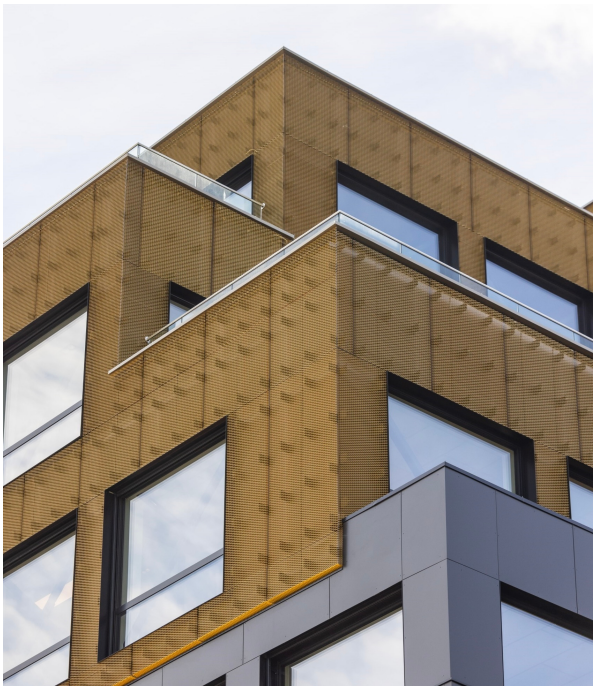
Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Mikal Leirvåg

Assessing Current Measures and Proposing Actions for Smart Building Security

Master's thesis in Experience-based Master in Information Security
Supervisor: Erjon Zoto
Co-supervisor: Marius Engan
June 2023



NTNU
Norwegian University of Science and Technology

intility | The Enterprise Cloud Solution

Mikal Leirvåg

Assessing Current Measures and Proposing Actions for Smart Building Security

Master's thesis in Experience-based Master in Information Security
Supervisor: Erjon Zoto
Co-supervisor: Marius Engan
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Glossary

BACnet Building Automation Control Networks

BAS Building Automation Systems

CPS Cyber Physical Systems

GUI Graphical User Interface

HVAC heating, ventilation, and air-conditioning

ICS Industrial Control Systems

IACS Industrial Automation and Control Systems

IOSP IT-OT Service Provider

IoT Internet of Things

IP Internet Protocol

IPD Integrated Project Delivery

ISMS Information Security Management System

IT Information Technology

KNX Konnex

NTNU Norwegian University of Science and Technology

NAC Network Access Control

OT Operational Technology

PropTech Property Technology

ROI Return Of Investment

Abstract

Smart buildings are a growing market trend in the real estate industry and the complexity of these buildings increase at the same time as Information Technology (IT) and Operational Technology (OT) environments are converging. This pose a challenge for information security as stakeholders in the industry are lacking the competence to plan, implement, operate and maintain building technology in a secure manner. This research project aims to assess the current state of stakeholders approach to information security in construction projects of smart buildings and to propose methods or measures that can mitigate potential challenges.

The study is using a qualitative design, using in-depth interviews as the primary method for collecting data. Predefined stakeholders that were involved in either planning, implementation, operation or maintaining connected systems in smart buildings were recruited. By analysing the participants answers from the interviews, answers would be categorized into "current challenges", "current measures", "future challenges" and "proposed solutions"

The findings indicate that smart building projects lack systematic approaches to risk management and insufficient planning of system implementation when it comes to information security. Furthermore, stakeholders in construction projects are seemingly not able to adapt fast enough to the increased complexity that smart buildings require. This has lead to systems not being implemented with adequate security controls. Also, the lack of planning for the operation and maintenance of the buildings leads to inadequate alignment of stakeholders being responsible for this phase. To solve these challenges, methods are proposed that are divided into three categories: national and industry solutions, proposed actions for the project owners and technological solutions. In general, the project owners need to address information security in early stages of construction projects and facilitate alignment between stakeholders when it comes to implementing security measures, as well as planning for operation and maintenance with information security in mind.

Sammendrag

Smarte bygninger er en voksende trend i eiendomsbransjen, og kompleksiteten til disse bygningene øker samtidig som IT- og OT-miljøene konvergerer. Dette skaper utfordringer for informasjonssikkerheten, da aktører i bransjen mangler kompetanse til å planlegge, implementere, drifte og vedlikeholde byggteknologi på en sikker måte. Dette forskningsprosjektet har som mål å vurdere aktørers nåværende tilnærming til informasjonssikkerhet i konstruksjonsprosjekter for smarte bygninger og å foreslå metoder eller tiltak som kan redusere potensielle utfordringer.

Studien bruker en kvalitativ design, der forskeren vil bruke dybdeintervjuer som hovedmetode for datainnsamling. Forhåndsdefinerte interessenter som var involvert enten i planlegging, implementering, drift eller vedlikehold av tilkoblede systemer i smarte bygg, ble rekruttert. Ved å analysere deltakernes svar fra intervjuene, ble de bli kategorisert som "nåværende utfordringer", "nåværende tiltak", "fremtidige utfordringer" og "foreslåtte løsninger".

Resultatene indikerer at smarte byggeprosjekter har manglende systematiske tilnærminger til risikostyring og planlegging av systemimplementasjoner når det kommer til informasjonssikkerhet. Resultatene peker også til at aktørene i byggebransjen ikke klarer å tilpasse seg fort nok til den økte kompleksiteten som smarte bygg innebærer. Dette har ført til at systemer ikke blir implementert med tilstrekkelige sikkerhetsmekanismer. Videre fører mangelen på planlegging for drift og vedlikehold av bygningene til utilstrekkelig samarbeid mellom interessenter som er ansvarlige for denne fasen. For å løse disse utfordringene, foreslås metoder som er delt inn i tre kategorier: Nasjonale og bransjeløsninger, foreslåtte tiltak for byggherrer og teknologiske løsninger. For øyeblikket må byggherrene selv sørge for at informasjonssikkerhet blir en større del av deres byggeprosjekter, og at relevante interessenter er samstemte og etablerer driftsprosedyrer som tillater sikker drift og vedlikehold.

Contents

Glossary . . . . . **i**
Abstract . . . . . **iii**
Sammendrag . . . . . **v**
Contents . . . . . **vii**
Figures . . . . . **xi**
Tables . . . . . **xiii**
1 Introduction **1**
1.1 Scope, Assumptions and Limitations 1
1.2 Research Questions 2
1.3 Outline of the Thesis Paper 3
2 Background and Related Research **5**
2.1 Construction Projects 5
2.1.1 Stakeholders in Construction Project 6
2.2 The Evolution of Smart Buildings 8
2.2.1 Operational Technology and Information Technology 8
2.2.2 Building Automation Systems 9
2.2.3 Smart Buildings 9
2.3 Information Security 11
2.3.1 Security Principles 12
2.3.2 Security Principles in OT and IT 12
2.3.3 Relevant Security Frameworks 13
2.4 Information Security in Smart Buildings 14
2.4.1 Market trends 14
2.4.2 Threat Landscape 15
2.4.3 Known Attacks 16
2.5 Related Research 17
2.5.1 Research on Security in Smart Buildings 17
2.5.2 Security Aspects to IT-OT Convergence 19
2.5.3 Adding Collaboration in Construction Projects 20
3 Methodology **21**
3.1 Research process 21
3.1.1 Design Phase 22
3.1.2 Production Phase 22
3.1.3 Finalizing Phase 23

3.2 Research Methodology . . . 23
3.2.1 Phenomenological Study . . . 24
3.2.2 Literature Review . . . 24
3.3 Interview Planning . . . 25
3.3.1 In-depth Interviews . . . 25
3.3.2 Interview Design . . . 25
3.3.3 Pilot Interview . . . 26
3.3.4 Interview Language . . . 26
3.3.5 Handling of Personal Data . . . 28
3.4 Recruitment . . . 28
3.4.1 Sample of Population . . . 28
3.4.2 Sampling Method . . . 30
3.4.3 Sampling Technique . . . 30
3.4.4 Sample Size . . . 31
3.5 Interviews and transcription . . . 31
3.5.1 Collection Method . . . 31
3.5.2 Processing and Analysis . . . 33
3.6 Validity and reliability . . . 33
3.6.1 Considerations on Validity . . . 33
3.6.2 Considerations on Reliability . . . 34
3.7 Ethics . . . 34
4 Results . . . 37
4.1 Current Challenges . . . 37
4.1.1 Organizational Challenges . . . 37
4.1.2 Technological Challenges . . . 40
4.1.3 Challenges Related to People . . . 41
4.2 Current Measures . . . 41
4.2.1 Current Organizational Measures . . . 42
4.2.2 Current Technological Measures . . . 43
4.2.3 Current Measures Related to People . . . 43
4.3 Predicted Future Challenges . . . 44
4.4 Proposed Solutions . . . 44
4.4.1 Proposed Organizational Solutions . . . 44
4.4.2 Proposed Technological Solutions . . . 46
5 Discussion . . . 49
5.1 Current State of Application of Information Security in Smart Buildings . . . 49
5.2 Proposed Methods and Solutions to Achieve Secure Smart Buildings 51
5.2.1 National and Industry Solutions . . . 51
5.2.2 Proposed Actions for Project Owners . . . 52
5.2.3 Proposed Technical Solutions . . . 56
5.3 Limitations of the Research Project . . . 58
5.4 Future Work . . . 60
6 Conclusion . . . 61

Bibliography **63**
A Intervjuguide **71**
A.1 Introduksjon 71
A.2 Spørsmål 71
A.2.1 Innledende spørsmål 71
A.2.2 Forskningsspørsmål 71

Figures

2.1 Construction Processes and Phases, adapted from [5, p. 36] 6
2.2 Comparison of traditional building networks and trending, converging networks [7, p.19] 10
2.3 Smart Building Readiness [18, p.14] 11
2.4 IEC 62443 Overview [22] 14
2.5 Impact from CPS-related Incidents [27] 15

3.1 Research Process 21
3.2 Venn Diagram of Sample 29

4.1 Categorized Current Challenges 38
4.2 Categorized Current Measures 42
4.3 Categorized Proposed Solutions 45

5.1 Information Security Risk Management, [source: own] 54
5.2 Collaboration Phase, [source: own] 55
5.3 Compared Processes for authenticating endpoints, [source: own] . 57
5.4 Venn Diagram of Actual Sample of the Population 59

Tables

3.1 Research and Interview Questions 27
3.2 Response Rates From Interview Recruitment 31
3.3 Off-line and On-line interviews 32

Chapter 1

Introduction

Lately, the construction industry have been constructing *smart buildings* that are connecting and integrating more and more systems that support the building's energy management, facility security and workplace technologies. The market for smart buildings is predicted by Gartner to double in size within 2030 [1], and in a report from McKinsey the estimated value of Internet of Things (IoT) in offices are predicted to have a annual growth of 17-22% up until 2030 [2]. As the traditional Building Automation Systems (BAS) are being connected and integrated, and the construction industry is lacking IT-literacy [3], the approach to information security has not been a priority in the industry. Another consequence of BAS adapting the Internet Protocol (IP) and becoming increasingly interconnected, is the convergence of IT and OT environments [4] , which introduces business opportunities as well as challenges regarding information security for the construction and real estate industries.

This research project look at relevant stakeholders in smart building construction and operation and assess how they plan, organize and implement systems in smart buildings with regards to information security. A total of 9 interviews were conducted with recruited stakeholders to gather information on what challenges they were facing, how they mitigated these challenges and what solutions they would propose the industry. Further, the researcher proposes methods and measures to improve information security based on the findings.

1.1 Scope, Assumptions and Limitations

The scope of the report is assessing the level of information security of commercial buildings including the construction and maintenance of such buildings. The report does not consider buildings requiring special design measures such as hospitals, factories or buildings approved for classified activities. A primary focus of the report is to look at the processes by actors that are responsible, or relevant for information security as technology is implemented and operated through the

lifecycle of the building. A qualitative study using in-depth interviews of industry stakeholders were conducted to gain insight into how information security is applied in smart buildings. Individuals representing different stakeholders in real estate, construction and IT were interviewed to gain a holistic view on the situation in the industry. The target audience of this research is individuals that are involved in planning, managing, implementing, operating, monitoring or maintaining the connected IT or OT systems in a smart building, as well as students or researchers studying the topic.

The research is conducted in Norway and all interviews were conducted with Norwegian citizens, leading to the possibility of challenges and proposed solutions being specific to the country, or the region of the world. At the time of writing, there was no existing national building regulations requiring information security measures to be implemented in construction projects, or in buildings in general.

The research only recruited participants from the private sector and does not compare any smart buildings between private and public sector. This was mostly due to time constraints related to recruitment of interview participants and data collection.

Even though the research project aims to present possible proposed measures and tools for mitigating industry challenges related to the application of information security, any such propositions will only be presented in brief. Due to the time constraints of the research project, further development of proposed methods and measures was kept outside the scope.

1.2 Research Questions

The following research questions have been set out to be answered in the project:

- **Research question 1:** How does the real estate industry stakeholders incorporate information security into smart buildings during the construction projects?
- **Research question 2**: How can the real estate industry achieve improved information security in smart building projects?

The first research question aim to identify challenges and measures taken when it comes to information security in constructing smart buildings. This will be an assessment of status quo of the application of information security in the industry. The second research question looks to see how stakeholders in construction projects can obtain increased security in smart buildings and then the researcher will present proposed methods and measures to achieve this.

1.3 Outline of the Thesis Paper

Chapter 2 presents background theory that is relevant to the research as well as a section about related research. The background theory and related research are separated into different sections as it is more convenient for the reader as they can choose what to read to a higher degree.

Chapter 3 describes the methodology for the research project. First the overall project process is described, and then each part of the process is presented in detail.

Chapter 4 presents the analyzed data from the interviews conducted in the research process. The results are visualized to make the data easy to interpret.

Chapter 5 discuss the results and three different categories of proposed methods on how to improve information security is presented, each in a different section.

Chapter 6 presents final conclusions and directions for future work on the topic.

Chapter 2

Background and Related Research

This chapter will give the reader background knowledge and show how it is relevant by looking at existing, related research. The chapter is structured in subsections as follows: An introduction to construction process and its stakeholder is presented. Then an introduction to the topic of information security is provided before smart buildings and their components is explained. A description on how information security is relevant for smart building is provided by looking at market trends, and known attacks. Finally, a description of related research is provided.

2.1 Construction Projects

This section will explain how stakeholders are organized during construction and delivery of the smart building, and the production and operational phase. The construction process and organization is described as shown in [5].

The generic construction project consist of three core processes that overlap in varying degree from project to project.

- *Programming process*: Identification of requirements that needs to be satisfied
- *Engineering process*: Development and formalization of the physical properties of the building
- *Production*: Construction of the building

Further, construction projects consist of four main phases that characterise how far into the project the organization is. The phases are as follows:

- **Idea phase**:The idea phase is where the purpose, goals and ambitions for the future real estate is defined. The phase often uses creative methods as well as systematic ones to keep the balance between visions and what is possible to achieve. The scope for both magnitude, complexity, cost and time is decided upon in this phase.

- **Development phase**: Development phase defines the physical implementations that are going to be realised in the construction of the building. Technical descriptions and, drawings and other documents describing the finished building are produced by engineers and architects. This phase uses input from the programming process where specifications from the project owners were defined, and outputs specific solutions that evolves through the engineering process. This phase is primarily goal-driven and less creative than the idea-phase.
- **Implementation phase**: In this phase, plans that were made in the previous phases are executed. Construction of the building starts in this phase which makes is a mostly activity-driven phase.
- **Operational phase**: This phase mark the end of the construction of the building and the beginning of the operational phase. Flaws that occurred during the construction need to be delivered in this period and disputes between project owner, contractors and tenants need to be settled. The roles in construction projects are discussed in Section 2.1.1.

To illustrate how the phases overlap with the processes in a construction project, see Figure 2.1.

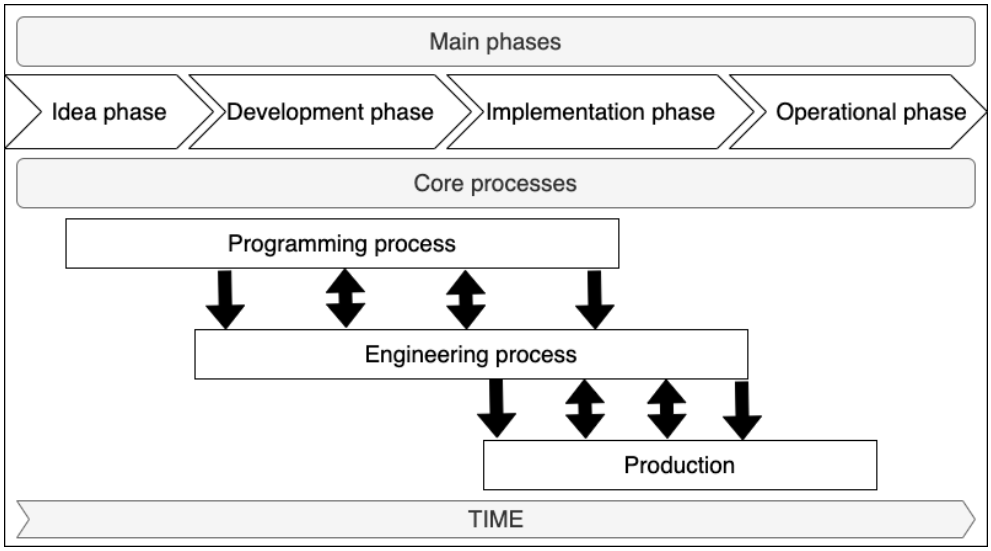


Figure 2.1: Construction Processes and Phases, adapted from [5, p. 36]

2.1.1 Stakeholders in Construction Project

Different stakeholders are required to have a building constructed. There are roles for creating the project itself, as well as others for planning, construction, deliveries, and making it ready for people to move in. Relevant roles in the building project are as follows [6]:

- Project owner, client

- Project management
- Engineering management
- General contractors
- Subcontractors
- Tenants

Project Owner The *project owner* is the person or company who owns the responsibility and rights for the construction project. The project owner is also the employer for most of the other stakeholders in the duration of the project. The project owner normally comes from a real estate company which is a different name of the stakeholder. Real estate companies are the owners of finished buildings. Both definitions will be used in the research project depending on whether the context is a construction project or an existing building.

