UiA University of Agder

Effective Cyber Security Strategies for IIoT

Industrial IoT in the industry sector: Trust and Scalability

Authors	Mathias Nygård Evensen & Jonas Tolås Omdal
Subject	IS-507: Master thesis
Supervisor	Devinder Thapa & Terje Gjøsæter
Date	04.06.2021

University of Agder, 2021
Faculty of Engineering and Science
Department of Engineering Sciences

Acknowledgements

We would like to thank our supervisors Associate Professor Terje Gjøsæter and Professor Devinder Thapa for an excellent effort as supervisors during our master's project. Both Terje and Devinder constantly gave us good feedback and also helped us with some of the challenges we encountered.

Thanks to Erland Kolstad at Agder Energi for providing us with good feedback and suggestions for the thesis. Erland also helped us to find some interview candidates.

Thank you to Eva Brekka for the help and finding of interview candidates. We appreciate the time and effort given.

Abstract

There has been great growth in the use of IoT. It is a modern technology and is becoming increasingly popular. It is also widely used in industrial sectors where it is referred as Industrial IoT (IIoT). Although the technology can provide great benefits, it also leads to some challenges. In this thesis we will explore the security characteristics of IIoT used in industrial sectors. We will determine why and if there is a correlation between trust and scalability in IIoT infrastructure. In order to do this we will be using qualitative methods for data collection and have performed both interviews and simulations. We also use systematic literature review is used to structure and review the literature. We performed a synthesis of all the data combined from literature review, interviews and simulations in order to provide an explanation to security aspects and trust with scalability. We discover that there is some contradiction between the results of the security aspects used in real world and the ones in literature. The relationship between trust and scalability was also discovered to strong. Trust in IIoT devices is needed to scale a network. The multiple ways you create trust is also discussed and can be done in multiple ways. The scalability is also affected by the topology of a system. As a result of our findings we will suggest some guidelines for establishing trust and scalability in IIoT infrastructure.

Contents

List of Figures

List of Tables

1 Introduction

Internet of things (IoT), has for several businesses become a central component in gaining a competitive advantage. In short, IoT enables "things" or devices internet connection. Devices such as smartphones, wearable, and small sensors are instances of common IoT. The term originated in the early 2000s as internet connectivity started to become more stable and better performing compared to earlier which opened up the use of IoT. (Chase, 2013). IoT have in recent times been widely used compared to earlier. In 2010 there was 0.8 billion IoT connections and by 2025 it is expected to be around 30.9 billion IoT connections (Lueth, 2020).

IoT can be used to create new services and business opportunities which can be tailor-made to fulfill specific tasks and processes and automate manual tasks. One could for example use IoT to monitor and control unnecessary usage of power. From a business perspective, IoT will help to reduce large costs, and increase the efficiency and productivity of certain work-tasks. In fact, 83% of organisations have improved their efficiency by introducing IoT technology. (Jovanović, 2021). It can also provide new business opportunities, as data gathered from IoT can further be monitored and analysed, which then can give predictions on trends and patterns. This can help companies personalise and design products for these trends and help to maintain a competitive advantage and stay relevant on the market.

IoT has also increasingly gained popularity in industrial sectors and is involved in several of their operations and procedures. In fact, IoT is more used in the industry compared to regular consumer related IoT. Business investment will grow from $215 billion to $832 billion versus consumers at $72 billion in 2015 to $236 billion in 2020 PwC (2016). In the context of IoT in the industry, the technology is often referred to as the Industrial Internet of things (IIoT). This was to distinguish between consumer related IoT and the industrial IoT of business to business (B2B) applications Novotek (N/A). The industrial sectors were early and fast adapters of IIoT, a trend that is known as Industry 4.0, or the Fourth Industrial Revolution. The core of IIoT is machine automation with few human input due to robotics, while IoT is more focused on the people using the machines.

Although IIoT offers several benefits for the industrial sector, the technology also faces some security concerns. As technology is getting more advanced so are the cyber criminals. New methods of attack can be very difficult to protect against and the consequences of this can be catastrophic. Using IoT opens up for new vulnerabilities and entrances to larger systems. The security of devices varies from device to device. If a company has one weakly protected IoT device it could potentially lead to unauthorised access and unwanted actions. This is a problem that has gained a lot of attention nowadays and has in several cases been the cause of successful cyber attacks.

1.1 Trust and Scalability

The security aspect of Industrial IoT is quite broad. This thesis we will focus on challenges regarding trust and scalability which is major concerns when it comes to IIoT and related security. Trust related to IIoT is how the units can be trusted. For example, how can one be sure that the data from the devices has not been modified by unauthorised persons? Or how can you know that a device has not been compromised?

IoT systems have a waste amount of connected sensors and other devices that shares a lot of information via the open internet. Scaling up larger IoT systems can be a demanding and challenging task to perform. There are several factors one need to take into account in order to accomplish this in a secure and efficient way. In the context of IoT there are two types of scalability; vertical scalability and horizontal scalability. Vertical scalability is also known as "*scaling up and is the ability to increase the capacity of existing hardware or software by adding more resources to it.*" Gupta and Manjula (2017). With horizontal scalability you "*scale out and is the ability to increase the capacity by connecting multiple hardware or software entities so that they can work together as a single unit.*" Gupta and Manjula (2017). In this research, we will examine both approaches.

1.2 Research Motivation

The motivation for the chosen topic comes from the fact that IIoT is starting to become very comprehensive in today's society. Several companies are starting to invest heavily in this technology and we think it is interesting to see how people utilise this and how involved they are in related security. Another element that motivates is that we can contribute to a relative new field. From existing literature, we see that there is little that specifically focuses on trust and scalability within IIoT. Therefore, we want to explore this, and investigate the relationship between trust and scalability in an IIoT infrastructure. As a result of this thesis, we want to propose a framework for securing IIoT. We want to help initiate thinking and the importance of security on this topic. During the literature review, we discovered existing standards and best practices for IoT and IIoT. The most talked about standards were The Data Distribution Serivce (DDS) foundation and the IEEE standard. These help enhance the security around this technology, but do not cover the areas around the concerns of trust and scalability. This in turn can lead to problems when companies, for example, have to use IoT and create a network with IoT devices. How can one expand such a type of network in the best possible way and how can one trust that incoming data is compromised.

1.3 Research Gap

By exploring previous research we found a few gaps that is important to address. In general, much of the found literature was related to the current state of Industrial IoT and the characteristics of the technology. Some of the papers were focused on specific sectors. For example a paper from Hossein Motlagh et al. (2020) takes on the use of IoT in the energy sector. As IoT characteristics was something that was repeated in several literature's, we feel that it is important to include in our research as well. This will be used further to build a better understanding on the areas of trust and scalability in IIoT infrastructure which is the main focus of this thesis. When it comes to trust and scalability, there was little information available. Establishing IoT infrastructure in a company and securing IoT devices are very critical elements that should be addressed. This can quickly become a weak link in companies and lead to unwanted access to larger systems and sensitive data. In short, we found that the main gap was that there were few standards and best practices. Little research had also been done in the areas of trust and scalability in IIoT infrastructure. Much was focused on specified elements, but we want to cover a slightly broader aspect.

This can be found in more details in the chapter section 4.2.1 Findings

1.4 Research questions

In this research, we will take a closer look at some of the security characteristics of IIoT infrastructure. We will also try to find if there are any correlation between trust and scalability in a such environment. Additionally, we will suggest effective cybersecurity strategies for this in form of some guidelines. We have therefore come up with the following research questions:

1. What are the security characteristics of an IIoT infrastructure?
2. What is the relationship between trust and scalability in an IIoT infrastructure in the industry sector?

1.5 Research Activities

In order to conduct this research we have planned out the following research activities;

1. **Literature review**

   For reviewing literature we will use stand-alone literature review methodology, but with a systematic, rigorous standard. This is also called a Systematic Literature Review (SLR). This method consist of 8 steps that involves excluding and including literature. Involved literature will be placed two different tables. One table contains excluded literature and the other included. As a result, we will present the literature review procedure in the form of a figure / diagram. This is a relatively large task and we have calculated that this will be one of the most time-consuming tasks.

2. **Qualitative interviews**

   The main method for collecting primary data will be qualitative interviews. We will make a semi-structured interview and plan to interview people from different types of industrial companies. The interviews will be digital and take place via Microsoft Teams or Zoom. The interview and transcription part is the most demanding and important task in our thesis and we have set aside plenty of time for this.

3. **Analysis of the interviews**

   In order to make the analysis of the interviews more structured and manageable, we will use Kvale's five methods for analysing the interview. (Kvale, 1997, p. 123-126)

4. **Simulations**

   After conducting and analysing the interviews we will start with the simulations. For this we will use a node network simulation program called Atarraya. The purpose of the simulation is to use it as a complementary method to the interview data.

5. **Establish Guidelines**

The guideline will act as a result of this thesis where we will propose different types of security measures to be able to secure industrial IoT infrastructure where we will propose effective cyber security strategies to secure Industrial IoT infrastructure in terms of trust and scalability.

1.6 Implementation

We address the research questions in this thesis by extracting data primarily from interviews and literature. This give us the opportunity to get real world examples of how IIoT is used and established. Along with this, the literature give us the chance to look at future improvements and opportunities that are on the horizon. Combining this data together provide us with a good holistic view of the research questions. The simulation in this thesis will add to case examples to gain insight to protocols and how a network might look like. The main findings provide concrete examples of how IIoT security look like a company. The findings also give us an indication that there is in fact a relationship between trust and scalability.

1.7 Ethical Aspects

The ethical aspects that needs to be considered in this thesis is privacy, data extraction, results and objectivity. Privacy of the interviews are used to ensure that personal information maintain private and that data collected is managed according to the law. The data also needs to be presented in a meaningful and objective way. The data extraction is done by analysing the data from the transcriptions made of the interviews. We also explained how we did this in chapter 2. The literature review is extracted by reading the papers and explaining them. We also went through topics and gaps in the literature. The simulation was analysed after the simulation was done, with the topology algorithms as the anchor for the data.

The results are a match of all this data and is presented, discussed and concluded in the last chapters. Objectivity is important. We do not receive or have received any grants, funds, benefits or donations for this research. The research is purely motivated with the interest of the topic and the need for information in this field. This is why we want to deliver the best possible research and master thesis.

We have given our research intents and the data that is to be collected to Norsk Senter for Forskningsdata (NSD) which approved the measures we have given to ensure privacy and data management. The reference number is 712093.

The interview candidates of this thesis is ensured privacy by increasing the anonymity of them. This way we call them informants, rather than displaying their names. The data collected is also protected at UiA's OneDrive since they have a Service Level Agreement with Microsoft. The data is separated and anonymity is given in form of codes, which are separated from transcriptions. All folders have access management, so that we can only allow certain users to see the data and see the access logs.

The steps we took to minimise the risk of participating were to give anonymity to participants. The general sectors of the interviews are mentioned to give context to answers. We have also provided data management plans and security precautions to NSD. These are as mentioned above, the storage and separation of data through the cloud environment of UiA OneDrive.

1.8 Report Structure

This thesis will further be structured in this way:

Chapter two concerns method used for reviewing the literature. We used systematic literature review (SLR). This methodology consists of 8 steps and describes how we excluded and included literature used in our thesis. It also describes how the data is extracted and how it is applied. The excluded and included literature can be found in the appendix. Chapter two continues with our takes on the included literature from SLR. Furthermore, included literature is placed in a concept matrix inspired by Webster and Watson (2002) which divides the literature into multiple categories. In this chapter we also present the main gaps in the literature compared to our study.

Chapter three presents the methodologies used in this study. The choice of research methods and how we are going to use them is explained here. We went for a qualitative approach and the method used for this study was mainly qualitative interviews. We also used supplementary simulations to back up the data from the interviews.

In the fourth chapter we present the findings from the analysis of the qualitative interviews, literature and simulations. First we divide the topics of the interview and go through examples and analysis of the answers we received. After that we present the finding from literature, which highlights areas of interest and gaps in the existing research. Lastly we give the findings of the simulation and give explanations to the setup and the parameters of the simulation.

In the fifth chapter we discuss the results from finding and the content from previous research along with the simulation. This is a synthesis of all the findings were we discuss the findings and compare each of the results together. We chose to divide them into categories where we could compare the different results.
After the synthesis, we present a guideline which incorporates our findings into a more presentable overview. With this we will propose effective cybersecurity strategies and will be the end result for this research. The guideline gives a graphical overview along with detailed description under.

Chapter six presents the discussion. Here is the discussion of the thesis, results and contribution along with the limitations of the research.

Chapter seven give a conclusion to the research and the thesis as a whole. We give our answers to the research question. We give our insight and reflection to the research and how the results can be utilised. Last of all we give recommendation to future work on the topic.

Appendix includes the exclusion and inclusion of literature, interview guide and a quick summary of the interviews sorted in topics.

2 Literature Review

Well conducted literature reviews can give several advantages such as assessing research topics' current state. When conducting research it is important to know what information is available and if there is anything written on the desired research topic. It also can be use full to find potential research gaps. Additionally, by reviewing literature one could also discover new angles on intended research that can further be explored.

When reviewing literature there are mainly three types of methodologies to take in use; theoretical background, thesis literature review, and stand-alone literature review. In our research we will use stand-alone literature review methodology, but with a systematic, rigorous standard Okoli (2015). This is also called a Systematic Literature Review (SLR), and we will use this to answer our research question. The methodology consists of 8 steps that revolve around filtering and validate literature. Van der Knapp defines the method as; "The most reliable and comprehensive statement about what works', systematic reviews involve identifying, synthesising and assessing all available evidence, quantitative and/or qualitative, in order to generate a robust, empirically derived answer to a focused research question." (van der Knaap et al., 2008)

The guide we followed is based on information from six other source guides which makes this approach quite credible. These are; "*Kitchenham's (2007) guide to SLRs in software engineering, Petticrew and Roberts' (2006) book on SLRs in the social sciences, Arlene Fink's (2005) guide on SLRs in health sciences; Rousseau, Manning and Denyer's (2008) article on SLRs in management and organisation science; Levy and Ellis' (2006) article on conducting literature reviews in information systems; and Webster and Watson's (2002) article on writing up literature reviews in information systems.*" (Okoli, 2015)

The figure below illustrates the steps and phases that the SLR methodology consists of.

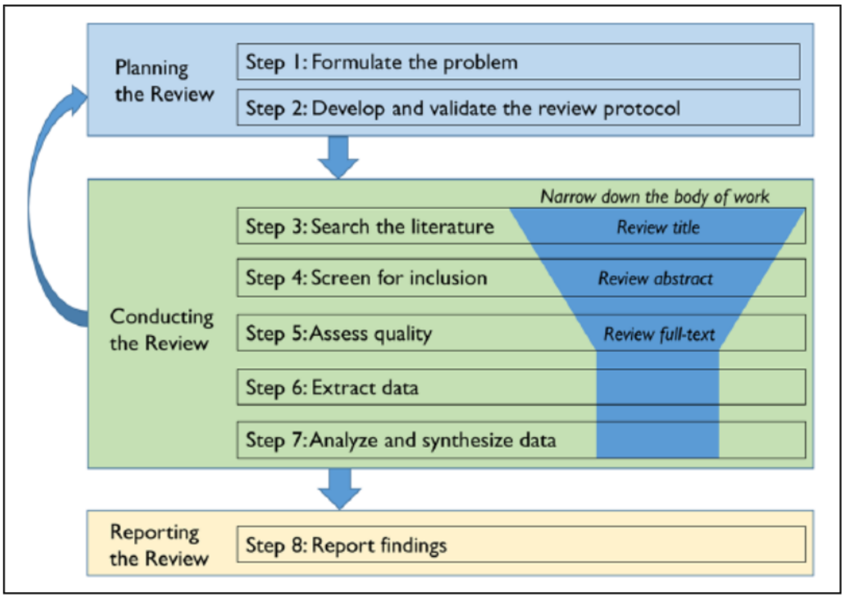

Planning the Review
Step 1: Formulate the problem
Step 2: Develop and validate the review protocol
Narrow down the body of work
Step 3: Search the literature
Review title
Step 4: Screen for inclusion
Review abstract
Conducting the Review
Step 5: Assess quality
Review full-text
Step 6: Extract data
Step 7: Analyze and synthesize data
Reporting the Review
Step 8: Report findings

Figure 2.1: SLR process
(Xiao and Watson, 2019, p. 103)

2.1 Step 1: Formulate the problem

With the use of SLR, we mainly want to investigate the thesis topic and to answer our research questions;

- What are the security characteristics of an IIoT infrastructure?
- What is the relationship between trust and scalability in an IIoT infrastructure in the industry sector?

In order to accomplish this, we need to identify relevant literature in a structured and efficient way. We also need to have a specific and concrete topic and research questions. By this, we can restrict the amount of necessary data, making the review more manageable.

By using literature to review the existing solutions and combining them with our interviews and simulation, we can give a contribution to the problem of trust and scalability in IIoT. With the help of the bullet points under we can look at the existing and future solutions to the problems.

The industrial side of IoT require different solutions to different problems to what you find in commercial IoT. Some of the challenging factors named in the research problem. Some of the challenging factor include things such as:

- Network and Connectivity
- Size and Power Consumption
- Scalability
- Integrity, Availability and Confidentiality
- Non-repudiation and Trust

The problem then becomes how one can solve these problems and utilise a framework to set up these devices in a manner that resolves these problems.

2.2 Step 2: Develop and validate the review protocol

In this step, we need to establish a common procedure to adhere to as reviewers. In order to accomplish this, we created a detailed protocol document that will help to guide the rest of the review process. This is important so that we as reviewers stay on the same page and can be consistent in our literature review. As a result of this can we save time, increase the effectiveness and reduce redundant work.

2.3 Step 3: Search for literature

There are three major ways to find literature; electronic databases, backward-searching, and forward-searching. Petticrew and Roberts state that electronic databases constitute

the predominant source of published literature collections (Petticrew and Roberts 2006). We found and used literature from multiple electronic databases, as this was our main method for finding literature. The reason for this is because with SLR you should use literature from multiple databases because no single database contains the complete set of published material. However, we mainly used Google Scholar to search for our literature, but we also used IEEE Xplore, ProQuest and Web of Science. Google Scholar provided us with a vast amount of studies/papers. Additionally, it has a feature that creates easy BibTex citations. Before performing a literature search we created a specific key-word list that related to our topic and research questions. This was done so we could easier find desirable literature. The key-word list consisted of the following words and terms;
IIoT, IoT, Scalability, Trust, ZeroTrust, Integrity, Availability, Sensor, Processing power, Encryption, Security, Framework, Privacy, Data collection.

2.4 Step 4: Apply practical screen

After conducting searches, we ended up with a total of 65 literature sources. This is a rather large amount of literature. Many of these will be inapplicable for our study so the next step is to narrow down the number.

In practical screening, or screening for inclusion, we tried to plan out explicitly what literature was necessary to have and to support our study. This would help us to easier exclude and include literature for further research. We created a set of criteria regarding the entirety of the literature. The literature was then weighed against the criteria and research questions and was then either included or excluded. We created the following criteria:

- **Content**: The articles or information had to relate to our topic and research questions. The content must not be too complex and technical. Further inspections of such papers can be very time-consuming.
- **Publication language**: The language must either be in Norwegian or in English.
- **Setting**: The information should come from a setting within the industry sector and IIoT. The setting should also relate to trust and scalability.
- **Date of publication or of data collection**: Newer studies will mostly be preferred with the thought of new technologies, vulnerabilities, frameworks, and security trends. The timescale will be from 2015 - today.
- **Source**: The information should only come from trustworthy sources and not from sources such as blogs and Wikipedia where the data/information may be incorrect.
- **Peer-reviewed**: The papers in the literature search must be peer-reviewed. Many of the found literature are from conferences and have a lower chance of being not peer-reviewed. This causes an uncertainty that we want to consider in our SLR.

2.5 Step 5: Quality Appraisal

The fifth step concerns screening of exclusion. This was short implied in the previous step but will be further explained in this step.

The process of reviewing sources went through iterations. First, we read through the title of each paper, then excluded those who were irrelevant to our research questions and criteria. Second, read through each abstract and excluded more. lastly, we read through the entire text of the literature and again excluded the non-relevant literature. This step should be completed thoroughly since this is the last step in the preparation before actually extract data and synthesis from the studies.

In order to show reviewed literature in a structured way, we created two tables. The first table shows the overview of excluded literature and reasons for exclusion. The second table contains included literature and provides an overview of included literature. This table also shows used data collection methods(qualitative/quantitative) and the literature's degree of relevance on a scale from 1 to 5, as well as a justification for given ranking. The table also maps the literature to the research questions, which was beneficial when finding information regarding the individual research questions.

2.6 Step 6: Extract data

The literature from the included tables was then further inspected and we started to extract relevant data which can be found in chapter 3.2 (Previous research). In this section we also created a concept matrix with the included literature. The concept matrix was used as an aid to categorise the literature which then helped to map the literature better so that data retrieval became an easier task.

2.7 Step 7: Analyse and synthesise data

In addition to the included literature we will also extracted data from interviews and simulations. With these three sources combined we will try to answer our research questions in details. Both the interviews and simulations are qualitative approaches. The included literature consist of both qualitative and quantitative methods. Each literature in the inclusion table A.2 is marked with used method for data gathering and the literature's degree of relevance as well as a accompanying small justification. The degree of relevance is based on our opinions. Literature with higher degree's was used than the others to an extent. This was and is used as a method to make retrieval and sorting of literature more transparent.

