A Secure Transition from Industry 3.0 to Industry 4.0 for Manufactures

Recommendations from a security perspective

Josephine Kjelsrud

Thesis submitted for the degree of
Master in Informatics: Information Security
60 credits

Department of Informatics
Faculty of mathematics and natural sciences

UNIVERSITY OF OSLO
A Secure Transition from Industry 3.0 to Industry 4.0 for Manufactures

Recommendations from a security perspective

Josephine Kjelsrud
Abstract

Cyber attacks targeted towards Operational Technology and Industrial Control Systems are increasing rapidly. With new technology from the fourth industrial revolution, manufacturers can automate more of the production process, but this also expands the attack surface. Securing industrial companies can be complex and resource-consuming, and the security controls will have to be carefully implemented.

This thesis will focus on how manufacturers can have a secure transition from the third industrial revolution to the fourth. By analyzing how a specific industrial company in Oslo is upgrading its security to match the new technology, the goal is to recommend how other similar manufacturers or industrial companies can do the same. In order to investigate how the situation is for other industrial companies in Norway, employees from Telenor who help with securing Norwegian industrial companies were interviewed. To address the importance of designing and implementing specific security controls for Industry 4.0, the recommendations have been linked to challenges and attack scenarios related to the fourth industrial revolution.

Findings from the analysis show that the manufacturers, including the industrial company, lack security controls, strategies, and measures for Industry 4.0. In addition to this, the results show that there is possible to decrease the risk of many challenges and attack scenarios by focusing on some key aspects of the company represented in this thesis.
Acknowledgements

Writing this thesis has been an incredible journey, and I would like to thank everyone who has been a part of the project.

Thanks to, The Department of Informatics at the University of Oslo for being an excellent place for education. I would like to especially thank Prof. Nils Gruschka from the Digital Infrastructure and Security section for the supervision during this master project.

Thanks to my co-supervisor, Jan Petter Torgersrud from Telenor, for all the support, the ideas, and for connecting me with interesting people. Especially thank you to the people in the project group, from Telenor and the industrial company. You have given of your knowledge and shared your perspectives with me without hesitation.

Thank you to all my friends for the support and enjoyable moments along the way. Writing this thesis during the pandemic has been challenging, and it would not have been possible without your endless positivity. Thank you for encouraging words, lovely dinners, fun bouldering trips, and late nights.

Last but not least, a huge thank you to my parents. Thank you for always supporting me and pushing me to achieve my goals!
# Contents

1 Introduction .......................................................... 1
  1.1 Motivation ......................................................... 1
  1.2 Scope and Research Question .................................... 2
  1.3 Contribution ...................................................... 3

2 Background ............................................................ 5
  2.1 Industrial Systems ................................................. 5
    2.1.1 OT .............................................................. 6
    2.1.2 ICS ............................................................. 6
    2.1.3 SCADA .......................................................... 6
    2.1.4 DCS ............................................................. 7
    2.1.5 PLC ............................................................. 7
    2.1.6 HMI ............................................................. 7
    2.1.7 Legacy Systems ............................................... 8
    2.1.8 Vendors ....................................................... 9
  2.2 Network Architecture in Industrial Systems ....................... 10
    2.2.1 Purdue Model ................................................. 10
    2.2.2 ICS Protocols ............................................... 10
    2.2.3 Remote Access .............................................. 12
  2.3 Industry 4.0 ...................................................... 13
    2.3.1 Historical Context ........................................... 13
2.3.2 Industry 4.0 Attack Scenarios and Challenges ............. 18
2.3.3 ENISA Challenges ............................................. 21
2.4 Relevant Frameworks and Documents ....................... 23
  2.4.1 NIST ......................................................... 23
  2.4.2 ENISA ......................................................... 26
  2.4.3 ISA/IEC 62443 ................................................. 29

3 Method ................................................................. 30
  3.1 Research Background and Design ......................... 30
    3.1.1 Research Background .................................. 30
    3.1.2 Research Design ......................................... 31
  3.2 Case study ..................................................... 32
    3.2.1 Overview ................................................. 33
    3.2.2 Procedures ............................................... 33
    3.2.3 Questions ................................................. 35
    3.2.4 Reporting .................................................. 35
    3.2.5 Confirming Findings .................................... 36
  3.3 Trustworthiness of the Study ............................ 37
    3.3.1 Generalizability .......................................... 37

4 Study Analyses and Results .................................... 39
  4.1 People ......................................................... 40
    4.1.1 Management ............................................... 40
    4.1.2 Defining an IT/OT Cybersecurity Team .......... 43
    4.1.3 Security Awareness Training ........................ 46
  4.2 Processes ...................................................... 49
    4.2.1 Asset Management ......................................... 49
    4.2.2 Risk Management .......................................... 54
    4.2.3 Vendor and Third Party Agreements ............... 59
  4.3 Technology ..................................................... 61
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Relationship between OT components</td>
<td>8</td>
</tr>
<tr>
<td>2.2</td>
<td>Purdue model</td>
<td>11</td>
</tr>
<tr>
<td>2.3</td>
<td>The four industrial revolutions</td>
<td>14</td>
</tr>
<tr>
<td>3.1</td>
<td>Methodology for structuring the case study</td>
<td>36</td>
</tr>
<tr>
<td>4.1</td>
<td>Asset Management Process</td>
<td>54</td>
</tr>
<tr>
<td>4.2</td>
<td>Risk Management process</td>
<td>57</td>
</tr>
<tr>
<td>4.3</td>
<td>Proposed High-reference model from ENISA</td>
<td>64</td>
</tr>
<tr>
<td>4.4</td>
<td>Network architecture design with remote access solution</td>
<td>70</td>
</tr>
</tbody>
</table>
List of Tables

2.1 Table showing the differences between IT and OT . . . . . . . . . 15

4.1 Table for challenges, attack scenarios and recommendations . . . 92
Chapter 1

Introduction

1.1 Motivation

In Norway, approximately six percent of the economic growth is generated by industrial companies. This number is expected to increase within 2030 \[29\]. To succeed, the industry will have to adopt to the fourth industrial revolution with its new technology solutions. This gives many new possibilities, but also creates new concerns regarding cybersecurity.

Historically, Operational Technology (OT) and Industrial Control System (ICS) were designed with few security controls, and one leaned on security by obscurity. When Information Technology (IT) components now are being integrated into these systems as a part of the new industrial revolution, the productivity will increase, but the systems will also be more vulnerable to outside attacks.

Protecting workers and the environment from technical failures or accidents caused by humans has been the main focus in industrial companies for a long time. The safety at plants is especially important as it can have catastrophic outcomes if an incident is to happen. With new digital ways to enter the industrial systems, the safety can be compromised by adversaries. Attackers can
gain access to the network and take control over physical equipment. This can lead to loss of life, damage to the production or have environmental causes.

IBM [48] reports that manufacturing replaced financial services as the most attacked industry in 2021. 61% of incidents at OT-connected organizations last year were in the manufacturing industry. One also saw increased reconnaissance by attackers of SCADA Modbus OT devices accessible via the internet.

In order to take up the fight against adversaries exploiting OT environments, industrial companies and manufactures need to have efficient cybersecurity strategies. IT employees will have to work together with OT employees to combat the challenges and secure the systems. There will not be a question whether one will be attacked, but rather when one will be attacked.

1.2 Scope and Research Question

This thesis aims to look into cybersecurity in manufacturing industries when approaching the fourth industrial revolution. The difference between cybersecurity and information security is therefore important to address. Information security is defined as the protection of the information’s confidentiality, integrity and availability, often referred to as the CIA-triad. In this case, the information can be data, IT-systems, infrastructure, configurations, software, applications or even human resources [27].

When it comes to cybersecurity, the definition varies more, but according to NIST [41] cybersecurity is “The ability to protect or defend the use of cyberspace from cyber-attacks”. While both expressions are suitable for this thesis, the decision to use the term cybersecurity was made as it is more used in the OT field.

Two research questions were designed to limit the scope of this thesis. The
questions lay the foundation of the main part of this thesis, mainly chapter 4. They are the following:

RQ1: How can industrial companies secure themselves against threats related to Industry 4.0?

RQ2: How can one link security recommendations to relevant challenges and attack scenarios for Industry 4.0?

The thesis will look into cybersecurity in industrial systems in manufacturing. The goal is to give security recommendations within some main areas to better prepare oneself for cybersecurity incidents.

The recommendations will then be connected to relevant challenges and attack scenarios related to Industry 4.0 in order to show the possibility to mitigate some of the risks these challenges and attacks rise.

1.3 Contribution

The thesis contributes with an insight to cybersecurity in industrial systems, specifically in the manufacturing industry. The insight has been gained through project work, meetings, semi-structured interviews and state-of-the-art documents.

In contrast to the oil, gas and power sector in Norway, cybersecurity is often down prioritized in manufacturing. The goal of this thesis is therefore to enlighten how these companies can take measures to protect themselves. The thesis aims to give a proper background for the recommendations, differing from many frameworks and documents with just listed recommendations. The document intends to be easily understandable for people with minor knowledge of cybersecurity.
To understand why one is to spend resources on security controls and counter measures, one also has to understand the threat picture. Therefore, the recommendations has been connected to Industry 4.0 specific challenges and attack scenarios.
Chapter 2

Background

This chapter provides background information about operational technology and security. Section 2.1 addresses the most common components of an industrial system. Section 2.2 presents traditional network architecture in industrial systems. Section 2.3 gives information about Industry 4.0 and challenges and attack scenarios related to the fourth industrial revolution. Finally, section 2.4 presents some relevant frameworks and documents for industrial systems.