Project Management Teams Working under the project owner, the *project management* maintains the organization, facilitation and coordination of the construction project in its entirety. Administrative tasks such as controlling the costs, leading hiring processes and ensuring progress are key tasks of the project management.

Engineering Management The *engineering management* is made up by building architects and engineers with different specialities and have the purpose of providing the following:

- Produce graphics or drawings for the project owners that is used to both for project owners to see a glimpse of the final result, but also to use in the application for building permits by the local government.
- Create the foundation for the construction of the building. This is done by making technical drawings for the specialized fields of expertise that will construct the building.
- Create the basis for contracts in certain projects.

General Contractors On the building site, *general contractors* are in charge of the construction on the site, which include administration of materials, planning of construction, and leadership of the contractors that are doing the physical construction and vendors who are supplying the project with materials. The general contractor is responsible for risks associated with subcontractors, procurement of materials and components.

Subcontractors *Subcontractors* provide materials and components to the construction site and installs them. Subcontractors are often specialized within many different fields of expertise such as concrete, roofing, window installation, surveillance systems, HVAC and so on.

Tenants The tenants are the stakeholder that rents, or owns space in a building. Tenants are in some cases involved in parts of the construction project if they require certain facilities for the building space that they rent or own.

2.2 The Evolution of Smart Buildings

2.2.1 Operational Technology and Information Technology

Comparing Operational Technology and Information Technology

OT is a term used to describe programmable systems and devices that either detects or makes changes to the physical environment. Such devices can together control processes and monitor environments and are used in many different sectors such as industrial control systems, building automation systems or transportation systems [7]. The main focus in OT is to maintain production output in some way of form, be it manufacturing goods, producing oil, producing power or creating a comfortable climate in an office building. The OT processes are often directly linked to revenue of a company and therefore, stable operations are of the highest priority [8].

IT on the other hand, is defined as being the term for all information processing software, hardware, communication technologies and related services. [9]. IT focuses on satisfying the informational needs of the organizations, be it storing of sharing information [8].

A type of system that is often brought up in conjunction with the OT environment is Cyber Physical Systems (CPS). CPS are systems that interact with the physical world by sensing and controlling the physical processes. The term is a umbrella term for systems such as Industrial Control Systems (ICS), BAS and IoT amongst others. In most conversations, the term IoT is used instead of CPS, even though IoT commonly refer to commercial consumer products [10]. In the IT environment, the term IoT can include devices such as printers, smart TVs, smart phones or smart watches [11]. The terms CPS and IoT will be used interchangeably through the project when referring to IT- or OT-systems that connect with the physical world.

OT-IT Convergence

OT systems were traditionally isolated from the IT environment, much because OT systems were using proprietary protocols that were not compatible with IT systems. In more recent times, the OT protocols have developed into being compatible with Ethernet and IP which layed the foundation for a convergence between IT and OT. This has happened in parallel to the industry demanding higher degree

of connectivity and being able to leverage IT systems in the operation of OT processes. While this trend is convenient for the industries, it contradict the isolated nature of the OT systems, and makes them more vulnerable from the internet. In modern IT-OT environments, security teams are faced with the challenge of making IT security mechanisms to function in the OT domain as well [7, pp. 24].

Service Providers for IT or OT environments are referred to as *IT service providers* or *OT service providers*. Service providers supporting both environments will be referred to as IT-OT Service Provider (IOSP) during the research project.

2.2.2 Building Automation Systems

A modern building uses BAS to monitor and control functions that are a part of the building with the goal of increasing user comfort and reducing operational cost. Such systems usually consisted of heating, ventilation, and air-conditioning (HVAC), lighting and shading. Utilizing BAS to reduce operational costs were prioritized as the cost of a building during its lifetime was far greater than constructing it [12]. Since the 1980s and the beginning of the 1990s, BAS were siloed systems existing on separate physical networks in buildings that were running non IP compatible, proprietary protocols that were developed by the manufacturers [13]. This meant that integration with other BAS and the enterprise environments were complex and sometimes, impossible, which also made remote management hard to achieve. The IT environment would often run isolated from the BAS, having IT personnel focusing on the enterprise, leaving BAS vendors tending to their own systems. Such siloed architectures are shown in Figure 2.2a

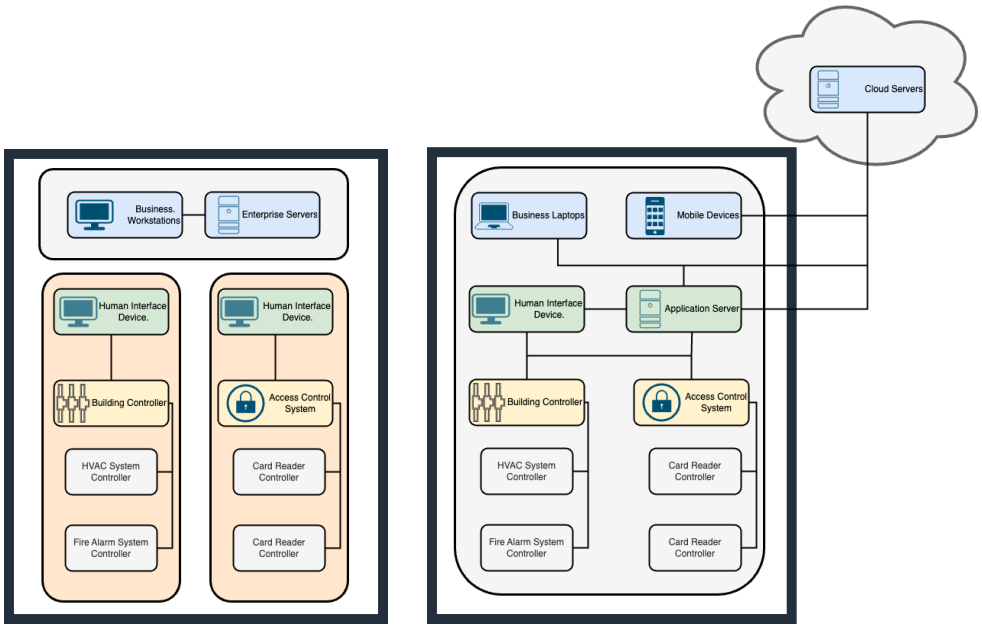
More recently, BAS have evolved to support the same physical cabling infrastructure as IT equipment and the protocols have been standardized, as well as adapting to use the IP for communication. This would enable BAS to be connected to the internet, which would allow for centralized remote management [14] and features such as cloud connectivity and wireless integration [13]. This converging architecture is illustrated in Figure 2.2b

The rapid development of BAS that supported higher degree of integration and connectivity has been very convenient for the industry, but it has also become increasingly vulnerable to cyberattacks as time went by, which is summarized in [15]. Recent discoveries reveal critical vulnerabilities with building automation manufacturers where attackers could gain control over BAS [16].

2.2.3 Smart Buildings

Smart buildings are buildings that deliver a converged infrastructure where the BAS and IT environment integrate together to offer a adaptable experience for all stakeholders and customers. The goal of smart buildings is to deliver energy

efficient, sustainable and user friendly environments for tenants and facility management with the purpose of reducing operational costs and increasing Return Of Investment (ROI) for stakeholders [17]. To achieve this, integration between systems is set up, such that the building is connected to both the systems and the people interacting with the building [13]. The market trend of the construction of smart buildings is substantiated by Gartner [1], that predicts the market worth of smart building IoT would double from 2020 to 2030 at an estimated 108 billion USD.



(a) Siloed Networks **(b)** Converged Networks

Figure 2.2: Comparison of traditional building networks and trending, converging networks [7, p.19]

In a report published in 2017 from the Buildings Performance Institute Europe (BPIE) [18], a study was made to indicate if different countries in Europe were ready for smart building environments. The indicators showed how a country was ready for smart buildings based on how smart-ready the wider infrastructure is. A map from the report seen in Figure 2.3, illustrate how assessed smart building readiness differ between countries in Europe. The figure shows that Scandinavian countries, including the Netherlands were classified as "front-runners", while most of eastern and southern Europe are lagging behind.

In a report published by the *The Counselors of Real Estate* in 2021, the author tried to predict how the future workplace would look in a post-pandemic world [19]. She writes that the workplace was becoming more employee-centric and

corporations would need to address hybrid working models to some degree as employees wish to have more flexibility in their careers. As corporate workplace strategies are changing, the need for what is referred to as *intelligent* and *healthy buildings* arises to make offices a place for collaboration. Such buildings leverage IoT sensors for environmental management as well as tracking buildings occupancy patterns. Workplace apps would be needed for tenants to be able to reserve meetings rooms or other facilities.

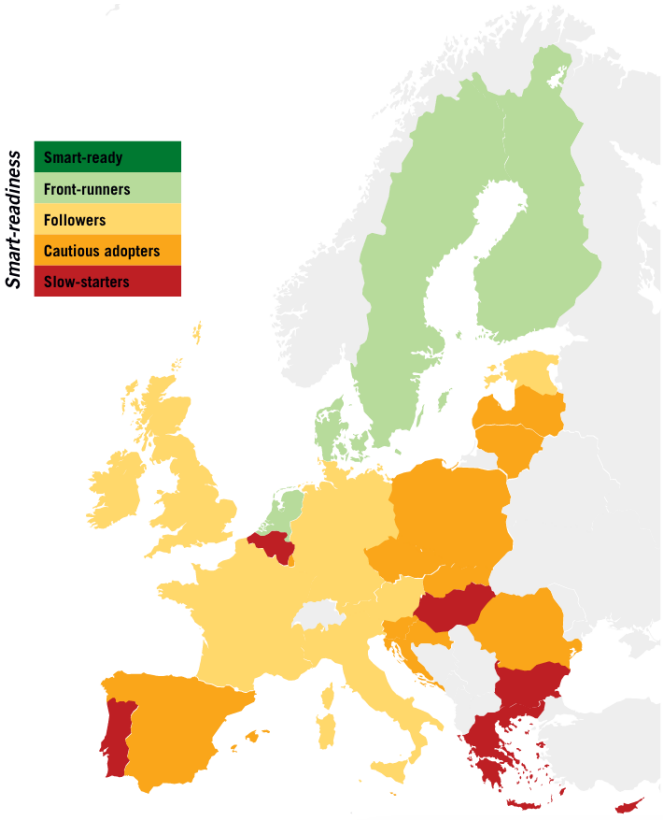


Figure 2.3: Smart Building Readiness [18, p.14]

2.3 Information Security

The definition of information security that will be used through the research project is the following given in [20] as "*Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology*". The purpose of information security is to protect both physical information and virtual information that only exists digitally. This means that information security aims to protect information written on paper, information that is verbally communicated, and digitally stored information.

2.3.1 Security Principles

There are three main security principles that information security aims to achieve: Confidentiality, Integrity and Availability. These principles are briefly explained below:

Confidentiality The term relates to the upkeep of secrecy and hiding of the information. This makes sure that the information does not become known to any outsiders that are not supposed to have the information. Cryptography is one of the most common methods for achieving confidentiality of the information, which is a technique of obscuring information such that only the sender and receiver can decrypt the information using some form of key [21, p.22].

Integrity Integrity is a property of information that describe if it can be trusted or not. Integrity ensures that information can not be altered by accident or on purpose by an attacker. Changes to information in contracts, personal information or parameters in a control system of a production facility are examples that can cause severe consequences for an individual or a company. Certain mechanisms within cryptography are designed for providing the property of integrity to information [21, p.22].

Availability This term explain the ability to access a service or piece of information when needed. Availability is critical for information security as authorized staff needs to have access to the required information. Having issues with accessing software or web services such as online banking are examples of breaches in availability for the information that the service would provide. Measures such as redundancy in infrastructure, and backup solutions can be implemented to increase availability of information [21, p.22].

2.3.2 Security Principles in OT and IT

Because of the fundamental differences between the focus of IT and OT, the security principles for the technologies differ as well. Information security have traditionally been divided into three different principles; confidentiality, integrity and availability. These have been covered in Section 2.3.1. When it comes to IT, the priority of these principles have been to prioritize confidentiality, then integrity and then availability. For OT the order of priority is reversed as availability is the priority, then integrity and confidentiality lastly. In addition, there have been defined additional security principles for OT due to the nature of the environments that OT exist in and its criticality in our society [22, p. 40]. The list below sums up the additional security principles for OT[22, p. 41]:

1. **Access Control**: Protects access to device or system. Measures can both be physical, as in lock pads for certain areas, or virtual, where identity policies would only allow certain identities to *access* the systems.

2. **Use Control**: Protects use of device or system. Measures implemented to only allow certain identities to *operate* a system.
3. **Restrict Data Flow**: Protect against leaked communication within system or between devices. Network security mechanisms can be used to prevent traffic from leaving certain networks.
4. **Timely Response to Event**: System being able to react properly to certain events, particularly to events related to mission- or safety-critical situations.

2.3.3 Relevant Security Frameworks

Several frameworks exist to aid organizations in approaching information security for their IT and OT environments. Some of them are briefly presented in the following paragraphs.

ISO/IEC 27000 Family

ISO/IEC 27000-family is known as a family of standards for Information Security Management System (ISMS) that provides frameworks to industries that needs to manage security of their assets, information, property and employees. An ISMS is an organizations systematic approach to establish, implement, operate and maintain information security based on policies. The first document, ISO/IEC 27000 gives an overview of what an ISMS is, how to establish it, and how to make it successful. Three standards from this framework are particularly relevant and they are as follows:

- **ISO/IEC 27001:** This standard explain how to establish, operate and maintain a ISMS [23].
- **ISO/IEC 27002:** The standard present information security controls, that are defined as *measures that maintain and/or modifies risk* [24, p. 2]. Different information security controls divided into categories such as 'organizational controls', 'physical controls', 'people controls' and 'technological controls' are listed and explained. These controls can be implemented to mitigate risks identified by risk analysis [24].
- **ISO/IEC 27005:** This standard is a guide in risk management and explain how to identify, assess, treat and monitor risks in an organization [25].

NIST SP 800-82r3

National Institute of Standards and Technology (NIST) has published a framework [7]. This guide explains how to develop an OT cybersecurity program, how to perform risk management for OT systems and how to apply an OT cybersecurity architecture.

IEC 62443

The International Electrotechnical Commission (IEC) propose a collection of documents that cover network and systems security for Industrial Automation and Control Systems (IACS) [22]. Figure 2.4 gives an overview of publications in the IEC 62443 framework. The framework describe how processes, systems and components can be secured by different stakeholders. Documents such as the IEC 62443-2-1 is aimed at business owners and stakeholders responsible for information security of the systems. The document describe how to set up a IACS security program that includes risk assessment, security policies and training of staff. IEC 62443-2-4 provide detailed system security requirements and is aimed at the stakeholder being responsible for design and implementation of the system. And for system providers and developers, the IEC 62443-4-1 describe how to integrate security into development of systems.

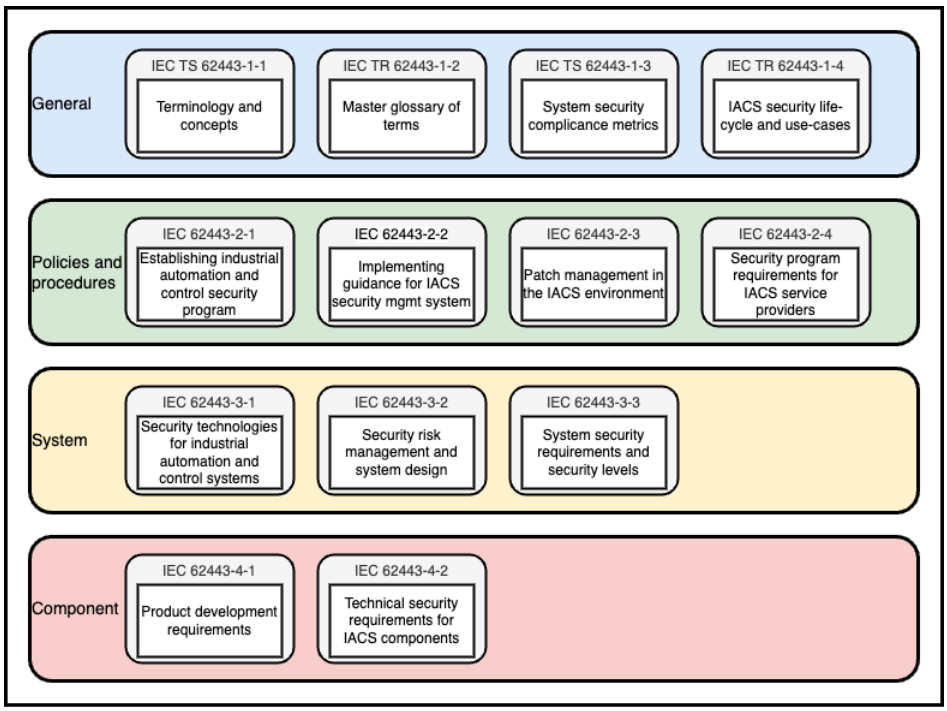


Figure 2.4: IEC 62443 Overview [22]

2.4 Information Security in Smart Buildings

2.4.1 Market trends

In a 2022 report from Gartner on the matter of OT Security [26], a rapidly changing market is described as IT and OT connect more and more. And as the two traditionally separated environments interconnect, the need to secure all types of

CPS increase. Gartner predicts that by 2025, 70% of asset focused organizations will have converged their security systems such that they align with both the needs of IT and OT environments. In addition, Gartner [27] point to the consequences that CPS-related incidents could have, as illustrated in Figure 2.5. The arrow on the left in the figure represents the severity of the impact of the CPS. The higher up and the more red the arrow becomes, the more severe the impact is.