2.8 Step 8: Report findings

The process of the systematic literature review must be reported in sufficient details so that the review can be reliable and independently repeatable Okoli and Schabram (2010). By this, one can perform same actions and achieve the same result. A strong factor for achieving this comes from the inclusion and exclusion criteria, which then shows the basis for the selection of literature. This must be done thoroughly. Each criteria should have justifications for why they are chosen. To sum up the findings in SLR, we have made a figure that shows the overview of the SLR process. Note that the number (n) on excluded literature does not match up because one paper can have several of the criteria. Additional methods and example papers, are used outside the literature review and was used as inspiration and to find additional information on already included literature.

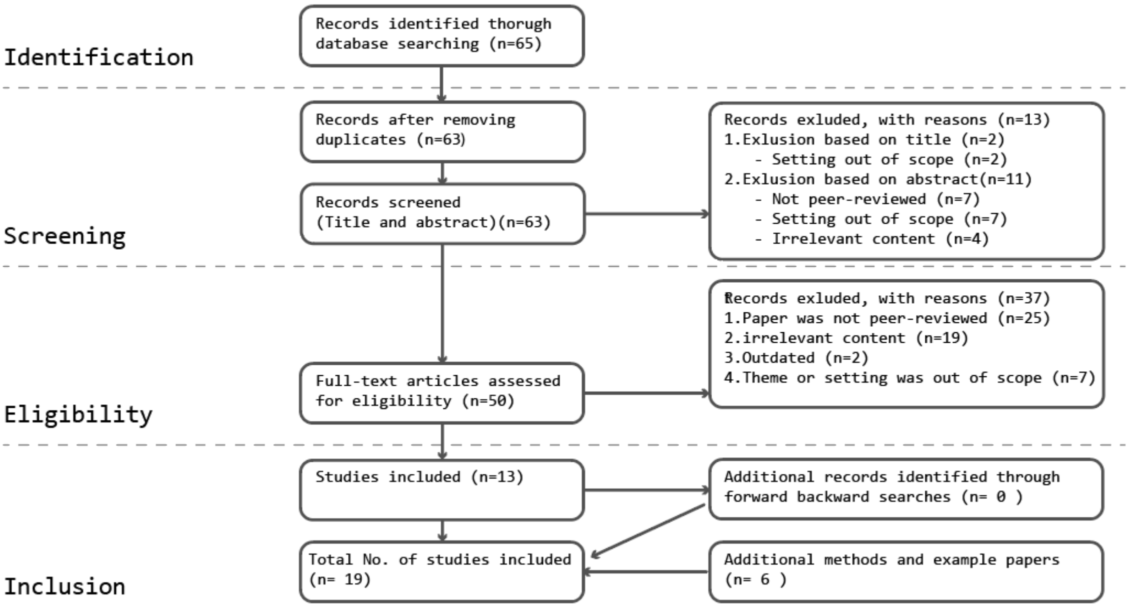

Identification
Records identified thorugh database searching (n=65)
Screening
Records after removing duplicates (n=63)
Records screened (Title and abstract)(n=63)
Records exluded, with reasons (n=13)
1.Exlusion based on title (n=2)
- Setting out of scope (n=2)
2.Exlusion based on abstract(n=11)
- Not peer-reviewed (n=7)
- Setting out of scope (n=7)
- Irrelevant content (n=4)
Eligibility
Full-text articles assessed for eligibility (n=50)
Records exluded, with reasons (n=37)
1.Paper was not peer-reviewed (n=25)
2.irrelevant content (n=19)
3.Outdated (n=2)
4.Theme or setting was out of scope (n=7)
Inclusion
Studies included (n=13)
Additional records identified through forward backward searches (n= 0)
Total No. of studies included (n= 19)
Additional methods and example papers (n= 6)

Figure 2.2: SLR Result
Based on: Xiao and Watson (2019, p. 108)

2.9 Review of included literature

This section will give an overview of relevant topics and research that has already been conducted. This research will give an in depth look at previous solutions and work in the field of IIoT with trust and scalability. After that, there will be an overview of them generally stating their findings [2.10]. The last section will include a concept-centric presentation of the literature we found useful and the conclusion of the literature review [2.11]. The findings of the literature review can be found in chapter 4.2 findings of literature.

In this literature search we will look at the security characteristics of IIoT and the relationship between trust and scalability. It will also cover other topics that may be relevant to acquire a better understanding of the IIoT solutions and problems that exists. This may be topics such as low power management, frameworks, hardware and security concepts.

2.10 Previous research

There is a lot of research to go through as this is an emerging topic. Therefor it is imperative to look at the previous research done in this field, before we continue. Some of the research concerns the general state of IIoT, however most of them go into details about different solutions that are provided. The previous research also covers some technical aspects of the IIoT solutions today.

Hossein Motlagh et al. (2020) gives a review of the existing literature and challenges on IIoT in the energy systems that are utilised in the sector. It also highlights a comparison of different wireless technologies which gives an understanding of the different protocols and the cost-benefit, usage, security and range in the different scenarios of which the devices can be used. The review also gives a look into how design, integration, standardisation, energy consumption and security affects the choices that has to be made in order to deploy such systems.

Xu et al. (2020) looks at the trust-oriented IoT with smart cities and edge computing with SPEA2 (Performance of the Strength Pareto Evolutionary Algorithm 2). This result gives reason to use trust-oriented method to reduce resource usage, load balance and power consumption. It gives mathematical evidence to support service placement strategies based on the value of each unit.

Singh et al. (2017) discusses the invention of lightweight algorithms for IoT. They recommend it because it has makes it possible to achieve end-to-end encryption with low power consumption. The footprints are smaller and has the possibility of more network connections on low power devices. The lightweight block cipher is proposed where it is implemented smaller block sizes, key sizes, rounds and simpler key schedules. An example of block ciphers is to divide 128 bit keys into four 32 bit keys with Tiny Encryption Algorithm (XXTEA). It is also recommended that hardware is specific to the application, and that many new devices have implemented hardware accelerated components specifically for encryption. There has also been proposed methods to implement AES in a lightweight system. Considering all this Singh et al. (2017), suggests a Hybrid Lightweight Algorithm which is a combination of lightweight symmetry and lightweight asymmetric encryption.

Boyes et al. (2018) reviews the terms and taxonomies of the IIoT world and sets up an analysis framework of IIoT. They aim to establish a framework that can analyse the nature of IIoT devices and their use, which include vulnerability and threat analysis. They have done this by enabling more taxonomies that does not base itself on "*product marketers to create new jargon to differentiate their products.*" as they say. By creating defined specifics they enable the use of accurate detail description and separation of different zones of IIoT solutions by mapping them. A classification schema.

Abuhasel and Khan (2020) proposes a framework for resource management in smart manufacturing. This is done by the use of SoftMax function (a multinomial logistic regression) in combination wit deep neural networks and improved RSA techniques. This is proposed using node degree(N), distance from the cluster(D), residual energy(R), and fitness(f) (NDRF) clustering. This is done to increase speeds, transmission and create energy efficiency by locating the best nodes for an operation.

Cheng et al. (2018) explores the possibilities of 5G in IIoT. It describes the characteristics which enable 5G to be a good option for IIoT. The 5G advantages create three prospects that use cases. There is:

- Enhanced Mobile Broadband (eMBB)
  - Video and streaming
- Massive machine type communication (mMTC)
  - Automation, storage and Real time monitoring
- Ultra-reliable and low latency communication (URLLC)
  - Man-machine interaction and automation

These different types of communication along with the technologies that already make 5G good, makes for a compelling case where IIoT and 5G can operate. It has *potential to promote IIoT and CPMS manufacturing system.*

Meng et al. (2017) gives a proposed ZMQ-based data oriented messaging mechanism to deal with the machine to machine (M2M) communication. This is used to deal with the discover, messaging, interaction and connectivity between devices. They demonstrate this with an experiment and where they use low-level TCP or UDP sockets to communicate between devices. The flexibility of cross-platform and efficiency can create a flexible network with ZMQ. ZMQ operates as an asynchronous messaging library used with distribution or real time applications. It runs without a dedicated messaging broker.

Liu et al. (2019) reports with an experiment on the multiple attacks that can occur in an IIoT network and focuses on multiple attacks rather than a single attack. This is achieved with the use of the algorithm named Perceptron(PD) which decides whether or not an input, based on vectors to classify if it belongs in a specific class. This study gives an example of how PD can achieve better accuracy on mixed multiple attacks over a more traditional hard detection. The detection depends on the network diversity to compute trust values for each node and be able to detect malicious nodes. The paper gives also an overview over the mathematical formulas needed for such a network in training.

Pinto et al. (2017) shows a view of why TrustZone is becoming a technology for securing edge IoT devices with trusted execution environments (TEE). TrustZone is a security extension implemented by ARM which again is an instruction set for computation. The API of TrustZone can specify how non-secure application sources can run and interact on the execution environment. This elevates security through hardware and can help secure the environment. "*The TEE is a secure area ensuring that sensitive data are stored, processed, and protected in an isolated and trusted environment.*". This can separate user mode an the kernel mode, which separates the dangerous applications from the protected environment. The ARM TrustZone aims to secure the components at the device level. There is still a need for end-to-end, network and other cloud level security.

Sanchez-Iborra and Cano (2016) explores the need for strict environments in IIoT. It discusses a novel paradigm for Low-Power Wide Area Network (LP-WAN). The advantage of this platform is its high scalability and range, roaming, real-time events and low edge-node energy consumption. With the use of star topology and star-of-star topology which enables the high scalability. The most prominent platforms for these are LoRaWAN, Sigfox and Weightless. Along with these platforms there are also proposed standards by the IEEE and 3GPP group.

George and Thampi (2018) provides a graph-based solution to represent the vulnerabilities in relation to an IIoT network. They also propose risk mitigation strategies to improve security on an IIoT network. The work simulates and creates a use-case where models and techniques proposed are used to help reduce overall threat level of a network with threshold values corresponding to threat, hop and hot-spot index. By storing the paths of data and the hops made between nodes, one can deduce threat and remove nodes.

Aziz Zahed et al. (2020) discusses the promising application of caching for IIoT devices that require long battery life. It is however prone to malicious attacks. This is suggested to be resolved with something called trusted caching nodes along with a proposition to a heuristic algorithm to solve optimisation problems. The trusted cache nodes can hold data until requested and can save on battery by reducing the amount of requests. This can also be a content delivery system.

Lyu et al. (2018) proposes a hierarchical transmission estimation approach which aims to achieve energy efficient and reliable transmission. This is achieved by creating a fog-cloud framework which reduces the computing load of each sensor by integrating it with a group based communication and data aggregation. They provide simulation results which show overall estimation of energy, error and consumption caused by the approach, which seems to be lower than other approaches.

2.10.1 Concept matrix

The concept matrix is generated from the research previously conducted and is derived from a concept matrix augmented with units of analysis suggested by Webster and Watson (2002, p. xvii).

O = Organisational, G = Group, I = Individual

Article	Concepts																							
	IoT characteristics			Trust			Scalability			Lifetime management			Encryption			Communication			Security Concepts			Hardware		
Unit of Analasys	**O**	**G**	**I**	**O**	**G**	**I**	**O**	**G**	**I**	**O**	**G**	**I**	**O**	**G**	**I**	**O**	**G**	**I**	**O**	**G**	**I**	**O**	**G**	**I**
\Xu, Liu, Xu, Dai, Zhang, and Qi (2020)				**X**	**X**							**X**		**X**	**X**					**X**	**X**			
\Singh, Sharma, Moon, and Park (2017)								**X**				**X**			**X**									**X**
\Boyes, Hallaq, Cunningham, and Watson (2018)	**X**	**X**	**X**																**X**	**X**				
\Abuhasel and Khan (2020)										**X**					**X**			**X**			**X**			
\Cheng, Chen, Tao, and Lin (2018)	**X**	**X**						**X**								**X**	**X**					**X**		
\Meng, Wu, Muvianto, and Gray (2017)								**X**									**X**	**X**						
\Hossein Motlagh, Mohammadrezaei, Hunt, and Zakeri (2020)		**X**	**X**									**X**					**X**			**X**				
\Liu, Ma, and Meng (2019)						**X**						**X**						**X**		**X**				
\Pinto, Gomes, Pereira, Cabral, and Tavares (2017)					**X**	**X**									**X**			**X**						**X**
\Sanchez-Iborra and Cano (2016)								**X**	**X**			**X**					**X**			**X**				
\George and Thampi (2018)												**X**						**X**		**X**	**X**			
\Aziz Zahed, Ahmad, Habibi, and Phung (2020)						**X**						**X**						**X**						
\Lyu, Chen, Zhu, and Guan (2018)												**X**						**X**						

Table 2.1: Concept matrix

2.11 Extraction of literature

In this section we will look at the key concepts of the literature. Many of the included sources touch upon the same topic in some form or closely relate in concepts. The key for this section will be to look and compare different strategies of the research and discuss the options available. The concepts that are discussed will be provided from the from the concept matrix. We will also look at some papers that may not be considered valid for a literature review, however might be interesting to look because of the topics they introduce. The reason these will be included is because the topic of "trust model with scalability" is in its infant state and does not have much peer-reviewed literature. So to introduce topics and ideas from this, we will look at some promising topics, that may include conferences from IEEE.

2.11.1 Overview

From many of the sources that are available and are peer-reviewed a large amount of them do not consider the fact we are trying to accomplish, which is to look at how a trust model work with scalability. From the literature we have identified three papers which talks about this topic. Those are the papers from Aziz Zahed et al. (2020), Pinto et al. (2017) and Lyu et al. (2018). We will start with them and then take a look at the perspectives they bring forth. The rest of the literature is still relevant because they introduce problems and solutions that directly affects the points in the three aforementioned papers. In order to understand the concept of trust models cooperating with scalability, we choose to look at examples of them individually in order to understand them, to later be able to combine them.

The topics that are brought up for trust models are:

- Fog computing
- TrustZone
- Topology

2.11.2 Fog computing

Yi et al. (2015, cited by Atlam et al. (2018)) defined fog computing such: "*Fog Computing is a geographically distributed computing architecture with a resource pool which consists of one or more ubiquitously connected heterogeneous devices (including edge devices) at the edge of network and not exclusively seamlessly backed by Cloud services, to collaboratively provide elastic computation, storage and communication (and many other new services and tasks) in isolated environments to a large scale of clients in proximity*".
This explanation gives us a good look into the paradigm of trust and scalability. The reason is that fog computing inherently already has some form of trust model that makes the nodes able to compute and talk to each other in the "edge" of the network. By looking at the trust that is needed in fog computing, we can start to understand problems and models that are available. Fogs are essentially devices that are closer to the IoT devices that receive communication between a central cloud and the IoT devices. You can almost see it as a middleman.
It is used to complement the already existing cloud network by reducing the load of the central node by applying more devices closer to actual edge nodes. The fog computer is relieving by computing, storing and network resources. Caiza et al. (2020). Location and allocation of resources is also an important factor. The internal nodes can be scaled with software and hardware while nodes can be added externally by providing a localised service and by that distributing the service tasks at the nodes and improving scalability and redundancy. Yuan et al. (2017, cited by Caiza et al. (2020)). By distributing the work evenly to other nodes, it can create good expansion capabilities and allow worker-nodes to send their data to the fog for computation and network processing.

An example of a basic fog structure

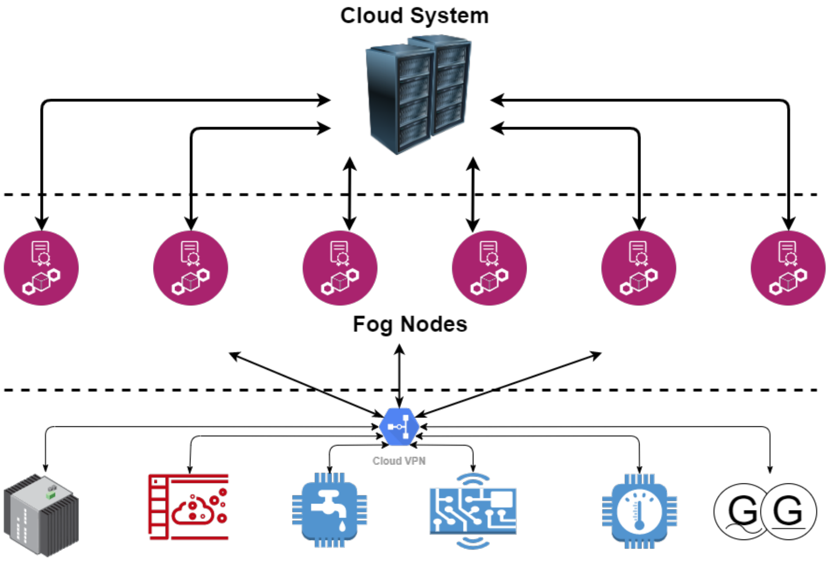


Figure 2.3: Fog computing

2.11.3 TrustZone

TrustZone is a concept of the ARM group which intends to enable the security needs for edge devices also like the ones seen in fog computing. This is protection on the individual hardware and software level of the components to allow for safe communication between them. The idea is that edge devices that require extra protection can enable a secure execution environment. This introduces however a small overhead. Zhang et al. (2019) introduced software-based memory protection approach with TrustZone and saw an overhead of roughly 20%. This is not bad if we consider the overall protection of the devices. Pinto et al. (2017) also explains that the confidentiality is enhanced since it has spatial isolation mechanisms and that separated parts can't access memory segments to the trusted zone. The only communication is between the communication channel which is known to not authenticate the access to resources.
Integrity is only provided during boot time. This is where other software solutions needs to be implemented in order to validate the health of the data.
Availability is again considered strong as the segmented memory controllers allow for high availability in both the trusted and untrusted zones.

2.11.4 Topology

Topology may have quite a lot to say when it comes to expansion and scalability. The ability to lay out your network of devices in a meaningful way can make it easier on the individual nodes and the traffic that go through the network. Navarro et al. (2020, p. 15) mention four popular typology's that are used in IoT networking, which are:

- Point to Point (PTP) or Point to Multipoint (PTMP)
  - Connection between two nodes. Can be used in SCADA systems.
  - Connection between one node and many nodes.
- Mesh
  - Each node connect to multiple nodes and can communicate with each other.

- Star or Star to Star
    - Nodes spread out from a central compute unit.
- Tree (Cluster)
    - Multiple linear structures out from a central compute unit.

Example of simple topology's

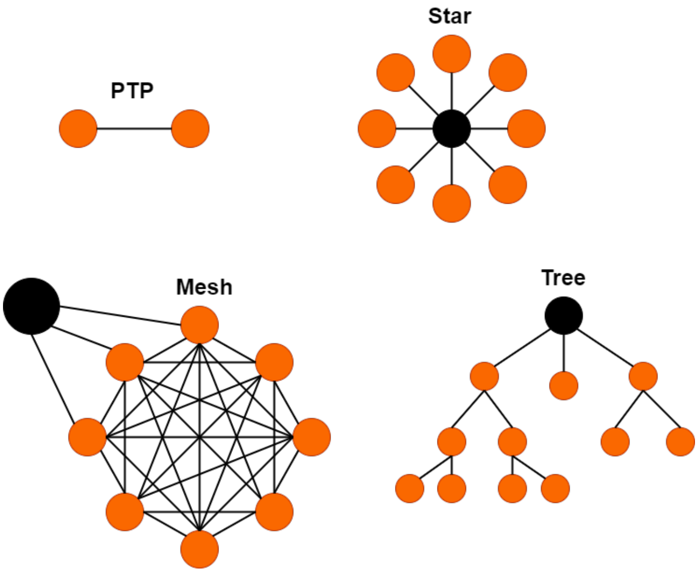


Figure 2.4: Topology of IoT

3 Methodology

In this chapter we will present the used methods for gathering primary data in our thesis. We used qualitative approaches to our research and conducted interviews and simulations In the chapter we also provide explanations for these methods, and justify why these methods are appropriate for our research. We also look at other methods and validate these.

3.1 Research approach

Quantitative and qualitative methods are two of the main methods we can use in research today. Our research will be based on a qualitative approach. Qualitative methods are based on theories of interpretation and human experience. It is a method of processing words rather than numbers. "*By using such methods we can systematically gather, process and analyse material from conversations, observation or written text. The goal is to explore the meaning of a social phenomena, as it is experienced by those who are involved themselves.*" (Hovland et al., 2019).

3.1.1 Justification

The reason for choosing a qualitative method rather than quantitative is because we seek to gather in-depth insights rather than establishing generalized fact about a topic. There has been conducted little research in regards to our topic, which makes in-depth insight more relevant in our case. That is, we want to gain more detailed and comprehensive answers which are achievable to obtain with use qualitative methods. In quantitative methods, such as questionnaires, there are multiple closed questions, where answers are often in fewer details and in the form numbers and statistics. (Streefkerk, 2019).

IIoT can suddenly become a technical and complex subject area for research. When creating a guidelines for trust and scalability in IIoT infrastructure, statistics will be less useful to us. By using qualitative methods can we more easily understand the use and concerns of this technology at a more detailed level. This will then contribute to answer our research questions, as well as establishing the guidelines.