2.1 Industrial Systems

The terms OT, ICS, and SCADA are often mixed and can be challenging to differentiate. To understand the uniqueness of the field, some clarifications are necessary. The following section will describe some of the foundational components in these systems. Figure 2.1 provides a visual description of the relation between the terms.
2.1.1 OT

OT stands for operational technology. The term is used for computer systems that are being used to manage industrial operations and can be found in all industrial sectors such as electric power, water services, manufacturing, and waste handling [16].

2.1.2 ICS

Industrial Control Systems (ICS) is one of the major segments within operational technology. The goal of the ICS is to control and monitor physical processes at an industrial site [18]. To do so, ICS uses various types of components such as sensors, controllers, and actuators. ICS typically controls processes related to critical infrastructure and therefore comes with a high-availability requirement. [28].

2.1.3 SCADA

SCADA is a type of ICS that is used to control assets with the need to be spread over thousands of square kilometers. There are four main functions of a SCADA system. Firstly, it is designed to collect field data. The data is coming in from different field devices, protocols, and sensors. Secondly, the system needs to facilitate communication between assets. This happens through specific communication protocols later described in this paper. To make monitoring easier for the operator, the SCADA system also needs to present the information either graphically or textually in a readable way. Lastly, it must allow the operator to monitor and control the entire system from a central location in real-time. Depending on the setup of the system, individual operations or tasks can either be controlled automatically or by operator commands [15].
2.1.4 DCS

A Distributed Control System (DCS) is a process-driven system. Where the SCADA system aims to collect and present data from a site, the DCS is supposed to monitor and supervise controllers, sensors, and actuators spread across the plant. The DCS often contains multiple Programmable Logic Controllers (PLCs) that are used to control specific applications or processes, such as power plant soot blower controls [15]. Through communication networks, the PLCs send data to the distributed control system, where it is monitored, before eventually being sent to the SCADA system [23].

2.1.5 PLC

Programmable Logic Controllers (PLCs) are small devices that control and monitor physical industrial infrastructures such as gas pipelines, power generation, and water management. They work closely with sensors and actuators, and together they make the foundation for industrial processes at a field site. In a gas pipeline, a PLC can be used to monitor the gas pressure. If the pressure is more than a given threshold, the PLC will communicate this to an actuator which will release some gas to get the pressure down in the pipe. The PLC is not always process-specific but can be configured and programmed at a workstation to fit its purpose. In many cases, the PLC has vendor-specific programming software to write the logic that defines the control of the physical process [1].

2.1.6 HMI

Human Machine Interfaces (HMIs) present the data coming in from PLCs in such a way that it is easy for operating personnel to monitor and control the processes on site. They allow the operators to start and stop processes, set cycles, adjust thresholds, and interact with the control processes. Before
HMIs, this was done by physically activating switches, controls, and dials.

Making a software-based interface decreased the work and made it easier to have a good overview of all the controls and processes on the plant. The user interface graphically presents the processes that are being controlled, including sensors, active pumps, output states, and motors in motion. As many different devices can connect to the HMI, small plants may only need one, as for bigger manufacturers, one often has multiple HMIs interacting with each other [28]

2.1.7 Legacy Systems

Due to the high availability and up-time requirement in industrial systems, maintenance and replacement of old equipment is often postponed. This results in legacy systems that are not updated nor patched but often have well-
documented vulnerabilities that may be easy to exploit. Historically, this was not a problem as the industrial environment was not connected to the network, but as the field develops and the devices are connecting to the internet and cloud-based services, the potential threat of someone compromising the system increases [22].

The systems often lack access controls, user authentication, and monitoring capabilities. Being made at a time when security testing was not commonly done, many of them might also have unknown vulnerabilities and backdoors. This, together with the fact that the equipment is not broadly used outside the OT field and the lack of OT security expertise, make them vulnerable to modern attacks [22].

2.1.8 Vendors

Where IT environments often can outsource business operations and processes connected to storage and automation, OT environments are in many cases dependent on the system vendor. As the equipment for industrial systems can be narrow and very specified, vendor lock-in is not uncommon. In contrast to IT vendors, it is not unusual for the industrial vendor to have direct access to critical systems or the manufacturing plant [22].

In some cases, this is written in the vendors’ contracts to assure valid product warranties. This can be beneficial for the industrial company as the vendor can remotely manage the systems and alert the company in case of troubling situations. The contract between the vendor and the customer often describes management requirements and equipment monitoring but, in many cases, fails to address questions regarding security [22].
2.2 Network Architecture in Industrial Systems

This section will provide some information about ICS-specific network architecture, network protocols, and the use of remote access.

2.2.1 Purdue Model

Historically, many ICS environments have used the Purdue model when designing their network architecture. The model consists of five levels [33]. Generally speaking, level 0-3 is recognized as OT zones, and level 4-5 is considered IT zones. Each zone represents a point separation, meaning that connections between zones are highly controlled, separated by firewalls. A common practice is to have restricted access to level 3 from level 4-5. From the bottom up, the lower levels are not interacting with level 4-5, but these are instead communicating with level 2-3. The IT zones are separated from the OT zones by an industrial Militarized Zone, which accommodates for untrusted communication between IT and OT. Figure 2.2 shows a possible implementation of the Purdue model. With the IT/OT convergence, the need for communication from the OT levels and up to the higher enterprise levels will be necessary, and the need for a secure, layered model will emerge [33].

2.2.2 ICS Protocols

To make the Industrial Control System useful and efficient, communication between all the devices and subsystems is crucial. Fast communication is facilitated with the help of well-structured communication protocols. Many of the protocols were designed at a time when security was not in focus [31]. Some common security issues included lack of authentication between endpoints, no way to secure data in transit or at rest, and insufficient methods to specify recipients. Another issue with the protocols is that the structure is
Figure 2.2: Purdue model. Based on figure from [49].

often publicly available online. When vendors first started selling them, the purpose was not for them to be broadcasted. To ensure interoperability and ease the job of constructing industrial control systems, they were published. This makes it easier for malicious actors to compromise the protocols and, in that way, gain access and control over the system [31].

One of the most common protocols is a master/slave protocol named Modbus. It has been in use since the 1970s and was created by the first programmable logic controller vendor, Modicon. Modbus is one of the most used protocols in
the ICS industry, and it is still developing through the Modbus Organization [28]. The original version of the protocol transmitted data over serial lines, but after the industrial Ethernet appeared, Modbus TCP/IP was developed. The original version was a typical master/slave protocol where one master could control the data transactions from 247 slaves responding to the master's request. Today, it uses a client/server architecture, and data transactions are directed from a Modbus client (master) to a Modbus server (slave) via an IP address. With the rapid development in technology, the need for different types of Modbus emerged. Some of these types include Serial RTU, Serial ASCII, and UDP/IP [47]

2.2.3 Remote Access

Not only are protocols a challenge within OT. Remote access is also proven to be difficult. Maintenance engineers, vendors, and operators need access at all times in case there is a problem with the system. Often, the problem needs to be fixed right away due to the high-availability requirement [31]. To do so, most organizations use a Virtual Private Network (VPN) to connect to the ICS from remote locations. A direct, secure VPN connection will require at the minimum two-factor authentication and solid control of authorization. If this is not implemented, the organization may face problems with too many people having access to the ICS system. When one first is inside the domain, there are often little to no controls regarding malicious software or suspicious activity. This means adversaries have the option to launch toolkit packages to create a persistent way into the system to later spread malware or perform other attacks [31]
2.3 Industry 4.0

With Industry 4.0, the field is moving towards even less human interaction, decentralized production, and more intelligent manufacturing based on large amounts of data [50]. The traditional ICS systems and OT technology will change. This section provides some insight to those changes.

2.3.1 Historical Context

Approaching Industry 4.0 marks an end to the last industrial revolutions, as shown in figure 2.3. A short summary of the four will now be given.

Water and steam enabled the first industrial revolution, leading to mass production [24]. This happened during the late 18th century and allowed goods to be produced without purely using humans or animals. This was followed by the second industrial revolution in the late 19th century. Taking advantage of oil, gas, and electric power as well as more advanced communications, mass production and some level of automation were introduced. In the middle of the 20th century, the third industrial revolution added computers, advanced telecommunications as well as data analysis to the factories. To help automate the process, devices like PLCs, HMIs, and SCADA systems were added [24].

One is now moving into the fourth industrial revolution, also known as Industry 4.0. Smart machines and factories will emerge, and valuable data from internet-connected systems will help produce goods efficiently. Information transparency will increase as data from the factory floor combined with enterprise operational data will be merged. This will help making better decisions for the manufacturers both in terms of production and hopefully also within cybersecurity. The field is moving towards even less human interaction, decentralized production, and more intelligent manufacturing based on large amounts of data [50].