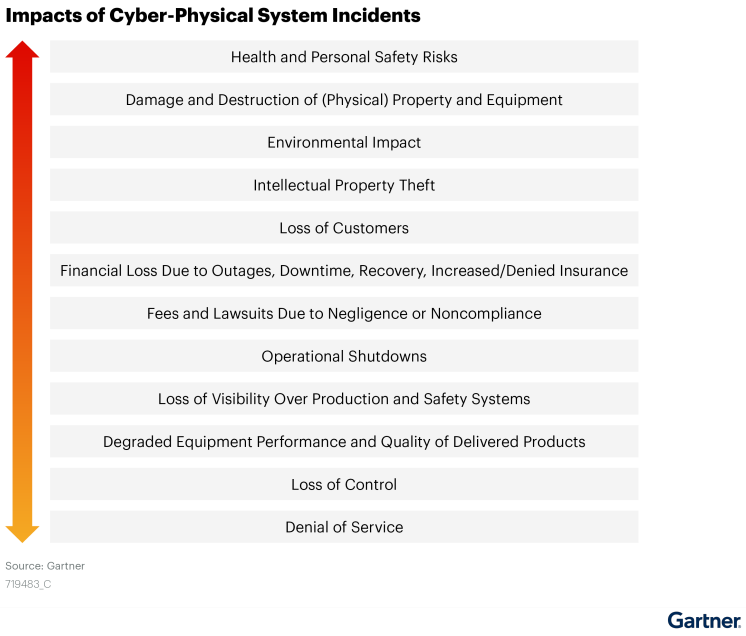


Figure 2.5: Impact from CPS-related Incidents [27]

2.4.2 Threat Landscape

An OT cybersecurity report by the network and security company Fortinet from 2022 showed that 49% of responding companies had experienced 3-5 intrusions in the prior 12 months, and 19% had experienced 6-9 intrusions. Further, they found that 40% of the intrusions only impacted the OT, while 21% impacted both OT and IT [28, p.22].

The term "siegeware" as mentioned in [29] is a term that describe a building being taken hostage by malware that takes control over the building. In such scenarios, building owners are often made to believe that they must pay ransom to have the hackers give the control back to the owners, which seldom happens.

Internet-facing smart buildings where BAS are connected to the internet is a challenge for the industry. By connecting BAS to the internet, this allows for remote access and maintenance, which is convenient for system providers, but it

also exposes the building for cyber attacks as pointed out in [14, p.38]. Such exposed BAS might be easy targets for remote attacks, and concerns for potential smart building botnets are also expressed in the study.

2.4.3 Known Attacks

There are several known attacks in the OT environment from the past decade, and some of these have been directly aimed at building automation.

A Distributed Denial of Service (DDoS) attack on several buildings in Finland caused failure in heating systems when temperatures were below freezing point [30]. The control systems that were attacked rebooted continuously while the attack was happening which lead to heating not being functional. The cause of the failing heating systems were not apparent to the facility staff as they had little knowledge about cyberattacks.

In Germany, a company supplying and monitoring building automation experienced loosing contact with hundreds of BAS [31]. A sophisticated attack had first used an internet exposed, unsecured UDP port to infiltrate the company before attacking Konnex (KNX) based systems. The KNX based BAS were wiped by the attacks and a new password was set that locked the company out from their own BAS. A security company that has analyzed what happened during the attack point to the underlying problem being that IT and OT teams not being sufficiently coordinated.

An attack that struck Scandinavian hotel company *Nordic Choice Hotels* in 2021 knocked out hotel access control systems and the elevators, forcing the staff at the hotel to operate the hotels with pen and paper before the systems were restored. The attackers performed a phishing attack utilizing a ransomware malware that is known as Conti to encrypt the hotel systems. Nordic Choice Hotels were offered the decryption key for 5 million USD but they ended up not paying the ransom, but rather managed to recover most of their operations within 48 hours [32] [31]. A similar attack happened in a U.S district when a ransomware attack encrypted critical systems which led to much of building automation and IoT in schools to be knocked out. This led to several schools being closed for several days [33]. Even if BAS were not the primary target in the two previous known attacks, these cases do exemplify how poorly converged infrastructures can make IT-systems more vulnerable.

The American retail company Target experienced a cyberattack that leveraged a HVAC contractor to further breach Target sale systems [34] [35]. A report describing the attack [36], explain how the attackers were able to retrieve login credentials to a Target billing portal for external parties from the HVAC contractor. The credentials was then used to get into the billing portal and further into the

sales systems of Target since the systems were not segmented from each other. The attack led to the attackers exposing information about 40 million debit and credit card . In 2017, Target had to pay 18,5 million USD in settlements as a consequence of the data breach. Even though the attack did not include hacking of BAS, it exemplifies how remote access management of contractors and vendors in day-to-day operations is crucial for securing services.

Malware known as *Pipedream* that was designed to target industrial control systems (ICS) was reported by American government agencies in 2022 [37]. Pipedream was identified as an expansive toolkit for hackers to target industrial network, and the kit contained several attacks for exploiting devices from Schneider Electric and OMRON. A white paper produced by cybersecurity company Dragos further explains the architecture of Pipedream and describing how an adversary can use the kit to achieve end-to-end attacks, intruding from the IT environment before traversing into OT [38]. Even though the toolkit was primarily designed for targeting ICS, an adversary could easily adapt the kit to work in other OT environments [37].

2.5 Related Research

2.5.1 Research on Security in Smart Buildings

A systematic literature review was made by Cihola et al. in [14] where security of smart buildings was assessed and the study found almost a complete lack of research on non-technical and organizational aspects on the topic. One study from 2016 [39] that was conducting a security analysis on BAS had found that there was poorly defined roles that were responsible for information security both in construction and operational phase. Lack of leadership during commissioning of systems as well as defined procedures for maintenance lead to poorly implementation of security measures as well as outdated documentation. In 2015 Caviglione et al. points out in [40] that there are human factors present for information security not being prioritized in BAS. Mostly they point to lack of awareness and knowledge in both vendors and consumers for security features not being a priority to being developed by the vendors, and not being ordered by the consumers. The paper also points out that there is a "non-optimized information exchange" between parties in BAS deployment projects, but there is little information about how such projects are organized or where the problem lies specifically.

There exists research on information security of construction projects where the focus is on the construction process and not so much on the finished buildings itself. In a study by Sonkor and García [41], they found that the lack of cybersecurity awareness in the construction industry was one of the main challenges in overcoming information security issues in the industry. In [42], a framework to

identify cybersecurity risk and assess vulnerabilities is proposed for the construction process. A simplified information security framework for the construction industry was proposed by [3], since the industry was known to have low IT-literacy. The framework identifies four kinds of elements that needs to be secured: Material stuff, information, people and systems. Furthermore, the framework defines security as the absence of three wrongs: stealing, lying and harming.

Opposed to the lack of research covering human factors, there have been several papers looking at the security of BAS. Valli et al. [43] provide historical explanation of why the BAS related protocol Building Automation Control Networks (BACnet) was and still is vulnerable. To make BAS more convenient to maintain for system providers, OT-teams have chosen to expose systems on the Internet which has increased the attack surface drastically. The BACnet protocol had failed to evolve with the market and known vulnerabilities could be exploited, unless other security mechanisms such as firewalls protected the system. The study also presented an attack that targeted the HVAC to increase the risk of fire in a building [43]. Vulnerabilities such as the one discovered by OT security company Nozomi give some context to how elementary security flaws in BAS can be [44]

In the book "Cyber-Physical Systems", a chapter on Security and privacy in CPS propose security measures to mitigate risk for cyber attacks as well as physical attacks on CPS [10]. By referring to real life examples they show how the importance of both information security and physical security matters in operation of CPS.

In [45] from 2010, Granzer et. al identifies attack targets in a network containing BAS. The targets are listed as follows:

1. **Field network:** Attacker interferes with the data being exchanged by the control applications.
2. **Backbone network:** Attacker might gain complete overview of all systems communicating over the network.
3. **Sensors, actuators and controllers:** Attacker tries to alter the behaviour of the devices in the BAS.
4. **Interconnection devices:** Devices such as routers, gateways or switches can be exploited to gain further access to, or knowledge about other networks that the BAS connects to. This can also be an access point from the internet.
5. **Management system:** Attacker can try to get access to system managing BAS to either alter behaviour or use to get foothold for attacks further into other networks via interconnection devices.

Furthermore in [45], attacks are divided into either *network attacks* or *device attacks*. For network attacks, the adversary would either need physical access to

the network, or access to a compromised device such as the management system of an interconnection device. Launching device attacks on the other hand would include either software attacks, physical attacks or side-channel attacks. Side-channel attacks are used to gain information about a device or system by observing or measuring certain parameters during operation. Technical solutions were proposed to mitigate the attack surface for both network and device attacks but the issue is pointed out to be that BAS were prone to attacks because systems lacked modern security features. Expanding on Granzel et. al, the paper written from [46] propose additional attack vectors for building automation and IoT. By using attack tree models they propose three attack vectors for building automation.

1. **Access local network through provider supplied device:** Provider supplied devices can be any kind of IoT or devices related to building automation. One of the ways to achieve this, is by first gaining access to the system provider, or by exploiting devices that are exposed out on the internet.
2. **Access user devices:** User devices can be laptops, workstations, phones or smart watches. Taking control over user devices can often be a intermediate step to further exploit other systems. Such devices can in some instances have access to controlling BAS or valuable information in an enterprise network. One attack vector to exploit is through storage providers. The next attack vector expands on these kinds of attacks.
3. **Access data at storage provider:** Storage providers can be cloud based storage providers such as Google or Amazon. BAS systems leveraging remote storage providers for storing data is a market trend that exposes the attack surface of the systems. An attacker that manages to alter the stored data might cause reactions in the BAS itself. Several methods to achieve access are proposed.

To mitigate risks of the proposed attack vectors in [46], network segmentation and cryptographically strong algorithms are advised.

2.5.2 Security Aspects to IT-OT Convergence

Graveto et. al raise concerns about security as buildings become more complex and traditional BAS integrate with IT systems. Integration between the two domains that traditionally were isolated from each other increase attack surface for both [15]. Maleh writes in [47] that mastering IT-OT convergence will require the organization to establish much better communication between the IT-people and the OT-people. The paper does not mention smart buildings specifically, but generalizes the trends in environments where traditionally IT and OT were separate domains, operated by separate people. Maleh also sums up the main challenges as follows:

- Lack of engineers and professionals that understands IT and OT.
- Lack of communication between IT and OT staff.

- Risk avoidance is highly prioritized in OT teams.

The cultural differences between people associated with the OT-environment and the IT-environment is also a factor that further increases the security issues that the convergence bring [48]. One of the core differences between the groups is that IT-teams value confidentiality over all, while OT-teams value availability the most. Such cultural differences might prolong the time that the industry is lacking a sufficient IT-OT security systems and practices. Grey literature from major industry players strengthens the prognosis about IT-OT convergence. They point out that the trend is caused by business demands and that the convergence will require changes in organizations, technology infrastructure and mindset [49] [50] [51].

If implemented correctly, a converged architecture can provide several benefits for organizations using them. Cost reduction, risk reduction, enhanced performance and better system flexibility are benefits of converged architectures according to [52]. Another study focusing on IT-OT convergence in the petroleum industry identified the convergence as an enabler for increased productivity, safety and efficiency [53].

2.5.3 Adding Collaboration in Construction Projects

Collaborative methods such as Integrated Project Delivery (IPD) has been proposed that involves key stakeholders early in design phases in order for them to improve deliveries in the projects [54]. The methods were also supposed to align contractors and engineering teams with the owner's goals. The IPD method is different from traditional construction methods, where information sharing, early knowledge contributions and collectively managed risk are key properties, opposed to traditional siloed processes and individually managed risks. A collaboration phase was introduced in a construction project in Norway to efficiently transfer knowledge from engineering teams to contractors, establish collaboration platform and review the plans for the project. One challenge that was reported the respondents in the projects, was that they were missing leadership and clearly stated responsibilities in the collaboration phase [6].

Chapter 3

Methodology

3.1 Research process

The research process was divided into three phases, with key processes and outcomes being relevant for the different phases. The relationship between the phases, processes, milestones and output over time through the project are shown in Figure 3.1.

The phases are and their relevant time periods were as follows:

1. Design phase (November 2022 - January 2023)
2. Production phase (February - April 2023)
3. Finalizing phase (May 2023)

The phases are explained further in the following paragraphs.

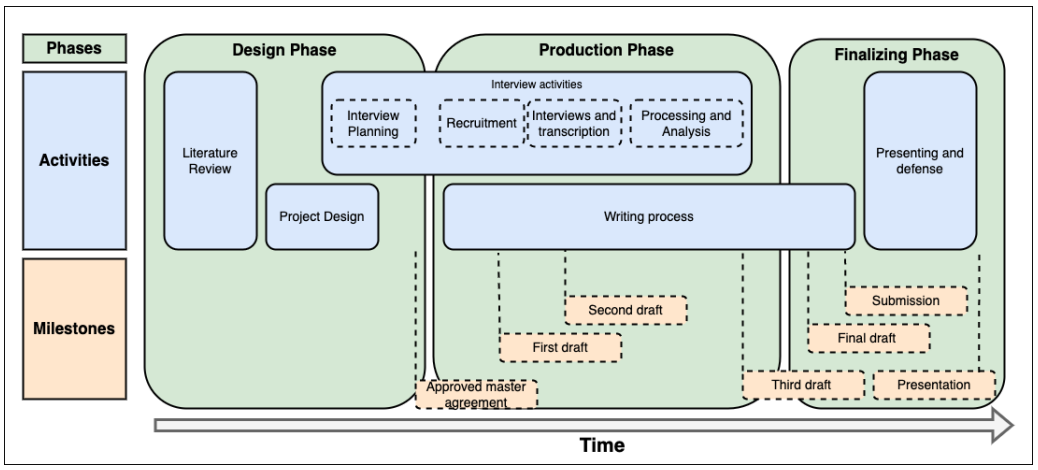


Figure 3.1: Research Process

3.1.1 Design Phase

This phase was started prior to the start of the master thesis course with the primary goal of formalizing the problem description, scope and project timeline to give time for writing the thesis in the production phase.

With regards to the project team, it was decided to have Intility as a external collaborator for the project for several reasons. First, the researcher had been employed by Intility for several years and needed time during working hours to work on the thesis. Secondly, the problem description was originally pitched by what would become the supervisor from Intility. Third, Intility had access to a professional network of relevant resources and people for the thesis. After it was decided that Intility would be a part of the thesis, a supervisor from Norwegian University of Science and Technology (NTNU) was recruited to be the primary supervisor for the project.

A literature review was also performed with the goal to acquire further knowledge about the field and familiarize with previous research and status in the industry. The exploration process also included discussions with the supervisor from Intility for deciding general scope and directions for the project.

Three outputs came from the introductory phase: A problem description for the thesis, a proposed timeline for the project, and a outline for the thesis report. The milestone marking completion of this phase was the approval of the master agreement between the researcher and NTNU.

3.1.2 Production Phase

During the production phase most of the interview activities were conducted as well as the majority of the work on the thesis report itself. Two main activities were progressing in parallel through this phase; the *Writing process* and the *Interview process*. The writing process started as soon as the plan for the project was finished, and lasted until the finalization of the thesis report. Having a continuous writing process was beneficial as it kept the researcher engaged in the material through the duration of the process. The interview process was made up of three smaller activities, *recruitment*, *interviews and transcription* and *analysis*. Participants for the study were recruited in the recruitment activity. Interviews and transcribed documents ensured that data was gathered, and transformed into readable text that could be used in the report. Finally, the analysis activity included processing and discussion of the data from the interviews.

The output of the production phase were the main chapters of the written thesis, being *Background*, *Methodology*, *Results*, *Discussion* and *Conclusion*. Each of the

chapters were considered as milestones in the project. Drafts of the written thesis were handed in to supervisor as chapters were finished.

3.1.3 Finalizing Phase

The last phase of the project was dedicated to complete the written thesis, submitting it and presenting the study. The last part of the writing process was completed in the period, and the output from that process became the completed thesis report. Two milestones such as, the final draft and the thesis being handed in marked the completion of the thesis report production. The final milestone was presenting and defending the master thesis.

3.2 Research Methodology

The primary goal of this thesis was to assess how information security was applied in smart buildings through its lifecycle. To achieve this goal, a qualitative method was chosen based on the some characteristics of the environment and what seemed to be most reasonable for achieving the most realistic and relevant results. The decision was based on the following traits that such a research project would seem to contain:

- In order to assess to which degree information security was applied in a certain part of a certain industry the researcher needed to explore a field and explain how the results might be of relevance. These characteristics were qualitative elements. A quantitative method would require the researcher to test some theory to validate it, which was not something that the researcher aimed to achieve. [55, p.99] This project was about creating theory.
- Further, the thesis was to provide a holistic snapshot of how something behaves in a very specific environment, which also is related qualitative aspects [55, p.99]. This was needed because the industry involved several stakeholders that would become the target audience for the thesis.
- As the thesis would explore the topic of information security in a smart building through its lifecycle, the collected information was expected to be mostly relevant by speaking to key stakeholders in the industry rather than looking for online information. This was due to the industry being fairly immature to the topic of information security compared to traditional IT-teams. Interviews are also typical characteristics for qualitative studies [55, p.99].

Because of the properties mentioned above, the researcher would choose a qualitative approach to the research, and the method that was chosen is explained in the next subsection.

3.2.1 Phenomenological Study

A phenomenological study is defined in [55] as being as study "... that attempts to understand people´s perceptions and perspectives relative to a particular situation". It is not unusual for the researcher to have personal experiences with such situations or events and wants to gain further knowledge about it. These studies often use long interviews on a small group of people that have had experience with the phenomenon. The interviews tend to be unstructured. A challenge for the researcher is to stay objective and focus on listening throughout the interviews when something familiar to the researcher is brought up by the participant, but it is crucial for the study that the interviews are not tainted by the researcher [55].

As this thesis is trying to uncover how information security is applied in smart building sector, people having experiences with either construction or operating such a building are believed to hold critical insights that might lead to a deeper understanding of how the situation really is. For this reason, the researcher chose to use in-depth interviews as a data collection method for the project which is further explained in Section 3.3.1. By speaking with key stakeholders in the smart building sector, different perspectives on the same processes could be uncovered and further make it possible to somewhat generalize about the situation in the industry.

3.2.2 Literature Review

The literature review was performed for the researcher to get familiar with the field of interest and to decide on how the research design was going to be. This was mainly done by using Google Scholar as primary search tool. This activity also lead to researcher being able to become familiar with industry specific vocabulary and expressions, further improving efficiency and accuracy for finding relevant material. The activity was also used to rule out existing research that would cover the topic of what the researcher had intended to study. The search engines used for the literature review was mainly Google Scholar and NTNU Digital Library.