Another reason for choosing the qualitative method over the quantitative is due to the number of respondents. Using quantitative methods requires many respondents which can be difficult to obtain in our case since the expertise for this area is limited. IIoT is a rather new technology and we want to get detailed information from experts in this type of field and will therefore focus on collecting more detailed information from a smaller number of people. (Streefkerk, 2019).

3.1.2 Evaluation

Before deciding to use interviews as our primary source, we also inspected other possibilities for collecting primary data. One of the alternatives was participant observations where we could possibly observe for ourselves how the IIoT is used in the industry sector and the involved activities. In this approach we would self participate in the social processes and activities in the research field. This could have been arranged with our collaborator, Agder energy, where we could agree on times for observations. This would allow us to see how the employees interact with each other and the technology. By this, we could get a better understanding of how they utilise the IIoT and the involved security processes and procedures related to the technology. However, This choice was not prioritised because of restrictions caused by COVID-19 and feedback from Agder Energy.

3.2 Qualitative Interviews

Within the qualitative research approach, we are planning to use interviews as our main method for gathering primary data. The goal is to come to the point where answers start to be similar to what other interview objects have said, According to Jacobsen (2005) there are four stages of qualitative interviews, which are; preparation, conduction, finishing work and analyses of the answers.

3.2.1 Preparation

In the first stage you take into account all the other stages in addition to ethical/moral aspects. As a part of the preparation we need to choose who we are going to interview (the respondents) and how many. For this, we have created the following criteria:

- The respondent must have knowledge about IIoT.
- The respondent must be able to explain about the security aspect of IoT.
- The respondent should have a background in IT.
- We will use the method variation selection. By this, we are capturing different experiences, opinions, arguments, perceptions, perspectives for the interview candidates.
- The amount of interviews should be at least 10. Due to our topic there have been some challenges in acquiring enough interview candidates. It is limited by expertise in our field of research which has led to us having to contact people from several different companies.

3.2.2 Interview type

There are several types of interviews. In our case we are having a semi-structured interview where we have a list of predefined questions with the possibility of follow-up questions that are structured after our topic. We largely use open-ended questions which gives the respondent the opportunity to speak more freely. Having a semi-structured interview will help the interview to become more fluid and perceived more as a conversation. We are planning to have individual interviews, which is a one to one conversation. Group interviews were also considered since it allows us to interview multiple candidates at the same time which can open up interesting discussions. This was rejected as the acquisition of interview objects was quite limited. We also want to conduct informant interviews, meaning, we want to interview people who know a lot about the theme of our thesis. Our research area is relatively new and specific, and we want to talk to experts with much knowledge about this type of technology and the related the security aspect of it. As a summary or answer of this thesis, we will propose a trust framework for scalable IIoT infrastructure. By talking to experts with much knowledge about IIoT and associated security features can provide us with valuable information that can help us to answer our research questions and to establish the framework.

3.2.3 Interview guide

In the preparation phase we also established the interview guide which is a structure for the interview process and questions. Our interview guide can be found in the appendix (A.3). The interview guide is presented in a table consisting of two columns, focus area and questions. The interview guide also consist of a explanation about the rights and consent to the respondent.

3.2.4 Interview format

When it comes to interview format are face-to-face interviews usually the best approach. This approach allows use of body language and it can help to resolve potential misunderstandings along the way. We had originally planned to have physical interviews, but due to COVID-19, physical interviews will be challenging. However, there are many different video communication platforms such as Zoom and Microsoft teams which we will instead make use of. We also need to inform about the interview agreements. This will be done via emails. We will inform the respondent shortly about our project, schedule time for the interview and estimated length of the interview.

3.2.5 Conduction

Before conducting the actual interview, we need to present our project to the respondent, this will also be short mentioned in the emails, but it may be okay with a refreshment. We will introduce them to the project theme / issue and how we will use the material gained from the interview. The data from the interview will be anonymised, which is important to inform the respondent about. This is in order not to disclose personal data that may reveal the interviewee's identity. We also need to mention that the interview will be recorded and deleted after the transcription.

In the interviews we try not to be too attached to the interview guide. This is to be able to create a better flow and a more natural conversation between us and the respondent. Other things we try to do is give positive feedback and ask follow-up questions if relevant, which in many cases will be.

3.2.6 Finishing work

The finishing work should occur short time after the interview is conducted, but since our interviews are recorded this is less of a concern. A large part of the finishing work involves the transcription of the interviews, where we convert speech from audio or video recordings to text. This is a long and time consuming process, which is important to note. Usually the transcript tends to take 2-4 times more time than the interview itself.

3.2.7 Analysis of the answers

In the last stage we analyse the answers or data gathered from the interviews. In order to accomplish this, we need to narrow down the total amount of information and only showcase the information that is most interesting / relevant. Analysing interviews can be a demanding task and there are many different approaches to take in use to make it more manageable. Kvale (1997, p. 123-126) propose five methods on can take in use to analyse interviews, which are the following:

1. Densification
2. Categorisation
3. Narratives
4. Interpretation
5. Ad hoc

For analysing the interviews we will use a mixed approach consisting of densification and categorisation. With use of the densification method, longer sentences are shortened. That is, one shortens the interview text and makes it more concise and precise.

Categorisation is a method where the interview is coded into categories and subcategories. (Kvale, 1997, p. 125). This approach is suitable because through the interview, we go through many different topics which enables the answers to be easier categorised. The categories can either be developed in advance, or occur during the analysis. We have developed the following categories in advance; characteristics, trust, security and scalability. These are not definitive as new categories and subcategories may arise during the analysis. The categories will further be represented in tables or figures.

The reason for a mixed approach is that both results in a good combination where we get to present the data in two different ways. Desification is a more detailed summary of the data and categorisation works as a structured visual representation of the data.

3.3 Simulation

Another alternative was simulation, which also is a qualitative method. This was a suggestion from Agder Energy. Although this was suggested by them, we decided not to take in use this method. From previous work we had no experience with use of simulations. We inspected this further by some online research and concluded that simulations would be too time-consuming and challenging for us to perform with given time and resources.

We encountered several problems that made it challenging to acquire interview candidates. The choice for simulations became more relevant with time and we decided to performed a combination of interviews and simulations. Simulation would serve as a complementary method for the interviews. Due to lack of interview candidates we acquired insufficient data and therefore had to find another solution, which came down to simulation.

Simulation can be defined in many ways and for our specific case it will be used to analyse the topology and resource usage of IoT nodes in a simulated network. By determining the optimal topology's we can deduce some information on how a network should optimally be placed and how that placement can affect your network. This will mostly be a combination of "computer performance modelling" and "manufacturing" as described by Henderson and Nelson (2006, p. 2-3). The definition of the two categories are as follows:

Computer performance modelling: "*From the micro (chip) level to the macro(network) level, computer systems are subject to unpredictable loads and unexpected failures. Stochastic simulation is a key tool for designing and tuning computer systems, including establishing expected response times from a storage device, evaluating protocols for web servers, and testing the execution of real-time control instructions.*" (Henderson and Nelson, 2006, cited by (Jain (1991)), p. 2).

Manufacturing: "*Stochastic simulation has seen extensive use in manufacturing applications. A few representative contributions include evaluation of production scheduling algorithms; work-center design and layout; estimation of cycle time-throughput curves; and evaluation of equipment replacement and maintenance policies.*" (Henderson and Nelson, 2006, p. 3).

3.3.1

Selection of simulation program In our case this blends well together because the Industrial side of IoT uses this technology quite heavily with manufacturing and business processes that depend computer performance. The selection of a simulator was tedious and difficult. There were some alternatives, however many required either payment or an organisational licence. The ultimate choice for simulation came down to convenience and usability, since we do not have the most experience with simulation. Some of the programs were very complex and simply required to much time to efficiently learn and use them. These are the simulators we took a look at:

- NS-3
  A free open source discrete-event network simulator for IoT targeted for research and educational use. This is complex program which looks good. The problem was the complexity to use and the time which we had to learn using it. This program required more time than we had.

- NetSim
  This is a paid program with a free demo, which is designed to simulate Cisco systems' networking and hardware. This was also a little outside the topic and required to learn Cisco IOS commands. This required too much time again and was a little outside the scope.

- Cooja simulator
  This is an free open source network simulator designed specifically for WSN. This

was also a good program with GUI. It had some nice features such as message traffic logs. The program itself could have been good for us, however the learning curve was high for the time we had.

- Atarraya
  This is also a free program for research and educational use, which enables topology control algorithms and protocols for WSN. It's purpose is to test topology controls. It has a simple GUI which made it more accessible for us and easier to learn and utilise. We ultimately decided that Atarraya could be utilised better for our cases.

For our simulation we will utilise a tool called Atarraya which is created by Wightman and Labrador (2009).
This tool is designed to be able to create deployments of nodes both random and with variables. This can include range, area of deployment, sinkholes and other parameters. The simulator is used to "*test a topology control protocol and get statistics like number of active nodes, energy spent, average number of neighbors, etc.*" (Wightman and Labrador, 2009).

Atarraya provides good opportunities for comparing different topologies and creating node networks from small to large scale. The scenarios will be ran with different deployment options from the program. The deployment options are a set of parameters where we must specify the simulation values. However, we only use the parameters that are relevant for the purpose of our simulation. After the deployment options are set and the simulation is created we need to adjust some of the visualisation options to make the simulation display clearer. Lastly we need to adjust some of the topology settings. "*Atarraya can be set to work in either of the following two modes related to topology control: Topology construction only, or All protocols. The first mode is designed to test a specific topology construction algorithm and measure the initial reduced topology that the algorithm produces.* Wightman and Labrador (2009)." This is the use case we will utilise for this paper. These settings are mostly based on how the company uses IoT and on the size of the IoT network.

4 Findings

In this chapter we will present the findings and the results we got from our literature review, interviews and simulation, which are our three main sources of information. This will be the basis for creating the IIoT guideline and to answer our research questions. The primary data sources which are interviews and simulation, will be used to compare with the secondary sources and by that we can form our own suggestions and answers to the research question.

In total, we conducted 11 interviews and came into contact with individuals from several different business areas. These were areas within the tunnel and construction industry, oil, gas and energy, silicon and ice cream producers. We also talked with experts in network and information security. The interviewees were found in different ways. We first talked to Agder Energi about potential interview objects and contacted them. Then, we asked our supervisors if they had any suggestions. We also did some research to find relevant companies and people to reach out to. Most of the interviews were arranged via emails. Here we agreed on time and what video communication platform we should use, since physical interviews were not relevant. The duration of the interviews was very variable. Some lasted 15 minutes, while others lasted up to an hour. We received many interesting and different answers from the companies that contributed to answering the research questions.

After conducting the interviews, we performed analysis. The analysis of the interviews was a long and demanding process and we performed the following steps to analyse the answers:

1. **Transcribed the interviews**

   Transcription of the interviews was a long and time-consuming. For this task we used a transcription tool in Microsoft Word that converted speech into text, which was used on UiA OneDrive, with a service-level agreement (SLA) that protects the data. This function worked to a large extent, but we still had to listen through the interview and do some spelling.

2. **Created categories and subcategories**

   After the transcription we created categories and subcategories with use of Kvale (1997, p. 123-126) method for analysing interview. The categories were based on the responses from the interviews and the research questions.

3. **Created a table**

   The categories were then further structured and placed into a table. The table consists of several major categories with associated subcategories. Each subcategory have small concluding summaries that is based on the responses from all the interviews. The table for analysis is in the appendix.

4. **Interview analysis**

   We then used the table and associated categories to structure a more detailed analysis of the interviews and the main findings. This comes in the next section.

4.1 Findings of interview

In this section we present the interviews with use of a thematic approach. The answers from the interviews were very varied, but could to a large extent contribute to answering our research questions:

- What are the security characteristics of an IIoT infrastructure?
- What is the relationship between trust and scalability in an IIoT infrastructure in the industry sector?

4.1.1 IIoT characteristics

We received good descriptions of characteristics of IIoT infrastructure and associated security.

When it comes to IoT, there are several types of devices and sizes. We made a distinction between small sensors, medium-sized machines such as the Raspberry Pi and larger machines such as servers. The answers from the interviews indicate that sensors are largely used in the industrial sector. This was mainly used for various types of measurements, such as electricity consumption and water metering. It turned out that it was the minority who used larger machine solutions in the form of IoT. No one specialised specifically in the larger solutions. Of those who took advantage of this, they used it combined with other smaller devices. Most of the IoT solutions came from suppliers, but there were also some who mentioned that they had created their own IoT solutions or had plans to do so. Informant 5, 8, 9, 10, 11 mentioned that they only used their own IoT solution in order to have more self-controlled security. They used sensors, switches, temperature sensors and utilise their own security equipment. Most of the equipment is owned and used by the customers themselves. They have some Raspberry Pi's, that are used as NTP servers, UPS with sensors, surveillance cameras, along with customers that use industrial IoT. It is primarily used to gather data and surveillance of the network. They use it for alarms, register changes and environments that they have to surveil.

We could see that IoT was for many a new field, and the usage and needs varied for the different companies. It turned out that most people used IoT to simplify manual processes, but for some it also created new opportunities and work tasks. As mentioned earlier, it was widely used for various types of measurements. The measurement of sensor data was very important in order to be able to optimise production and production planning and reduce various types of costs. This could also help detect new trends. For example Informant 3 and 6 utilised IoT in hydro power production. Here, the IoT was used to measure water levels, precipitation and the type of things used in relation to hydrological calculations. IoT also helped them to measure the water flow in surrounding rivers. Informant 3 used IoT a little more simplistically. The main use of IoT was to be able to measure how much power consumption was in different types of departments.

Informant number 6 said they use communication devices for the purpose of information gathering. They have smart power management systems that is used to measure power, power failure and alarms. It is sent through radio mesh and 2G connectivity. Among other devices are switch controls used in order to break up a network, in case the power goes out for external reasons. Such events could be trees that fall over power lines and lightning. This way they are able to redirect the necessary power from other areas. Another feature to the network is weather stations that measures weather in the environment around. Inside power-stations there are also sensors that measures vitals for that station. By hydroelectric stations they measure and can detect problems such as waste and other problems that can clog the power generation. With this they have enabled a small robot that can remove clogged materials and can be controlled remotely.

IoT was also provided benefits for administration, tracking and surveillance. Informant 1 mentioned they used some IoT for monitoring and to secure communication channels. They also used IoT for administration and tracking of various types of vehicles, equipment as well as users. The users had to take a blood alcohol level check every time they were to use the construction machines established using a Raspberry Pi. Informant 6 also mentioned that IoT was utilised for tracking. For tracking they also used drones to detect damage on infrastructure.

When it comes to the areas of use for IoT in the industry sector, we could see that much of the use-cases of IoT were outdoors. IoT was for example placed in tunnels, forests and hydro stations. The IoT was also used in some factory work and various means of transport such as construction machinery, trucks and cars.

Most companies had some form of security functionality on their devices. We found that the smaller the units, the harder it was to secure. The use of security measures also varied somewhat in the various companies. Some felt that their data were not significant enough to cyber-attacks, which made the need for very strict security less needed. Others, were very aware of having secure devices and communications. This was usually in connection with critical infrastructure. Many of the security measures came from vendors, but this was often combined with self-established measurements. Informant 1's devices were largely secured by Azure's EDGE framework. In addition, certificates and keys for devices were also used. VPN was also used as a security method. Other methods that were mentioned several times were encryption and hashing. Several informants also mention that access control was widely used in the form of passwords and two-factor authentication.

4.1.2 Security policies

There are some different variations of what security policies we see, however many have a combination of security provided by vendor and already established security polices in the company.

There were instances where the companies only used security features from the suppliers. They mentioned that IoT was a new field for them and that they were therefore dependent on security from the IoT providers. Informant 6 said that security policies are provided both from vendor and the company itself. There are clear guidelines that need to be followed. One of the examples provided is that you should not be able to communicate out on the open network. Securing the communication is an important aspect. There are certain specifications and rules towards storing and transmitting data. Access control is also an important security policy.
It is mention that even though someone manages to climb up in a mast and connect physically to a device, one should not be able to connect to the network in any way. Devices should be isolated and network segmentation can enable that. Devices are enabled to be in a zero trust environment. The device may be lost but you can not get in to the network or do something else with it. They have SOC (Security Operations Center) teams that analyse and have emergency responses in case of alarms.

More expensive items and more critical items also needs to be physically secured. It is mentioned that drones may be one of those items that are physically secured away, when they are not in use.

We see that informant 7 also mentioned that much of the security is already in place, however the IoT security is provided by partners. They have their own security routines that were created and established before, which makes it easier to establish the ones needed for expansion. Unusual data can be controlled and have alarms which can detect anomalies.

Meanwhile the informants of interview 5, 8, 9, 10 and 11 create strong security policies of their own. They do provide customers with solutions and have therefore already established strong guidelines themselves. They see "Internet of Things" more as "Intranett of Things" as IoT should not be on the open network. All IIoT devices and network is segmented behind a VLAN (Virtual Local Area Network). Things should not be open to the network unless decided by either the customer or special cases. If they see possible attacks, they close down the ports that the IoT is connected to.
All security routines are provided by them and they do not allow external devices out to the open network. This way the devices cannot communicate outside the network and can only communicate with other devices inside the segmented VLAN.
It is sometimes necessary to provide access to the open internet for customers, so in that case, they guide the customers to provide the best possible solutions and understanding of the risk associated with that. They have 24/7 surveillance with alarms that is used to protect the network. They also have a SOC team to provide support in case of emergencies.
They have strong routines for emergencies, and has among other things, an emergency preparedness team that is activated in case of problems. Outside of that, their general security is that things should not be accessible from the internet. They segment and create their own VLAN so that outsiders does not have the opportunity to go in from the outside. If you need access to the segmented network it needs to be from the operational network with the use of jump servers. The operational network should not "speak" with the office network. Clear separation of boundaries is required.
They create their own network for IoT which is not connected to any office network or any other process network. It is separated and then communicated with on separated layers. Segmentation of network is again very important. Keep a closed loop that doesn't communicate with others. Firewall is used and ports that are not necessary are also closed. They can build their own network and also provide separate networks for customers, such that the devices does not have to access the open internet.
If customers need to go out and communicate with IoT devices it is important to have a VPN tunnel to connect with. Zero trust should be used for the process or industrial network.
Reading documentation and doing research is important to get the security right. They also say they test units in a locked sandbox environment before using the items.

4.1.3 Challenges for IoT infrastructure

We examined some of the challenges that came with using IoT. Many of these came from networks, connections, devices and integration of new devices. We interviewed people from a number of different disciplines, which meant that there were various factors that influenced these challenges. Several of the companies had the same challenges.

Informant 1, 3, 5 and 6 mentioned that one of the main concern came from connectivity and use of network type. Informant 1's devices used only 4G and the IoT was located in areas where there could be limited connectivity. Use of 4G led to both advantages and disadvantages. It was also mentioned that due to this there could be cases where one was not allowed to communicate with certain units over several weeks. Informant 3 and 6 used multiple networks types. The devices ran on 2G, satellite (SAT), Radio (VHF) and Wi-Fi which could lead to some bandwidth limitations. They also mentioned 5G could potentially make it easier to create your own slice of the private telecom network in the future.

Informant 2's challenges revolved around the use of the units. There were cases where people abusing the technology to do something other than what it is suitable for, which was difficult to control. A general challenge around the IoT units was price and what the cost benefit was. How can one defend spending 1 million NOK on new devices, if they do not receive that value back from it? The need to find the cases that give business value. In some cases, there were also problems with making the devices robust enough. The units could be deployed in areas where they could be exposed to bad weather conditions and in a few cases vandalism. IoT could also be difficult for some of the informants to use at all. This was in areas that involved critical infrastructure and where the use of IoT was generally a major risk due to the open internet.

Informant 6 tells us the challenges that they face are; that IoT is another layer that they have to control. For IoT to be secure they need to be able to separate the networks and include extra safety procedures for it to be realistic in use. The problem is that they need separation of networks and some of the challenge is deciding where IoT needs to be. The fact is that the industrial network has to be separated from the administrative network. So they point out that IoT may be somewhere in-between these two networks. It is pointed out that one does not want someone to be able to get in to the administrative network to be able to control IoT solutions. That would be a big problem, which can cause difficulty's and harm. You may not want to place IoT in the (Supervisory Control And Data Acquisition) SCADA network or control network as well, because it may not belong there either. This could lead to an expansion of unsecured devices in a secure environment. IoT may need to come in its own network and layer it away from other networks.

Informant 7 tells us more a history of acquisition of company and partners that help with the specific challenges they have. Many of the challenges initially was solved with partners that specialise in the making of industrial IoT solutions. Another challenge for them is that rapid scalability creates more access points and attack vectors that needs to be considered.