13
The new industrial revolution will change industrial systems drastically. The new PLCs use more common OS and internet protocols. New IT devices like smartphones can connect directly to field devices and get real-time data instantly. Internet of Industrial things (IIoT) will make it possible to connect more devices and let them communicate with each other without human interaction. Together with cloud solutions, this will erase the historically clear boundary between OT equipment and IT equipment.

**The IT/OT Convergence**

One of the main aspects of Industry 4.0 is the convergence between IT and OT. How these two merge in the coming years will be revolutionary for industrial systems. But in order to understand how this merge is significant, the different nature of the two fields should be pointed out. The presented table 2.1 shows the main differences pointed out by Huba [12] between the IT field and the OT field.
Table 2.1: Table showing the differences between IT and OT

<table>
<thead>
<tr>
<th>Feature</th>
<th>IT</th>
<th>OT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary function</td>
<td>Process data efficiently to produce and store information valuable to the organization, often using commonly known software and hardware</td>
<td>Monitor and control physical processes with the use of rather a field-specific hardware and software equipment</td>
</tr>
<tr>
<td>Types of common systems and equipment</td>
<td>PCs, servers, TCP networks, applications, tablets, smartphones</td>
<td>PLC, DCS, SCADA, Industrial networks, servers, sensors, cameras, and robots.</td>
</tr>
<tr>
<td>Expectations</td>
<td>Systems fitting the need of the organization and employees, high-bandwidth, delays not great but accepted, back-up acceptable</td>
<td>24/7 control and monitoring systems, low-bandwidth, real-time data, redundancy, downtime unacceptable</td>
</tr>
<tr>
<td>Expectations</td>
<td>Systems fitting the need of the organization and employees, high-bandwidth, delays not great but accepted, back-up acceptable</td>
<td>24/7 control and monitoring systems, low-bandwidth, real-time data, redundancy, downtime unacceptable</td>
</tr>
</tbody>
</table>
Focus areas

- Focus on confidentiality, integrity, and availability.
- Focus on safety and availability. Safety due to possible fatal consequences and loss of human life if something goes wrong. Availability due to the need for constant production.

Incident handling

- With so many things connected to the internet, incident handling is common. Not unusual to handle small to medium incidents every month.
- Historically, few connections to the internet. Not that many incidents, but when something first happens, incidents can be very destructive.

Patching and updating

- Frequently patching and updating all the time. Relatively easily done without affecting too much of the work or employees.
- Patching and updating is rare and might just be done once a year as it often requires a stop in production.

Despite the main differences pointed out in the table above, the two fields will intertwine with Industry 4.0. The ongoing revolution is pushing intelligent autonomous manufacturing equipment and systems to industrial companies. This is done by applying domain expertise within OT companies with IT technologies. These technologies include artificial intelligence, cyber-physical systems, cloud systems, and IIoT. A short description of these technologies will now be given.
Cyber-Physical Systems

According to the NIST Special Publication 1500-201 for Framework for Cyber-Physical Systems [39], CPS are smart systems that include engineered interacting networks of physical and computational components (NIST). The system consists of both IT and OT technology and is fundamental when moving from Industry 3.0 to Industry 4.0. It differs from today’s embedded systems and automated control process systems in a way where CPS can integrate software and hardware, and make it work in a way where it reacts, adapts, and respond to the environment without human interaction [3].

Industrial Internet of Things (IIoT)

IIoT stands for Industrial Internet of Things. A simple definition of IIoT would be the Internet of Things components used in an industrial environment. By this, one excludes typical IoT devices such as smartwatches and smart TVs and focuses on industrial components connected to the internet.

However, as pointed out by Boyes et al. [6] this might not be sufficient. More thoroughly, IIoT is a system made up of internet-connected objects, cyber-physical assets, IT, and possible cloud or computing edge platforms. These empower real-time and autonomous access, communications, and exchange of information. This again increases production value in the forms of product delivery, increased production, and reduced energy consumption [6]. This differs from today’s PLCs and RTUs through being very easy to connect to the internet and thus making it easy to retain real-time data.

Cloud

Cloud-based manufacturing is a relatively new concept. Physical devices, machines, products, and processes can transform into cloud entities. This is called
virtualization and enables the devices to share their own statues and information with the cloud. The information can be used for the optimization of the manufacturing process. It can also help the security work as more data will be visible, and attacks can be cached earlier [11].

2.3.2 Industry 4.0 Attack Scenarios and Challenges

To understand how to protect industrial systems in the Industry 4.0 era, the field needs to know what attacks to possibly encounter. As the era evolves, the attacks will change continuously, as will the knowledge of how to protect the systems. However, it is important to start identifying possible attack scenarios with the information one has now, to be better protected against common attacks, as well as to start building a knowledge base of Industry 4.0 attacks within the field.

The European Union Agency for Network and Information Security (ENISA) works with security experts in the EU, EU’s member states, the private sector, and Europe’s citizens. ENISA develops advice and recommendations on good practice in information security based on the work with these groups [36]. From the report “Good practices for security of Internet of Things in the context of Smart Manufacturing” [36], ENISA provides 12 attack scenarios specifically designed for Industry 4.0. Each attack has been assessed with a criticality level of either not important, low, medium, high or crucial. A summary of the 12 possible attack scenarios will now be given.

AS1 Attack on the connection between controllers (DCS, PLC) and the actuators. An attacker can make use of a compromised system and send data of executed code through lines that are not monitored. This causes loss of control in the systems as well as damage to the manufac-
turing process or infrastructure.
Criticality level: High.

**AS2 Attack targeting sensors.** An attacker can get control over sensors and manipulate the data or the configuration at the endpoints. Manipulating important measures can cause wrong operator decisions. It can also cause problems regarding legal emission levels.
Criticality level: High.

**AS3 Attacks targeting actuators.** Manipulating the actuators through modifying configurations and causing disruption in their normal behavior. This can affect the production process.
Criticality level: High - Crucial.

**AS4 Attack on the information transferred over the network.** Manipulating data in the lower layers of the OSI model (2-4), but let data values in upper layers (5-7) seem correct. Can affect the production process.
Criticality level: High - Crucial.

**AS5 Attack against the IIoT gateways.** An attacker can compromise IIoT devices in the industrial system. Efficient and successful if the devices have vulnerable protocols or default passwords. Possible to gain access to the network and therefore get access to subsystems, devices, and other equipment.
Criticality level: High – Crucial.

**AS6 Control of remote controllers.** For larger environments with remote plants, an attacker can compromise devices used to control the local processes far away from the distributed control system. Could possibly get access to the network and cause damage to the industrial process. Access to devices and tools as well as the system and the control layer.
Criticality level: High.
**AS7** **Attack targeting Safety Instrumental Systems.** A highly dangerous attack that affects the environment and/or the safety of human lives. It can lead to destruction or interruption of the industrial process. Defecting the SIS system which can affect other systems and operations and cause great harm to humans or the environment.
Criticality level: Crucial.

**AS8** **Malware.** A well-known attack is causing malicious software to spread in the network and by that give access to systems or data. Possible for the attacker to take control over crucial IIoT devices, e.g., measuring temperature and emission.
Criticality level: High.

**AS9** **DDoS attacks with the use botnets.** The attacker can use IIoT devices as a botnet to attack other devices. This is possible if the IIoT devices are vulnerable in terms of default protocols or weak passwords. Target devices are being flooded with malicious traffic and goes down.
Criticality level: Medium - High.

**AS10** **Stepping stones attack.** Attackers can compromise intermediary hosts and use this to mask themselves during intrusion of networks. Possible to compromise many hosts and use them as stepping stones for future attacks.
Criticality level: Medium.

**AS11** **Social Engineering attacks.** Attackers can gather information, get unauthorized access to the system, manipulate employees or place malicious devices in the system. Can let the attacker have a way into the system, gain high privileges to a system or steal internal company data such as crisis plans.
Criticality level: High.
AS12 Attacks using Artificial Intelligence Technologies. Gathers a lot of what seems to be uninteresting data and uses AI to comprehend the data and find a hole in the security. Can target people with high privilege, such as administrators, to gain the right type of data. Can be the first attack in an attack chain. Criticality level: Medium - High.

2.3.3 ENISA Challenges

In the same report [36], ENISA provides 12 challenges specifically targeted toward Industry 4.0. For a company that is about to transition into Industry 4.0, being aware of these challenges is important. A summary of the 12 challenges will now be given.

C1 Vulnerable components. The fourth industrial revolution will bring millions of connected IoT devices to industrial companies. As one no longer looks at ICS systems as isolated islands, IT and OT security have to be implemented alongside physical safety. When shifting to a more interconnected system, the security of the devices will play an important role. As most ICS systems were not designed with cybersecurity in mind, the vulnerabilities these devices might possess will be crucial to detect and protect against.

C2 Management of processes. Managing the processes within an industrial system with cybersecurity in mind will be challenging. As production efficiency has had a higher priority than cybersecurity for a long time, a change of thoughts will be necessary. Good management with security in mind for people, processes, and technology will be an advantage.

C3 Increased connectivity. Collaboration between the systems of different plants will be necessary. For some industrial companies, this also
involves collaboration across multiple organizations and countries. This can be a safety and security issue if not handled with care.

**C4 IT/OT convergence.** Managing IT/OT integration is a remarkable challenge. This is because it will utilize insecure network connections, use technologies with known vulnerabilities, and have too little knowledge of requirements for ICS environments.