The following search keys were used for the literature review:

- <Information Security> OR <Cyber Security> OR <Convergence> AND <in> AND <Smart Building> OR <Building Automation System> OR <Cyber Physical System>
- <Information Security> OR <Cyber Security> AND <Framework> OR <Standard> AND <For> AND <Smart Building> OR <Building Automation System>
- <Information Security> OR <Cyber Security> AND <in> AND <Construction>

There were requirements to how old the literature could be, and there were different requirements for different uses of the literature. Three different categories were defined:

- Background theory: Literature used for background theory in the research, should not pre-date the year 2010. Some foundational information security concepts and smart building concepts have not changed much during the time from 2010 to 2023, so this was considered as relevant information.
- Construction Industry: The Construction industry was evolving more slowly than other technological industries and literature was required to not pre-date the year 1990
- Related research: For the related research, the most strict requirement was set. Effort was made to avoid using literature pre-dating 2017, and literature older than 2010 would not be used.

3.3 Interview Planning

This section and its subsections describe all planning related to the interviews in the research project.

3.3.1 In-depth Interviews

For the project, in-depth interviews were chosen as the primary data collection method. In such interviews, a set of predefined questions are asked to a participant, that can be answered freely. Follow-up questions can also be used by the interviewer to further probe into the topic of relevance . These kind of interviews are used when the researcher have knowledge about the domain, but wish to study it on a deeper level and need to investigate other peoples perspectives and meanings [56, p.197]. Such interviews can help the researcher with gaining deep knowledge that would be hard to retrieve by using other methods such as surveys [57], which made it a preferable method for this project where the researcher was looking for deep insight into a specific phenomena. As the participants in the interviews would have different backgrounds and most of them not having very in depth, technical experience with IT, the researcher anticipated that some interviews would need some clarifications or explanations to ensure that the participant understood the context and the questions. This added to the arguments that in-depth interviews would be the chosen data collection method for the project.

3.3.2 Interview Design

The interviews were structured into two parts which were:

1. Introduction
2. Interview Questions

a. Introductory Questions
b. Investigative Questions

The introduction part of the interview would ensure that the participant had an understanding of the context of the topic as well as knowing how the data were going to be used in the project. First, the researcher would present himself with his background. Then, a brief summary of the research project was explained by the researcher to make the participant settle into the context. Third, a statement about the right to withdraw from the project was made, as well as a statement about how personal data was handled in the project. Finally, the signing of the consent form for the interview was made, if that was not already in place.

In the second part of the interviews questions were asked to the participant. There were two sub-parts of the questions: introductory and investigative questions. The introductory questions helped in warming up the participant for the investigative questions, which would make the interview more natural in the sense that the conversation would gradually go deeper into the topic as the interview progressed. The introductory questions were the following:

1. What tasks does your work include on a daily basis?
2. What roles have you had in relation to smart building in either construction or operation?
3. How would you describe a smart building?

The investigative questions were used to answer the research questions for the thesis and their relationship is shown in Table 3.1.

3.3.3 Pilot Interview

To prepare the researcher for conducting the interviews and to verify that the interview questions gave the interview a natural flow, a pilot interview was conducted before other participants were interviewed. The pilot interview was conducted with the supervisor from Intility as participant. The pilot interview was considered as a success as it sparked some ideas for easing the participant into the topic before diving deeper. Changes were made to the introductory part and the question about how the participant would describe a smart building was added. The second change, was that a question was added at the end of the interview to have the participant gather thoughts and ideas into one answer. These changes can be seen in the final versions of the questions as the third introductory question and the last investigative question in Table 3.1.

3.3.4 Interview Language

The language of the interviews were chosen to be Norwegian as this was the native language of the participants to ensure that the conversational form of the interviews were as natural and smooth as possible. And by using in-depth interviews

	Introductory Question
	1. What kind of tasks does your current position involve? 2. What other positions have you had related to constructing or operating smart buildings? 3. What is a smart building to you?
Research Question	**Investigative Question**
How does the real estate industry stakeholders incorporate information security into smart buildings during the construction projects?	1. Do you and the stakeholder you represent have any responsibility for providing information security for smart building in either construction or in operation? If so, responsibility of what? 2. How do you and the stakeholder you represent make sure that information security is sufficiently implemented in smart buildings? 3. Do you have any specific examples of how information security might not be implemented optimally or mismanaged in construction and operation of the building?
How can the real estate industry achieve improved information security in smart building projects?	1. In your opinion, do you think smart buildings are designed with adequate information security today? If no, explain any measures or methods that might improve security. 2. What are your thoughts on the priority of information security during construction and operation of smart buildings? 3. How would you describe a sufficiently secure smart building, and how would you achieve it?

Table 3.1: Research and Interview Questions

any potential misunderstandings could be clarified. This was believed to extract better answers from the participants as they were able to use familiar terms and expressions. Forcing the English language on people that were not used to speaking it daily might have lead to information being miscommunicated or not communicated at all if the participants were uncertain of how to explain scenarios, relationships or technical phenomena. As the thesis is written in English and interviews being held in Norwegian, the answers had to be translated before discussing the answers in the report. The process of translating might have induced some errors by the researcher, if not done correctly. Certain words and expressions can be hard to translate directly word-by-word from Norwegian to English. This risk

was judged to be outweighed by the advantage of having the participants speak in their own language.

3.3.5 Handling of Personal Data

The researcher had decided to keep all participants of the research project anonymous through the project and in the final thesis report for the following reasons:

- The participants right to privacy was a priority in the project as there was no reasonable cause for having the individuals to be identified by anyone other than the researcher through the project, or in the final report.
- By hiding the identity of the participants, their professional integrity would not be risked of being compromised if some opinions were shared that others in the field would not agree with.
- Anonymous participants could be argued to lead to better and more honest interviews, because participants doesn't have to be stressed about people knowing what their opinions on the matter was. For this project, it was expected that some participants representing one stakeholder might blame other stakeholders for problems with information security in smart buildings, which might make such opinions sensitive for the participants.

To ensure that collection of information and storing of information would not compromise the identity of any participants in the project, the researcher used two guides for collection and storage provided by NTNU [58] [59]. The data collection guide explain how to securely collect data in accordance with the classification of the data. The data storage guide explain how to choose the correct medium for data storage depending on the classification of the data. The guides also provide guidance on how to classify data relating to how sensitive the data is and how much personal information the research requires.

According to the NTNU data collection guide [59] a the researcher had to notify the "Norwegian Agency for Shared Services in Education and Research" [60] with a description of what personal information that was to be collected as well as how the data would be stored and deleted. When the notification was approved by the agency, collection of data could begin.

3.4 Recruitment

3.4.1 Sample of Population

As the thesis was looking at information security in smart buildings, a sample of individuals that had experience and was active in the fields of information security and smart buildings was the target group. In addition, the research was looking at

the matter of information security in smart buildings during construction and day-to-day operations. Therefore, individuals that were responsible for construction of smart buildings, implementation of connected systems and/or for information security were also a target group. Figure 3.2 illustrate the sample of individuals that would be able to represent a relevant population. Only individuals that were either holding a "senior" title, or that were known for their long experience were considered for being recruited. The researcher would verify potential participants' experience by either looking at their work title while using LinkedIn or e-mail, or having heard of individual experiences from other sources.

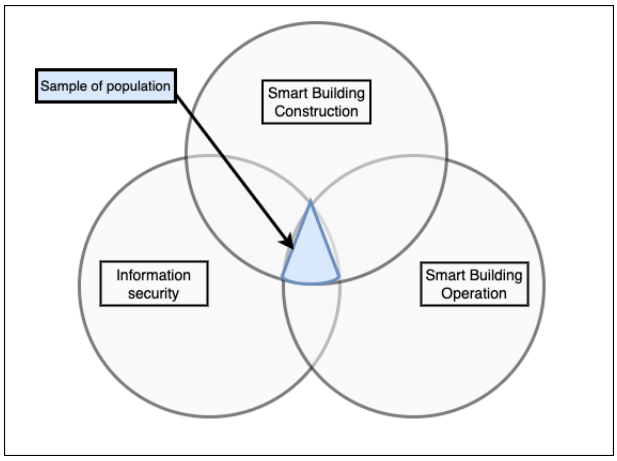


Figure 3.2: Venn Diagram of Sample

From the defined sample, six stakeholders were identified to provide relevant perspectives on the topic. The stakeholders were as follows:

- Project owner, real estate owner
- Engineering management in construction
- General contractors
- Subcontractors
- IT/OT/Security operations
- Relevant experts in the field

Even though IT or OT service providers can be considered as subcontractors in construction projects, they are identified in a separate category due to their importance when it comes to information security implementation and operation of smart buildings. Building tenants were not identified as a stakeholder in the context of information security in smart buildings. Tenants are the end users of the building and were believed to have little impact in the way other stakeholders implement security measures for systems and infrastructure.

For the research project, no effort was made to achieve balance between genders of the population. There were two main reasons for this not being prioritized at

all for the project: First, the relevance between the genders and the research questions seemed to be weak and not important. As the sample consisted of a relatively small number of individuals, and many of them with different backgrounds, differences between opinions of men and women would be hard to identify. Secondly, both the construction industry and the IT-industry are male dominant environments [61], which would require much more effort in the recruitment process for the researcher to achieve equal representation of the genders.

Participants were not recruited based on age. As there were requirements for having minimum 5 years experience and that they had to be active in the field, this would rule out most individuals below 25 years of age, and retired individuals. Requirements for education was not considered in the recruitment process either due to that the stakeholders would have mostly different backgrounds which would be hard to generalize without narrowing down the sample too much.

Biases from the different stakeholders were expected due to their experiences at construction sites or in operating smart buildings. As they might have experiences where they would not agree on responsibilities or terms with other stakeholders, fingers pointed to those being to blame for their challenges were expected.

3.4.2 Sampling Method

The target population was very specific in an industry with several types of stakeholders and companies. Because of this, the researcher would sort to non-probability sampling and use the business network to aid the recruiting process. Even though non-probability sampling designs describe sampling methods where researcher cannot guarantee that characteristics of the sample is representing the population of interest [55, p.182], they do give the researcher access to methods for choosing individuals for their sample based on their own judgement. A purposive sampling method was applied in order to find individuals who had experience from projects or operations within the world of smart buildings. In a purposive sampling method individuals are chosen to fill a particular purpose. Such a method is suitable when researcher needs individuals that have knowledge or experience from certain fields [55, p.280].

3.4.3 Sampling Technique

The primary method for finding relevant participants for the study was to use the researchers professional network and the snowball sampling method [62]. As the researcher and one of the supervisor had experience with different stakeholders in the real-estate and construction industry, these were approached and asked to further recommend individuals that had experience with smart buildings. This way, the researcher was able to reach further than was possible alone, and a list was made of potential participants, that fitted with the target sample that is described

in Section 3.4.1. In the first round of recruitment, e-mails were sent to some of the potential participants from the student e-mail account of the researcher. The e-mails contained information about the research project and the problem description, as well as some information on how the interview was to be conducted as well. Out of five e-mails that were initially sent, only one participant replied. In addition, two other participants were approached using the social media platform LinkedIn. Only one responded through LinkedIn. Finally, two people were asked in person which resulted in a response. A second attempt on recruiting participants was made, only using the business e-mail account of the researcher. By using the professional e-mail, 75% of the potential participants responded. Every person that were asked to participate int the research project, responded "yes". Table 3.2 show the response rates from the different methods of recruitment.

	Student e-mail	LinkedIn	Verbally	Professional e-mail
Approached	5	2	2	8
Responded	1	1	2	6
Response rate	20%	50%	100%	75%

Table 3.2: Response Rates From Interview Recruitment

3.4.4 Sample Size

The typical sample size for phenomenological study is between 5-25 individuals [55]. There were defined 6 categories of stakeholders that were relevant for the thesis, each stakeholder representing a different perspective of information security for smart buildings. The goal was to have at least one person for each of the categories and maximum three, which would bring the sample sized to between 6 and 18. Ultimately 10 individuals were interviewed in 9 separate interviews.

3.5 Interviews and transcription

3.5.1 Collection Method

Off-line and On-line Interviews When it came to deciding on conducting the interviews face-to-face or via online, streamed video, the researcher offered both methods when recruiting the participants. In [56, p.182], several perspectives on off-line versus on-line interviews are presented and some point to off-line, face-to-face interviews providing better relationships between researcher and participant, as well as adding greater depth to the interview. In addition, on-line synchronous interviews was something that would require the participants to have a certain degree of technical ability, which they did not always have. However, in a post Covid-19 world, online video conferences has become the new normal for many people in society, in private as well as business-related. Also, both video and audio quality in synchronous interviews have improved drastically since 2012. These

arguments made the researcher offer on-line interviews as a alternative to off-line interviews for this project. Another argument for the researcher to use on-line interviews was the convenience for the participants. The research project would require researcher to recruit experienced individuals from the construction and IT-industry, and by conducting on-line interviews the process would take up less time in the schedule of the participants than an off-line interview. Off-line interviews require one of the parties to book a meeting room, travel to the destination, and acquire access to the building where the meeting is to be held. These tasks were nonexistent if done on-line. The researcher also believe that if the participant were able to choose what type of interview they wanted, they would be more comfortable and the chance of accepting to participate would be higher. As shown in Table 3.3, 6 of the 9 interviews were conducted on-line.

	Off-line	On-line
Number of interviews	3	6
Percentage of interviews	33%	67%

Table 3.3: Off-line and On-line interviews

Data Collection Tools The primary method for collecting the data from the interviews, was to use Microsoft Teams to record them. This was done both in the off-line as well as the on-line interviews. After doing a risk analysis on the potential risk of the recording becoming corrupt, or Teams-application crashing during the interview, causing a loss of recording, a voice recorder was used as to achieve redundancy for the recording mechanism.

Conducting the Interviews At the start of the interviews, a brief outline of the interview guide was given to the participant. Following the outline, the interview guide was followed as it is described in Section 3.3.2. After the introduction of the interview, and consent form being signed, the recording was started. For the questions an interview guide from Appendix A was used in all interviews As the participants in the interviews had different backgrounds, and not always having much experience with information security, some questions were given some additional context to make sure that the participant did not misinterpret the question. That was particularly the case when speaking to participants with a construction background that might not have the correct technical vocabulary. Through the interview the researcher would let digressions occur if it was potentially productive. Interview question would sometimes lead to new, unscripted follow-up questions as is normal in in-depth interviews [57, p.107]. Having the interviews flowing more naturally while moving onto different topics and following up with questions was a skill that improved as the project went along, and as the researcher became more comfortable with holding the interviews.

Transcribing In the first three interviews, Microsoft Teams was used to record the audio during the interviews, and then the researcher manually transcribed the recording. For the remaining six interviews, transcription happened in two steps: First, Microsoft Teams transcribing feature the interview while recording. Second, go through the automatically transcribed document and correct what the application had interpreted incorrectly. Having Microsoft Teams transcribing the documents made the process go faster even though it introduced a lot of interpretation errors.

After transcribing, a copy of the transcribed document was e-mailed to the relevant participant to let them read through it themselves and wait for their approval to be able to use the data further in the project. At this stage, any sentences needing to be reformulated was edited or information that the participant would not like to share could be withdrawn from the transcribed documents.

3.5.2 Processing and Analysis

The analysis of the data was done using NVivo analysis application. The whole analysis process was made by the researcher alone. A general process of analysis was followed according to [55, p.310] and the following steps were made:

1. Preliminary categories such as 'current challenges, 'current measures', 'future challenges' and 'future measures' were pre-defined.
2. Phrases from the interviews were coded into the preliminary categories where they fitted.
3. Subset of codes were drafted and tried out until they reflected to total amount of data. These codes were defined according to what kind of challenge or measure that stated by the participants.
4. Phrases from interviews were coded into the subcodes.
5. Additional categorization of the data was added to separate the codes in relevance to different categories of a typical information security management system proposed in publication ISO/IEC 27001 [25].

3.6 Validity and reliability

3.6.1 Considerations on Validity

Validity is a property of research that describe the degree at which the results were accurate and true for the process of solving the research problem . Further there are two kinds of validity known as internal validity and external validity: Internal validity describe to which degree the design and data make it possible to draw conclusions about relationships in the data. External validity of a study is to what extent the results could be applied to situations outside the study and generalized [55, p.103-104].

Regarding the validity of the research, two measures were mainly taken to ensure this:

- Having participants from different backgrounds answer the same question to see if their answers converge on matters.
- Recruiting a representative sample of the industry with hands-on experience that are able to answer based on real-life experiences.

The participants being recruited for the research project represented each of the of six different stakeholder that were considered to be relevant for the application of information security in smart buildings. Several of these had different backgrounds and had different motivations in either constructing or operating smart buildings. By asking these different participants the same questions and identifying points of convergence in their answers and opinions, this would strengthen any conclusions based of the collected data. This meant that as more participants pointed to the same challenges in the industry, validity would increase for the particular challenge.

3.6.2 Considerations on Reliability

Reliability is defined in [55, p.104] as the consistency of measurement by a measuring instrument of an entity that does not change. One measure that the researcher implemented to increase reliability was to conduct a pilot interview to attain experience as well as test the interview questions.

3.7 Ethics

In research that involves interaction with humans, some ethical considerations has to be made. According to Leedy and Ormrod, most ethical issues falls under the following four categories [55]:

- Protection from harm
- Voluntary and informed participation
- Right to privacy
- Honesty with professional colleagues

Protection from harm is about not exposing participants to situations where they can experience physical pain or psychological pain in form of stress or embarrassment. Actually, the researcher should strive to provide the individuals with something that benefits the participant. Voluntary and informed participation is more self-explanatory, and requires the researcher to inform the potential participants of what they will be involved, while not forcing the individuals. Ethics related to the right of privacy revolves around protecting the personal information of participants during the project and in the final result of the thesis. Any information about the participants needs to stay confidential unless an agreement states

otherwise. Responsible handling of documents, e-mails and recording is key to respect the right to privacy. Finally, researchers must stay honest with professional colleagues, which includes presenting data accurately without misrepresentation or falsification. This includes plagiarism.