Informant 8, 9, 10, 11 tell us about the challenges of properly structuring a network. The network might be seen as just as important for the IIoT solutions to work. The difficult part is to segment the network properly. It is also a struggle that some customers might enable default passwords and settings which in term harms the customer itself. By opening up the network, you automatically attract outsiders. They tell us that it is difficult to balance IoT as they provide very many good services, however they are difficult to control in a good environment. Another challenge that they face is that some equipment are made so that they require an internet connection out to the open web in order to gather updates, which creates a threat in itself. The damage may have already happened if they open it up to external network. There are cases like the Solarwinds attack where updates have been hijacked and contain malware, which is something that they need to consider. This creates challenges for things that need licences and updates from the open internet. Another point mentioned was the individual sensor security. The lack of security options and limited security that can be implemented on the devices itself. They mention that you need to protect the environment around it instead, which itself can be a challenge. The lack of control for devices on the open internet is also a challenge. You may not always know what a device is sending and receiving.

4.1.4 Scalability and trust

For many, scaling up and establishing trust in IoT infrastructure can be challenging. This came from several different reasons such as; control and management over the devices, use of different devices, use of older devices, network and segmentation. There were also few instances where scaling up IoT infrastructure was a lesser concern. Informant 1 mentioned that they used a framework that made it easy to integrate new devices and scale up IoT infrastructure. However, there were challenges when the number of incoming and outgoing messages increased.

Informant 2 finds it difficult to have control over the units, what they do, what type of unit it is and what values they give. They used large amounts of sensor which then had to be logged and managed in a system. If several different devices from many different suppliers were used, it could also lead to difficulties with updates and management.

Informant 3 and 6 used mixed units. Some were legacy devices that could also make it difficult to integrate newer devices.

Informant 6 provides a thorough explanation on their views of trust, scalability and the general challenges around the topic. The interviewee explains that it is difficult to enable enable zero trust through the entire network, however, where possible it should be implemented. An example mentioned in the interview is if somebody needs to transfer data from an IoT device to an administrative network or out of the IoT network, there should be a zero trust environment. An interesting point mentioned is also that devices that may be accessible by others should not allow a way further in the network. That device alone may be destroyed, however nothing more.
It is further explained that the use of certificates is a solution to secure communication. One can change the basic authentication process with the use of certificates that have limited use and a time limit. This is a solution to the identification process. It is also mentioned that anonymisation of data can also help with sensitive data that needs to be transferred and analysed. Semantics and syntactical information can help reveal problems in data traffic and anomalies in the data that comes in.
Some of the scalability problems that they see are; how and where to connect new devices. The integration process may not be as easy if it is located in a rural area. How do one connect and maintain a secure communication channel? The need to connect and create a secure communication channel from a rural area is a difficult task with many communication standards that may be needed. Some areas do not have internet and then the need for satellite, radio or telecommunication may be used.
Large scalability need the use of scripting in order to enable mass expansion. One cannot just manually implement each device from scratch, so the possibility to enable mass configuration is needed. It then becomes important that tolerances and redundancy is used when scaling in large numbers.

Informant 7 also explained that mapping sensors and creating ID's for them, becomes important to keep control during scaling. Sensors that are damaged or stolen can be removed from the system from software. Expansion and scalability is seen on a necessary base, where they can add items when needed.

Informant 8, 9, 10 and 11 have very strict guidelines however to the whole trust process of IoT. Trust in IoT devices is something you should not have. The network structure provides the trust you need for the devices. In this case they limit communication between networks and create segmented internal network to trust the devices. They explain that zero trust within a company should be used with two factor authentication as a minimum. If it is implemented properly in a company it is more of a case of habit rather than a problem. Users should be required to use authentication when interacting with the network. It is further explained that zero trust may be cumbersome and there needs to be a balance between that. It is stated that in an ideal world we would have it. Two factor should be a requirement for all systems however. On the more critical systems you need it. It is also a consideration on how critical a system is. Segmentation and firewall is an important factor to gain trust in a network. One could consider segmenting the VLAN's in to each specific sensors when scaling a network. Combining this with network controllers could make additions in the network more convenient, as one has to just update the network controller which updates and adds an item. This is an interesting point that could create both a form of control and security at the same time.
Adding items in a network could however be a little bit complicated if there are many segmentation's within the network. They add that if you have done the job of segmenting in to different VLAN's, the work of adding new devices, scaling, and have the controllers needed, the job should not be too difficult. From a command center you could add updates and send out commands.

One could also add units that are there specifically to surveil the conditions and send them back to provide feedback on the network.
A central server that the IoT device connects to and communicates with is a good solution for inter connectivity. A central server that receives and puts out commands behind a firewall.
The chance of losing control in a scalable network is a factor one needs to consider when expanding. By adding a lot of units, you may not have as good of an overview. An interesting point mentioned is that if a thousand units are on the internet, one may loose control pretty quickly. It may be difficult sometimes to include new devices into a network as sometimes one has to include a device and open it up and make it vulnerable in the time period when you deploy a new unit. The more units the more you may expose the network, with more access points. Margins for bad configuration may increase. Therefore by segmenting it to its own network and not allowing outside traffic, one can reduce the number of attack vectors.

4.2 Findings of literature

A major part of any methodology is to have a literature review and a synthesis of data. As for this paper we have provided both a literature review and a synthesis of our interviews (the data). The synthesis of simulation will be the next section and will contain the data we found from that part. However, in this section we will look at the answers from our literature.

4.2.1 Gaps in the literature

In this part we will go through the gaps in literature. The process of finding specific literature on the topics of scalability and trust was time consuming and there were only a few results, which lead us to the topics which are missing in research papers. The main ones we identified are:

- Few standards and best practices.
- Almost none of the literature's focuses on the relation between trust and scalability in IIoT infrastructure.
- Big picture missing. Found models/literature is quite specified towards one particularly element.

4.2.1.1 Standards and best practices

There are of course standards and best practices for the field of IoT and IIoT, however there are very few that we could identify that resolves the problem of trust and scalability. The two main standards we came over were the The Data Distribution Service (DDS) foundation and IEEE's standard on respectively connectivity standard and OpenFog reference architecture for fog computing. This creates a problem where there are not many easily accessible standards that one can refer to or look for when creating and IIoT network.
It is difficult to start somewhere when one do not have some sort of reference to start with. We also acknowledge the good that come out of standards and best practices. This is something we can see in the general ICT industry where the uprising of web development created a more consent driven data management with the GDPR and the more secure environment that resulted from the focus of web vulnerabilities. This came from more secure protocols and standards that resulted in a more secure internet.
The hope is that by highlighting the problem, we address and bring light to the problem.

4.2.1.2 Little focus on relationship of trust and scalability

This master thesis focuses on the problem of utilising trust and scalability together. The problem then becomes how to address and present this, since this is one of the gaps we could identify. Many of the research papers that we read do in some form or another present some ideas or concepts of trust OR scalability. If they present concept of these topics they are separate and may not contain much information about the topic at all. We therefore have adapted to read about the individual topics and try to deduce the best concept out from that. Even though we try to extract the most out of the individual topics, there are few papers that represent these two topics. The fact that we want to achieve trust in a scalable network is going to be a challenge.

4.2.1.3 Big picture missing

The literature present is understandably focusing on individual parts of a larger picture, however we miss the fact that there is little high level overviews over the subject that take into account the larger picture of IIoT. There are models and literature present that describe components of the problems, nonetheless are quite specific to a particular element of a topic. In order to create and introduce a framework, we would like more high level or big overview over an IIoT network, which can provide an understanding of what a network should look like. That is why we introduce this in this thesis.

4.3 Findings of simulation

After analysing the interviews we started the process of simulation. The answers from the interviews were quite varied and we therefore thought of a scenario based approach for the simulation part. We concluded that it is difficult to choose one specific structure that covers all needs for the various companies. This was because the companies varied in size and need for strict security measures. For the simulation, we have created three different fictional scenarios. One for small IoT infrastructure, one for medium sized and one for large IoT Infrastructure.

To set the boundaries of the simulation we used these settings:

- Deployment Options:
  - Nodes: Sets the total amount of nodes for the simulation.
  - Comm Radius(r_{comm}): Sets the transmission radius of range.
  - Sensing Radius: Sets the sensing radius of range.
  - Deployment Visibility Area: Sets the size of deployment area.
  - Node Location Distribution: Sets the size and grid for the deployment location distribution.
    - Uniform: Spread in a square area of (height) h and (width) w where it is centered in position (x, y).
    - Grid H-V-D: Distributes nodes in the distance area with a distance of $r_{comm} \times \sqrt{2}$ between nodes, so nodes are adjacent with their vertical, horizontal and diagonal neighbors. (Wightman and Labrador, 2009)
- Visualisation Options:
  - Atarraya: Creates a view of nodes.
  - Active Nodes: Active nodes are highlighted.
- Topology control:
  - TC (Topology Construction): Sets the topology algorithm for the simulation.
  - TM (Topology Maintenance): Sets the maintenance mode used for monitoring an area. Set to "none" in our cases.

4.3.1 Topologies included in Atarraya

In order to understand the simulations we need to explain what the different topologies do since this is the core aspect of Atarraya. We will use these topology algorithms to explain the possibilities for scalability and coverage of an wireless sensor network (WSN). We use these topology algorithms to look at different scenarios and try to understand what difference they make.

A3:
In the A3 algorithm all nodes besides the starting node is set to an *Unvisited* state. The starting node is set in *Active Candidate* state which then sends a HELLO message to its neighbors. The node who start sending out this message is also known as the sink node. This node also has a timer for receiving replies from the *Unvisited* neighbor

nodes. "*The neighbors sends back a PARENT RECOGNITION message that includes their ID as well as data regarding the ratio of remaining energy and the ratio of distance over the maximum transmission range.*"Wightman R. and Labrador (2010) In addition, they change their state to Child and recognise the sender as parent. After some time, the *Active Candidate* stops listening for messages and sorts the recognised "children" nodes in a list in decreasing order. If the *Active Candidate* receives one answer, the state will be changed to *Active*. If it does not receive a response, the state will be changed to *Sleeping* and will be turned off at a specific time. Children nodes recognises their position in the list and wait for their turn. If the timer expires and the node has not received a SLEEPING message, the node will send a sleeping message and change its state to *Active Candidate* and start the process from the beginning. (Wightman R. and Labrador, 2010).

The A3 tree algorithm is a rather simple and energy efficient topology as it turn off all redundant nodes in the network. Nodes can also be set in a low energy consumption mode or sleep mode when not needed which enables the node to save more energy. Less amount of active nodes leads to fewer messages to transport in the network. This can then lead to reduced latency and the possibility of collision. Wightman R. and Labrador (2010). Another advantage of this is that they can help reduce implementation costs. (Alexandru and Valentin, 2013).

The downside with this algorithm is that it sometimes can be less reliable when there are few nodes involved. It provides proper connectivity, but the coverage can be limited.

A3 Coverage:
A3 Coverage or A3Cov is quite similar to the A3 algorithm. The topology makes no change in the computational complexity. However, A3Cov guarantees better coverage ratio than the A3 algorithm, but it is also using a higher number of Active nodes. This is due to a new variable in the nodes called *Sensing Covered* that A3Cov introduces. This occurs when nodes have not received any PARENT RECOGNITION messages, meaning that the nodes does not depend on communication. Such nodes are used to extend the network's sensing coverage. (Wightman R. and Labrador, 2010).

CDS Rule K:
This algorithm uses the a pruning rule. You start from a large set of nodes that produces a minimum criteria and prune it according to a rule. The nodes will start by interchanging databases. A node will remain if there is one pair of separated neighbors. After all this the nodes will unmark themselves if they determine that all the neighbors are covered by marked nodes with "high presidency", which in turn is given by the degree of the node in the tree. A lower level in the tree is higher presidency. The final tree is another version of the initial with all the redundant nodes with higher or equal priority removed. Pachnanda and Chaudhary (2013). Discard all nodes whose neighbors are covered by other active nodes with higher priority. (priority pre-assigned).

Just Tree:
This algorithm makes one sink node responsible for message broadcast. The sink nodes are sending and receiving messages from neighbor sensor nodes. The messages or events in the network are propagated in the network with the concept of parent and child nodes, where the parent initiates the message and the transfer to other sensing nodes that act as a child. This algorithm ensures that the deployment area will increase if needed or stay constant. It makes it flexible for either a constant or flexible deployment area. (Gupta and Gupta, 2015)

KNEIGH-Tree:
This algorithm starts with the sink node transmitting a HELLO message to all the neigh-

bors at its highest power. This message has the ID number and the tree level contained in the message. The first node to accept the message stores the ID of the transmitted node and the tree level, which in turn calculates the distance with the node transmitting and sets its state to stay. After accepting the message the first time, a node transmits a new HELLO message to its neighbors and starts a timer, to listen to other neighbor messages. The sender of the first message will sort the list of neighbors and say that they are the closest neighbor. The sender then reduces its power to reach to the k^{th} neighbor, hence its name. The algorithm assumes that the nodes have no knowledge of their locations. Labrador and Wightman (2009, cited by (Gupta and Gupta (2015))). The positives of this network is that it follows a growing tree mode, that starts at a determined node (the sink node), and progresses sequentially. This provides a good way to guarantee connectivity to the network. When every node can reach at least one node in a lower level in the tree, the network can guarantee that every node will have a way to the sink. (Wightman R. and Labrador, 2010).

4.3.2 Assumptions of simulation

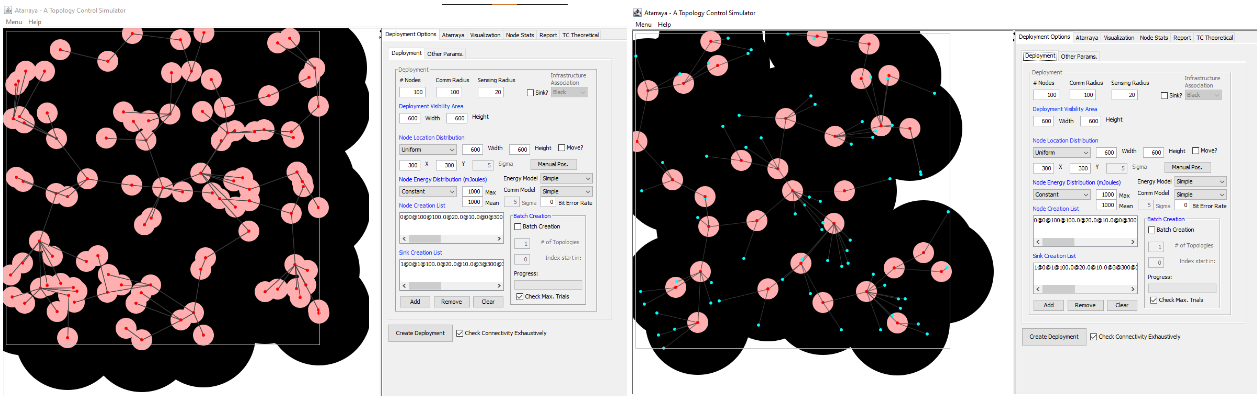
The performed simulations are done in a two dimensional plane which does not take into account the height differences of the sensing and coverage of the nodes in height. This is a limitation of the program which we cannot do anything about for now.
We opted to not include data loss or packet loss in this simulation as we would like to see the optimal conditions for the scenarios created. Packet loss is very network dependant and we do not have the ability to simulate network connection type in this simulation. It therefore would not make any realistic difference to the simulation.
The sensors are considered with perfect sensing coverage disk since this is created in a two dimensional plane.
All distances are used in metric scale.
The sink node is assumed to be powered from an external source of energy.

4.3.3 Scenario 1 - Small IoT infrastructure

Scenario 1 concerns an industrial start-up company. They have newly invested in IoT and are planing to create a small IoT network consisting of 100 devices. They will test the capabilities of IoT and how the technology can be utilised in their work processes. The company's IoT is in the form of GPS sensors that are used to keep track of tools on a construction site. The distance between each device in the network will be relatively short and the need for long range is less important. The units will be run in a test environment and the need for solid security is less relevant to them. Security functionality is thus handled by their vendor. The table below shows the different settings used to simulate scenario one.

Parameters	**Simulation values**
Number of nodes	100
Communication radius	100
Sensing radius	20
Deployment area	Uniform distribution within 300 x 300 m
Node energy distribution	Constant 1000 mJ
TC protocol	Just Tree and A3
Performance metrics	Area covered

They want to compare topologies optimal for their company and has decided to try out Just Tree and A3. They try these two algorithms as they see they fit on their small network. From figure 4.1 we can see that the *Just Tree* topology clearly has the better coverage and can utilise a larger area. This can cut on the use of power, which in case of GPS would have an internal battery. The company have to review the positives of longer battery life to sacrifice some range. By turning off unnecessary nodes which is seen as the blue dots in the figure, one can save quite some money by not having to replace battery as much as one might do with the *A3Cov* method. Since *Just Tree* is suited for scalability, it could be a solution for a future network, however as the current situation is, the *Just Tree* topology seem to make most sense here. *Just Tree* has a good coverage area and low power consumption which makes it a good choice for this situation.



Deployment

Nodes: 100 | Comm Radius: 100 | Sensing Radius: 20 | □ Sink? | Infrastructure Association: Black

Deployment Visibility Area: 600 Width, 600 Height

Node Location Distribution: Uniform, 600 Width, 600 Height, □ Move?

300 X, 300 Y, 5 Sigma

Node Energy Distribution (mJoules): Constant, 1000 Max, 1000 Mean, 5 Sigma

Energy Model: Simple

Comm Model: Simple

0 Bit Error Rate

Node Creation List: 0@0@100@100.0@20.0@10.0@0@300

Sink Creation List: 1@0@1@100.0@20.0@10.0@3@300@3

Batch Creation: □ Batch Creation, 1 # of Topologies, 0 Index start in:, Progress:, ☑ Check Max. Trials

☑ Check Connectivity Exhaustively

(a) Just Tree topology

(b) A3 topology

Figure 4.1: Coverage of Just Tree VS A3

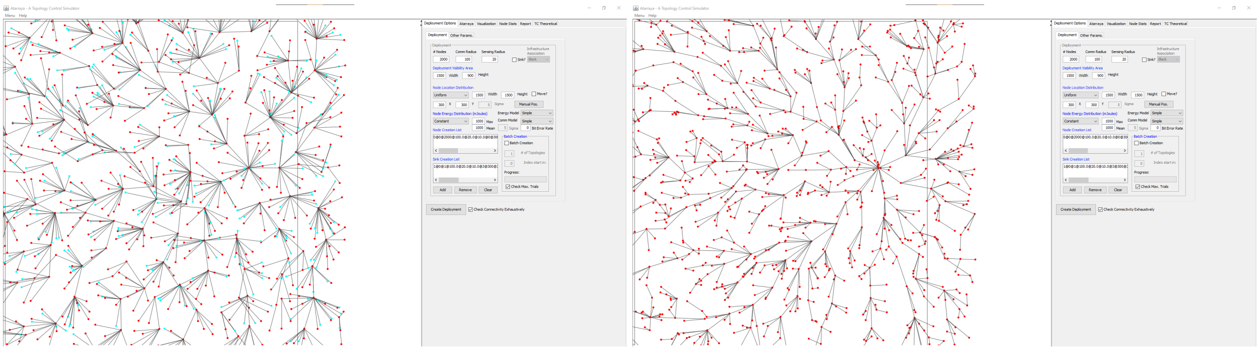
4.3.4 Scenario 2 - Medium IoT infrastructure

The second scenario involves a larger company. They use railroad and sensors to maintain location, conditions and switches for rail connections around the railroad. They have a relative straight railroads and most of their devices are located along the tracks. It is therefore important for them to look at the coverage of a grid like system. They then decide to simulate the topologies and see what gives them coverage over their respective lines. They need to have good coverage because of tunnels and varying terrain.

Parameters	**Simulation values**
Number of nodes	~2000
Communication radius	100
Sensing radius	20
Deployment area	Uniform 1500 x 1500m & GRID H-V-D 3000 x 3000 m central node within 300 x 300 m
Node energy distribution	Constant 1000 mJ
TC protocol	A3 Coverage, KNEIGH-Tree
Performance metrics	Covered areas in grid formation

When conducting the medium scenario we saw that not everybody may have their IoT devices in a random distribution. The railroad company requires more of a grid like function for their operation, such as a railway. This is the reason we included both a set of random order node placement and a more fixed order with a grid view.

We see from the topology of *A3 Coverage*(A3Cov) that it has a good coverage over the area that is 1500 x 1500 meters. The same can be said for *KNEIGH-Tree*. However the difference comes in how the topology branches out like seen i figure 4.2. The *KNEIGH-Tree* is seen branching out more from a single point where all paths lead down to the central node. *A3Cov* does have some branching features, however it divides it more in to chunks which creates more localised "hot-zones". Both methods seem to work well for a random pattern node distribution. When the option for coverage was turned on, both topologies covered the entire area they were assigned to.