**C5 Supply chain complexity.** The length of the supply chain will increase massively when adding new devices and solutions. Keeping track of the security controls in all the devices, and especially if parts of the device are from a third party, will be challenging.

**C6 Legacy industrial control systems.** Legacy systems in OT are a major challenge. With Industry 4.0, adding IoT devices to outdated systems may give adversaries new ways to attack the system.

**C7 Insecure protocols.** Legacy ICS systems already struggle with insecure and outdated protocols. With new IIoT devices and multiple protocols, this will add to the challenge. Many of these protocols fail to ensure proper protection and are, therefore, a target for cyber-attacks.

**C8 Human factors.** Workers adapting to the new systems and having to handle new types of data, devices, and networks can easily be targets if they do not know the value of their knowledge.

**C9 Unused functionalities.** Industrial devices do often come with multiple functions and services. As they may not all be relevant for the specific tasks, unused, insecure functions can expand the threat picture and give the adversaries another way into the system.

**C10 Safety aspects.** The ICS system, with its actuators, performs tasks on physical systems and is thus important for the safety aspect. Merging
security with safety becomes important as security threats can influence the safety of workers and the environment.

**C11 Security updates.** Updating IoT devices is a major challenge as it often does not allow traditional update mechanisms. Trying to secure the technology behind the updating mechanism is hard. This adds to the challenge of updating existing OT equipment, especially since it often has to happen during downtime.

**C12 Secure product lifecycle.** Device security should be highly prioritized throughout the entire device's lifecycle, including end-of-life or end-of-support.

### 2.4 Relevant Frameworks and Documents

To efficiently and securely shift from Industry 3.0 to Industry 4.0, a company needs guidance and strategies on how to do so. There are already some frameworks, recommendations, and cyber programs that are used today. The next chapter will give a summary of these and explain how well they will fit in Industry 4.0.

#### 2.4.1 NIST

The National Institute of Standards and Technology (NIST) is a part of the U.S. Department of Commerce [37]. Its mission is to promote U.S. innovation and industrial competitiveness. This is partly done through creating critical measurement solutions, and equitable standards. They are recognized for their SP-800 series frameworks on security [37]. Two of their publications relevant to this thesis will now be summarized.

23
Guide to Industrial Control Systems (ICS) Security

In 2015, NIST published a comprehensive guide as to how secure ICS systems [19]. The guide starts off by giving an introduction to ICS systems and components. When the foundation has been outlined, they propose a risk management process described in section 4.2.2 in this thesis. The next chapter discusses security program development and how one can define and train with business cases. Further, the guide discusses ICS-specific security architecture before giving a guide on how to implement security controls [19].

The guide is broad and designed for many types of companies operating industrial control systems. As it was designed in 2015, it does not touch upon how Industry 4.0 will affect the recommendations. Technologies for the next revolution are not mentioned, but the security foundation the guide gives is thoroughly and still highly relevant.

Cybersecurity Framework Manufacturing Profile

In 2017, NIST created a Cybersecurity Framework [34] with implementation details for the manufacturing sector. This framework is based on the original NIST cybersecurity framework, but one saw the need for a specification for manufactures. The framework is risk-based and uses industry standards and the best practices to construct a common language for the industry. It was formed through collaboration with both the private sector and the government [34].

To make it easy for the industry to use, NIST created the framework in such a way that it is easy to make a “Target” Profile. The Target Profile represents the desired state of cybersecurity for the organization and can be compared with the organization’s Current Profile, meaning the outcomes from the frameworks that represent the current cybersecurity state.
Comparing the two profiles (Current and Target) can help to identify improvements and goals, as well as make it easier to set priorities for cybersecurity. The Profile contains a Framework Core with specific practices. The Core consist of five functions – Identify, Protect, Detect, Respond and Recover. For each Function, there are multiple Categories and Subcategories.

The first Function is Identify. The purpose of the function is to create an organizational understanding of cybersecurity risk connected to systems, data, assets, and capabilities. This builds a foundation for the business context and helps the business prioritize resources so it aligns with their risk management. The second function, Protect, identifies different protection mechanisms. This is critical to limit the impact of a cybersecurity event. The third category is called Detect and covers the implementation of different activities to help the organization detect and identify any ongoing cybersecurity event. The goal of this category is to lower the amount of time from a security incident happens to action taken.

The fourth function is Respond. This function was created with the purpose of the organization being able to take action in case of a cybersecurity incident. The last function is the Recover function. This was created to let the organization develop and implement activities to rebuild themselves after a cybersecurity event. The goal is to as soon as possible restore to normal function and reduces the impact of the incident [34].

The framework is comprehensive and covers many different areas. It was designed for manufacturers wanting to improve their cybersecurity. As it was created in 2017, the newest technologies like cloud and IIoT are not mentioned. The framework does however, cover many of the core principles of securing ICS systems and will therefore be relevant also in the coming years.
2.4.2 ENISA

ENISA has given out multiple documents regarding information and cybersecurity. Two of the documents especially relevant for Industry 4.0 will now be given a short summary.

**Good Practices for Security of Internet of Things in the context of Smart Manufacturing**

Good Practices for Security of Internet of Things in the context of Smart Manufacturing [36] was released by ENISA in May 2018. Its focus is on how IoT/IIoT devices can be secured in new Smart Manufacturing systems. It presents the challenges and attack scenarios connected to Industry 4.0 presented earlier in this chapter. It gives recommendations within the categories of Policies, Organisational practices, and Technical practices. Each of the three categories have subcategories with bullet point recommendations [36].

It is an extensive document with very many relevant recommendations. To be able to fully understand all the recommendations, previous knowledge about security in industrial systems is needed. The bullet points do not give any further explanation, and thus many readers might be challenged. As the document does provide a very good overview based on many different existing frameworks and the best practices in the field, it was used as an inspiration for parts of this thesis.

**Industry 4.0 - Cybersecurity Challenges and Recommendations**

In May 2019, ENISA released their report Industry 4.0 Cybersecurity: Challenges & Recommendations [13]. The aim of the report is to list recommendations regarding cybersecurity and Industry 4.0, as well as to contribute to the enhancement of Industry 4.0 across Europe. The paper is divided into three
sections; People, Processes, and Technologies, each with different recommendations and corresponding stakeholder groups to be associated with [13].

The People category consists of two challenges and corresponding recommendations. The first challenge is the “Need to foster and align IT/OT security expertise and awareness.” When the industry now heads into a new area, competence is needed. Today, there is a lack of specialist who knows both the OT field and the IT field. For the transition into Industry 4.0 to be successful, employees need skills regarding detecting anomalies in the systems, knowledge of how to use security features in components, and knowledge of new protocols regarding Industry 4.0. Moreover, the need for specialized security awareness training in both the IT and OT field is needed.

The second challenge is called “Incomplete Organizational policies and reluctance to fund security.” The organizations are in different stages of the Industry 4.0 adaption, but common for most of them is that there are little to no policies or cyber programs stating how to ensure both safety and security when implementing new technologies. From a board level, cybersecurity is often looked at as costly without contributing much to profit-making; thus, it is being dismissed. Investing in cybersecurity could be beneficial for the organization as it would not only prevent or decrease the outcome of a cybersecurity event but also make the organization more attractive and give it competitive advantages.

The Process category consists of three challenges with corresponding recommendations. “Liability over Industry 4.0 products’ lifecycle is poorly defined” is the first challenge ENISA address in this category. Due to the complexity of Industry 4.0 systems with OT devices, IIoT devices, cloud solutions, and cyber-physical systems, the question of where the liability lies can be difficult. Responsibility can be divided between developers, end users, manufacturers, vendors, or support operators.
The second challenge in the Process category, “Harmonize efforts on Industry 4.0 security standards,” states that standards and initiatives for the manufacturing sector regarding Industry 4.0 are rather divided. There are many articles regarding IoT and cybersecurity, but there is a lack of defined standards specifically designed for Industry 4.0 and Cyber-Physical systems. ENISA recommends comparing the standards and guidelines to make sure all requirements and activities are covered.

The last challenge addresses the complexity of supply chain management. Industry 4.0 will require many assets, vendors, and technologies. It will be important to have a holistic approach when securing the systems. Securing only parts of a longer supply chain will not be sufficient; therefore, end-to-end decryption will be essential for Industry 4.0.

The Technology category includes two challenges. The first is “Interoperability of industry 4.0 devices, platforms, and frameworks”. One of the main goals of Industry 4.0 is automatic information flow between different devices. To make this work, one must ensure good interoperability between new IIoT components and legacy systems. This also requires the systems to have the same baseline of security, making sure that the cybersecurity is strong across the entire chain.

The last challenge is “Technical constraints hampering security in industry 4.0 and smart manufacturing”. It has been proven difficult to ensure security in embedded systems with both legacy systems and Industry 4.0 components. Especially low-end devices such as ICSs and PLCs lack advanced security measures like authentication or encryption. Today, there are not enough Industry 4.0-specific tools that are dedicated to cybersecurity within Industry 4.0, and those that exist are often expensive. New tools to ensure OT security have increased, but not all of them are compatible with new smart devices.
The document provides a good overview of some of the challenges connected to Industry 4.0 and recommendations for how to solve them. They enlighten challenges for both legal entities, vendors of Industry 4.0 equipment, leaders, and education systems. It is rather broad as it is aimed at many different people and sectors. This gives an important view of the new revolution but is not specific enough for leaders or companies to use.