The research itself was about gaining deep knowledge about a certain process in a specific sector and relied on recruiting and interviewing experienced 'experts' to acquire good quality data that was representative of the industry. The individuals themselves were not the focus of the research, but the information they brought forward was. Conducting one-to-one interviews require that the participant is engaged and willing to give as much insight as possible. Therefore, there was only benefits in treating the participant with respect and creating a comfortable process for them from the recruitment stage to the final interview stage. Further, any material that was to be used in the thesis, would presented to the participants, having them approve the material before it was to be published. When the thesis was finished, the participants were to be given a copy of the report to use for their own benefit. This way, the participants were not only protected from any harm during the project in the sense of being humiliated or stressed in any way, but were given fresh insight from experts in their own industry.

To avoid any issues, some considerations have been made by researcher, especially for the interviews, while other measures are in large degree forced to be included in the research process by the University. To handle personal data in any form for the research, a data management plan had to be sent to the Norwegian Agency for Shared Services in Education and Research. The data management plan contains details on how the researcher was going to collect and handle personal data during the project. Methods to achieve separation of personal information in documents such as the interview guide and consent form were described in the data management plan. The data management plan had to be approved before any interviews could take place. This process ensures that the researcher plans for the participants right to privacy and voluntary and informed participation.

Chapter 4

Results

In this chapter the results from the data collection are presented. The chapter is divided into four sections, 'current challenges', 'current measures' and 'proposed solutions'. These sections are based on answers from the interviews and each of the sections visualize the results in a bar graph. The bar graphs show what topics the participants have brought up in the interviews, further divided into categories based on ISO 27002 control types [24] as they describe the generic information security controls for all types of industries. In addition to the bar graphs, quotes from the participants are displayed according to the category and topic that the quotes fits within.

4.1 Current Challenges

During the interviews, several challenges and issues were pointed out by participants. The challenges have been divided into topics to make easy to identify challenges that participants agreed on. Figure 4.1 present the results.

4.1.1 Organizational Challenges

Lack of Knowledge in Information Security

Lack of knowledge and awareness about IT, OT and information security is one of the top challenges reported by interview participants. Results from the interview points to challenges with knowledge and awareness among project owners, general contractors and contractors. An experienced chief of IT stated that *Most of the engineering departments that I work with know little or nothing about information security. They have no interest for it*.

Poor Requirement Specifications

When interviewing a senior technical engineer of a subcontractor and supplier of BAS on the matter of requirement specifications, the reply was that in many projects, the requirements are often bad or non-existent. The following was also said

on the matter *Sometimes, there are contradicting statements in the requirement specifications as the wish of the project owner might not be compliant with best practices. A consultant working for the project owner might have copied some best practice requirements from some framework, and then the project owner requirements are just added below, without seeing that the requirements cancel each other out*.

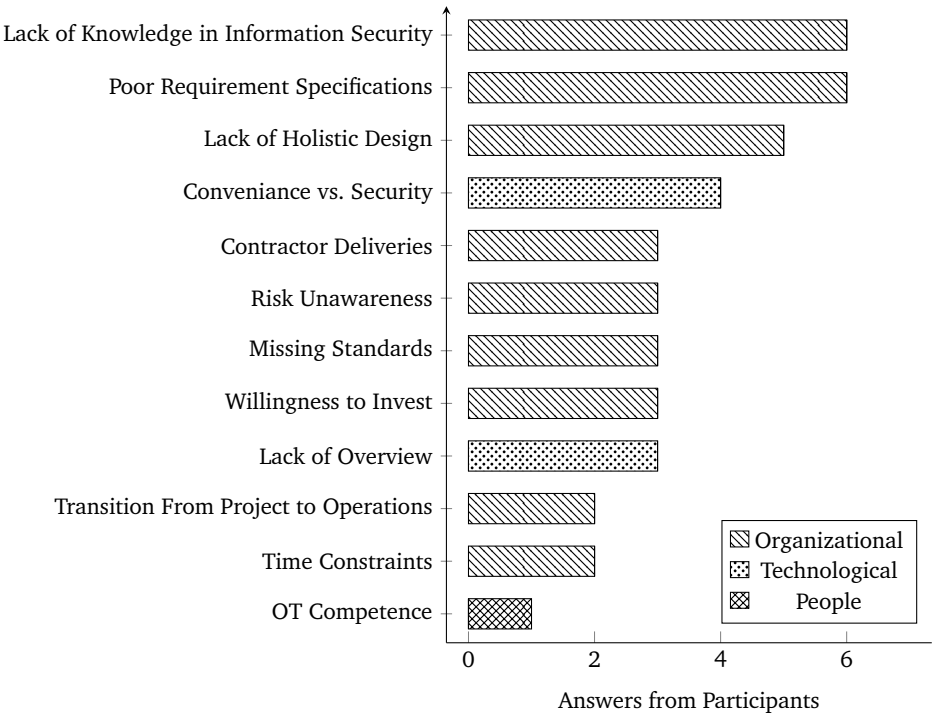


Figure 4.1: Categorized Current Challenges

Holistic Design

A security expert had the following to say on the matter of why information security was not applied sufficiently in many projects: *One of the challenges in these projects is that there seems to be a gap between people working with BAS and the IT-people working with what they believe to be the endpoints of their organization. The IT-people are thinking that the endpoints are laptops, workstations, printers and smart phones, when all the connected components in the building are actually endpoints as well. These perspectives do not work well together most of the time as there are traditionally different domains of administration for endpoints related to IT and OT*

Contractor Deliveries

Regarding how contractor deliveries are validated in smart building projects, a participant from senior management in a real estate company said the following:

The project owner has to make accurate requirements and make sure these requirements are delivered on. As the general contractor is the responsible party on the construction site, they are required to make sure that contractor deliveries are implemented according to the design and plan, either by trusting the contractors, or validating the delivery. Validation of deliveries is not being practiced very much, and we often trust that contractors operate according to their contract.

A network architect said the following when asked about challenges with information security in smart buildings: *When a new system or service is being implemented in the operational phase, I have experienced that there is a lot less information sharing and planning opposed to when systems are being implemented in construction projects. Shortcuts are often taken, and the IT-provider might not have been informed of what is going to happen, which makes it being implemented in a ad-hoc manner. Things are implemented in the easiest way possible to make it work, but that might compromise some of the information security*.

Risk Unawareness

When it comes to knowing the risks of not securing their assets properly a participant said the following: *... the problem is that the real estate companies does not know the risks, so they do not do anything about it. This leaves them with simple networks that are randomly put together, and they do not have any documentation of them. And on top of that, they want to implement Property Technology (PropTech) in these networks and give access to the internet. It's kind of on the brink of madness, but you can't judge them, because one does not know what one does not know. And they have not understood as it hasn't exploded nor imploded yet*. As the industry seem to not have a specific incident that had major consequences for a building owner or tenant inside the building, the risks of not investing in security measures might seem affordable to real estate owners.

Missing Standards

Another participant stated: *When it comes to contractors, they are willing to go a long way to meet the requirements specified, and use terms that they might not understand. The reason for this is that there is so little to choose from when it comes to frameworks and defined standards*. This point to missing standards and frameworks being the cause for lack of knowledge in the industry

Willingness to Invest

This could be felt in some projects according to a engineer who had been working with providing network infrastructure for project owners. The participant had the following to say on the matter:*We try to follow frameworks such as the Purdue-model when we plan for implementing systems on our network, but it is not always possible to follow the established practices as willingness to invest by the project owner*

is not always sufficient and it can get too complex for the contractors that deliver their systems.

Transition from Project to Operations

As smart building projects transition from construction to operational phase, challenges rise about how knowledge is transferred between the phases, and design decisions that sometimes are made in the project are poorly aligned with the facility staff that are to operate the building. One participant states: *There is a air gap between project and operation of a building. Operational staff takes over whatever comes out of a project. The operational staff have little influence on choices regarding solutions and requirements for contractors, which can be challenging in the operational phase*. Another participant explain how the lack of training and awareness of building facility staff can become a problem for information security, as follows: *Building facility staff does not have much focus on security other than that they do not let anyone connect to the network. That might be the only barrier that I know of. I am yet to witness building facility staff verifying the contents of my laptop before I connect to the network*.

Time Constraints

Construction projects have been described as "unstoppable trains" where economic sanctions are enforced upon delays. One participant had the following to say about the how time affects the application of information security in projects: *In recent construction projects, the time from construction starts to the building is complete is shorter than earlier. In some projects, the engineering phase and construction phase happen more in parallel because of the time constraints of the project. And because of this, some shortcuts are taken by contractors when they implement their solutions. Compromises on information security are often made*. The compromises refer to security measures being excluded from system implementation to be able to deliver on time.

4.1.2 Technological Challenges

Convenience and Security

Challenges with inconveniences related to tighter security have been mentioned by several participants, and especially when it comes to give access to new components in a network with Network Access Control (NAC) implemented. One participant stated the following on the matter: *I do have some experience with construction projects with high security networks, where the slightest change triggers a big process to implement even a single component into the network. I believe 95% of people involved would consider this inconvenient and not very sustainable. They would not see the benefits of the added security*. Another participant stated the following on the same matter: *In projects where IT-provider requires MAC-addresses of*

components to give them access to the correct subnet, this demands for the contractors to be more precise in their deliveries and for them to make lists with every single MAC-address... If they don't get in the correct information, they might not be able to get contact with certain components... For our part, it would be more preferable with an open network which would make all contractors to successfully have their components online, and there are less barriers and errors in that process. For the process of provisioning devices onto a network with NAC a participant explained the process from the project owner side: *We have some projects where all devices across all BAS are whitelisted by MAC address. When devices needs to be replaced or added I need to reach out to the service provider and tell them "we are going to replace this device with this one. Can you add this MAC-address and remove the old one?*". This exemplify how such project would be slowed down as a lot of individuals need to be involved in adding one component to the network.

Lack of Overview

Maintaining control of implemented systems and their components in smart buildings seems to be a problem in the industry according to a participant: *Having been responsible for IT in several real estate companies, there have been no exception when it comes to lack of control of implemented systems in the buildings*. Another senior engineer said the following about how documentation of IT and OT infrastructure is lacking in the construction industry: *It is paradoxical that the most sophisticated digital twin for a building, there will be no trace of network components or the access points. Information about the digital infrastructure is non existent. This seems to me as a blind spot for the industry. If you speak to an building architect, they do not see the digital space as a critical function for a building to be able to operate*.

4.1.3 Challenges Related to People

OT Competence

On the subject of security of OT networks, a senior consultant mentioned the following challenge when IOSPs lacked experience with OT systems: *[In OT systems] there are a lot of static IP addresses and specially configured switch ports, so when normal software upgrade routines are performed in these networks, the OT systems stop working from time to time. Operating these systems require special knowledge and experience, which becomes my focus in these projects, when we are trying to find someone to operate these OT networks. Those organizations needs to accept their golden standard might not always be applicable to these kinds of networks.*

4.2 Current Measures

Current measures taken by the stakeholders that were asked about in the interviews, and the respective results are shown in Figure 4.2 below.

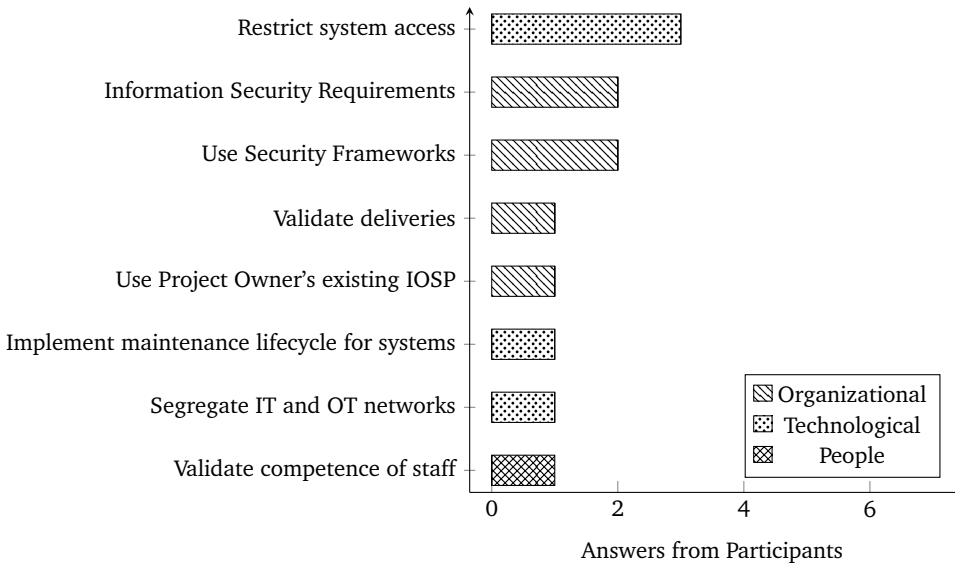


Figure 4.2: Categorized Current Measures

4.2.1 Current Organizational Measures

Information Security Requirements

To improve information security in construction, a consultant primarily focused on the requirement specifications and said the following: *We advice on the requirement specification of the customer, which is how we can affect it [information security]. The requirement make the foundation for which contractors are being chosen for these projects.*

Use Security Frameworks

A cyber security engineer said this about what measure he/she used in projects to increase information security: *To use and adapt existing security frameworks to the needs of the project. It is normal to use a combination of IT and OT security frameworks.*

Validating Deliveries

A participant from IT-management in a real estate company had the following to say on validation of contractor deliveries *We do a periodic review of the property and the connected systems once every three months or so. We go through all components and an overall status of each system is given, as well as for the whole building*.

Use Project Owner's existing IOSP

As the real estate companies might lack information security staff, and juggling several IOSPs for different buildings, the following measure being recommended by a consultant: *Mostly, I recommend that project owners keeps network infrastructure outside the construction project because operating networks is a highly specialized field and it might make more sense to look at several buildings by one provider. And for me it seems hard to get the general contractor to deliver a enterprise grade network that is supposed to serve building systems, so I normally include a professional provider for this*.

4.2.2 Current Technological Measures

Restrict system access

Managing system access with a firewall is used as a measure according to general contractor representative, who said the following: *When systems needs to be connected to the internet, they are given access via the firewall, but no other measures are implemented unless specified in the requirements*. A network engineer stated the following on the subject: *We strive towards segmenting different services in different domains with access control, and we map out what is trying to communicate with what. To achieve this, we leverage technologies that we have deemed to be secure, and it is all about restricting access to the systems that are implemented in a smart building to just exactly what is needed*.

Implement Maintenance Lifecycle for Systems

To keep their systems secure through their lifecycle, a systems engineer stated the following about their maintenance lifecycle: *We deliver four software patch releases and one feature release every year. Every three months we review software where bugs or other things are identified and implemented into next software release*.

Segregate IT and OT Networks

When asked to share thoughts on the matter of IT-OT convergence, a participant said the following: *For the OT-network, I like to keep it physically separated from the IT-network. Then it keeps the tenants out of reach. That might be a possible attack vector for an attacker, to reach the building tenants via a vulnerable OT-network. I don't see the benefits of converging the networks*.

4.2.3 Current Measures Related to People

Validate Competence of Staff

A project owner makes sure to have sufficient IT competence of critical roles in construction projects according to a participant: *We have actually started to hold*

interviews for the role which is responsible for managing the implementation and integration of BAS in the construction project... This role is super important in order to get BAS delivered on time in a project. If he or she does not have the competence that is needed, there will be delays in the project, and that often gets expensive. It is important that the person knows something about IT and information security.

4.3 Predicted Future Challenges

One participant shared thoughts about future challenges if the real estate industry would digitize too fast without the proper frameworks: *If real estate companies are constructing smart buildings and offer a shared network infrastructure with WiFi to all tenants, and the infrastructure is implemented in a way that exposes the building tenants and BAS to new threats, what happens if such infrastructure fails and the tenants are critical to society? If such infrastructures are implemented without the use of models or frameworks making it resilient and robust, how do we handle incidents of disruption or disaster? ...I believe when as the industry digitize and implement new technology, we have to do it slowly enough to know the consequences and make it robust, but still fast enough to compete in the global markets*.

4.4 Proposed Solutions

Proposed challenges by the stakeholders that were asked about in the interviews, and the respective results are shown in Figure 4.3.

4.4.1 Proposed Organizational Solutions

Collaboration Between Owner and IOSP

One informant said the following about how the lack of knowledge in the real estate companies is keeping them from gaining control of all implemented and integrated systems in the buildings they own: *One contractor operates the network, another provide the application, another provide the access control system. All the contractors that provide these services need to integrate in many cases, and there is no real estate company in Norway that has the competence to be able to facilitate these integrations. To be able to do this properly, one needs to have a agreement with a system integrator that can help them with these tasks*.

Implement Holistic Design

On the matter of having the industry taking a more holistic approach to implementation and integration of security measures in systems delivered by contractors, a participant said the following: *The contractors delivering BAS should be held responsible to a higher degree than they are today to make them go a little further when it comes to integrating systems. Another way to improve would be to make sure*

that the provider of the OT networks take lead on information security and train the contractors on how to improve deliveries... circling back to your question: if all BAS contractors had to use the network provider as point of contact when it came to implementation and integration, the end results might get better.