Deployment
Nodes 2000
Comm Radius 100
Sensing Radius 20
□ Sink?
Infrastructure Association Black

Deployment Visibility Area
1500 Width 900 Height

Node Location Distribution
Uniform 1500 Width 1500 Height □ Move?
300 X 300 Y 5 Sigma

Node Energy Distribution (mJoules)
Constant 1000 Max 1000 Mean
Energy Model Simple
Comm Model Simple
5 Sigma 0 Bit Error Rate

Node Creation List
0@0@2000@100.0@20.0@10.0@0@30

Sink Creation List
1@0@1@100.0@20.0@10.0@3@300@

Batch Creation
□ Batch Creation
1 # of Topologies
0 Index start in:
Progress:
☑ Check Max. Trials

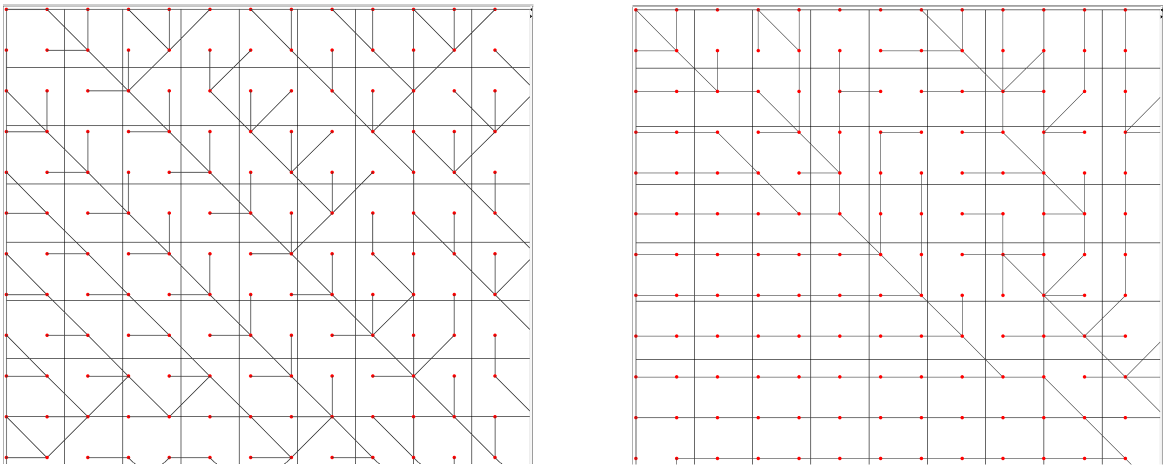
☑ Check Connectivity Exhaustively

(a) A3 Coverage

(b) KNEIGH-Tree

Figure 4.2: Simulation of random uniform deployment KNEIGH vs A3Cov

The grid pattern is included as it looks more like a railway and it would show a more "accurate" picture of how the actual implementation along a rail network would look like. When we look at the grid formation in figure 4.3, we see a different approach to the pattern. In the grid picture you only see the active gateways that are established. The reason this is brought up is because if we turn on the setting "show all gateways", we see that the *KNEIGH-Tree* has more gateways and all their nodes are connected in a square pattern, while *A3Cov* has all its gateways already in the picture. That means that the *KNEIGH-Tree* has only used the necessary gateways in the picture and has more possibilities to transform the grid. In this case it might be a better solution to use the *KNEIGH-Tree*. These two pictures can show us that topology plays an important role, when deciding on layout and possibility for scalability.



(a) A3 Coverage Grid

(b) KNEIGH-Tree Grid

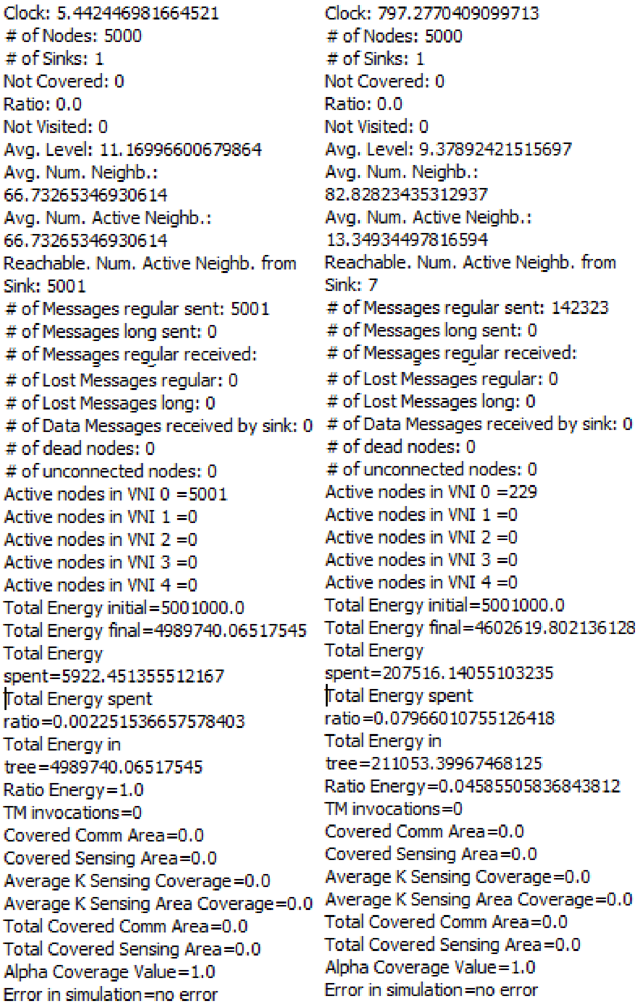
Figure 4.3: Zoomed in view of Grid H-V-D deployment KNEIGH vs A3Cov

4.3.5 Scenario 3 - Large IoT infrastructure

The third scenario is about a power generation company that largely uses IoT for several of their processes. The area where IoT is most used is in private homes where they supply and install electricity meters. In total, close to 5,000 units or sensors have been installed. These are randomly distributed in a rather large area. The devices are installed in a WSN that is constantly expanding and the need for good scalability combined with long range is important. Another major feature to consider is that the devices have proper connectivity. Customers can see their own power consumption and it is therefore important that they can trust that the electricity meter shows the correct consumption.

Parameters	**Simulation values**
Number of nodes	~5000
Communication radius	100
Sensing radius	20
Deployment area	1500 x 1500 m with central 1500 x 1500
Node energy distribution	Constant 1000 mJ
TC protocol	KNEIGH-Tree and CDS-Rule-K
Performance metrics	Area covered

The power generation company is looking for a suitable topology for their mentioned requirements. Their network revolved around measuring power consumption for customers over a large area and and is dependent on good scalability and range capabilities. For this we tested out two different topologies, KNEIGH-Tree and CDS-Rule-K. Again, we use the KNIEGH-Tree algorithm. The reason is that it had good results in several areas. In this scenario we found that KNEIGH-tree can guarantee connectivity to networks, meaning that customers can have more stable access to their current measurements. KNEIGH-Tree also has a low energy consumption and a fast simulation time. The total amount of energy spent was 5922 mJ and the simulation time was 5.4 seconds. The result of The CDS-Rule-K algorithm shows that there are a large amount of inactive nodes (the blue dots). This lead to a lower sensing coverage and higher energy consumption compared to the KNEIGH-Tree. The total amount of energy spent with this topology was 207516 mJ. The simulation time was also extremely long and took almost 800 seconds to complete. CDS-Rule-K gives poor values to a network of this size and desired functionality.



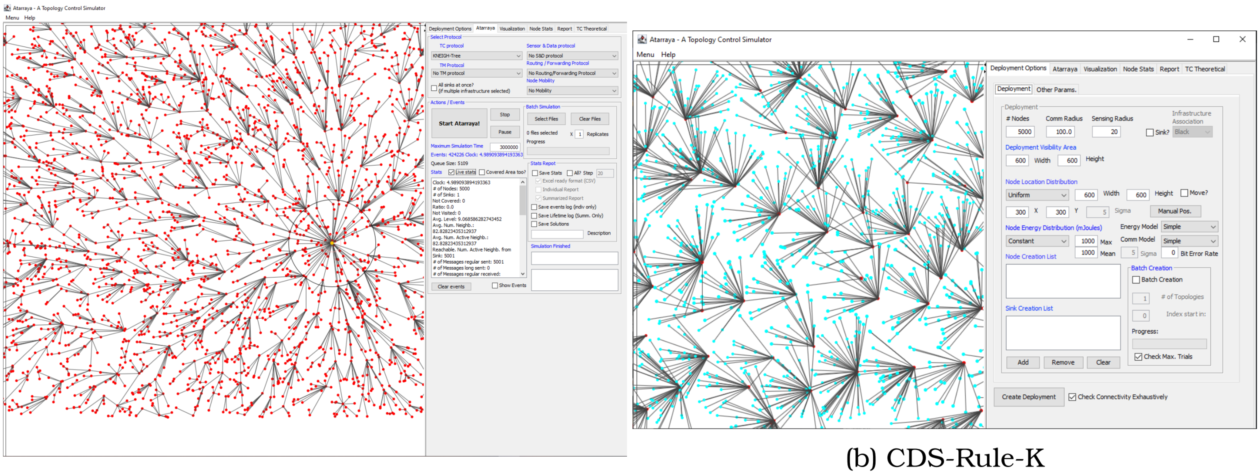
```
Clock: 5.442446981664521
# of Nodes: 5000
# of Sinks: 1
Not Covered: 0
Ratio: 0.0
Not Visited: 0
Avg. Level: 11.16996600679864
Avg. Num. Neighb.:
66.73265346930614
Avg. Num. Active Neighb.:
66.73265346930614
Reachable. Num. Active Neighb. from
Sink: 5001
# of Messages regular sent: 5001
# of Messages long sent: 0
# of Messages regular received:
# of Lost Messages regular: 0
# of Lost Messages long: 0
# of Data Messages received by sink: 0
# of dead nodes: 0
# of unconnected nodes: 0
Active nodes in VNI 0 =5001
Active nodes in VNI 1 =0
Active nodes in VNI 2 =0
Active nodes in VNI 3 =0
Active nodes in VNI 4 =0
Total Energy initial=5001000.0
Total Energy final=4989740.06517545
Total Energy
spent=5922.451355512167
Total Energy spent
ratio=0.002251536657578403
Total Energy in
tree=4989740.06517545
Ratio Energy=1.0
TM invocations=0
Covered Comm Area=0.0
Covered Sensing Area=0.0
Average K Sensing Coverage=0.0
Average K Sensing Area Coverage=0.0
Total Covered Comm Area=0.0
Total Covered Sensing Area=0.0
Alpha Coverage Value=1.0
Error in simulation=no error
```

(a) KNEIGH-Tree stats

```
Clock: 797.2770409099713
# of Nodes: 5000
# of Sinks: 1
Not Covered: 0
Ratio: 0.0
Not Visited: 0
Avg. Level: 9.37892421515697
Avg. Num. Neighb.:
82.82823435312937
Avg. Num. Active Neighb.:
13.34934497816594
Reachable. Num. Active Neighb. from
Sink: 7
# of Messages regular sent: 142323
# of Messages long sent: 0
# of Messages regular received:
# of Lost Messages regular: 0
# of Lost Messages long: 0
# of Data Messages received by sink: 0
# of dead nodes: 0
# of unconnected nodes: 0
Active nodes in VNI 0 =229
Active nodes in VNI 1 =0
Active nodes in VNI 2 =0
Active nodes in VNI 3 =0
Active nodes in VNI 4 =0
Total Energy initial=5001000.0
Total Energy final=4602619.802136128
Total Energy
spent=207516.14055103235
Total Energy spent
ratio=0.07966010755126418
Total Energy in
tree=211053.39967468125
Ratio Energy=0.04585505836843812
TM invocations=0
Covered Comm Area=0.0
Covered Sensing Area=0.0
Average K Sensing Coverage=0.0
Average K Sensing Area Coverage=0.0
Total Covered Comm Area=0.0
Total Covered Sensing Area=0.0
Alpha Coverage Value=1.0
Error in simulation=no error
```

(b) CDS-Rule-K stats

Figure 4.4: Statistics between KNEIGH-Tree and CDS-Rule-K



(b) CDS-Rule-K

(a) KNEIGH-Tree

Figure 4.5: Simulation of random uniform deployment KNEIGH-Tree vs CDS-Rule-K

5 Synthesis of findings

In this chapter we will combine all the different findings that comes from our different data gathering methods. We have findings from literature, interviews and simulation. However when we look at the data we see the interviews and the literature as the main data and the simulation as a support tool to enable a better understanding of them.

5.1 Synthesis

Some of the major findings in the literature review was that there are little to no focus or research on the topic of relationship between trust and scalability. So during the interviews we had some specific question to address both scalability and trust as seen in the interview guide in table A.3. In the literature we can see some of the papers such as Pinto et al. (2017), Xu et al. (2020) and Liu et al. (2019) give security solutions to enable the trust in individual nodes in a network, however the answers we got from the interviews give other solutions to the problem. We receive a much broader explanation of trust in nodes. Informant 6, 8, 9, 10, 11 mentioned that they focus more on segmenting the network in order to create trust among nodes. So they shift their focus from individual node protection to a network solution that protects all nodes. This is an interesting shift in what we see from literature to the real world. From what we heard in the interviews, they still have protection on the individual devices, that comes from vendor, however there are not any specialised solutions like we see on the network level.

For the simulation part of this we had to look at the specific algorithms used in order to determine the trust in the nodes. The reason for this is because the simulation itself does not have a specific measurement of trust. We therefore decided to look at the topology algorithms in order to understand how they work in the network. From the topology algorithms we do not see any significant solution that help with trust in the network, however they play a more important role in the scalability.

Scalability is another important factor that we have studied. When we conducted the literature review, we found again that they focus heavily on specific technologies. We can see e.g. that Sanchez-Iborra and Cano (2016), Meng et al. (2017) and Cheng et al. (2018) focus on the scalable technology and not so much on the topic around establishing the scalability through distribution and the management around it. Through the interviews, we see that the real world could have different problems when scaling a network. Informant 3 and 6 tells us that they have some legacy systems that make it difficult to scale their existing network. In this case, they may have to upgrade their legacy systems or create a whole new sub-system that works along the legacy in order to scale. This creates an interesting dynamic where literature proposes new exciting technology and standards, where the real world has the difficult task of solving existing legacy problems that may come with an expanding network. Informant 8, 9, 10 and 11 seem to have good solution again for scaling their systems as they utilise the segmentation of network to scale their systems. The process of grouping devices into their own VLAN seem to work well. This can also make it easier to navigate the devices they have, as they have grouped different devices into their own specific VLAN.

For the simulation of scalability we again rely on the different topology algorithms to see what works well with different scenarios. From the simulation we see that the *KNEIGH-*

Tree algorithm works well for medium and large networks and that it scales well on both time and efficiency. The *Just Tree* algorithm could however be a good choice for small expanding networks, as it works well with constant and expanding networks. So by deploying either of the two with segmented networks, one could see good coverage and scalable network. This is however a general statement and needs to be considered on the needs of the users.
Scalability was mentioned with the help of 5G by informant 6. It is reported that 5G can help much with both bandwidth and scalability options in the future. Along with the more secure communication standard, it was mentioned that it can be sliced up in to different sub nets outside of the public bandwidth. They can purchase their own slice of the secure 5G bandwidth so that it is separated from normal everyday 5G that cellphone customers use. This is also a concept that Cheng et al. (2018) takes up in the literature. With more reliable and low latency communication, it could allow for a better opportunity to add IIoT devices outside and span long distances.

Security characteristics of IoT is also a question that is presented in our thesis, as this plays a somewhat important role of IIoT. From the literature there are some security protocols and principles that are brought up. They are often on the hardware and software level and secures the devices themselves. We see from the interviews that they are good at implementing security features to their devices. Informant 1, 3 and 6 reports that they use e.g. certificates and key pair values assigned to their devices, which makes identification and secure communication possible. If an unauthorised person where to try an connect, they would not be able to as only identified devices are allowed to connect. The certificates and keys are established and distributed by the administrators. This is a case of device security. Another way is to segment the network as mentioned earlier. The segmented network is in a VLAN separated by logic and makes it not possible to access from the outside without either a VPN/tunnel or with jump server.
The use of hashing and encryption was also mentioned as good practises to keep the data in transfer from being read by others. Along with strict access control such as zero trust and two step verification on users accessing the network. This creates a strong separation of networks and access control that will severely limit the possibilities for unknowns to connect or access.

Some of the answers on security routines were vague. We are not sure if that is because they did not want to reveal them or because they did not know. Even though some were vague, we had the impression that they had some form of security routines either from vendors or self-made. Other were very open about their routines and described very strong routines for preparedness, response and handling.

Zero trust is a concept we have looked into when conducting the interviews and literature. In the literature it was difficult to find any relevant information on the topic. On the other hand we found an interesting concept on the software side of devices that correlates quite well with the real world concept of zero trust. Both Zhang et al. (2019) and Pinto et al. (2017) conducted research into the TrustZone concept which is introduces by the ARM group. This is the software solution to devices where memory is separated in safe and trusted zones. We see that zero trust is something the interviewees agree is a good idea. With zero trust users and devices have to authenticate themselves every time, in order to execute something. The downside for the interviewees is that it might not be achievable for practical reasons, although they agree that it should be on safety critical systems. The concept of separation of zones to create trust is a concept that serves well to increase the overall protection, both for the devices and the network.

We also introduce the question of topology to the interviews and asked if a central node or node to node communication should be utilised in a network. All agreed and used some form of central communication hub to manage communication. This is a little bit different from the literature. They introduce concepts of fog computing as seen by Yi et al. (2015). Fog computing is introduces briefly in this thesis at is might be an interesting solution to communication and workload overhead that may be produced by a single point. The simulation however confirmed the same as the interviewees, that central nodes or a sink node is mostly utilised to gather and communicate. Many of the protocols in the simulation have some from of tree structure, which creates a central communication hub for the data to aggregate. Even though the most common structure of the interviewees is a central command center, it is important to highlight the possibilities that fog computing or other forms of topology can create.

A point to mention about security is disaster recovery planning. From the interviews it seemed very loosely answered. The different companies did not seem to have a clear answer about the security routines their organisations had. For the most part there were some plans and some had full on 24/7 security teams with emergency planning in place. However it did not seem like everybody had it. This could be because they did not think about it at the time of the question, but it is worth mentioning. Another point to mention is not everybody had implemented IIoT in to production and did only have sandbox environments and were still in a planning phase.

5.2 MATNAS Guideline for trust and scalability in IIoT infrastructure

After synthesising the findings we had sufficient information to form guidelines for general IIoT security. The guidelines also covers the trust and scalability aspect of an IIoT infrastructure. It proposes measures for scaling IIoT networks effectively and at the same time create trust in the IIoT devices.

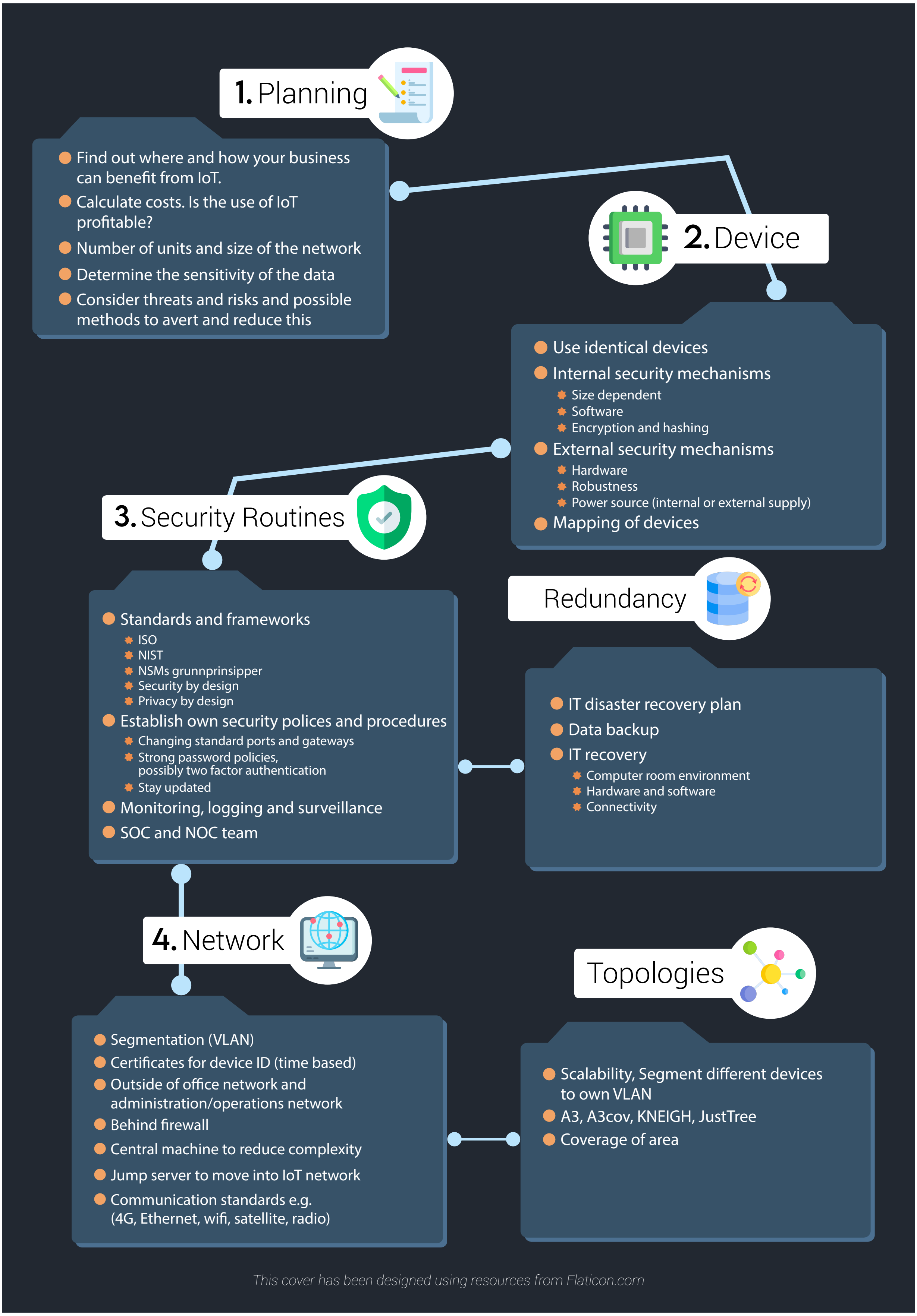
The guidelines are largely based on the findings from literature review and the qualitative methods, but we have also conducted additional research on related security methods. This guideline is in turn a result of the research questions.