2.4.3 ISA/IEC 62443

IEC 62443 is a well-know cybersecurity standard for industrial control systems [25]. The standard was developed by the ISA99 committee of the International Society, and Automation after many rounds of input from different field-specific groups and stakeholders [46]. The standard is divided into four groups with corresponding documents with more in-depth information. The four groups are General, Policies and Procedures, System Level requirements, and Component Level requirements. The standard is being updated continuously and is likely to accommodate for the new industrial revolution in the next years [25].
Chapter 3

Method

This chapter presents the methodologies used in this thesis. Section 3.1 clarifies the purpose and the design of the research. As a case study was used as the main method, this is presented in section 3.2. Section 3.3 studies ethics and validity in connection to thesis work.

3.1 Research Background and Design

3.1.1 Research Background

To explore the possibilities for writing a master thesis about cybersecurity in industrial systems, Norway’s leading telecommunications company Telenor was contacted. As they were currently conducting a project to upgrade cybersecurity within an industrial company in Oslo, it was a good opportunity to participate and learn from this project.

The project was initiated by the industrial company in Oslo in 2020. One saw the need to upgrade the cybersecurity in order to accommodate for technologies like cloud computing, IIoT, and remote access. As the company itself did not have the competence and knowledge needed, Telenor was approached. The
The telecommunication company has recently started a bigger project where they aim to help secure industrial companies in Norway. The main focus areas are providing better network security, helping with risk management, establishing a Cybersecurity Operation Center (SOC) for industrial companies, and helping with the overall process of upgrading the cybersecurity. As they work with many different industrial companies in Norway, there insight is valuable. Discussing the security situation in these companies and how this relates to the industrial company in Oslo has been done through the research process in order to do some comparisons.

To see how the project between Telenor and the industrial company could benefit this thesis, a meeting was arranged in May 2021. It became clear that the project was of interest, and the opportunity to participate in both internal meetings in the company as well as the project meetings were given. Having the chance to follow the project process closely during the fall and gaining knowledge about the needs of the industry resulted in the topic for this thesis.

### 3.1.2 Research Design

When choosing the research method, different options were considered. As the qualitative method includes non-numeric data like observations of interactions and in-depth interviews, this seemed like a good approach in contrast to collecting quantitative data through, for example, using surveys [20]. Qualitative research also reflects the opinions and feelings of the people participating in the study. As cybersecurity is as much of a people and process topic as a technological topic, having different thoughts and points of view seemed important.

Furthermore, studying a group or individual using a case study method is often suitable, especially when having a defined group of interest, such as the
participants in the industrial company’s cybersecurity project. The final plan for the thesis, therefore, became to use the case study strategy and collect qualitative data using semi-structured interviews.

### 3.2 Case study

In his book, *Real World Research* Robson [40] discusses how a case study is a well-established research method suitable for deep studies of people or groups. Using this research method includes multiple ways of collecting data, with the qualitative method being one of the main techniques. Wanting to study employees, leaders, and experts working on the cybersecurity project, interviews seemed like a better option than surveys to gain in-depth information from multiple points of view. The main method for collecting data would therefore be through interviews, participating in meetings, reading internal project documents, and doing a literature review.

Robson [40] proposes a case study plan with four steps in order to structure the case study. The four phases are Overview, Procedures, Question, and Reporting. This methodological approach is supported by Hancock and Algoizzine in the book *Doing Case Study Research* [21]. In addition, they underline the importance of getting information from three different sources, those being Interviews, Observations, and Documents, in order to get a broader perspective. They also include a final phase called Confirming Findings. In this phase, one is to evaluate the work done together with experts from the field and link it to the findings of others. The case study was therefore approached using a mix of these methodologies, as shown in figure 3.2 and will now be presented.
3.2.1 Overview

This step covers background information about the project to give context. Investigating the issues, reading relevant papers, and discussing why the project should take place [40].

In the aspect of the thesis, this phase included writing a mandate, attached in the appendices [1] for the industrial company to understand my interests and the aim for following the project. This was done to set the right expectations for all the involved parties. An important part of the mandate was to limit the scope as the project was rather large. The agreement was, therefore, to only concentrate the thesis work around the most critical and technical industrial plant possessed by the company.

As the project between the industrial company and Telenor evolved, it became clear that the information to fulfill the original mandate was inaccessible, and the mandate and scope was changed to better fit both parties. The first step also included visiting the plant in order to understand the critical infrastructure and the company’s responsibility for the society in Oslo. Information about the company’s earlier cybersecurity strategies was investigated together with their company goals.

3.2.2 Procedures

According to Robson [40], this step should include major tasks in collecting the data, such as access arrangements, finding available resources, and scheduling data collection activities. Hancock and Algoizzine [21] recommend using interviews, observations, and documents when gathering the information. The interviews should follow an interview guide, be conducted in a neutral environment free of distractions, and interviewees must give their consent. When gathering data from observations, it is important to identify what one is to
look into in order to answer research questions. The researcher should not be disturbing when observing. Using documents as a resource is a good way to conduct data, as long as it is reliable and based on facts.

The data collecting for this thesis was mainly done through arranging interviews, participating in weekly meetings, creating a literature review database, and reading internal project documents. The interviews were conducted by Zoom and Microsoft Teams due to the Corona situation, and the surroundings were therefore not in the researcher’s control. The interviews were semi-structured to create some room for impulse questions and answers. They followed an interview guide where the aim was to start by asking some simple questions before moving into the central part with more in-depth questions, and then a round off with more simple questions again, as recommended by Robson [40].

In all, seven people from Telenor and the industrial company were formally interviewed. They all hold different positions within the companies but were all in a way connected to the project. The multiple positions and knowledge helped get a diverse view of the situation, as well as contribute to different aspects of the thesis. Interview guides were therefore constructed specifically for each person, depending on what position they hold and the information they would contribute with. These are attached in the appendices [2]. With their consent, the interviews were recorded. As they revealed company sensitive information, a decision to not attache the material was made. The data was noted and analyzed, and connected to the right subchapter and recommendations.

The observations were done mainly through participating in the internal meetings, in a more informal setting. The meetings were held three to four times a week depending on where in the project process the team was. Due to the pandemic situation, they were online. This was not necessarily a hindrance,
as it allowed the researcher to participate often. The aim was to not disturb the participants during the meeting and rather ask questions afterward. The knowledge gained through the meetings was noted before being analyzed in the context of the interviews.

The internal documents reviewed in the data collection phase were given through an internal database. They were collected and structured after relevance before being analyzed. Some of the documents were old and were therefore considered outdated. More specifically, the documents written for the specific project were of more interest. These were stored securely, with limited access to others to provide confidentiality.

### 3.2.3 Questions

This section aims to answer the research questions using the sources outlined in the previous section. For the thesis, this meant to use the collected data, analyze it and answer the research questions raised in chapter[1] This phase also opened up for going back to the previous step, Procedures, if anything were unclear and needed to be discussed with participants from the company. This was done a multiple times in order to make sure that the information was correct. Specifically, a meeting was conducted between the researcher and the industrial company in January 2022. This was to discuss findings and make sure the information was correct. To answer the second research question and link the recommendations with the challenges and attack scenarios, knowledge from previous cybersecurity courses, experience from work and internships as well as incident reports were used.

### 3.2.4 Reporting

When the analyses were done, the reporting was initialized. Robson[40] states that the report may vary in length and content dependent on the audience. As
for this thesis, this meant writing a report in accordance with the master thesis format given by the University of Oslo. The focus on using understandable language, visual effects in the form of figures, and a clear structure was composed to make the thesis understandable for people with little knowledge of cybersecurity in the industrial sector.

3.2.5 Confirming Findings

As for the final part, Confirming Findings as addressed by Hancock and Algoizzine [21] was executed. This meant that the first draft of the thesis with its recommendations and connections to challenges and attack scenarios were discussed with the experts from the industrial company. The goal of gaining feedback from the participants is to gather their perceptions of the findings based on the information that they themselves provided. This part is important to ensure the information is correct as well as to gain some knowledge about how well the case study fits their perception of reality. Their feedback was noted and analyzed and is presented in chapter 5.

![Figure 3.1: Methodology for structuring the case study.](image-url)
3.3 Trustworthiness of the Study

3.3.1 Generalizability

According to Robson [40], generalizability is how well the findings can generally be applicable outside the specific study. As this thesis is only concentrated around a specific company, the generalizability can be questioned. One can ask if the findings are specific to this company and how the recommendations can be relevant for other industrial companies.

During the first phases of the thesis, it became clear that the oil and gas, as well as the power sector is quite good at cybersecurity. This was confirmed by one of the Telenor informants, and the reason behind this is strict laws and regulations in these sectors. However, the informant also pointed out that the industrial companies that Telenor is trying to help with cybersecurity now are often in the same place as the company in the case study. These are small to medium-sized companies within manufacturing and logistics and other smaller industrial operations. Common for them all is that they have little resources to secure themselves. One can therefore argue that the generalizability is taken into consideration but that a comparison of similar companies would have been preferred.