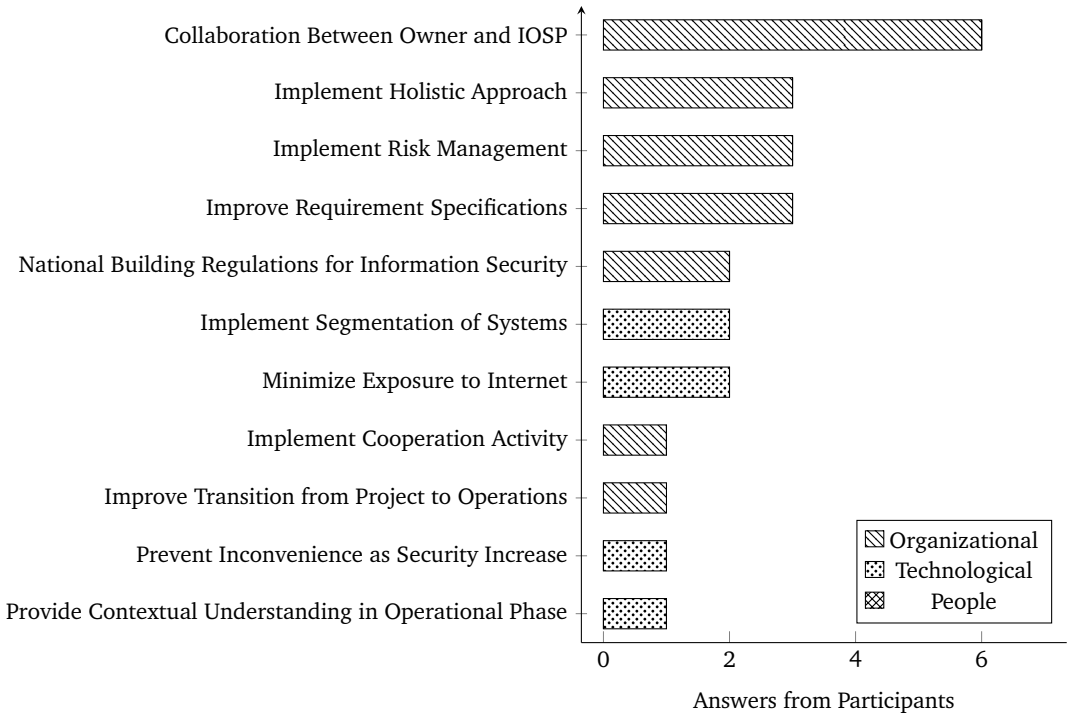


Figure 4.3: Categorized Proposed Solutions

Implement Risk Management

When asked how to achieve a secure smart building, a senior consultant said the following: *I would achieve that while cooperating closely with the IT organization. The IT organization would be crucial in the engineering phase of the project, because they know security. Let's say that a datacenter is being built. Then we would perform a risk analysis together with the project owner to become aware of the financial consequences. One can not only implement security from your own preferences. One must listen to what is needed in the project and that is the goal*

Improve Requirement Specification

An engineer from a general contractor made the following statement when asked about if the person could identify any areas of improvement for information security: *The project owner tells us how things are going to be, and we take those requirements down to the subcontractors, but there are not many detailed requirements that we get. There should be more formalized requirements other than "we*

need a network for BAS". Another participant proposed the following to make contractor comply to security requirements. *I would not trust the contractors that are working in these buildings. I would make requirements that forces the contractors to be compliant with a much more strict environment in the project when it comes to information security, network, communication design, storing data and access to data*.

Introduce National Building Regulations for Information Security

A participant proposed the following to incentivize the industry to focus more on information security: *In the Norwegian building regulations, there is missing standards when it comes to cyber and information security in construction projects. The industry might have to take the initiative, or public sector might have to. And I believe that introducing such a standard would not be a big issue... as the industry is very used to constructing everything according to existing standards that they would adapt to new standards quickly*.

Implement Cooperation Phase

In order to achieve better alignment of the stakeholders involved in the construction project, one participant proposed the following: *I would introduce a collaboration phase to my project. I would require the contractors that were to deliver systems that would integrate with each other to collaborate and perform a risk analysis, and then challenge them on how they would solve these tasks, not just individually, but collectively*

Improve Transition from Project to Operations

A proposition to improve the transition from project to operational phase was made by a participant, who stated: *I would focus on not treating the project as something that is constructed, commissioned and delivered when finished. It should be a continuous process. Services and processes being established early in the lifetime of a building needs to be addressed through the whole lifecycle of the building. I would not allow that gap between the construction project organization and the building operating staff to exist*.

4.4.2 Proposed Technological Solutions

Minimize Internet Exposure

One participant said the following about restricting access of systems: *The most important measure, is to not expose the systems on the internet. They do not need to be exposed at all. Not surveillance cameras, not access control or anything else.*

Provide Contextual Understanding in Operational Phase

The following vision was described by a participant to achieve better system visibility and control for the industry: *I would like to have a monitoring of all BAS with status indicators across all buildings, and for these to be presented in an overview dashboard. This way, I would be able to pinpoint to what the reason was for a building to have a 'yellow' state. Further I should be able to see if that was because of a firewall lacking maintenance, and who was responsible for that*.

Chapter 5

Discussion

5.1 Current State of Application of Information Security in Smart Buildings

The participants of the research project had a variety of measures that they would implement to increase information security in a smart building. The results shown in Figure 4.2 display several measures that also overlap with the current challenges of the industry shown in Figure 4.1. One example is 'requirement specifications' where two participants stated that they implemented information security requirements to address information security, while six other participants stated that poorly defined or non-existent requirements for information security is a challenge in the industry. Regarding the use of information security frameworks, two participants stated that they use such frameworks in construction projects. Even though this measure is implemented by a few actors in the industry, there is a considerable amount of participants lacking measures providing holistic approaches, risk awareness and accurate requirement specification which points to lack of use of security frameworks. In addition, three participants mention the lack of industry specific standards as a concern.

Further, looking at how current measures and current challenges is categorized in Figure 4.2 and Figure 4.1, the information regarding measures are more focused on the technological aspect (44% of stated measures), while the challenges are more directed to organizational issues (75% of stated challenges). This points to that the industry should focus more on organizational measures to be able to improve the application of information security for smart buildings. Several of the challenges such as 'poor requirement specification', 'lack of holistic design', 'risk awareness' are challenges related to tasks and processes that should happen in early phases of of a construction project. These challenges should be dealt with by the project owner, its representatives and consultants in the development phase of the project. Challenges related to 'time constraints' and 'contractor deliveries' are issues that might become visible later in the project. As pointed out by one

participant from the research project, the construction industry is characterized by *economic sanctions upon delays in deliveries*, and fast paced project timelines Section 4.1.1. This might be a cultural problem that has driven stakeholders to deliver in accordance with the requirement specification, but avoids to harden their system deliveries, as it requires more time to be spent on an implementation. Since requirement specifications often lack requirements for information security, stakeholders such as the subcontractors might not be willing to add more security, which often leads to more complexity in their deliveries.

As smart buildings are finished and building facility staff take responsibility of the building's operational and maintenance needs, several participants have expressed concerns about the sub-optimal nature of these events. A participants is describing in Section 4.1.1 an "air-gap" between construction and operational phase due to little knowledge transfer and planning of operational procedures between the ones responsible for information security and the building facility staff. This might be another cultural problem in the construction industry, as the temporal nature of the organization during construction is focused primarily on construction of the building and not so much on the remaining lifecycle of it. This might suggest that the project methods used in construction are not compliant with smart buildings, as they would need end users and operators to be more involved in the project.

When it comes to looking at the current measures, as shown in Figure 4.2, the one defined as 'have the project owner use their own IOSP in project' is a rather specific organizational measure that is stated by a participant. The participant stating this measure also said the following about involving a professional party: *It is the most important thing I do [in a construction project].* As the industry is challenged with lack of knowledge for several key stakeholders, the measure of a project owner to be using the same IOSP for all their smart buildings might be crucial if they lack sufficient IT or information security staff.

From the data collected, the industry seem to be lacking a systematic approach to information security from the early planning phases of buildings, that is followed up on through the construction project, and into the operational phase of the finished building. Several stakeholders are aware of technological controls that can be implemented for securing building systems, but few mention the use of existing frameworks that allow an organization to take a more holistic approach.

5.2 Proposed Methods and Solutions to Achieve Secure Smart Buildings

5.2.1 National and Industry Solutions

One of the biggest challenges in the industry is the lack of knowledge about IT in general and information security across most of the relevant stakeholders that this research targets. As the industry has been evolving rapidly in the past 10-15 years with more connected and integrated systems, and with no known major security incident for smart buildings to look to, information security has not become priority with real estate owners. This lack of knowledge about information security is likely the reason to most of the other challenges that have been identified for the industry as well. Even though there are few disasters for the industry to look to, the market growth, the trend of IT-OT convergence and the fact that OT systems can be exploited to harm humans [43][27] suggest that the consequences of a cyberattack on smart buildings will increase with time. By incentivizing the industry to incorporate and prioritize information security in projects, the real estate industry would become more resilient during operation and more prepared for disasters. Two solutions for incentivizing the industry is proposed: national building regulations, and building security certifications.

National Building Regulations

As proposed by a participant in Section 4.4.1, by introducing national building regulations that require the application of information security in buildings, the industry would be forced to address information security and the knowledge gap that exists. National building regulations addressing information security would have an impact for all relevant stakeholders in the industry. Project owners would need to allocate budgets for information security and hire staff with relevant knowledge to aid in future projects where buildings are to meet the demands of the new regulations. General contractors would have to acquire staff that is familiar with information security in order to ensure correct deliveries throughout the construction projects. It would also affect the contractors who would need to make their systems and organizations compliant with regulations that require information security measures or monitoring. When it comes to adapting such standards and regulations, the construction industry is already familiar with following technical regulations for all fields in construction as pointed out by the same participant that proposed the measure in Section 4.4.1. In Norway, there exists a group of industry representatives that are in the early stages of proposing something that might be adopted by a future national standard, but the timeline is unclear at the time of writing.

Building Security Certifications

As national standards might differ a lot from country to country, an industry certification for security in buildings might have a more global reach. Such a certification would become a symbol of to which degree a building or organization incorporates security measures and how well they perform in day-to-day operations. The security certification would consider both physical security as well as information security to resonate with as many potential tenants as possible. As Energy certifications for buildings have a tendency for increasing tenant rental value [63], and information security certificates increase market value of firms [64] a security certification for buildings might prove to be valuable for property owners. In addition, this might also lead stakeholders in the industry attaining information security knowledge faster.

5.2.2 Proposed Actions for Project Owners

Ultimately, every stakeholder that is involved for the planning, implementation, validation, operation and maintenance of IT and OT systems in a smart building is working for the project owner. The project owner needs to make information security a part of their construction projects from the very beginning to have the other stakeholders being required to live up to their standards. In the next subsections different actions are proposed for the project owners to improve their ability of ensuring that information security is implemented at a degree that meets their business needs, as well as how to prepare organization for efficient building operation.

Leveraging IOSP Competence and Converged Architecture

As discussed in Section 5.1, real estate companies lack staff to manage information security both in construction projects and in the operational phase. The study also found that projects owners should include IOSP more in construction projects to create more secure buildings as shown in Section 4.4. For real estate companies that plan, build, own and maintain their own buildings, integrating the IOSP in the project and making use of their information security staff would make the foundation to manage information security more effectively. The partnership or collaboration with IOSP might primarily help the real estate companies achieve two things:

1. Outsourcing information security staff that can advise in construction projects as well as provide means to implement, monitor and operate security measures to secure building assets.
2. Making construction projects and building operations more effective as well as increasing security.

An IOSP could be leveraged both as a consultant or advisor in construction projects by bringing in security staff to collaborate with the project owner and the

engineering teams. By involving information security staff from the IOSP early in a construction projects, challenges with risk awareness and poorly defined requirement specifications could be mitigated. The chance of having implemented a more holistic design for both IT and OT should also increase as the IOSP would be responsible for both.

Some literature point to several benefits of using a converged IT-OT infrastructure as in [52]. An IOSP delivering a fully converged network would be in a position to provide better security and better solutions for customers when operating and maintaining their assets. Technical solutions as mentioned in Section 5.2.3 are examples of what IOSP could offer to improve real estate companies ability to make projects and operations more efficient and more transparent.

For a real estate company to reap all potential benefits by collaborating more with an IOSP, it would be critical to choose a fitting IOSP that would have the organizational and technological capabilities to assist, advise and take responsibility in construction projects and building operation. The matter of making the right choice of IOSP is discussed further in Section 5.4.

Adapting Information Security Risk Management

As information security requirements in the industry are either not clearly written, or non-existing, project owners need to address this to ensure secure operation of their smart buildings. According to information security standard ISO/IEC 27002 [24, p. 9], there are three main sources of information security requirements, those being:

- Information security risk assessment.
- legal, statutory, regulatory and contractual requirements that an organization must comply with.
- principles, objectives and business requirements that a organization has defined for its information assets.

As risk unawareness is also reported by participants as one of the main challenges for the industry, the systematic introduction of information security risk analysis will aid in solving both issues. The participants of the research have been proposing to use risk analysis to decide on what security controls to implement, as well as improving requirement specifications, and as these are tightly connected challenges, risk management is a key to solve both issues. Figure 5.1 illustrate the inputs and outputs of the risk analysis process.

By implementing an information security risk assessment for systems, infrastructure and integrations for a smart building project one can define information security requirements that will treat any risk that the project owner does not want

to take. To manage information security risk, frameworks such as ISO/IEC 27005 [25] can be used. One can also leverage simplified frameworks such as the one proposed by [3] which would be easier to implement in an organization with less knowledge about information security.

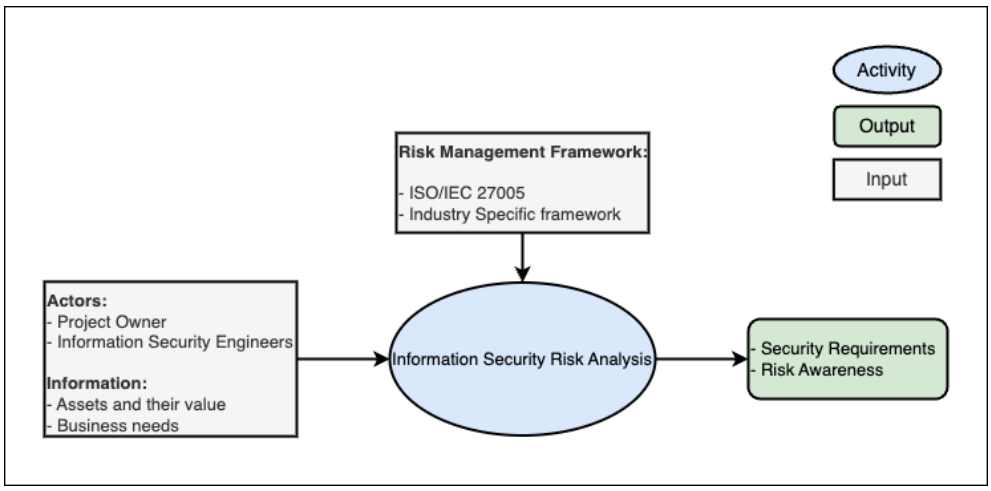


Figure 5.1: Information Security Risk Management, [source: own]

ISO/IEC 27002 gives guidance to implementation of security requirements for project management as a form of organizational control [24, p. 29]. An additional organizational control describe what to consider in scenarios when agreements are with suppliers, where information security requirements needs to be agreed on by all parties [65, p. 35]. This is highly relevant for smart building projects which involves a high number of contractors and vendors that deliver connected systems. For developing security requirements for applications that are being acquired through a project, a list of considerations is presented as a part of ISO/IEC 27002 technological controls [24, p. 118]. Additional references to information security requirements are made through ISO/IEC 27002 and needs to be studied in more depth by responsible stakeholders.

Furthermore, the implementation of a risk management framework such as ISO/IEC 27005 in combination with the information security control standard ISO/IEC 27002 will also achieve the provision of a holistic approach to information security. A holistic design for systems in smart buildings has been reported by several participants of the research project as being a challenge.

To summarize, three challenges of the industry might be solved by using security frameworks such as ISO/IEC 27005 and ISO/IEC 27002, these challenges being risk unawareness, poorly defined information security requirements and lack of holistic design for smart buildings.

Introducing Collaboration Phase to Improve Deliveries

In the construction project of smart buildings, the IOSPs that implement the network and the contractors that deliver BAS and IoT need to be able to follow the timeline of the construction project, as well as delivering systems according to information security requirements. This task can be complex on its own as there can be many systems that need to integrate, and all parties has time working against them. By including a collaboration phase before construction starts, the contractors, IOSP and the representatives from the project owner will have the ability to become aligned when it comes to understanding how to collaborate during the project, and identifying potential risks. The collaboration phase would include meetings and possibly workshops if needed. Meetings between the stakeholders will also help break the silos between them at an early stage, that might facilitate better dialogue through the project. Such an activity can also be used for the involved stakeholders to specifically agree on design and processes related to security of the systems, as well as identify potential problems. This can be helpful to decide on what tasks must be prioritized as systems are being implemented through the project to avoid falling behind on time. Figure 5.2 illustrate the inputs and outputs of the collaboration phase.

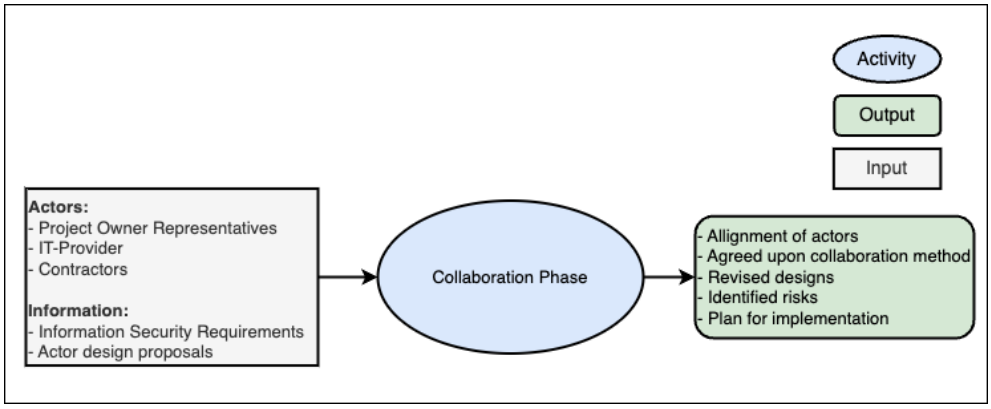


Figure 5.2: Collaboration Phase, [source: own]

The collaboration phase might also be used for IOSP to define operational procedures for the building facility staff.

Involving Building Facility Staff to Prepare for Operational Phase

As several participants stated in Section 4.1, there are challenges related to the transition from construction to operational phase of buildings because of a management gap between the two phases. The building facility staff, who will work inside the building and operate the building are not sufficiently involved in the project and have little input to decisions that are made during construction. Focusing on the building operation and maintenance when designing and constructing the building was proposed by an participant in Section 4.4.1. As there will often

be many contractors working in the building maintaining their systems during the lifetime of a building, formal procedures needs to be established between relevant stakeholders and the building facility staff. The IOSP for the building would need to communicate procedures and policies for maintenance on the network and BAS as they would be responsible for security and they would to some degree be dependent on the building facility staff to ensure that no shortcuts are taken when it comes to information security.