The guideline "MATNAS" (Mathias & Jonas combined) is a fictional name we made up, to create a name for our guideline.

The guideline consist of the following four steps;

1. Planning
2. Device
3. Security Routines
    (a) Redundancy
4. Network
    (a) Topologies

This is shown in more details in figure 5.1.



1. Planning

- Find out where and how your business can benefit from IoT.
- Calculate costs. Is the use of IoT profitable?
- Number of units and size of the network
- Determine the sensitivity of the data
- Consider threats and risks and possible methods to avert and reduce this

2. Device

- Use identical devices
- Internal security mechanisms
  - Size dependent
  - Software
  - Encryption and hashing
- External security mechanisms
  - Hardware
  - Robustness
  - Power source (internal or external supply)
- Mapping of devices

3. Security Routines

- Standards and frameworks
  - ISO
  - NIST
  - NSMs grunnprinsipper
  - Security by design
  - Privacy by design
- Establish own security polices and procedures
  - Changing standard ports and gateways
  - Strong password policies, possibly two factor authentication
  - Stay updated
- Monitoring, logging and surveillance
- SOC and NOC team

Redundancy

- IT disaster recovery plan
- Data backup
- IT recovery
  - Computer room environment
  - Hardware and software
  - Connectivity

4. Network

- Segmentation (VLAN)
- Certificates for device ID (time based)
- Outside of office network and administration/operations network
- Behind firewall
- Central machine to reduce complexity
- Jump server to move into IoT network
- Communication standards e.g. (4G, Ethernet, wifi, satellite, radio)

Topologies

- Scalability, Segment different devices to own VLAN
- A3, A3cov, KNEIGH, JustTree
- Coverage of area

This cover has been designed using resources from Flaticon.com

Figure 5.1: MATNAS Guideline

5.2.1 Step 1: Planning

The first and most important step when establishing IoT infrastructure is having thoughtful planning. The use of IoT is a modern solution that we today see being used in a number of industrial areas. The technology has many different uses and it is important to find out how your business can benefit from it as well as how to secure the use of it. One must also calculate costs and find out how profitable the use of IoT is. The units should be of good quality and the price is reasonable. The price of the units is increasing with the quality. Before purchasing units, one should think about where the units should be located and possible threats they are exposed to. IoT is often located in outdoor areas where weather conditions can be a challenging factor. In such cases, you may want to spend a little extra money to get more robust units.

Once you have figured out what and where to use the IoT for, you should also limit the number of devices and the characteristics and size of the network. What kind of network topology is most suitable? What kind of connection should the devices be run on? For devices that are deployed in outdoor areas, one can, for example, consider 4G or radio connection.

Data collection is very central to the IoT and data is a central part of the digital economy. When investing in IoT, one should also take a position on who owns the data? If you buy IoT solutions, there may be cases where the supplier has access to the data. Policies for the ownership of the data should therefore be created. What does the company own? and what is being shared? What can the different parties use the data for?

One must also determine the sensitivity of the data and make adjustments based on this. IoT related systems should be designed based on the type of data they are to handle. In critical systems that handle sensitive information, extra strict security requirements must be set. Examples of this type of information can be sensitive information such private or personal. It can also be classified information.

One of the most important aspects of planning is safety and security. The use of such devices, especially with internet access, opens up several vulnerabilities that the company must address. The company should consider the threats and risks for the use of IoT and how to address these. This can, for example, be done with risk-and vulnerability analysis (ROS analysis). This is a method that helps to map the probability and consequences of adverse events. These can be, for example, data breaches, power outages and vandalism. When using ROS analysis, the various vulnerabilities are prioritised and different types of measures are planned to reduce or prevent the consequences if the vulnerability first arises. ROS analysis can be used to assess new technology, but also for technology that is already in use. It is also used to comply with various laws and regulations that set requirements for risk analysis. When performing ROS analysis, the following points are analysed;

- List the causes of the events. New and external measures for the causes are then described.
- How often can the incident occur? If measurements have been made, enter the frequency
- Describe the consequences of the unwanted incidents and define the various impact areas, such as IT systems, personnel and customers.
- Damage mitigation measures. New or already existing measures are described.

- Risk analysis based on assessment of probability and consequence.
- Suggest risk-reducing measures and priorities.

(Brudvik, 2010)

5.2.2 Step 2: Device

When most of the planning is completed one should explore in more detail different types of IoT devices and related security measures.

A key point from the interviews was that using identical devices could save both time and effort, as well as addressing some of the security concerns. If you want an IoT network that consists of many different devices from different vendors with different polices, a lot more work is required. With a wireless sensor network consisting of identical devices, you can in many cases use same patches and updates on all devices. This makes the devices easier to handle and manage. Outdated devices and systems open up vulnerabilities that can make it easier for unauthorised persons to gain access.

Another important aspect to cover is the internal and external security mechanisms for the IoT devices. A dilemma with IoT is that the implementation of security functionality becomes more demanding the smaller the devices are. This should also be considered in the planning. One should be careful with what data is collected and transmitted. The less secure devices should preferably not have sensitive data involved, especially if they have open network connection.

From the interviews we found out that some companies used self-produced units or had plans to do so. IoT components are manufactured in several different parts of the world. These are usually specially designed for specific applications which make safety stands vary. Security functionality is to a greater extent determined by the supplier and not the company itself, which can lead to some uncertainty. This is especially true in cases where critical infrastructure is involved.

IoT devices can be located in areas that make them accessible to unauthorised persons. This is especially true for units located in public areas. These are people who have intentions that can cause harm or unwanted actions. This could be, for example, hackers who are looking for new challenges or who are trying to steal sensitive information. There may also be people who are just driven by curiosity. It is therefore important to have external security mechanisms.

One form of physical security is to remove connectivity options, such as radios and optical ports. These can be potential entrances for unauthorised persons. It will not be real to remove all ports, there must be at least one left for the connection of the local network.

In some cases, unauthorised persons may remove chips with critical functionality from the circuit boards of the device. The chips can then be used for testing and analysis purposes in order to find potential weaknesses of the device and associated systems. Such chips should be secured with a functionality that causes the chip to be damaged when trying to remove it.

5.2.3 Step 3: Security Routines

After planning and assessment of devices has been done, IoT related security routines need to be established. There are many reasons why this is important. Today's attack methods are becoming increasingly difficult to protect against, using different standards and frameworks can help create a better understanding of security. It will also be able to help reduce and prevent security breaches. Within IoT, there are a number of different standards and frameworks that can be used to establish or increase security.

Standards and frameworks
There are very many standards and frameworks one can use for securing IoT and increase the overall security. These are in many cases specialised to specific areas, which can make it challenging to decide what is urgent for your business and needs. Below are suggested different types of standards and frameworks that can be used to secure IoT with some focus on trust and scalability;

International Organisation for standardisation (ISO)

ISO standards was mentioned multiple times in the interviews. These are different standards that are verified internationally by experts. ISO standards are a useful tool that can provide credibility and improve quality. It can be applied to a number of activities such as production, technology, delivery of a service or handling of processes. In our case, we will take a closer look at ISO standards related to IoT.

1. ISO/IEC 30141
   This standard is reference architecture for IoT that will help ensure that connected systems are seamless, safer and more resistant. This involves a framework that designers and developers can take in use for IoT applications in order to create reliable systems that are secure and protect privacy and be able to withstand disturbances such as natural disasters and cyber-attacks."*It highlights functional requirement such as Data Management, Device Management, Security, Confidentially and privacy, it also highlight non-functional requirement such as maintainability, reliability, usability, high availability, and scalability of your system.*" (Mynster, 2021). The standard was published in 2018 and costs 220 dollars.

2. ISO/IEC TR 30166:2020
   "*This standard describes general IIoT systems and landscapes which outline characteristics, technical aspects and functional as well as non-functional elements of the IIoT structure and a listing of standardising organisations, consortia and open-source communities with work on all aspect on IIoT. This involves considerations for the future standardisation perspectives of IIoT including risk analysis, new technologies and identified collaboration.*" (ISO, 2020). The standard was published in 2020 and costs 220 dollars.

Another ISO proposal that can be mentioned is ISO / IEC CD 27400.3. This consists of a number of cybersecurity guidelines aimed at IoT security and privacy protection. The standard has not been published and is still under development. Expected publication is in 2022. ISO/IEC 30149 is also expected to be released in near future. This is framework is regarding trustworthiness with the use of IoT.

National Institute of Standards and Technology (NIST)
NIST is a non-regulatory government agency. "*NIST's goal is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.*" (NIST, 2021).

NIST has developed a framework for improving critical infrastructure cyber security. The framework will help companies manage their cyber security risks by integrating industry standards and best practices. It will also help create a common understanding of the cyber security risks the company faces and how these can be reduced with customised measures. (NIST, 2019).

NIST also plans to publish a practice guide for securing industrial IoT with a focus on cyber security for distributed energy resources. This is called NIST SPECIAL PUBLICATION 1800-32A. This is a practice guide that suggest standards, best practices and commercially available technology to protect digital communication, data, control of cyber-physical grid-edge devices. The guide also demonstrates examples of solutions for monitoring and detecting unusual activities in IIoT and how to build trust in data flows. (McCarthy et al., 2021). So far, a preliminary draft has been published and this was released April 2021. NIST SPECIAL PUBLICATION 1800-32A can be a relevant tool to use when fully released.

National Security Authority (NSM) basic principles for ICT security
NSM basic tips is a set of measures to protect information systems, data and services by preventing damage, misuse or unwanted access. Information systems are systems that relates to hardware, software and associated infrastructure. The target group for NSM is IT operations, system owners, security managers and business and process owners. It is mainly aimed at Norwegian companies and can be a useful tool for raising the safety competence and the level of safety for companies.

The basic principles are divided into 4 main categories: "identify and map", "protect and maintain", "detect and manage" and "recover".

Identifying and mapping is about understanding the business and identifying what needs to be protected and how to protect it. Find vulnerabilities also map out to protect them.

Protecting and maintaining is about protecting yourself. This is done by resisting computer attacks, limiting the damage of an attack.

Detecting and managing is about maintaining the safe state over time and in the event of changes, but also discovering other threats that can affect the business.

Managing and recovering is about being able to handle cases or scenarios where one has been attacked. Restoring the safe condition that one had before a vulnerability or attack. This is done by logging, audit, logs etc.
(NSM, 2020)

Security by design
Security by design is an approach where one tries to make software and hardware development as secure as possible and also make it as difficult as possible to be attacked. It is about implementing security functionality from the very beginning and not when the system is already fully developed. Violations of security can be both costly and punishable. It is therefore important to take a position on this as early as possible. Security by design can be achieved by following these 9 steps;

1. Build on proven technology
2. Create awareness
3. Limit instruction
4. Manage maintainability
5. Automate checks
6. Carry out manual checks
7. Expand to include privacy
8. Improve gradually
9. Security by design for both new and existing system
   (Veer, 2019)

Privacy by design
The data protection authority in Norway, Datatilsynet, also suggest to incorporate privacy in all phases of development in a system. This can be especially useful for systems that process personal information. There are different types of standards for privacy by design. In our case, we have examined the Datatilsynet principles of privacy by design

Datatilsynet privacy by design is an approach that consists of 7 principles;

1. Be ahead, prevent rather than repair:
   This principle is about assessing the risks to privacy as early as possible in the development process.
2. Make privacy the default setting:
   By making privacy the default setting, one should not collect unnecessary personal information. There must also be a legal purpose for the collection and the information collected must be deleted when the purpose has been achieved. You should also only have access to your own information.
3. Build privacy into the design:
   It is important to build privacy into the design and architecture of systems. The principle is about involving privacy early in the development process so that it is not added as a function afterwards.
4. Create full functionality:
   By taking privacy into consideration from the start, one can avoid reprisals that may affect the functionality of the release. Subsequent changes may cause the system to deteriorate. One seeks an approach that can do both and rather than one or the other. This is to take care of the company's needs and interests, and at the same time take into account the data subjects' privacy.
5. Take care of information security from start to finish:
   An important part of the solution is to ensure information security. Everything that happens in the system should be risk assessed in advance and appropriately secured. Personal data must be secured against unauthorised access, alteration, destruction and dissemination.

6. Show openness:
   One must show openness about how the system works and how privacy is taken care of. The company must provide good information to the user and the user must also have access to their own information. It must be possible to check that the system safeguards the privacy as stated by the supplier.

7. Respect the user's privacy existing system:
   The most important thing about embedding privacy is that the developers, customers and administrators give users privacy high priority. Privacy must be safeguarded through standard settings, clear terms of use, and solutions for the user to be able to control their information themselves.

   (Datatilsynet, 2018)

Safety routines
One could also establish basic safety routines within the company. The measures will vary based on how safety-critical the company is, but it is nevertheless important to establish your own safety routines and make employees aware of safety and make this a part of their work day.

Some concrete examples of such measures can be regular updates and making sure that the latest updates are running. These are updates that regularly address bugs and vulnerabilities in the device's software. One can, for example, schedule automatic updating instead of manual. As previously mentioned, the use of similar devices in an IoT infrastructure can make patching and updating easier.

Another measure is that the company conducts thorough research before any investment in IoT. One may ask whether the device comes from a reputable and reliable vendor? What kind of data should be collected, and what security measures should be used for the various data? It is wise to have control over the kind of functionality that comes with the IoT device and disable unnecessary features. If a device comes with geolocation functionality for example, one can consider whether it is necessary to use this as it reveals the device's position.

Other general measures are to have good password policies. The most basic step here is to never reveal your password to others. You should also use different passwords for different users. There are also requirements for the difficulty of the password. For example, one should not use passwords that are related to personal interests. With social engineering, unauthorised persons can acquire information related to the interests that make password cracking easier. Passwords are harder to crack the more complex they are. Therefore, you may want to use passwords that consist of lowercase and uppercase letters, numbers, and symbols. Such passwords can be difficult to remember, but programs like LastPass can store such passwords securely and make the passwords available to you easily.

Password changes should be done regularly. This can, for example, be after 90 days. By limiting the password duration, one can reduce password related attacks. If an unauthorised person first gains access to a password, it will be replaced after a certain period of time.

Another method of password policies is two factor authentication where authentication consists of something the user knows and something the user has. For example, a default password and verification codes via SMS. Even if unauthorised persons have access to your password, they can still not gain access.

Securing routers and communications may also be a good idea to do thoroughly. One should make sure that the encryption is at a high level. If a router is running on standard Wi-Fi Protected Access (WPA) protocol, it should be replaced with a newer version such as WPA3. This will make it difficult for hackers to infiltrate systems or devices.

Other useful measures are to establish adequate mechanisms for monitoring, logging and surveillance. This can help prevent security breaches, or detect where any breaches occurred and who committed them. If a human error has been made, this can potentially be traced.

The company may also consider having its own Network Operations Center (NOC) and Security Operations Center (SOC) teams. These have similar roles with different processes. NOC teams are responsible for detecting, investigating and resolving conflicts in systems and providing technical support. SOC teams, on the other hand, are responsible for averting alerts and incidents that have a negative impact on data security. They must protect both the company's data and the customer's. (Revolution, 2018).

5.2.4 Redundancy

It is crucial to have sufficient redundancy and recovery strategies when using solutions such as IoT.

Every business should develop an disaster recovery plan. From our qualitative research it seems that several industrial companies did not have concrete plans for what to do if a disaster occurs. If one of the system's vulnerabilities occurs, it must be possible to respond to this in an quick and effective manner. If the system is down for a long time, it can cause catastrophic costs for a company. Violation of the GDPR can also lead to large fines. Therefore, it is important to know which processes need to be performed if something goes wrong. The plan should also include methods for ensuring that valuable information is baked up properly. Test is important to perform in order to make sure that every aspect of the plan is working accordingly.

Strategies for recovery of Information Technology (IT), applications and data are recommended to be established. "*This involves networks, servers, desktops, laptops, IoT devices, data and connectivity. Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes.*"(Ready, 2021). An information system requires of the following components; hardware, software, data and connectivity. If one of these components is compromised, it may cause the system to stop running. Therefore, recovery strategies should be made to expect losses for the various component

Development of plans for data backups is also recommended to do. The company must identify data on wireless devices such as IoT, desktops, laptops and network servers and make regular backups of this data. You must also plan how often you make backups, how secure the backup should be and where the data should be kept. There are several ways to make backups. For example, data can be stored on backup servers, large USB drivers and tapes. Several providers also offer online backup services where the data is stored in the cloud. This is a cost effective solution, but also causes the business to become dependent on the security of the service and their policies. If you are handling very confidential data, you should perhaps consider other storage solutions or conduct thorough research on the possible service. (Ready, 2021).

5.2.5 Step 4: Network

The network phase is important to get right as this can make the environment surrounding your devices more secure. From the findings of this thesis we found that network can play a whole other role to preventing access to the IIoT devices.

To start off, we recommend that the network is to be segmented into different VLAN's and preferably segmented on a device level, so that every different device you have is grouped into a device category. E.g. Sensors in one VLAN, GPS in another VLAN, Actuators in another etc. This way one can keep control over devices in tidy groups and have them separated with boundaries of how critically important they are.

When you establish the network one should also have identifiers to enable secure connections in the network. We got the understanding that certificates and device ID could really help you integrate new devices to network and exclude non-valid devices as only approved ID's can connect. By distributing certificates you can also create a safe way to communicate with the devices as it is encrypted. These certificates are distributed with a time limit on them and needs to be from an official certificate authority. This can of course be automated.

Placement of the network may also play an important role. The office network should not be used as this may not be considered a "safe" environment. In the office network there are all sorts of business that happens, and it is the more target friendly network for attackers, as email and other forms of communication happens here. You may also consider leaving it out of the operational/production network as well, however this needs to be seen on the case of the network. The operational network may contain other sensitive data that should not be mixed with other devices and sensors. For practicality and security you may want to deploy it in its own network separated from other. This way one can also limit problems if they arise. By separating the network you can isolate problems to each network and problems in one network will not affect the others. It is well described by Microsoft Documentation where they say:
"*To effectively secure systems against attacks, a few general principles should be kept in mind:*

You should never administer a trusted system (that is, a secure server such as a domain controller) from a less-trusted host (that is, a workstation that is not secured to the same degree as the systems it manages).

You should not rely on a single authentication factor when performing privileged activities; that is, user name and password combinations should not be considered acceptable authentication because only a single factor (something you know) is represented. You should consider where credentials are generated and cached or stored in administrative scenarios.

Although most attacks in the current threat landscape leverage malware and malicious hacking, do not omit physical security when designing and implementing secure administrative hosts." (Foulds et al., 2017).

From the interviews we see that everyone work with a central hub that distributes their updates and management of the network. This also seems to be the the more convenient way of communicating with the network from our interviews. Fog computing and other edge frameworks can be difficult to set up properly, so in the end we recommend a central server to distribute messages.

Firewalls are an important factor to reduce the problems of incoming connections. Securing the VLAN behind a firewall is a good step to secure the segmented network.

In order to access the network one might consider a jump server. A jump server is used to access and manage devices in separate security zone and can go over networks. It is a means to access different zones. Foulds et al. (2017). This can be done both with a physical and logical implementation. It is therefor important to restrict the access. This includes people, access to the rest of the network and programs. It is also important to keep logs of this so one can identify people or programs going between networks.

One also needs to consider the communication protocols used for the network. The easiest would be with Ethernet and WLAN. However there comes scenarios where one might have to use cellular, satellite or radio for remote locations. These should be from either licensed bands or government provided bands if the operation is safety critical.

5.2.6 Topologies

In this section we will look at some of the possible topologies available to user of IoT. We have reviewed the different topology algorithms in section 4.3. In the interviews, we asked questions about topologies. We received some interesting answers, but not enough information. We take this up again in the simulation, but go more in depth on this aspect in order to create a better understanding of this area and the importance it has for scalability within IoT infrastructure. The findings from the simulation show that the choice of topology algorithm has a great influence in a number of areas. We also found that there is no specific topology algorithm that is optimally suited for all networks. The choice of topology will vary depending on the application of the IoT, the company's intentions and the size of the network.

Topologies can play an important role to how the network traffic performs. It also has an impact on how much coverage you get. We have explored A3, A3Cov, KNEIGH-Tree, CDS-Rule K and JustTree. From the findings we see that CDS-Rule K is both slow to generate a structure as well as its coverage is not as good. A3Cov, KNEIGH-Tree and JustTree were the clear winners when it comes to both performance and coverage. Just Tree works well form networks that are scalable, while the other two have good perfomance and range. The decision on which topology to choose comes down to how you want to structure the network. Both JustTree and KNEIGH-Tree have tree like structures that create good possibilities for a central node with transmission from the center. A3Cov gives you the possibility to clump more nodes in single location before branching out, which makes it good for many nodes in a single location.
The decision ultimately comes down to how and where you have your devices located along with performance.