Reliability

Aiming for reliability should always be a goal; however, as Robson [40] points out, this can be hard in qualitative studies. If the results are to be reliable, they must be replicated and consistent over time so that the same results can be gathered later. This is not easy when interviewing people. Different interviewers can get various answers from the same informants, even when asking the same questions. This is due to the relation and setting that emerges when two people are talking. The answers may reflect the informant’s mood,
internal processes, or external events. This makes it hard to recreate the exact answers. Due to this, all interviews were recorded and stored together with a database of internal documents as well as state-of-the-art documents. This will not help recreate the data collection but can prove the way of working with the thesis.

This thesis aims to give neutral recommendations, and thus the focus has been on distinct personal thoughts and gathered knowledge from existing literature. However, this is not always easy as one might look for literature that supports one's conclusions or thoughts. This might lead to a halt in the literature search if one finds information that fits the objective. This will weaken the study and should be prevented. Hopefully, the thesis gives neutral recommendations based on the knowledge gathered in the case study as well as state-of-the-art papers.

Ethics

When joining the project, presenting the thesis project and its goals was always done before starting meetings or when new people entered the project. This was to ensure that everyone was comfortable with the situation and had the possibility to address topics they did not want to be stated in the thesis. This was important, but the team has been overly helpful and eager to discuss and share their knowledge with me.

When conducting the interviews, everyone was informed about it being recorded and had the possibility to withdraw their consent to both the recording as well as the information given. The information about the company stated in this thesis has been discussed and confirmed with the industrial company to ensure that no information is sensitive or somewhat wrong.
Chapter 4

Study Analyses and Results

This chapter will give recommendations on security aspects when moving from Industry 3.0 to Industry 4.0 in manufacturing. The chapter is divided into three categories People, Processes, and Technology, corresponding to the ENISA structure as explained in section 2.4.2. Each chapter has insights and findings from the case study on the industrial company. Quotes from the informants have been marked in blue. The recommendations are based on state-of-the-art research, insights from interviews, and knowledge gained from following the project.

Each subsection will also be tied to challenges and attack scenarios provided by ENISA from section 2.4.2. They are explained under "Related Challenges" and "Related attack scenarios" for each subcategory. This is done to show that some mitigation against these challenges and attacks can be taken if using the recommendations. The subsection with their belonging challenges and attack scenarios are summarized through a table at the end of the chapter.
4.1 People

Good security starts with people. The way management look at security will reflect the security in every part of the company. This section will provide some insight and guidelines on how to handle the next industrial revolution’s security requirements for the management as well as the workers.

4.1.1 Management

When interviewing IT and OT personnel in the industrial company, the first thing that stood out was the absence of focus on cybersecurity in the management. Many of the informants expressed the wish for a more interested and initiative taking management. The informants saw the need for securing both the IT and the OT side of the company but felt that this was not being prioritized by the leader group.

Talking to the operational leader in the leader group, he stated that they do what the municipality wants them to do regarding cybersecurity but that the knowledge of this topic was sparse in the management. This results in little interest and ad-hoc security projects that do not really fit together or make the overall security better as they are not aligned.

"I think the leader group look at (cyber) security with little knowledge, as it is a new way of thinking for us" - operational leader

Though cybersecurity knowledge was limited among the leaders, the company had taken some measures to improve its security. After a revision done by the municipality in 2015, one saw the need to organize the work connected to cybersecurity. To do so, the company created a one-person position whose tasks were to work with the organizational aspects of cyber security and increase the knowledge of this topic among other employees.
When interviewing this person, she stated that she loved her job but that she had too little knowledge of the field as she had no former competence. She clearly did everything she could when trying to raise security awareness, read upon standards, facilitate security projects with help from consultant companies, and more. However, she said that it was lonely, and she would have wanted a proper security team that had people with formal competence in both IT security and OT security in the company.

The industrial company is not alone in this matter. For many leaders, the focus has been on safety for a long time [7]. Security controls may seem too expensive, one lacks internal competence, and many leaders might find it difficult to understand how cybersecurity contributes to the production goals. The knowledge within the leader group is often limited, and this makes it hard to make good cybersecurity strategies [14]. When discussing the topic with Telenor employees, they stated that in many of their ongoing security projects, unknowing management was the greatest concern.

Learning from the security employee in the industrial company as well as the informants from Telenor, steps can be taken. First and foremost, leaders need to take responsibility and engage in cybersecurity. There should not be considered a problem having little knowledge about cybersecurity in the OT field, as long as one has the drive to admit this and are willing to learn. As a leader, it is important to remember that in the end, one cannot think that security is someone else’s responsibility, e.g., the vendors. Specific cybersecurity programs designed for business leaders in OT companies are yet to become common as pointed out by ENISA [13], but a good start is to take basic courses, attend conferences and conduct online learning regarding cybersecurity. To use this information and create a culture where cybersecurity thrives among the workers will beneficial.

As one adapts to Industry 4.0, there will be a growing community with the
need for education, discussion platforms, and information sharing. To share knowledge with people in similar sectors, engaging in creating cybersecurity communities in the same field will be important and something one should strive to participate in. There will also be a need to prioritize cybersecurity in budget processes, and set aside enough funding for the security projects.

**Related Challenges**

Managing the industrial process and personnel, as well as creating company goals with Industry 4.0 and cybersecurity in mind will be demanding, and C2 Management of process is therefore relevant. It will challenge the prioritization ability among leaders as production efficiency is usually seen as having a higher priority than cybersecurity. Having the right knowledge about the challenge of C4 IT/OT convergence and how this effects the security in ICS systems will be crucial. The challenge of gaining that knowledge together with knowing how to create a holistic security strategy for the system will be significant.

**Related Attack Scenarios**

When lacking the knowledge about how company information can be valuable to others; leaders, managers, and industrial workers are vulnerable to AS11 Social Engineering attacks and AS12 Highly personalized attacks using artificial intelligence. Both attacks aim to gather company sensitive information either through manipulation of people or using technologies to gather what seem like uninteresting data but, when mapped together, can give away important information about security and vulnerabilities at the plant or in the system. Building an organizational culture including cybersecurity and letting everyone in the company participate in cybersecurity work can help mitigate some of the risks connected to these attacks.
Recommendations

To overcome the challenge and reduce the risk of the overstated attack scenarios, the following recommendations are given.

- As a leader, take the responsibility to educate oneself through online courses and webinars. OT specific if possible, but general information security courses are also important.

- Build an organizational culture which includes cybersecurity.

- Budget for cybersecurity controls. It will cost, but an incident will most likely be more expensive.

- Let everyone participate in the cybersecurity work. A knowledgeable workforce is the first line of defense when mitigating an incident.

- Do not think that you can give out the security responsibility to everyone else. You are still the person who has the responsibility.

4.1.2 Defining an IT/OT Cybersecurity Team

When the management is knowledgeable and onboard about why to prioritize cybersecurity, they will need a strong team to actively implement the security.

Through conversations with the security employee in the industrial company, it became clear that there was room for improvement when it comes to collaboration between IT and OT regarding cybersecurity. The organizational model was constructed in a way where IT was having their own team, strategies, and ways of reporting to management. There was no similar team for OT, and cybersecurity was therefore not something the plant workers knew much about, and it resulted in the security employee trying her best to secure that side of the company. The concern for a common team was expressed by one of the long-time workers in the IT department.
”We need a security team consisting of both IT and OT personnel. They need to work together and should preferably sit in the office together. They have to exchange knowledge and report to the management.”

To construct such a team may not seem challenging, but it has proven to be more difficult than first thought. According to the report ”2021 State of Industrial Cybersecurity” by Dragos [26], the primary challenge when IT and OT are working together is cultural differences between engineering, IT staff, and security personnel. Often, the traditional IT way of doing procedures such as patch management, updates, and system embedding does not work for OT. This is due to the requirements of high availability and constant uptime as described in chapter 2. 43% of the respondents also find it difficult to understand who is responsible for industrial cyber risk, reflecting the problem stated in the section above regarding the lack of initiatives from the management side and the drive to implement cyber programs [26].

Despite cultural differences between IT and OT, there is a need for an intermediate security team. The team should work closely together, exchanging knowledge and educating each other in their respective fields. The focus should be on how one can reach the highest level of security maturity.

Tasks for this team have to be set by the team together with the company’s leaders. Some ideas for these tasks can include conducting risk assessments for both IT and OT environments and researching how incidents in one of the fields affect the other field. Work on policies, procedures, and frameworks is important. Assisting with security knowledge when management is seeking to buy new equipment. This may ensure better compatibility as well as security for the devices. Propose and follow up on yearly security projects in order to lift cybersecurity. They should also give frequently status updates regarding incidents, downtime, and the day-to-day operations in connection to cyberse-
curity. Being the first line of response in case of incidents. Collaborating with other security teams in the field, exchanging experiences and knowledge.

Discussing with Telenor, many of the industrial companies they secure lack OT security in terms of security personnel, strategies and incident handling. A common IT/OT security team can tackle this problem and build on each others knowledge.

**Related Challenges**

The process of creating an IT/OT security team will demand great management, openness, and patience. This will be a challenge for the team leaders and company leaders to overcome. The C4 IT/OT convergence challenge needs to be addressed within the team, making sure everyone feels that they contribute with their knowledge either within IT or OT. If this succeeds, one will be a step closer to overcoming the cultural aspects of the challenge. A security team may also help with tackling parts of the C8 Human Factor challenge as such a team can enlighten and spread awareness about security and the cyber risks that the company is facing.

