[6] E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests," in *2016 IEEE International Smart Cities Conference (ISC2)*, October 2016, pp. 1–6.

[7] M. Mylrea and S. N. G. Gourisetti, *Cybersecurity and Optimization in Smart "Autonomous" Buildings*, 1st ed. Springer, 2017.

[8] C. Cerrudo, "Hacking smart cities," in *RSA Conference, San Francisco*, April 2015, pp. 2–18.

[9] ENISA, "Baseline security recommendations for iot," European Union Agency for Network and Information Security, Tech. Rep., November 2017.

[10] P. E. F. Dribble, R. Imhof, and U. Drafz, "Cybersecurity in smart buildings: Preventing vulnerability while increasing connectivity," Continental Automated Buildings Association, Tech. Rep., February 2015.

[11] T. Mundt and P. Wickboldt, ""security in building automation systems - a first analysis"," in *"IEEE International Conference On Cyber Security And Protection Of Digital Services "*, London, UK, June 2016, pp. 1–8.

[12] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," *Journal of Hardware and Systems Security*, no. 2, pp. 97–110, May 2018.

[13] L. Wustrich, M. Pahl, and S. Liebald, "Towards an Extensible IoT Security Taxonomy," in *"The 25th IEEE Symposium on Computers and Communications (ISCC 2020)"*, Rennes, France, July 2020, pp. 1–6.

[14] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *"IEEE Symposium on Computers and Communication (ISCC)"*, Larnaca, Cyprus, July 2015, pp. 180–187.

[15] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the internet of things (IoT): a security taxonomy for IoT," in 17^{th} *IEEE International Conference On Trust, Security and Privacy In Computing and Communications (IEEE TrustCom-18)*, New York, USA, July 2018, pp. 163–168.

[16] CPNI, "Asset identification guide," Centre for the Protection of National Infrastructure (CPNI), Tech. Rep., July 2020.

[17] N. Lindsey, "New Kaspersky Report Suggests 4 in 10 Smart Buildings at Risk of Cyber Attack," *CPO Magazine*, 2019.

[18] T. Frantti, R. Savola, and H. Hietalahti, "Risk-Driven Security Analysis and Metrics Development for WSN-MCN Router," in *The* 4^{th} *International Conference on ICT Convergence (ICTC 2013)*. Jeju Island, Korea: IEEE Communications Society, 2013, pp. 22–26.

[19] W. Stallings, *Effectice Cybersecurity*, 1st ed. New York, USA: Addison Wesley, 2020.

[20] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y. Choong, K. K. Greene, and M. F. Theofanos, "NIST Special Publication 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management," NIST, Tech. Rep., 2022.

[21] M. Hovard and D. LeBlanc, *Writing Secure Code*, 2nd ed. Microsoft Press, 2003.