6 Discussion

Our findings deliver a view of how scalability and trust plays an important, but difficult role in IIoT. If we take a look at the research question, we can discuss each of them to start off this.

- What are the security characteristics of an IIoT infrastructure?
- What is the relationship between trust and scalability in an IIoT infrastructure in the industry sector?

To start off the discussion we will discuss the security characteristics through literature, interviews and somewhat from simulations. The literature focuses a lot on security concepts and comes with examples that might be future implementations, however many of them also discuss current security concept which illustrates how the security of an IIoT infrastructure might look like. From the interviews we also see some of these security concepts as described in the literature. An example that confirms the same security concepts in literature and real world are Singh et al. (2017), Cheng et al. (2018), Sanchez-Iborra and Cano (2016) with informant number 1 and 6. From the literature we see security characteristics such as cryptography and encryption, 5G or cellular and communication protocols discussed. This is something that both informants stated they used, however which form of security mechanism was not explicitly mentioned as that is sensitive data. They confirmed that they used hashing, encryption and long range communication protocols. They also mentioned the good possibilities of 5G, which they were starting to look at, when 5G is fully rolled out.

Informants 5, 8, 9, 10 and 11 also provided good insight into security concepts of network and trust. Network security is arguably a necessary foundation that needs to be secure in IIoT. This concept was not much written about in the literature, except for Meng et al. (2017) and Sanchez-Iborra and Cano (2016). This is something that the aforementioned interviewees felt strongly about and disagree somewhat with the literature. They have strong routines that dictate that an IIoT network shall not be connected to the open internet and shall only be contained in its own segmented network separated from everything else. They are very critical to how security on some IIoT devices are implemented and therefore secure their network very heavily. They also see machine to machine(M2M) communication as more difficult to use as there may be less control over the devices compared to administrating it from a central machine, which then disagrees with Meng et al. (2017). Informant number 2 also states that they are in an early experimental phase to understand the device security more, as they are not confident enough in them to deploy to their network.

Zero trust is an implementation we have looked at in this study, and both the literature and interviews back up that this concept creates an important factor to a secure an IIoT network. In the literature we see it in form of device security with secure memory allocation and execution, while in the interviews we see that the interviewees utilise in the network to create a barrier of entry and to maintain the barrier.

Then comes the question of how the relationship between trust and scalability in an IIoT environment. This is a somewhat complex question and has many answers to it.

The overall conclusion we have come to is that there is a strong relationship between the two. The reasoning for this is from literature, simulation and the interviews we conducted. Literature focused a lot on individual components of trust and the individual components of scalability. This is somewhat contradicting to our finding because there were not many papers that had brought up this topic or even mentioned it. The literature seem to be focused on either trust in devices or the scalability frameworks. It does not argue specifically for both, rather argues why you need scalability or why you need trust in the devices. This contradicts the findings from the interviews and the examples we have from companies that operate with IIoT. They argue that you can not scale if you do not trust the devices or trust in the network. Scalability should come as a result of trust in both the network and the devices. In order to scale, we saw that the topology of the network should be in place. A scalable network with the right topology algorithms can help massively with performance and coverage over the network.

6.1 Contribution

Our contribution is to the security concepts and the relationship that trust and scalability have in IIoT. We discovered that trust and scalability are a combined factor that needs to be considered when establishing and and expanding an IIoT network. The thesis establishes important criteria to consider and to implement in order to efficiently have trust in a scalable infrastructure with the help of the MATNAS guideline and expert opinions through interviews, literature and some simulation. This can also serve as a reminder of important steps that should be done when using an IIoT network.
We address shortcomings of previous studies by enabling the MATNAS guideline and focus on the combined process of trust and scalability. Previous research have to little extent addressed the problems of both trust and scalability, and with this thesis, we establish guidelines to address that problem.

These findings can be used to further establish and improve an IIoT network by addressing the problems that we highlight. The MATNAS guideline is an overview of multiple security methods with focus on creating trust and scalability for an IIoT infrastructure and is provided with a more detailed description.

Future improvements to this study can be to conduct a more technical in depth explanation of the topic provided. This work is made on a more management level and a technical implementation could be worth exploring.
One could also explore more on the simulation part of this study and give a more detailed look at the role topology plays in scalability and trust.

We want to highlight that this is an emerging topic that has potential to be further explored and studied. The topic of IIoT is quite new in business sense even though the actual technology have been available for a long time. It is the concepts and components around the security in IIoT that is new, and we wish for this topic to be further explored. Even so, some of the legacy equipment may provide some sense of security by obscurity. It is not a recommendation to do so, however we acknowledge that this can sometimes be the case with legacy IoT systems.

This thesis is made to enhancing the understanding of IIoT and the role that both scalability and trust has to offer to it. With the study we try to connect the findings to the real world and cases that are close to how businesses operate today.

6.2 Limitation of research

In this section we will discuss some of the limitation of this thesis. We will go through some points that we consider limitations and that could impact the study.

We set out this thesis to have interviews and literature as our sources. That did not fully come to fruition as we struggled quite a lot to achieve the number of interviews we deemed necessary for the study. We hoped to reach at least 20 interviews when we started the interview search in late February. There are multiple reasons this did not go according to plan. There were not as many resources as expected at some places, and many companies did not have time or did not answer at all. This process was quite time consuming and made the progression and flow hard to manage. Small workload periods followed with high workload periods disrupted the natural flow of work.

We therefor had to add some additional data-points that could contribute to our problems. This is where simulation comes in. The simulation was a good addition, however as it is with simulation of IoT, it can be quite difficult, time consuming or unreliable. Simulation tools for IoT were often behind paid services or with complexity that would require an entire thesis in itself. We used a lot of time to find the right tools to simulate with. The simulation tool in itself was not perfect either, which we described earlier in the thesis.

This is also an emerging field were the data is ever-changing and focused on improvement. For this reason it was difficult to find relevant or good literature that could guide the thesis forward. The topic of trust and scalability combined was also a relatively new concept that has not had much research done. Finding the right information has been time consuming, however an important part of this thesis.

The pandemic that is ongoing during the writing, is another limitation to the project. This made hands-on or observation something that we could not really do. It was not the plan from the start, however the option could have been there. Observation could have given us a deeper understanding and a real world perspective into operation of IoT. All interviews were also conducted through Microsoft Teams. Reactions can sometimes be valuable to interviews, to see how a person reacts to questions. Isolation and "cabin fever" has been a factor for motivation and workloads.

7 Conclusion

Answers to the research questions

We largely managed to get answers to our research questions. In regards to the first research question; what are the security characteristics of an IIoT infrastructure? This is a descriptive questions with many answers. The purpose of the question was to be able to create a better understanding of IIoT and related security, something that we have to a certain level managed to achieve. From the literature review, we mostly found information regarding concepts for future securing of IIoT. Information received from interviews was more about how security was nowadays and the challenges surrounding this. Overall, we gained a good understanding of how security for IIoT is currently and how IIoT can be secured in the future.

IIoT is secured by a number of different measures. Networking, communication and connectivity were possibly the biggest challenges in IIoT infrastructure. The devices generally became vulnerable if they were connected to open networks. Several methods were used to secure this. Communication was, for example, secured by hashing, encryption and long range communication protocols. Cyber-attacks can occur and it is important to restrict access to the network. Several companies used segmentation. If an attack occurred, the attacker would only gain access to less critical parts of the network. We found that necessary security was determined by how critical the infrastructure was. Companies that handles less sensitive information often do not need strict security routines for using IIoT.

There were also several ways to secure devices. By using IIoT solutions from vendors, security is made less controllable. It becomes more dependent on vendors' policies and security mechanisms. If you develop your own IoT solutions, you get greater insight into how the units are controlled and how security can be established. The units were also easier to control and manage if the infrastructure consisted of identical units. Using devices from different vendors that have different policies and updates leads to a lot of extra work and you can easily lose control. Security functionality became more difficult to implement the smaller the devices were. The reason for that is because there is less security functionality that can be fitted to the device.

Safety routines were largely determined by vendors. It seemed that there were few companies that had their own defined security routines for IoT. However, companies that worked with critical infrastructure had this. We still think that every company should establish some security routines in regards to IIoT. How strict these routines are depends on how safety-critical the area of the company is. There were also few companies that had concrete processes and actions for handling security breaches. It also seemed that there were few companies that had concrete processes and actions for handling security breaches. If a security breach occurs, it is important that this is handled quickly and efficiently to avoid fines and other large costs. One should therefore perform ROS-analysis using technology such as IoT for example, where one assesses related threats and risks and how these can be addressed. Disaster recovery plan also goes a little below the same. The plan establishes specific measures for handling various disasters. The plan also includes methods for backing up valuable information.

The second research question is about the relationship between trust and scalability in an IIoT infrastructure in the industry sector. This is also a question with many answers, but is more complex. The overall conclusion is that there is a strong correlation between trust and scalability in IIoT infrastructure. Previous research addresses both trust and scalability aspects, but did not explain the relationship between these. We have concluded that you can not scale IIoT infrastructure if you don't have trust the network and associated devices. From the first research question, we get to know the security characteristics of IIoT and various methods of securing devices and network in order to increased the trust to them. It can still be challenging to scale a IIoT infrastructure if the network is large and consists of many different devices with different policies and security mechanisms. Segmentation can also be more difficult as you have to have more segmentation's in the network which means that there is more to keep track of and to manage. The choice of topology also has a great influence on scalability. We tested several topology algorithms on wireless sensor networks with different sizes and came to the conclusion that the best results came using KNEIGH-tree and A3Cov.

Reflection

We are generally satisfied with the result of the assignment and the learning outcome. Nevertheless, we have encountered a number of challenges that have meant that the pace of work has not been as even as expected. Many of these challenges were caused by the interview part and due to limited resources. Our thesis was mainly to be dedicated to IIoT in the energy sector and managed to get a collaboration with Agder Energy. We believed that a collaboration could help us to a large extent to provide sufficient resources for the execution of the various research activities. However, there were limited resources and finding interview candidates was a little harder than expected which meant that we had to make some adjustments to thesis. As a result of this we expand the scope to not only cover the energy sector specifically, but to cover industrial sectors in general.

We felt that the execution of the literature review was done in a good way. Literature reviews with such a large number of sources were new to us. We used SLR, which greatly helped to handle the literature and structure and present them. It also helps to show the actual processes of exclusion and inclusion of literature.

At the beginning of the semester, we were good at planning the work assignment and had created a calendar that contained these with associated deadlines. Later, this was done less as more obstacles arose. One of the main problems was that we did not have a sufficient number of interview candidates. The plan was initially to conduct between 15 and 20 interviews, but we eventually found that this was difficult to achieve. We received multiple rejections from the emails, and there were also many who did not respond. This made it a little more difficult and time consuming to reach the goal of estimated interview objects. We set a new goal for 10 interviews that we managed to achieve. In total, we conducted 11 interviews where we came in contact with many interesting companies from several industrial areas.

We still felt that 11 interviews was a little underwhelming and that we needed to add a complementary method. We chose to use simulations additionally. This also led to some challenges as we have not had experience with simulations before. It was a long process to find the right tools for this and how to utilise them. Several of these tools had to be set up in a Linux environment or cost money which also made it more difficult. What we were going to get out of the simulations was also something we had to decide on. After considering the various tools, we came to the conclusion that Atarraya would work best in our case. The benefits of simulation were valuable as it helped us gain a better understanding of the scalability aspect and how to structure a wireless sensor network efficiently.

Even though we encountered challenges, we managed to adapt to these and got the research questions answered.

Utilisation of the research

The research can help create a better understanding of the use of IIoT in industrial sectors and how to secure IIoT infrastructure in an effective way. We propose different types of measures that can be used to scale IIoT infrastructure and at the same time have trust in the units involved. The research can also be used to map the kind of challenges that come with the use of IIoT.

Future work

The research can be continued by having security experts validate and make suggestions on the proposed guidelines for scalability and trust in IIoT infrastructure (MATNAS). Certainly someone with technical competence as we have largely focused on the management aspect. A technical counterpart to this could help create a more defined structure both management and technical side. Suggested frameworks and standards were found via research and interviews, but how these actually work in real terms is difficult for us to judge. Several of the frameworks and standards cost money to be able to use. They still had good descriptions that made us use them. Some of the frameworks and standards in the guideline section was not fully released. In the future, these may also be described in more detail as available information was quite limited on this right now.

A Appendix

A.1 Exclusion Table

Citation: Number and title	Title exlusion	Abstact exclusion	Full-text exclusion	Criteria
4: A secure communicating things network framework for Industrial IoT using blockchain technology	✗			✗ Setting: Outside the scope
5: Blockchain technology in the energy sector: A systematic review of challenges and opportunities	✗			✗ Setting: Outside the scope
1: A Distributed Systems Perspective on Industrial IoT	✔	✗		✗ Content: too specific ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
7:A Distributed Systems Perspective on Industrial IoT	✔	✗		✗ Setting: Poor abstract. Did not contain much information about their study. ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
8: Enabling Trust and Security: TIPPSS for IoT	✔	✗		✗ Setting: Outside the scope(AI modelling)
15: A view on privacy & trust in IoT	✔	✗		✗ Setting: Outside the scope. Was about commercial IoT ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
26: IoT security (IoTSec) considerations, requirements, and architectures	✔	✗		✗ Content: Too short and not specific ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
29: Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models	✔	✗		✗ Content: Very specific and heavily revolved around cloud ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
40: Evaluating Critical Security Issues of the IoT World: Present and Future Challenges	✔	✗		✗ Setting: Outside the scope (SIoT)
42: A survey on IoT communication and computation frameworks: An industrial perspective	✔	✗		✗ Setting:Outside the scope(Fog, Edge & Cloud) ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
43: Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-things in Industry 4.0	✔	✗		✗ Content: Cost money ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
58: A Novel Framework of Three-Hierarchical Offloading Optimization for MEC in Industrial IoT Networks	✔	✗		✗ Setting: Outside the scope(Mathematical simulation)
60: An Efficient Clustering Framework for Massive Sensor Networking in Industrial IoT	✔	✗		✗ Setting: Outside the scope(AI modelling)
2: Security analysis on consumer and industrial IoT devices	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
6: A Scalable and Secure Publish/Subscribe-based Framework for Industrial IoT	✔	✔	✗	✗ Content: Too technical and specific on MQTT.
9: An IoT trust and reputation model based on recommender systems	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
10: Establishing Trust in the Emerging Era of IoT	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
11: A Novel Security Framework for Industrial IoT Based on ISA 100.11a	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
12: Things, Trouble, Trust: On Building Trust in IoT System	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
13: Trust-Oriented IoT Service Placement for Smart Cities in Edge Computing	✔	✔	✗	✗ Content: Too technical. ✗ Setting: Outside the scope.
14: A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed and was short.
16: Security of IoT systems: Design challenges and opportunities	✔	✔	✗	✗ Date of publication or of data collection: 2014 ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
17: Privacy and Security Challenges in Internet of Things	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
18: Securing future decentralised industrial IoT infrastructures: Challenges and free open source solutions	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
19: Pass-IoT: A platform for studying security, privacy	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
23: A lightweight attribute-based encryption scheme for the Internet of Things	✔	✔	✗	✗ Content: Too technical. ✗ Setting: Outside the scope.
24: Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT	✔	✔	✗	✗ Content: Too technical and specific. ✗ Date of publication or of data collection: 2014 ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
25: A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature	✔	✔	✗	✗ Content: Too technical.
27: A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment	✔	✔	✗	✗ Content: Too technical and specific. ✗ Setting: Outside the scope.
30: Hardware-security technologies for industrial IoT: TrustZone and security controller	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
32: Zero-Trust Hierarchical Management in IoT	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
33: Zero Trust based Internet of Things	✔	✔	✗	✗ Content: Editorial release on 2 pages to inform about a topic.
34: Access Control Policy Enforcement for Zero-Trust-Networking	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
37: A Survey on IIoT Security	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
38: Trustworthiness in Industrial IoT Systems Based on Artificial Intelligence	✔	✔	✗	✗ Content: Implementation of AI model. Outside of scope.
39: A Survey on Security and Privacy Issues in Internet-of-Things	✔	✔	✗	✗ Content: Literature review
44: Increasing the Trustworthiness in the Industrial IoT Networks Through a Reliable Cyberattack Detection Model	✔	✔	✗	✗ Content: Proposed detection model. Outside the scope
45: Optimizing Sensor Network Coverage and Regional Connectivity in Industrial IoT Systems	✔	✔	✗	✗ Content: Too technical. ✗ Setting: Mathematical proof of a model
47: A Novel Data Collection Framework for Telemetry and Anomaly Detection in Industrial IoT Systems	✔	✔	✗	✗ Content: Anomaly detection with AI models. ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
48: Evaluation of communication latency in industrial IoT applications	✔	✔	✗	✗ Content: IoT latency. ✗ Setting: Not in the scope ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
50: Reaching 10-years of battery life for industrial IoT wireless sensor networks	✔	✔	✗	✗ Content: Not related to our research questions ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
53: 5G Enabled Codesign of Energy-Efficient Transmission and Estimation for Industrial IoT Systems	✔	✔	✗	✗ Content: Too technical. ✗ Setting: Mathematical proof of a model
54: Solar energy prediction for constrained IoT nodes based on public weather forecasts	✔	✔	✗	✗ Content: Weather prediction for IoT, outside scope ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
55: Deriving Impact-driven Security Requirements and Monitoring Measures for Industrial IoT	✔	✔	✗	✗ Content: Not relevant for Energy sector ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
56: An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
57: TLS-Level Security for Low Power Industrial IoT Network Infrastructures	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
59: SEMIoTICS Architectural Framework: End-to-end Security, Connectivity and Interoperability for Industrial IoT	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed
61: ATT-Auth: A Hybrid Protocol for Industrial IoT Attestation With Authentication	✔	✔	✗	✗ Content: Too technical. ✗ Setting: Mathematical proof of a model
62: OpenMote: Open-Source Prototyping Platform for the Industrial IoT	✔	✔	✗	✗ Content: Not related to our research questions ✗ Peer-reviewed: Conference. The paper is not peer-reviewed
63: eeDTLS: Energy-Efficient Datagram Transport Layer Security for the Internet of Things	✔	✔	✗	✗ Peer-reviewed: Conference. The paper is not peer-reviewed

Table A.1: Exclusion of literature

A.2 Inclusion table

Research Questions	Citation: Number and title	Synthesis type	Rank 1-5 (Relevance)	Justification
1	21: Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions	Qualitative (Scenario)	4	Discusses IoT device constraints and low resources. This concern is also related IIoT devices in the energy sector. Shows different methods to address such challenges
	34: The industrial internet of things (IIoT): An analysis framework	No primary data, only used existing literature	3	Show areas of use for IIoT. Describes IIoT devices characteristics based on six interesting categories.
	35: A Secure Industrial Internet of Things (IIoT) Framework for Resource Management in Smart Manufacturing	Qualitative (Analysis)	4	Wireless connection for IIoT devices/sensors. Takes on the reliability and security aspects. Related to IIoT in the energy sector as it concerns challenging factors for trust and scalability.
	45: A Data-Oriented M2M Messaging Mechanism for Industrial IoT Applications	Qualitative (Case study)	4	Concerns communication between IIoT devices. Very informative. provide descriptive characteristics and mechanisms of IoT devices.
2	19: Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks	Qualitative (Experimental)	3 (Technical)	Technical paper with focus on how to detect attacks in a IoT network. Can be useful to address IIoT trust issues.
	27: IIoTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices	Qualitative (Experimental)	3	Related to IoT software and hardware and takes on how to establish trust in IoT devices.
	40: Industrial IoT in 5G environment towards smart manufacturing	No primary data, only used existing literature	2	Specific. Takes on benefits from up and coming 5G connection. How to manufacture new devices to 5G. Can provide answers to the challenges of scalability
	48: Weaving the Wireless Web: Toward a Low-Power, Dense Wireless Sensor Network for the Industrial IoT	No primary data, only used existing literature	3	Very related to scalability. Takes on low-powered IIoT sensors, which is much used in the energy sector, and challenges with wireless connectivity and power.
	50: State of the Art in LP-WAN Solutions for Industrial IoT Services	No primary data, only used existing literature	4	Takes on modern and recent ideas and methods for connectivity solutions for IIoT services with focus on low-powered devices/sensors.
1 & 2	2: Internet of Things (IoT) and the energy sector	No primary data, only used existing literature	5	Informative and descriptive in terms of characteristics of IoT in the energy sector. Shows security and privacy challenges. Additionally, takes on some scalability and trust concerns.
	20: A Graph-Based Security Framework for Securing Industrial IoT Networks From Vulnerability Exploitation's	Qualitative (Modelling and scenario)	3 (Technical)	Technical paper. Uses an interesting graph-framework that illustrates IIoT exploitation's in a good and descriptive way.
	30: Content Caching in Industrial IoT: Security and Energy Considerations	Qualitative (Simulations)	3	Takes implementation of trusted system/nodes at the network and how to prevent maliciously actives on nodes. This can establish better trust and scalability for IIoT infrastructure. Contains some characteristics of IIoT.
	51: Secure Information Sharing in an Industrial Internet of Things	Qualitative (Proposition/Roadmap)	5	Different takes on how to improve security in IIoT infrastructure. Includes interesting best practices and solution on protecting IIoT devices..