**Related Attack Scenarios**

The possibility of AS11 Social Engineering attacks and AS12 Highly personalized attacks using artificial intelligence is present. The team will be the core of security in the company, and the information they hold is valuable. Due to this, they are targets for the overstated attacks. Raising security awareness and discussing these kinds of attacks within the team will therefore be important in order to mitigate these risks.
**Recommendations**

To overcome the challenge and reduce the risk of the overstated attack scenarios, the following recommendations are given.

- Create a cybersecurity team with both IT and OT personnel
- Spend time on culture caps. Good collaboration start with understanding each other
- Assess the team with specific tasks where the need for collaboration is important
- Set up a list of tasks and activities throughout the year in order to have frequent meetings and discussions
- Address topics like social engineering and information gathering in order to prevent information disclosure

**4.1.3 Security Awareness Training**

Many companies are now offering security awareness training to their employees. Often, one has to take a mandatory course during the onboard program, and then there are frequent courses throughout the year. As human failure and naivety are one of the greatest problems when it comes to security [42], courses like these are very important.

The courses often contain information about how to handle suspicious emails, creating strong passwords, caution when using memory sticks, and information about social engineering. These are all very important also when talking about OT, but there will be a need for more specific awareness training for Industry 4.0 in the OT field [13]. Implementing security solutions for the new industrial era will not be successful unless one has well-trained employees with knowledge of cybersecurity.
When raising awareness of cybersecurity, it is important to remember the receiver [8]. IT personnel have different knowledge compared to operational personnel; hence they will need different types of training. Common for them both should be that the training represents real-life scenarios that one can easily recognize. This is especially important for operational workers who have little to no experience with cybersecurity beforehand and therefore need to see the importance of doing the training. For the knowledge to build over time, the training should also not be too long but rather short and frequent [8].

In their recommendations referenced in section 2.4.2, ENISA [13] recommends specific state-of-the-art cybersecurity training for all employees. However, as they point out, there are not that many well-designed Industry 4.0 security programs for both IT and OT personnel today. They are either not specific enough, too expensive, or do not cover all the essential areas. This causes a greater responsibility of the management when deciding how to train employees. As the most important thing is for the workers to recognize the environment and see how the training can be useful to them, each management should tailor it to their systems. If the company has cloud solutions, IIoT devices, remote access solutions or other new technologies, this should be addressed and one should look into if it is possible to incorporate this into the learning.

**Related Challenges**

C8 Human factor, C4 IT/OT convergence and C2 Management Process are all related challenges that can be tackled by open dialogue, knowledge building, and discussions. A way to ensure that everyone is familiar with cybersecurity threats, risks, and the security controls in the plant is to have a proper security awareness program. This will not solve all challenges related to security and Industry 4.0 but will undoubtedly ensure better security in the company by providing a common understanding and language for cybersecurity.
Related Attack Scenarios

Attacks on the connection between controllers (AS1), attacks targeting sensors (AS2), and attacks targeting actuators (AS3) are all in the ENISA’s attack scenarios list. To protect oneself against this, proper device security, as well as network monitoring, will be important. However, this will not help if the operational personnel is not trained to recognize, react, and respond to unexpected behavior in these devices. This will have to be a part of the awareness training specially targeted toward workers operating the systems. Alongside this, all personnel should be trained in AS8 Malware attacks. Malware attacks against industrial systems have increased over the last couple of years and are often through phishing emails sent to workers. Explicit training on this topic and how to recognize such attacks is necessary to minimize the damage.

The next section provides some recommendations as to what to focus on in a security awareness program in order to overcome the challenges and minimize the possibility of damage regarding the possible attack scenarios.

- How to detect and react to suspicious behavior in operational assets like PLCs, DCSs, and IIoT devices
- Get familiar with new technology used at the plant and their protocols, functions and security controls
- Learn about specific attacks like malware and DDoS attacks and how to react in such situations

These recommendations are targeted toward Industry 4.0 risks mentioned in chapter 2. They are in addition to the traditional security awareness training content like secure passwords, social engineering, network security, secure mail handling, file sharing, and memory stick cautions.
4.2 Processes

Having well-informed management and workers is essential but of little use if there is no drive to implement change. Processes involving documentation are therefore necessary. This may include asset management, risk management, and communicating needs through in-depth agreements. This section will accordingly give recommendations on how to address this type of process work in order to secure oneself for the next industrial revolution.

4.2.1 Asset Management

An industrial system tends to have many different assets, with lots of different information and connections. Industry 4.0 and IIoT will contribute to the number of assets, and strong asset management is therefore important. One of the informants from the industrial company who works primarily with IT but also with OT addressed the problem with little knowledge of the assets in both the IT and OT environment in their company.

"Right now, there is no one in our company that has control and knowledge of all the assets. The closest we will come is me and (name of another employee), but we will soon retire. There is no plan on how to pass on this information, and I am afraid they will lose important knowledge and have to start from the very beginning when trying to map all the assets”

This was said in connection to talking about documenting existing information. As there were no systems or procedures in place to gather asset information, the company relied on people who had been working there for a long time. Their knowledge is very valuable, but it is of little help when they are retiring and have not documented or transferred it to other people. For this to be done, one has to see the value of good asset management.
Benefits of Asset Management

Good asset management is fundamental for other processes in the company. According to the National Cyber Security Center in the UK [45], there are multiple benefits to having good knowledge of the assets. Risk management will undoubtedly be easier and also more precise when one knows the assets, their information, and their connections. This can help discover risks and identify more precise security controls.

Many OT systems also suffer from legacy systems, as pointed out in chapter 2. Having a good overview of end-of-support assets will help set the correct focus when buying new equipment. An asset database will also contribute to better patch management as one can immediately search for an asset and its configurations if there is a known vulnerability that needs to be patched. This will, of course, depend on the vendor notifying all parties affected by the vulnerability. Responding and recovering from an unwanted incident will also be much easier if the assets are known. If time is crucial, which is often the case in OT, knowing which assets to shut down quickly and the effect of this on other systems will be an advantage [45].

Definition of an Asset

An asset is something of value to your company. This can include people, data, devices, systems, hardware, software, and company internal information [45]. Before making asset identification, a clear definition of what an asset is should be established. In a large ICS environment with many assets, there might need to be a prioritizing based on importance and risk for the assets.

Asset Management Program for ICS

There are few asset management programs or modules specifically designed for ICS with a focus on both IT and OT assets. One module is suggested
by CRR from Carnegie Mellon University [43]. It consists of four phases, as shown in figure 4.1 and can easily adapt to both small, mid-sized and large industrial companies.

Plan for Asset Management
Planning for asset management involves getting the support needed from the company management and leaders. As the project is fundamental for many other activities, it should be prioritized in order to strengthen cybersecurity. As addressed in the previous section about management, cybersecurity management in ICS is often overlooked. In order to get the funding and resources for the project, the selling point should be that it is fundamental for all other activities and can help reach the company's business goals. Solutions for storing the asset register should be a concern in this phase [43].

Identify Assets
Identifying the assets might be the hardest part, especially in combined IT/OT systems. Active sources like network scanning can be an efficient way to detect assets; however, this is not always possible in OT environments as this can disturb the production and availability requirement, but also since not all OT assets are connected to the internet yet. Passive sources like DNS logs or authentication logs can be used to see what other systems the asset communicates with but are more likely to give less detailed information than the active scanning. As there can be very many assets, those who support critical services should be prioritized [43].

Document Assets
When the assets are identified, the important job of documenting starts. Whether the information they hold is sensitive or not should also be addressed. The owners or the internal group being responsible for the asset should be stated. In case of a bigger incident, it will be valuable to know the other assets and solutions connected or dependent on the asset as well. Lastly, security controls,
as well as backup information, should be provided [43].

**Manage Assets**

Finally, a routine should be established to manage the assets. The database should be regularly updated, and if there is any change to an asset, this is to be addressed with, for example, notes or color changes. For the asset management to work, there should be someone responsible for this process in the cybersecurity team. Obtaining support from the management is crucial [43].

**Related Challenges**

Challenges that can partly be solved through asset management include C1 Vulnerable components, C3 Increased connectivity, and C5 Supply chain complexity. Vulnerable components such as IIoT devices lack proper device security. Security controls such as network segmentation and monitoring will be necessary, but having registered the asset in a database will also serve security. With the challenge of increased connectivity, knowing how the devices interact with each other, what security controls they have, and their redundancy and backup options will be very important. As the supply chain will grow complex, knowing the system in detail through asset registering will be extremely important if an incident is to happen. Having proper asset management can also help for the C11 Security updates challenge. The solution for this challenge is better updating possibilities in the design, but having an overview of which assets to be patched in case of an incident is important.

**Related Attack Scenarios**

To prevent AS8 Malware and AS9 DDoS attacks from spreading, knowing which devices are connected with each other and how they are secured is crucial. This can possibly stop the attack from spreading if the affected systems and devices are detected, and one knows how these are connected to the rest
of the system. Knowing the assets can also be beneficial against the AS10 Stepping stones attack, where the attacker compromise hosts and use them as stepping stones in order to launch a bigger attack.