Establishing the relationship between IOSP and building facility staff should happen before operational phase in order for staff to get the proper training if needed. The building owner, IOSP and building facility staff should schedule workshops during the design phase in order to define responsibilities, procedures and policies. Leveraging frameworks such as [24] and implementing controls such as 'documented operating procedures' and 'change management' can aid in creating the procedures and establish responsibilities. Planning and designing the building with operational phase in mind might also lead to more effective building operations and might reduce operational costs as standardized operational procedures will lead to more secure implementations and lower risk.

5.2.3 Proposed Technical Solutions

User Friendly Solutions to Provision Building Automation System Devices

As stated by several interview participants in Section 4.1.2, implementing network access control and authenticating endpoints poses management and implementation inconveniences. As a smart building can have many different subcontractors, with variable degree of information security knowledge, each delivering BAS or IoT, a user friendly solution for getting endpoint devices securely on the network infrastructure is needed to increase efficiency. The primary goal of such a solution would be to make it easier for both contractors and vendors to have their endpoint devices authenticated onto restricted networks. The second goal would to be more independent from the expertise of the IOSP. Ideally, the subcontractors would be able to use this solution through some sort of remote access solution by themselves with some basic training.

Most likely the IOSP would be the party offering the solution to subcontractors and building staff. It would require system automation and development of a Graphical User Interface (GUI) and would require the IOSP to leverage some sort of policy node to handle authentication requests. The solution should also support different types of authentication methods depending on the endpoints that would need to connect. Some companies do offer solutions like this [66].

Possible benefits of implementing such a solution in smart building projects or in the operational phase of a smart building are as follows:

- Increase cost effectiveness by reducing the amount of time subcontractors need to spend on implementing system components.
- Less parties involved in managing endpoints would make such projects more efficient would save time during construction.
- More accurate deliveries as an endpoint would only gain access to whatever network segment it was supposed to have. This might reduce time in troubleshooting and more time to commission the systems.

Potential challenges springing from using such a solution might be as follows:

- Require subcontractors to choose the correct authentication method depending of the type of endpoints. It would still be more work that having a smart building with no network segmentation or access control for endpoints.
- All subcontractors would require user access to the solution which might be challenging in large construction projects if not planned for.

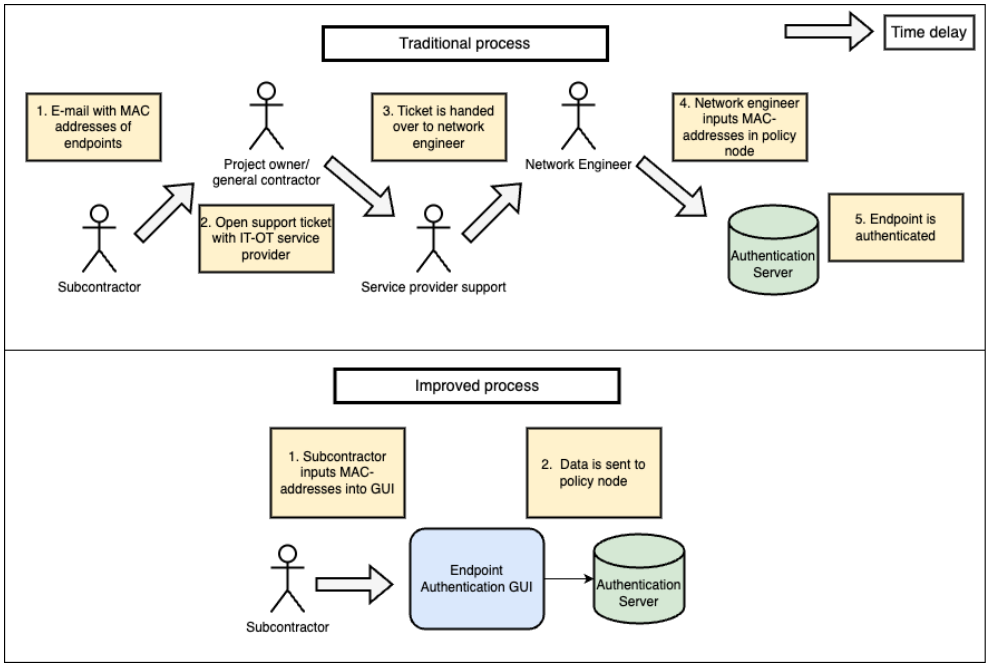


Figure 5.3: Compared Processes for authenticating endpoints, [source: own]

Figure 5.3 visualize some of the main differences between the processes of the proposed solution and methods described by a research participant in Section 4.1.2. In the top part of the figure, the process of provisioning endpoints by registering MAC-addresses of devices is shown. This process involves several parties, often including time delays between them and sometimes even additional costs due to support tickets being generated and handled by service provider. The

improved process in the bottom part of the figure illustrate the use of a solution for authenticating endpoints, requiring fewer steps and no sources of time delays.

Maintaining Visibility and Awareness Through Project and Operation

The real estate industry already have a lot of connected devices and systems in their buildings, with more to come in the following years according to [1]. As stated by interview participants on the matter of visibility and control in Section 4.1.2, the industry is challenged by the lack of knowledge of what systems and components are on their networks, and how they are integrated. A solution for providing real estate companies and IOSP with greater awareness would require the following:

- Asset inventory for components belonging to systems across building portfolio
- Monitoring of systems and their components.
- Security compliance checks of endpoints and systems.
- Design plans of system implementation and integrations that were agreed upon in the project.
- Relevant security policies pulled dynamically from infrastructure and security nodes.

Such a solution should be presented through a GUI from the IOSP to be used by the IT and building facility staff of real estate companies. Solutions for managing OT do already exist [67] [68] [69] and can provide real estate company management, building facility staff and OT-teams visibility into operational and security monitoring of BAS.

5.3 Limitations of the Research Project

The building facility staff was originally not identified as one of the key stakeholders for information security in smart buildings by the researcher. In hindsight, this group should have been included and recruited to interviews for the research project as they might have had valuable information about their experiences, especially in the period as the smart building is transitioning from construction to operational phase. This could have provided the research with greater validity. But even though the stakeholder might have brought up new challenges or solutions, this would not alter what the most significant challenges of the industry were according to opinion of the other participants.

As the participants had different backgrounds, and varying degree of information security literacy, some interviews needed more aid from the interviewer as the participant did not fully understand the question, or answers were not as clear because of the lack of knowledge and vocabulary from the information security

field. Even though the interviews with participants having little knowledge of information security would to some degree provide answers with less quality than the interview with information security architects, both perspectives were considered to be valuable to strengthen the validity of the research. Comparing the planned target population in Figure 3.2, the actual population that was recruited for the research look more like the one illustrated in Figure 5.4

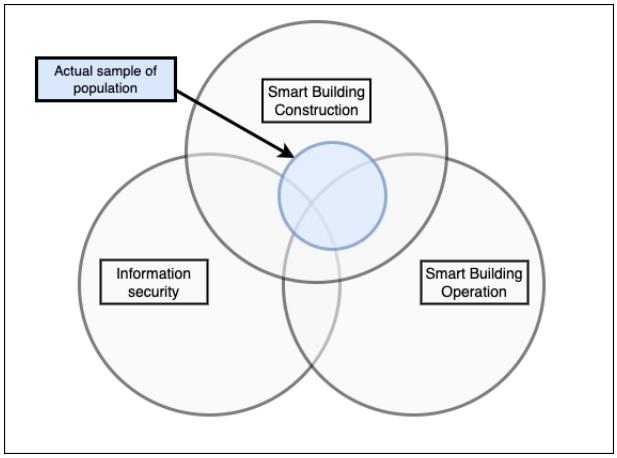


Figure 5.4: Venn Diagram of Actual Sample of the Population

The researcher made an effort to recruit experienced individuals that were active in the field to have a representative sample from the construction industry. The professional network of the researcher was primarily used to recruit participants. In addition to recruiting different stakeholders in the industry such as projects owners, engineering consultants, and contractors, some effort was made to diversify in terms of size and geographical properties of the companies that the researcher recruited from. This effort was only partly successful as most companies that participants were recruited from were big national players in Norway, but few were big international companies. Only two participants were from larger international companies.

During coding of the data, the researcher did the coding alone, which weakens interrater reliability of the analysis process. Efforts to recruit someone to aid in the task of coding were not made.

The response from the participants might have external validity as to depict the situation in Norway, but less so for the rest of the world. As there were few international companies and not one participant from outside Norway, this limits the external validity of the research since the construction industry seems to be at very different stages when it comes to being able to construct smart buildings.

Cultural, social and economic factors in Norway might lead to different situations for the real estate and construction industry than in other countries.

5.4 Future Work

One of the possible directions would be towards making a framework for real estate companies for choosing a suitable IOSP to manage both their traditional IT environment as well as connected assets in their building portfolio. The framework should model the maturity or readiness for planning, advising, implementing, commissioning, operating and maintaining smart buildings and in regards to information security frameworks.

To create incentives for the real estate industry, the work on a Smart Building Security Certification should also be investigated further. First, it would be valuable to look into how such a building security certification might lead to increasing rental costs or value of building. Second, a framework for the building certification should be proposed.

Chapter 6

Conclusion

Even though the research project could have included another stakeholder group as source for data, the study manages to provide an overview of present state of application of information security in smart buildings, as well as proposing methods to meet the industry challenges. In general, there is a lack of competence in information security amongst stakeholders in combination with little use of systematic approaches, which leads to low risk awareness and poorly defined security requirements for the contractors. IT-OT Service Providers (IOSP) stand out from this generalization, but is too little involved and their potential might not be fully made use of.

For the construction projects there are also several challenges. There seem to be a industry culture where information security is not valued and the project methods used do not seem suited for design and construction of smart buildings. These factors leads to poorly implemented security controls in smart buildings from stakeholders responsible for implementation, and inadequate alignment between stakeholders that will have responsibilities in operation and maintenance of the building.

To improve information security in smart buildings several efforts are proposed by the researcher. The efforts are categorized as national or industry efforts, actions proposed for project owners and technical solutions for the industry. To solve the most fundamental challenges of lack of knowledge and willingness to invest, the researcher has proposed making national building regulations for information security and building security certifications. As the project owner is the key stakeholder for all smart building functions there have been proposed several actions for how the project owner can facilitate for secure smart buildings. First, the project owner is recommended to leverage their IOSP and their security organization to cover their own knowledge gaps and lack of information security staff. Second, project owners are recommended to implement information security frameworks to increase risk awareness, improve requirement specifications and taking holistic approaches. Further, a collaboration phase has been proposed to align stake-

holders and improve subcontractor deliveries. Lastly, the building facility staff is advised to be included in the construction project to prepare staff for the operational phase of the building. Technical solutions are proposed to enable efficient subcontractor deliveries in both construction project and building operations, and for real estate companies to have control of their system and building portfolio. All in all, as long as there are no national building regulations requiring security to be implemented by law, the project owner will be the key to make information security a higher priority in their construction projects. The project owner needs to take use of both organizational and technological measures to achieve more secure implementations, as well as preparing future operation and maintenance staff for building to stay secure after it is constructed.

Bibliography

[1] Kay Sharpington and Milly Xiang, *Forecast Analysis: Smart Buildings IoT Endpoint Electronics and Communications Revenue, Worldwide*, en, 2021. [Online]. Available: https://www.gartner.com/en (visited on 25/04/2023).

[2] Michael Chui, Mark Collins and Mark Patel, *The Internet of Things: Catching up to an accelerating opportunity*, en, 2021. [Online]. Available: http://ceros.mckinsey.com/internetofthings-exhibit1-desktop (visited on 02/05/2023).

[3] Ž. Turk, B. García de Soto, B. R. K. Mantha, A. Maciel and A. Georgescu, 'A systemic framework for addressing cybersecurity in construction,' en, *Automation in Construction*, vol. 133, p. 103 988, Jan. 2022, ISSN: 0926-5805. DOI: 10.1016/j.autcon.2021.103988. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0926580521004398 (visited on 06/04/2023).

[4] Cigref, *[Cigref report] IT/OT convergence: A fruitful integration of information systems and operational systems*, fr-FR, Feb. 2020. [Online]. Available: https://www.cigref.fr/cigref-report-it-ot-convergence-a-fruitful-integration-of-information-systems-and-operational-systems (visited on 02/05/2023).

[5] P. T. Eikeland, 'Samspillet i Byggeprosessen,' no, Samspillet i Byggeprosessen, Tech. Rep. P10602, Aug. 2001.

[6] Bråthen, Ketil and Leif E. Moland, 'Samhandlingsfase og BIM på byggeplass,' Tech. Rep., 2016.

[7] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri and S. Lightman, 'Guide to Operational Technology (OT) Security: Initial Public Draft,' en, preprint, Apr. 2022. DOI: 10.6028/NIST.SP.800-82r3.ipd. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf (visited on 25/01/2023).

[8] Cisco, *How Is OT Different From IT? OT vs. IT*, en, 2023. [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html (visited on 27/01/2023).

[9] Gartner, *Definition of Information Technology (IT) - Gartner Information Technology Glossary*, en, 2023. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/it-information-technology (visited on 26/01/2023).

[10] G. Fink, T. Edgar, T. Rice, T. MacDonald and C. Crawford, 'Security and Privacy in Cyber-Physical Systems : Foundations, Principles, and Applications,' in *Cyber-Physical Systems*, 2017, ISBN: 978-1-119-22607-9. [Online]. Available: https://web.p.ebscohost.com/ehost/ebookviewer/ebook/bmxlYmtfXzE1ODM3NDlfX0FO0?sid=57f703ca-f547-49c2-a069-c80da8ff8b77@redis&vid=0&format=EB&lpid=lp_327&rid=0 (visited on 08/12/2022).

[11] Palo Alto Networks, *Confidently Segment Devices and Apply Zero Trust Policies with Enterprise IoT Security*, Feb. 2023. [Online]. Available: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/segment-iot-enterprise.

[12] W. Kastner, G. Neugschwandtner, S. Soucek and H. M. Newman, 'Communication systems for building automation and control,' *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1178–1203, Jun. 2005, Conference Name: Proceedings of the IEEE, ISSN: 1558-2256. DOI: 10.1109/JPROC.2005.849726.

[13] S. Wendzel, T. Jernej and K. Jaspreet, 'Cyber Security of Smart Buildings,' in *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*, Conference Name: Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications, IEEE, 2017, pp. 327–351, ISBN: 978-1-119-22605-5. DOI: 10.1002/9781119226079.ch16. [Online]. Available: https://ieeexplore.ieee.org/document/8068897 (visited on 08/12/2022).

[14] P. Ciholas, A. Lennie, P. Sadigova and J. M. Such, *The Security of Smart Buildings: A Systematic Literature Review*, arXiv:1901.05837 [cs], Jan. 2019. DOI: 10.48550/arXiv.1901.05837. [Online]. Available: http://arxiv.org/abs/1901.05837 (visited on 09/01/2023).

[15] V. Graveto, T. Cruz and P. Simões, 'Security of Building Automation and Control Systems: Survey and future research directions,' en, *Computers & Security*, vol. 112, p. 102 527, 2021, ISSN: 0167-4048. DOI: 10.1016/j.cose.2021.102527. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821003515 (visited on 08/12/2022).

[16] E. Kovacs, *Researcher Finds Over 60 Vulnerabilities in Physical Security Systems*, 2020. [Online]. Available: https://www.securityweek.com/researcher-finds-over-60-vulnerabilities-physical-security-systems (visited on 16/01/2023).

[17] A. Buckman, M. Mayfield and S. B.M. Beck, 'What is a Smart Building?' *Smart and Sustainable Built Environment*, vol. 3, no. 2, pp. 92–109, Jan. 2014, Publisher: Emerald Group Publishing Limited, ISSN: 2046-6099. DOI: 10.1108/SASBE-01-2014-0003. [Online]. Available: https://doi.org/10.1108/SASBE-01-2014-0003 (visited on 08/01/2023).

[18] M. D. Groote, J. Volt and F. Bean, 'Is Europe ready for the smart buildings revolution?' en, Buildings Performance Institute Europe, Report, Feb. 2017, ISBN: 9789491143182 Journal Abbreviation: Mapping smart-readiness and innovative case studies. [Online]. Available: https://apo.org.au/node/202856 (visited on 19/01/2023).

[19] J. Amoils, 'The Evolving Workplace: Where To Next In A Post-Pandemic World?' en-US, *CRE Real Estate Issues*, vol. 45, no. 23, pp. 1–, Aug. 2021. [Online]. Available: https://cre.org/real-estate-issues/the-evolving-workplace-where-to-next-in-a-post-pandemic-world/ (visited on 21/03/2023).

[20] Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security* (Information Security), Sixth. Cengage Learning, 2017, ISBN: 978-1-337-10206-3.

[21] Håkon Bergsjø, Ronny Windvik and Lasse Øverlier, *Digital Sikkerhet*. Universitetsforlaget, 2020, ISBN: 978-82-15-03422-5. (visited on 21/02/2023).

[22] NEK, *NEK 820:2021*, 2021. [Online]. Available: https://standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1382968 (visited on 22/12/2022).

[23] ISO, *NEK ISO/IEC 27001:2022*, 2022. [Online]. Available: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1446508 (visited on 28/01/2023).

[24] ISO/IEC, *ISO/IEC 27002*, 2022. [Online]. Available: https://www.standard.no/no/Nettbutikk/ (visited on 12/04/2023).

[25] ISO, *NEK ISO/IEC 27005:2022*, 2022. [Online]. Available: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1446508 (visited on 28/01/2023).

[26] K. Thielemann, *Market Guide for Operational Technology Security*, en, 2022. [Online]. Available: https://www.gartner.com/en (visited on 16/01/2023).

[27] Katell Thielemann, *Facing New Threats — Cyber-Physical Systems*, en, Oct. 2020. [Online]. Available: https://www.gartner.com/en (visited on 22/02/2023).

[28] Fortinet, *2022 The State of Operational Technology and Cybersecurity*, en-US, 2022. [Online]. Available: https://www.fortinet.com/resources-campaign/research-papers/2022-the-state-of-operational-technology-and-cybersecurity (visited on 23/02/2023).