Table A.2: Inclusion of literature

A.3 Interview guide

Other topics and questions may arise throughout the interview. We look for a fluent conversation through a semi-structured interview.

Introduction
Hi and thank you for taking the time to interview. We must inform you of your rights and consent before we begin. Do you agree that we may use personal information such as Name and background information such as Workplace and Position in this assignment? If you answer Yes, you can withdraw your consent at any time by sending an email to us at mathie16@uia.no or jonaso15@uia.no. In order to be able to transcribe the interview later, we want to record audio. The audio recording will be deleted after transcription. Do you agree that this conversation can be recorded on audio recording? If you answer Yes, you can withdraw your consent at any time by sending an email. You also have the right to access your data (Audio Recording and Transcription) should there be anything you want to see or change, this will be given access to by sending us an e-mail. You have also received an information letter that says something about why and what we are doing this interview for.

Note. *Questions after "-" are follow-up questions. Some of the questions are aimed towards the energy sector only and will be modified based on the interviewee*

Focus Area	**Questions - Semi-structured interview**
IoT Characteristics	What kind of industrial IoT devices do you use in the energy sector? - What is most used? Small (sensor), Medium (Raspberry) or Large (machines)?
	What kind of benefits do you get from this technology?
	If the IoT devices are secured, how do you ensure that the connection remains secure and efficient?
	Do you have your own security routines, frameworks, or policies regarding IoT security? Or does this come via vendors? - What are these?
	What are the challenges of using IoT?
Trust / security	How are IoT devices secured? This may vary from unit to unit, but what are the basic safety precautions that are being implemented?
	How do you think one can create trust in a network? Should one have a central node or machine to machine communication that resolves conflicts?
	How do one secure remote devices? Some devices are not always online or put into power-saving mode when connected to the Internet. How do you secure such devices?
	How can you tell that data has not been modified by unauthorized persons?
	If it is discovered that the incoming data has been modified by unauthorized persons. What kind of procedures / processes are implemented then?
	What do you think about a ZeroTrust network where nobody trusts each other in a network? - How would this solution be handled when there are many users connected.
Scalability	How can large quantities of units be distributed and deployed in the field efficiently and safely? How do you update and maintain devices?
	What are the challenges of integrating new IoT devices into the network?
	How is IoT security affected by scaling IoT infrastructure? How can one go from 100 to 1000 units e.g.
	How do you scale a ZeroTrust network? - What are the concerns when scaling such network?

Table A.3: Interview Guide

Summary of Interviews by topic

Category	Subcategory	Summaries
IoT characteristics	Area of use	We have interviewed companies from several different types of industries which use IoT in many different fields. Much of the IoT was located outdoors. For example, some IoT was used for tunnel work, and other was used for hydro power production. There was also used IoT for factory work/production and there were also instances where IoT was used for prototyping and testing.
	Benefit	From the interviews we could see that several companies benefited greatly from the use of IoT. There were also companies that had recently started using the technology and used it more to explore and test out new opportunities. It was interesting to hear how differently companies utilized IoT. IoT was mainly used for measuring in different types of areas such as power consumption for example. It was also mentioned that it was used for tracking, monitoring and drone footage.
	Most used device type	Based on responses from the interviews, sensors were mostly used in an industrial context. Some companies only used sensors, but there were also some who went for a mixed approach and used for example sensors, Raspberry Pi, drones and some large machines. Generally it was very rarely used larger machines. Much of IoT devices came from larger vendors, but some companies also opted for their own IoT solutions, as it was easier to rely on.
	Security mechanisms	Many of the security mechanisms for the IoT devices came via the suppliers. Various types of certificates and standards such as ISO are also used to secure the devices. This could be used to secure communication channels and encrypt data securely. VPN and specialized SOC teams were also mentioned. Several companies focused heavily on the security aspect, but there were also some who were less concerned about good IoT security, because they had non-critical data.
Organisational security policies	Standards and licenses	A number of different solutions were mentioned regarding standards and licenses. Several mentioned solutions from Microsoft. Some used ISO standards and followed different types of principles such as NSM basic principles and Security by design. This varied with regard to the area of use and the purpose of using IoT.
	From vendor or self-made	The vast majority used solutions from the suppliers and followed different types of regulations. Some had created basic security for the company, however there were surprisingly few who mentioned they had their own specified security routines or measures regarding IoT.
	Security mechanisms	Many of the different interviewees have somewhat equal solutions to their security mechanisms. They employ encryption, hash values, keys and certificates to secure their devices and traffic. They also have different built solutions to provide monitoring and detection of anomalies. Semantic and syntactic checks. Many mentioned firewall protection. Some had their own intrusion detection systems as well.
	Processes for data breaches	It seems that few companies had developed a special plan in the event of a data breach. A few different measures were mentioned, but few had defined procedures for such incidents. Some of the measures mentioned were; monitoring, checking code and logs. Clean data and flag anomalies. Notify customers and disconnect the machine or machines in question.

Challenges	Network	When it comes to securing networks, there were several challenges. For example intruders could obscure messages with blanks. Range and connectivity were that of the major problems. Several companies relied on mobile internet such as 2G and 4G. This has its ups and downs, but was often the most challenging to use in areas with poor connectivity. This could possibly be better with upcoming 5G. Updating and patching can become a challenge when using several types of IoT devices in the network. In general, having an internet connection can be quite challenging.
	Devices	Price, robustness and updates play a big part in finding and using the right devices. Sensors and devices have different purposes and one challenge is to secure that a device is not used for something it is not intended for. Sensors might be in redundant pairs and need the ability to disconnect if something is wrong. It also needs to be robust enough to handle any production or abuse it may incur. The device also needs to be robust in order to survive different types of weather conditions. Lastly they need to be affordable enough and updatable to secure the device for future problems that may head its way. The separation of inside and outside networks may also decide what devices you want to get. The critical infrastructure makes it difficult to implement IoT as they require special attention to security, which all devices do not have.
	Scalability	Scalability has not been as large of a challenge for most interviews as we expected. The major IoT hubs and platforms seem to handle this aspect quite well. The problem might not be how many devices you have, however it might be how many messages that are sent. The network load is an important factor in the realm of scalability. Introducing new equipment to legacy systems and other SCADA systems may very well be as much of a problem. The different configurations of the devices may also pose a problem for scalability as some are behind a firewall while other tunnel inn with VPN. The problem might also be to mix in all these solutions to one common area.
	Integration of devices	There are many factors that come into play when you want to add new devices in the network. They have to be compatible, have the right specification, what data should they send, what their location is, how they communicate with the server and if they are serviceable. Geographical placement does also come into factor, because if they are far away they might not be able to communicate as well and they need some form of power management. The traditional IoT software hubs can usually manage the integration well, however there are special cases that need to be considered. There should also be plans on how to maintain and further roll out the devices which need to be determined before acquiring a new device.
	Trust	To establish safe connections and trust in the network, we see that some of the interviewees mention communication channels, such as VPN with the use of also encryption when available and some form of key infrastructure and certificates. This creates trust because only the specified keys and certificates are allowed to communicate with the server. Some also have a redundancy system that ensures that the same sensors provide the same answers back. Logging and monitoring can also be used to ensure that the traffic is secure.

Network	Scalability	Scalability does not seem to be an issue for the most part. It depends on some factors. If you have many similar or equal devices and sensors, it does not seem or pose any problems to scale. One can introduce a new sensor and establish a link and you have it going. The problem comes when you introduce many different units that have their own software and come from different vendors. Specialised software may be needed if there are many different devices. However on the scale of a few thousand devices it does not pose any real problems. Scalability in itself does not seem to be a major issue for most people. The vendor solutions establish a good enough framework to enable this.
	Topology	Most of the interviews declared that they had a central machine or server that took care of the balancing and messaging system with the devices. Edge computing is not as prevalent as expected. The more typical topology of a central node is used, where this node retrieves and sends out informasjon to all the other nodes. The server then manages the message distribution and the traffic between the nodes. What we see here is that there are many types of communication protocols that can be utilised in this case. In rural areas there might be need for other communication protocols such as satellite, 2G or radio in some cases.
	Zero Trust	There were not many who had opinions regarding this. The general consensus among those who answered was that it is a good idea in practise, however might be difficult to achieve in all places, because of convenience. They added that it should be in place for critical systems and places.
	Securing incoming data	Most of the interviews have come forth with message encryption which is a good idea. It looks like vendors come with prebuilt keys on the devices which makes it easy to add to a network. In some form all of the interviews related to a form of security of the datastream. Either encrypt the data if the device has the capabilities or if it is a safety critical device. If it is not safety critical data or device, they could still limit access with different communication channels, IP filtering, server side output and retrieval or verification of users.

Table A.4: Summary of Interviews

Bibliography

Khaled Ali Abuhasel and Mohammad Ayoub Khan. A secure industrial internet of things (iiot) framework for resource management in smart manufacturing. *IEEE Access*, 8: 117354–117364, 2020. ISSN 2169-3536. doi:10.1109/access.2020.3004711.

Lavric Alexandru and Popa Valentin. Performance evaluation of topology control algorithms that can be integrated into a street lighting control sensor network. *2013 11th RoEduNet International Conference*, pages 1–4, 2013. doi:10.1109/RoEduNet.2013.6511741.

Hany F. Atlam, Robert J. Walters, and Gary B. Wills. Fog computing and the internet of things: A review. *Big Data and Cognitive Computing*, 2(2), 06 2018. URL https://www.proquest.com/scholarly-journals/fog-computing-internet-things-review/docview/2124676199/se-2?accountid=45259.

M. Ishtiaque Aziz Zahed, Iftekhar Ahmad, Daryoush Habibi, and Quoc Viet Phung. Content caching in industrial iot: Security and energy considerations. *IEEE Internet of Things Journal*, 7(1):491–504, 2020. ISSN 2327-4662. doi:10.1109/jiot.2019.2948147.

Hugh Boyes, Bil Hallaq, Joe Cunningham, and Tim Watson. The industrial internet of things (iiot): An analysis framework. *Computers in Industry*, 101:1–12, 2018. ISSN 0166-3615. doi:10.1016/j.compind.2018.04.015. URL https://dx.doi.org/10.1016/j.compind.2018.04.015.

Marie Brudvik. Ros-analyse - helsebiblioteket.no, 2010. URL https://www.helsebiblioteket.no/kvalitetsforbedring/metoder-og-verktoy/ros-analyse.

Gustavo Caiza, Morelva Saeteros, William Oñate, and Marcelo V. Garcia. Fog computing at industrial level, architecture, latency, energy, and security: A review. *Heliyon*, 6(4):e03706, 2020. ISSN 2405-8440. doi:10.1016/j.heliyon.2020.e03706.

J Chase. The evolution of the internet of things, 2013. URL https://www.ti.com/lit/ml/swrb028/swrb028.pdf?ts=1619881070210&ref_url=https%253A%252F%252Fwww.google.com%252F.

Jiangfeng Cheng, Weihai Chen, Fei Tao, and Chun-Liang Lin. Industrial iot in 5g environment towards smart manufacturing. *Journal of Industrial Information Integration*, 10:10–19, 2018. ISSN 2452-414X. doi:10.1016/j.jii.2018.04.001.

Datatilsynet. Innbygd personvern, Jun 2018. URL https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/.

Iain Foulds, Kent Sharkey, Elizabeth Ross, David Coulter, Tom Pratt, John Flores, Liza Poggemeyer, Bill Mathers, Catherine Watson, and Sudeep Kumar. Implementing secure administrative hosts, May 2017. URL https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-secure-administrative-hosts.

Gemini George and Sabu M. Thampi. A graph-based security framework for securing industrial iot networks from vulnerability exploitations. *IEEE Access*, 6:43586–43601, 2018. ISSN 2169-3536. doi:10.1109/access.2018.2863244.

Christie Gupta and Manjula. Scalability in internet of things: Features, techniques and research challenges. *International Journal of Computational Intelligence Research*, 13(1): 1617–1627, 2017. ISSN 0973-1873. doi:10.1177/0739456x17723971.

Satyam Gupta and Gunjan Gupta. Simulation time and energy test for topology construction protocol in wireless sensor networks. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, 3, 06 2015. doi:10.11591/ijeei.v3i2.139.

Shane G. Henderson and Barry L. Nelson. Chapter 1 stochastic computer simulation. In Shane G. Henderson and Barry L. Nelson, editors, *Simulation*, volume 13 of *Handbooks in Operations Research and Management Science*, pages 1–18. Elsevier, 2006. doi:https://doi.org/10.1016/S0927-0507(06)13001-7. URL https://www.sciencedirect.com/science/article/pii/S0927050706130017.

Naser Hossein Motlagh, Mahsa Mohammadrezaei, Julian Hunt, and Behnam Zakeri. Internet of things (iot) and the energy sector. *Energies*, 13(2):494, Jan 2020. ISSN 1996-1073. doi:10.3390/en13020494. URL http://dx.doi.org/10.3390/en13020494.

B. I Hovland, K Bakken, O Dale, W Johnsenm, T Lunde, P. A Melson, J. A Skolbekken, V. S Møller, A Staff, C. P Ulrichsen, L Vatten, and Å Wifstad. Veiledning for forskningsetisk og vitenskapelig vurdering av kvalitative forskningsprosjekt innen medisin og helsefag, 2019. URL https://www.forskningsetikk.no/retningslinjer/med-helse/vurdering-av-kvalitative-forskningsprosjekt-innen-medisin-og-helsefag/.

ISO. Iso/iec tr 30166:2020, Apr 2020. URL https://www.iso.org/standard/53286.html.

D Jacobsen. *Hvordan gjennomføre undersøkelser?* Høyskoleforlaget, 2005. ISBN 9878276346633.

Raj Jain. *The art of computer systems performance analysis : techniques for experimental design, measurement, simulation, and modeling*. Wiley, New York, 1991. ISBN 0471503363.

B Jovanović. Internet of things statistics for 2021– taking things apart, 2021. URL https://dataprot.net/statistics/iot-statistics/#:~:text=Key%20IoT%20statistics&text=It%27s%20estimated%20that%20the%20number,in%20economic%20value%20by%202025.

S Kvale. *Det kvalitative forskningsintervju*. Gyldendal Norsk Forlag, 1997. ISBN 9788241708077.

Miguel A Labrador and Pedro M Wightman. *Topology Control in Wireless Sensor Networks: with a companion simulation tool for teaching and research*. Springer Science & Business Media, 2009.

Liang Liu, Zuchao Ma, and Weizhi Meng. Detection of multiple-mix-attack malicious nodes using perceptron-based trust in iot networks. *Future Generation Computer Systems*, 101: 865–879, 2019. ISSN 0167-739X. doi:10.1016/j.future.2019.07.021.

K. L Lueth. State of the iot 2020: 12 billion iot connections, surpassing non-iot for the first time, 2020. URL https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/.

Ling Lyu, Cailian Chen, Shanying Zhu, and Xinping Guan. 5g enabled codesign of energy-efficient transmission and estimation for industrial iot systems. *IEEE Transactions on Industrial Informatics*, 14(6):2690–2704, 2018. ISSN 1551-3203. doi:10.1109/tii.2018.2799685.

James McCarthy, Eileen Division, Don Faatz, Nikolas Urlaub, and John Wiltberger, Apr 2021. URL https://csrc.nist.gov/publications/detail/sp/1800-32/draft.

Zhaozong Meng, Zhipeng Wu, Cahyo Muvianto, and John Gray. A data-oriented m2m messaging mechanism for industrial iot applications. *IEEE Internet of Things Journal*, 4(1): 236–246, 2017. ISSN 2327-4662. doi:10.1109/jiot.2016.2646375.

Anders Mynster. Ieee and iso/iec standards for iot, 2021. URL https://nordiciot.dk/ieee-and-iso-standards-for-iot/.

Emerson Navarro, Nuno Costa, and Antonio Pereira. A systematic review of iot solutions for smart farming. *Sensors*, 20(15):4231, 2020. URL https://www.proquest.com/scholarly-journals/systematic-review-iot-solutions-smart-farming/docview/2429631690/se-2?accountid=45259.

NIST. Cybersecurity framework, Nov 2019. URL https://www.nist.gov/industry-impacts/cybersecurity-framework.

NIST. Nist general information, Feb 2021. URL https://www.nist.gov/director/pao/nist-general-information.

Novotek. Beskrivelser og forklaringer av iot, iiot og industri 4.0, N/A. URL https://www.novotek.com/no/l-sninger/iot-for-industri-prosess-og-bygg/beskrivelser-og-forklaringer-av-iot-iiot-og-industri-4-0/.

NSM. Introduksjon, Aug 2020. URL https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/introduksjon/.

C Okoli and K Schabram. A guide to conducting a systematic literature review of information systems research. *Journals at AIS Electronic Library (AISeL)*, 2010. ISSN 1529-3181. URL https://chitu.okoli.org/media/pro/research/pubs/Okoli2015CAIS.pdf.

Chitu Okoli. A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, 37(1):43, 2015.

Glory Pachnanda and Rajan Chaudhary. Comparative study of a3, eecds, cds rule k and kneigh tree protocols in a grid manner. *Advances in Electronic and Electric Engineering*, 3(4):509–514, 2013.

Sandro Pinto, Tiago Gomes, Jorge Pereira, Jorge Cabral, and Adriano Tavares. Iioteed: An enhanced, trusted execution environment for industrial iot edge devices. *IEEE Internet Computing*, 21(1):40–47, 2017. ISSN 1089-7801. doi:10.1109/mic.2017.17.

PwC. The industrial internet of things. Technical report, PwC, 2016. URL https://www.pwc.com/gx/en/technology/pdf/industrial-internet-of-things.pdf.

Ready. It disaster recovery plan, Feb 2021. URL https://www.ready.gov/it-disaster-recovery-plan.

Server Revolution. So what are the noc and soc?, Jun 2018. URL https://www.serverrevolution.com/so-what-are-the-noc-and-soc/.

Ramon Sanchez-Iborra and Maria-Dolores Cano. State of the art in lp-wan solutions for industrial iot services. *Sensors*, 16(5):708, 2016. ISSN 1424-8220. doi:10.3390/s16050708. URL https://dx.doi.org/10.3390/s16050708.

Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park. Advanced lightweight encryption algorithms for iot devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, 2017. ISSN 1868-5137. doi:10.1007/s12652-017-0494-4.

Raimo Streefkerk. Qualitative vs. quantitative research: Differences & methods, Apr 2019. URL https://www.scribbr.com/methodology/qualitative-quantitative-research/.

L.M. van der Knaap, F. L. Leeuw, S. Bogaerts, and L.T.J. Nijssen. Combining campbell standards and the realist evalution approach: The best of two worlds? *American Journal of Evaluation*, 29(1):48–57, 2008. ISSN 1098-2140.

Robert Veer. Security by design in 9 steps, 2019. URL https://www.softwareimprovementgroup.com/resources/security-by-design-in-9-steps/.

Jane Webster and Richard T. Watson. Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2):xiii–xxiii, 2002. ISSN 02767783. URL http://www.jstor.org/stable/4132319.

Pedro M. Wightman and Miguel A. Labrador. Atarraya: A simulation tool to teach and research topology control algorithms for wireless sensor networks. In *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, Simutools '09, Brussels, BEL, 2009. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). ISBN 9789639799455. doi:10.4108/ICST.SIMUTOOLS2009.5565. URL https://doi.org/10.4108/ICST.SIMUTOOLS2009.5565.

Pedro Mario Wightman R. and Miguel A. Labrador. Reducing the communication range or turning nodes off? An initial evaluation of topology control strategies for wireless sensor networks. *IngenierÃa y Desarrollo*, pages 66 – 88, 12 2010. ISSN 0122-3461. URL http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0122-34612010000200006&nrm=iso.

Yu Xiao and Maria Watson. Guidance on conducting a systematic literature review. *Journal of Planning Education and Research*, 39(1):93–112, 2019. ISSN 0739-456X. doi:10.1177/0739456x17723971.

Xiaolong Xu, Xihua Liu, Zhanyang Xu, Fei Dai, Xuyun Zhang, and Lianyong Qi. Trust-oriented iot service placement for smart cities in edge computing. *IEEE Internet of Things Journal*, 7(5): 4084–4091, 2020. ISSN 2327-4662. doi:10.1109/jiot.2019.2959124.

Shanhe Yi, Zijiang Hao, Zhengrui Qin, and Qun Li. Fog computing: Platform and applications. In *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*. IEEE, 11 2015. doi:10.1109/HotWeb.2015.22.

X. Yuan, Y. He, Q. Fang, X. Tong, C. Du, and Y. Ding. An improved fast search and find of density peaks-based fog node location of fog computing system. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 635–642, 2017. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.100.

Meiyu Zhang, Qianying Zhang, Shijun Zhao, Zhiping Shi, and Yong Guan. Softme: A software-based memory protection approach for tee system to resist physical attacks. *Security and Communication Networks*, 2019, 2019. URL https://www.proquest.com/scholarly-journals/softme-software-based-memory-protection-approach/docview/2455785773/se-2?accountid=45259.