[29] ESET, *Siegeware: Ransomware targeting buildings*, en-uk, Aug. 2022. [Online]. Available: https://digitalsecurityguide.eset.com/en-uk/siegeware-don-t-let-hackers-hijack-your-smart-building (visited on 22/02/2023).

[30] Janita, *DDoS attack halts heating in Finland amidst winter*, Nov. 2016. [Online]. Available: https://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter (visited on 08/12/2022).

[31] K. J. H. E.-C. December 20 and 2021, *Lights Out: Cyberattacks Shut Down Building Automation Systems*, en, Section: attacks-breaches, Dec. 2021. [Online]. Available: https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems (visited on 08/12/2022).

[32] P. Bijl, *Case study: Ransomware attack against Nordic Choice Hotels*, en, Oct. 2022. [Online]. Available: https://www.visma.com/blog/case-study-ransomware-attack-against-nordic-choice-hotels/ (visited on 01/02/2023).

[33] M. Slagter, *Ransomware attack responsible for shutdown affecting Jackson, Hillsdale schools*, en, Section: Jackson, Nov. 2022. [Online]. Available: https://www.mlive.com/news/jackson/2022/11/ransomware-attack-responsible-for-shutdown-affecting-jackson-hillsdale-schools.html (visited on 01/02/2023).

[34] J. Vijayan, *Target breach happened because of a basic network segmentation error*, en, Feb. 2014. [Online]. Available: https://www.computerworld.com/article/2487425/target-breach-happened-because-of-a-basic-network-segmentation-error.html (visited on 04/03/2023).

[35] *Target Hackers Broke in Via HVAC Company – Krebs on Security*, en-US, Feb. 2014. [Online]. Available: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ (visited on 04/03/2023).

[36] Committee on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach*, Mar. 2014. [Online]. Available: https://www.covert.io/research-papers/security/A%20Kill%20Chain%20Analysis%20of%20the%202013%20Target%20Data%20Breach.pdf.

[37] A. Greenberg, 'Feds Uncover a 'Swiss Army Knife' for Hacking Industrial Systems,' en-US, *Wired*, Apr. 2022, Section: tags, ISSN: 1059-1028. [Online]. Available: https://www.wired.com/story/pipedream-ics-malware/ (visited on 11/12/2022).

[38] Dragos, 'Pipedream: Chernovites emerging malware targeting industrial control systems,' Whitepaper, Apr. 2022. [Online]. Available: https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf?hsLang=en.

[39] T. Mundt and P. Wickboldt, 'Security in building automation systems - a first analysis,' in *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*, Jun. 2016, pp. 1–8. DOI: 10.1109/CyberSecPODS.2016.7502336.

[40] L. Caviglione, J.-F. Lalande, W. Mazurczyk and S. Wendzel, 'Analysis of Human Awareness of Security and Privacy Threats in Smart Environments,' en, in *Human Aspects of Information Security, Privacy, and Trust*, T. Tryfonas and I. Askoxylakis, Eds., ser. Lecture Notes in Computer Science, Cham: Springer International Publishing, 2015, pp. 165–177, ISBN: 978-3-319-20376-8. DOI: 10.1007/978-3-319-20376-8_15.

[41] M. S. Sonkor and B. García de Soto, 'Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective,' EN, *Journal of Construction Engineering and Management*, vol. 147, no. 12, p. 04 021 172, Dec. 2021, Publisher: American Society of Civil Engineers, ISSN: 1943-7862. DOI: 10.1061/(ASCE)CO.1943-7862.0002193. [Online]. Available: https://ascelibrary.org/doi/10.1061/%28ASCE%29CO.1943-7862.0002193 (visited on 06/04/2023).

[42] B. R. Mantha and B. G. de Soto, 'Cyber security challenges and vulnerability assessment in the construction industry,' en, in *Proceedings of the Creative Construction Conference 2019*, Budapest University of Technology and Economics, 2019, pp. 29–37, ISBN: 978-615-5270-56-7. DOI: 10.3311/CCC2019-005. [Online]. Available: https://repozitorium.omikk.bme.hu/handle/10890/13197 (visited on 06/04/2023).

[43] C. Valli, M. N. Johnstone, M. Peacock and A. Jones, 'BACnet - Bridging the Cyber Physical Divide One HVAC at a Time,' in *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, ISSN: 2473-9391, May 2017, pp. 1–6. DOI: 10.1109/IEEEGCC.2017.8448236.

[44] Nozomi Networks, *Nozomi Networks Discovers Vulnerability in Siemens Building Automation Software*, en-US, May 2022. [Online]. Available: https://www.nozominetworks.com/blog/nozomi-networks-discovers-vulnerability-in-siemens-building-automation-software/ (visited on 16/01/2023).

[45] W. Granzer, F. Praus and W. Kastner, 'Security in Building Automation Systems,' *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3622–3630, Nov. 2010, Conference Name: IEEE Transactions on Industrial Electronics, ISSN: 1557-9948. DOI: 10.1109/TIE.2009.2036033.

[46] D. Meyer, J. Haase, M. Eckert and B. Klauer, 'New attack vectors for building automation and IoT,' in *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, Oct. 2017, pp. 8126–8131. DOI: 10.1109/IECON.2017.8217426.

[47] Y. Maleh, 'IT/OT convergence and cyber security,' en, *Computer Fraud & Security*, vol. 2021, no. 12, pp. 13–16, Dec. 2021, ISSN: 1361-3723. DOI: 10.1016/S1361-3723(21)00129-9. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372321001299 (visited on 16/01/2023).

[48] G. Murray, M. Johnstone and C. Valli, 'The convergence of IT and OT in critical infrastructure,' *Australian Information Security Management Conference*, Jan. 2017. DOI: 10.4225/75/5a84f7b595b4e. [Online]. Available: https://ro.ecu.edu.au/ism/217.

[49] A. Oba, *What is IT/OT Convergence in Smart Buildings? | Ingenuity | Siemens*, en-US, 2022. [Online]. Available: https://ingenuity.siemens.com/2022/03/what-is-it-ot-convergence-in-smart-buildings/ (visited on 08/01/2023).

[50] Schneider, *Cybersecurity at Schneider Electric:Addressing IT/OT convergence in a versatile Cyber ecosystem User guide | Schneider Electric USA*, 2018. [Online]. Available: https://www.se.com/us/en/download/document/IT_OT/ (visited on 08/01/2023).

[51] AlliedTelesis, *Smart Buildings and the Benefits of Convergence*, en, 2022. [Online]. Available: https://www.alliedtelesis.com/no/en/white-paper/smart-buildings-and-benefits-convergence (visited on 08/01/2023).

[52] R. Paes, D. C. Mazur, B. K. Venne and J. Ostrzenski, 'A Guide to Securing Industrial Control Networks: Integrating IT and OT Systems,' *IEEE Industry Applications Magazine*, vol. 26, no. 2, pp. 47–53, Mar. 2020, Conference Name: IEEE Industry Applications Magazine, ISSN: 1558-0598. DOI: 10.1109/MIAS.2019.2943630.

[53] S. Z. Kamal, S. M. Al Mubarak, B. D. Scodova, P. Naik, P. Flichy and G. Coffin, 'IT and OT Convergence - Opportunities and Challenges,' en, OnePetro, Sep. 2016. DOI: 10.2118/181087-MS. [Online]. Available: https://onepetro.org/SPEIE/proceedings-abstract/16IE/All-16IE/186698 (visited on 25/04/2023).

[54] American Institute of Architects, *Integrated Project Delivery: A Guide*, en-US, 2007. [Online]. Available: https://learn.aiacontracts.com/articles/64146-integrated-project-delivery-a-guide/ (visited on 10/04/2023).

[55] P. D. Leedy and J. E. Ormrod, *Practical Research: Planning and Design, 12th Edition*, en. Pearson, 2019, Publication Title: Pearson ERIC Number: ED594592, ISBN: 978-0-13-477565-4. (visited on 10/11/2022).

[56] Jaber F. Gubrium, James A. Holstein, Amir B. Marvasti and Karyn D. McKinney, *The SAGE Handbook of Interview Research : The Complexity of the Craft*, English. Thousand Oaks, Calif: SAGE Publications, Inc, 2012, vol. 2nd ed, ISBN: 978-1-4129-8164-4. [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=986779&site=ehost-live&scope=site (visited on 26/02/2023).

[57] Jaber F. Gubrium, James A. Holstein, Amir B. Marvasti and Karyn D. McKinney, 'Chapter 6 - The Interpersonal Dynamics of In-Depth Interviewing,' English, in *The SAGE Handbook of Interview Research : The Complexity of the Craft*, vol. 2nd ed, Thousand Oaks, Calif: SAGE Publications, Inc, 2012, ISBN: 978-1-4129-8164-4. [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=986779&site=ehost-live&scope=site (visited on 24/01/2023).

[58] NTNU, *Storage guide*, Feb. 2023. [Online]. Available: https://i.ntnu.no/wiki/-/wiki/English/Data+storage+guide (visited on 15/02/2023).

[59] NTNU, *Data collection*, Feb. 2023. [Online]. Available: https://i.ntnu.no/wiki/-/wiki/English/Data+collection (visited on 15/02/2023).

[60] SIKT, *Sikt - Norwegian Agency for Shared Services in Education and Research | Sikt*, en, 2023. [Online]. Available: https://sikt.no/en/home (visited on 22/04/2023).

[61] Statistics Norway, *Fakta om likestilling*, nb, Feb. 2023. [Online]. Available: https://www.ssb.no/befolkning/faktaside/likestilling (visited on 26/02/2023).

[62] C. Parker, S. Scott and A. Geddes, 'Snowball Sampling,' en, *SAGE Research Methods Foundations*, Sep. 2019, Publisher: SAGE. [Online]. Available: http://methods.sagepub.com/foundations/snowball-sampling (visited on 26/04/2023).

[63] F. Fuerst and P. McAllister, 'Green Noise or Green Value? Measuring the Effects of Environmental Certification on Office Values,' en, *Real Estate Economics*, vol. 39, no. 1, pp. 45–69, 2011, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.6229.2010.00286.x, ISSN: 1540-6229. DOI: 10.1111/j.1540-6229.2010.00286.x. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-6229.2010.00286.x (visited on 23/03/2023).

[64] J. K. Deane, D. M. Goldberg, T. R. Rakes and L. P. Rees, 'The effect of information security certification announcements on the market value of the firm,' en, *Information Technology and Management*, vol. 20, no. 3, pp. 107–121, Sep. 2019, ISSN: 1573-7667. DOI: 10.1007/s10799-018-00297-3. [Online]. Available: https://doi.org/10.1007/s10799-018-00297-3 (visited on 14/12/2022).

[65] ISO/IEC, *ISO/IEC 27000*, 2018. [Online]. Available: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html (visited on 04/05/2023).

[66] Concia, *Conscia IoT Device Portal*, en-US, 2023. [Online]. Available: https://conscia.com/whitepaper/conscia-iot-device-portal/ (visited on 27/04/2023).

[67] R. ServiceNow, *Operational Technology Management*, en, 2023. [Online]. Available: https://www.servicenow.com/products/operational-technology-management.html (visited on 03/05/2023).

[68] Palo Alto Networks, *What Is IoT Security*, en-US, 2023. [Online]. Available: https://www.paloaltonetworks.com/network-security/what-is-iot-security (visited on 10/05/2023).

[69] Nozomi Networks, *Industrial Strength OT, ICS, & IoT Security and Visibility*, en-US, 2023. [Online]. Available: https://www.nozominetworks.com/ (visited on 10/05/2023).

Appendix A

Intervjuguide

A.1 Introduksjon

1. Introduser intervjuer
2. Introduser masteroppgaven
3. Informer deltaker om hvordan data behandler og at de kan når som helst velge å trekke seg fra prosjektet
4. Deltaker signerer samtykkeskjema

A.2 Spørsmål

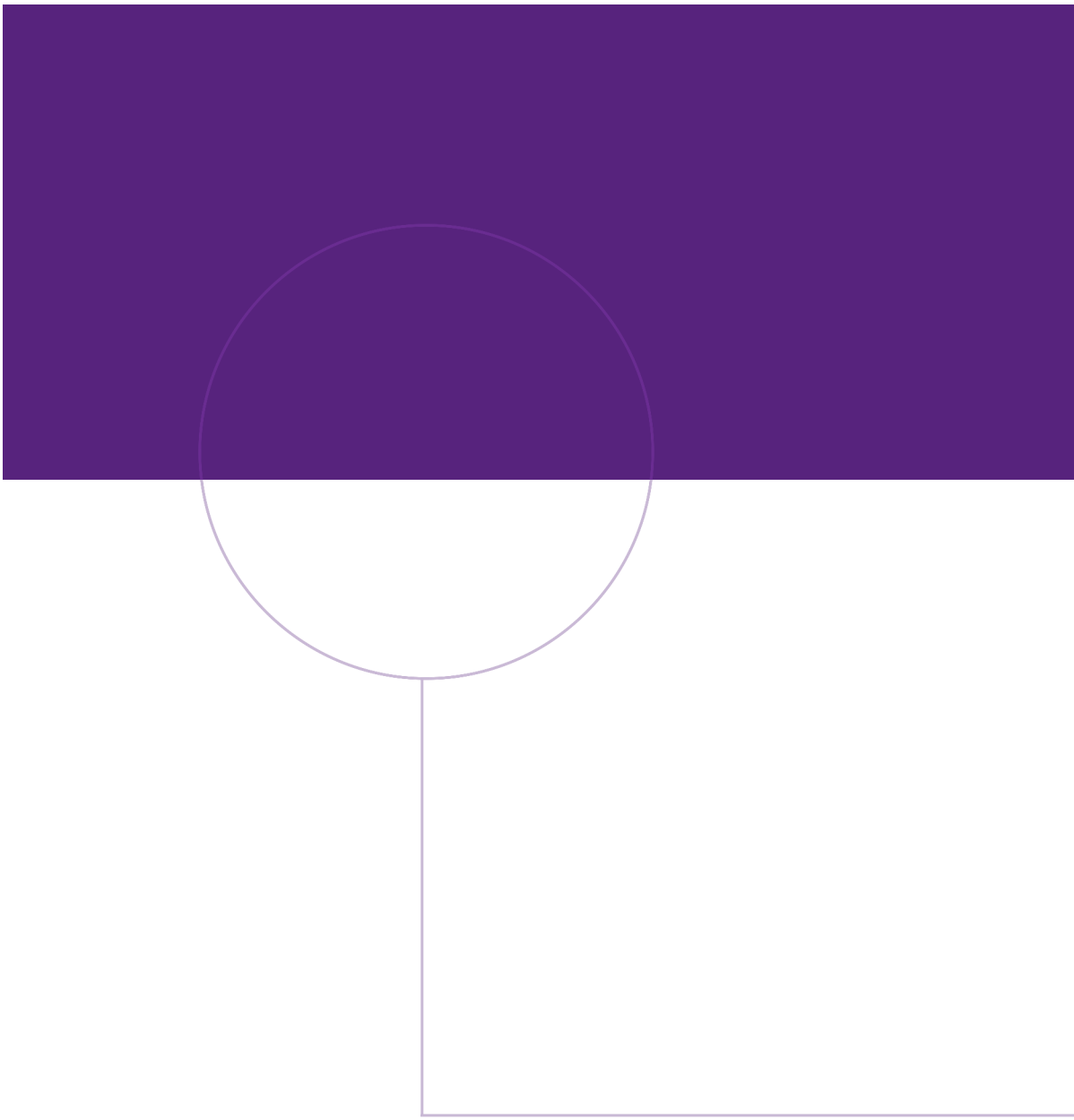
A.2.1 Innledende spørsmål

1. Hvilke oppgaver innebærer stillingen som du sitter i nå?
2. Hvillke roller har du vært i opp mot byggeprosjekter eller drift av smarte bygg?
3. Hva er et smartbygg for deg?

A.2.2 Forskningsspørsmål

1. Har du og aktøren du representere noe ansvar for informasjonssikkerhet for enten prosjekt eller drift knyttet til smarte bygg, hva har dere evt. ansvar for?
2. Hvordan sørger du/dere for at informasjonssikkerhet i smartbygg blir ivaretatt?
    - Møter dere på/genererer dere kravspesifikasjoner som innebefatter at leverandører og entreprenører skal ha kompetanse eller sertifiseringer innenfor informasjonsssikkerhet?
    - Er krav til leveranse innenfor informasjonssikkerhet kontraktsfestet?
    - Er det fokus på informasjonssikkerhet i selve prosjektet? Gjøres det for eksempel tester underveis? Hvem tar ansvaret?
    - Til hvilken grad er det fokus på informasjonssikkerhet i driftsfasen? Patching, lifecycle, deteksjon og respons?

3. Vet dere om konkrete eksempler på områder prosjektet eller drift av bygg hvor det finnes svakheter eller mangler som kan føre til svakheter i informasjonssikkerhet?
    - Kunne det vært bedre presisert i kravspesifikasjon og kontrakt hva som forventes av cybersikkerhet når det kommer til leveranse og drift?
    - Er ansvarsfordelingen tydelig rundt slike kompetanseområder?
    - Sørger noen for at leveranser blir levert på en så sikker måte som mulig?
    - Hvilke prosedyrer har man i drift for å sørge for opprettholdt cybersikkerhet
4. Mener dere at smarte bygg leveres med tilstrekkelig informasjonssikkerhet i dag? Forklar eventuelle forbedringspotensiale som dere kan komme på?
    - Mangel på insentiv?
    - Mangel på kompetanse? hvorfor?
    - Mangel på erfaringer på grunn av at temaet er for nytt?
5. Hva mener du om prioriteringen av informasjonssikkerhet i smartbygg-bransjen i dag?
    - Stilles det krav til aktørene?
    - Kan kulturen i bransjen være en utfordring?
    - Er aktører i bransjen kjent med risikoer rundt manglende cybersikkerhet?
    - Hvordan er fortjenesten knyttet til fokus og investeringer i cybersikkerhet?
6. Hvordan ville du beskrevet et smartbygg som er (informasjons)sikkert, og hvordan ville du oppnådd det?



NTNU
Norwegian University of
Science and Technology

intility | The Enterprise Cloud Solution