To overcome the challenge and reduce the risk of the overstated attack scenarios, the following recommendations are given.

**Recommendations**

- The benefits of having proper asset management are many - address this when discussing with management
- Prioritize the most critical assets if there are too many
- Having a good plan for how to define and detect assets as well as how to manage and upgrade the database is crucial
- Use both passive and active sources when detecting assets if possible.
- Defining who is responsible for which assets and how this group or person should react in case of an incident
- Have frequent routines for how often one takes backup and updates the asset register. New assets should be added when connected to the system
4.2.2 Risk Management

Industry 4.0 will mark a shift in how one approaches risk management in manufacturing. The IT/OT convergence creates a need to look at the security perspective from the OT field when doing risk assessment. With IIoT and cloud solutions, the attack surface has expanded and needs to be considered when managing risks.

"We often see that when a company has done risk assessments, they have only done it for the IT side of the company, not knowing they need to do it on the OT side as well" - Telenor security architecture informant
**Risk Management Frameworks**

One of the most used standards for risk management in information security is ISO 27005 [5]. The standard describes a generic risk management process with sequential phases. After establishing the context of the risk management, one does risk assessment with corresponding treatment and acceptance measures. The final phase consists of monitoring and reviewing. The framework is not too specific and can, therefore, in many cases, be a good alternative when discussing risk management in ICS.

Another possible risk management framework to use is the one presented in Nist’s ”Guide to Industrial Control Systems (ICS) Security” [44]. They present a four-phase model as shown in figure 4.2. The point is to construct a framing component, meaning to review existing documentation and then make a framework for the risk management decisions to be made. Then the company assesses, Responds, and Monitors this frame contiguously. As one is to assess risk on the organization level, business process level, and ICS/IT level, this framework is more targeted towards ICS systems compared to ISO 27005. This might be a better fit for some companies; however, the most important aspect is to establish a proper risk management framework that is fully understood by both IT, OT, and management personnel.

The framework points out that there often can be a conflict between safety requirements and good security practices in OT environments. Compromising safety can have a disastrous outcome with the potential of risking human lives. ICS environments have long been good at addressing this risk, and often safety assessments connected to the physical world are in place. With OT intertwining with IT, this now has to be connected to the cybersecurity risks in the digital world. A common risk assessment addressing both environments and how they interact and affect each other on a risk level is therefore needed.

Addressing the physical damage a cyber incident can cause in ICS is impor-
tant. The NIST framework [44] recommends doing this in three steps. First, one looks at how the incident can manipulate actuators and sensors. Losing control over these devices will, in many cases, mean to lose control over the production and operation of the system. Secondly, one is to look at redundant controls and how these can be used and configured to minimize the impact. Thirdly, looking at how this can impact the surroundings is important. This means communicating how it can increase emissions, damage controls, and safety systems, expose energy systems and lead to explosions. As ICS systems are complex and often geographically spread out, this is a difficult task yet very important.

"Assessing risk is extremely hard, especially in OT environments. Some do risk assessments every second year, but when the report is done, the information is already outdated due to equipment changes in the system. It is very complex. There is no explicit well-used framework for this today, which makes it hard" - Telenor informant

When asking the informant how and where to start when wanting to do risk assessments in ICS systems, the answer was clear. One has to start with the documentation. Sometimes, the company will have a lot of documented processes and procedures, but very often with industrial companies, this is not the case. The informant recommends starting at the top to try to figure out what the procedures are, what assets one has, and how they are managed.

Using a proper framework will ease the process and make sure everyone uses the same approach and language. It will be important for both IT, OT, and management personnel to participate. If possible, one can also start from the bottom and concentrate the risk assessment around actuators, sensors, and controllers before moving further up in the system.
Figure 4.2: Risk Management process. Based on figure from [19]

**Related Challenges**

Having proper risk management could be beneficial for many of the challenges listed by ENISA. Assessing risk in accordance with vulnerable components and the legacy system will be an important step to minimizing the challenges they bring into the system. How challenges like supply complexity and increased connectivity effect the security of the system will also be important. However, the main challenge that good risk management will address is the C10 Safety aspects. Discussing with both IT and OT personnel how cyber in-
cidents will affect the safety of the workers at the site as well as how they will affect the environment will be significant. Security for safety starts with proper risk management and evaluation of what can go wrong and how it affects the industrial process and people.

**Related Attack Scenarios**

The company will benefit from proper risk management for many of the attacks listed by ENISA as one has discussed and made an incident response plan for cries. Having assessed attacks targeting AS7 Safety Instrumental Systems will be very important as this is a dangerous attack affecting the environment and/or human lives. When doing risk assessment, this system should be on top when prioritizing what to assess in order to minimize the risk.

To overcome the challenge and reduce the risk of the overestimated attack scenarios, the following recommendations are given.

**Recommendations**

- OT, IIoT, and Industry 4.0 threats and attack scenarios must be taken into account when doing risk assessments
- When doing risk assessments on OT, make sure there is OT personnel helping out with the assessment
- Use a pre-defined framework to make sure there is a common understanding of what needs to be done
- The definition of what an acceptable risk varies between IT and OT. Be prepared for trade-offs
- Address the safety and environmental aspect in light of cyber security
• Conduct risk assessment annually if possible, especially in the most critical parts of production

• If possible, implement both a top-down as well as a bottom-up approach when doing risk management

4.2.3 Vendor and Third Party Agreements

Adding new devices and implementing modern solutions to the industrial system will require good communication with vendors and third parties. There is a need for good security in the devices and solutions, as well as discussions about backup and crisis management. If this is not addressed early on, the consequences can be fatal.

"We have an agreement with this (...) company who has access to our systems. It is a third party, and the productions in the two companies rely on each other. But no one knows what the agreement really is and how the solutions between the two companies are constructed and how our common systems are secured. We do not communicate with them unless there are some issues."

This was said by one of the operational informants from the industrial company. The agreement was made a long time ago, and no one knew exactly what had been technically done to ensure good security. Exactly how an attack on the other company would affect their industrial process was not clear, and one lacked written documentation, technical details, knowledge about both systems, and communication between the companies.

Speaking to the security architectures in Telenor, this challenge was not new to them. As systems tend to grow over time, adding new devices with a lifetime of 15-20 years which is common in industrial systems, the weak collaboration and documentation are not unexpected. This stands for both third-parties and customers, as well as vendors. The problem is possible to improve, especially
with technology allowing to have updated databases. Improving this starts with demanding security in agreements.

"Security requirements are often non-existing in Service Level Agreements and when discussing buying new devices."

This is pointed out during a discussion about Service Level Agreements (SLAs). To improve the overall security in new cloud solutions as well as IIoT devices, the vendors need to be pushed through SLAs. Learning from the Telenor informants, setting security as a "must-have" is not always possible, so one sets it as a "should-have" instead. This is because is not always that many vendors to choose from, so having it as a "must-have" result in too few to no vendors to choose from. If enough customers do have security as a part of their SLAs, huge companies, the vendor is forced to prioritize it and put it on their road map.

**Related Challenges**

Creating detailed and secured-orientated service level agreements will be beneficial in the challenges regarding C1 Vulnerable components, C6 Legacy control system, and C12 Secure product lifecycle. Demanding proper security controls from the vendor is not always easy, and it will take some years before vendors use state-of-the-art security controls. Until then, pushing security in SLAs both in new equipment as well as communicating this to vendors of legacy systems will help the industrial field move into a more secure future. This will also be important to address with exciting third parties and customers of the industrial companies.

**Related Attack Scenarios**

Having proper SLAs can help mitigate risks connected to IIoT devices (AS5), controllers (AS1), sensors (AS2), and actuators (AS3). Stating in the SLA
that these devices need proper device security, authentication methods, cryptographic controls, and secure communication protocols are important. If it is possible to get devices with strong security, this should be prioritized as it can be the first line of defense in an attack.

To overcome the challenge and reduce the risk of the overstated attack scenarios, the following recommendations are given.

**Recommendations**

- Check existing SLAs and see if it is possible to upgrade the security part
- Establish good and frequent communication with vendors
- Ensure IT and OT collaborate on the security when signing new SLAs
- Push security in all SLAs, even if it turns out to be "should-have" instead of "must-have."

**4.3 Technology**

Cybersecurity focus among management and workers as well as well-documented process is important. To securely transfer from Industry 3.0 to Industry 4.0, the need for upgrades in accordance with technology is also necessary.

**4.3.1 Network Architecture**

As the shift to Industry 4.0 technologies will lead to great amounts of data and thus a bigger attack surface, a network architecture focused on security is important. The attack surface will expand, and it will be crucial to manage the network in order to protect oneself against attacks and minimize the possible expansions of these attacks.
"We often see that the network is not properly segmented. In some companies, we still see that the enterprise and OT network is within the same IP range."

The quote above was collected when interviewing the network security expert in Telenor. The knowledge gathered from working with Norwegian companies was that the network is not always properly segmented; it is rather complex and lacks a strategic implementation plan. This is concerning when thinking about adding new devices such as IIoT and implementing cloud solutions. Separating the enterprise network from the manufacturing network will not only minimize the risks but also make it easier to monitor and control [38].

**A new model to accommodate for IIoT and cloud**

According to Leander et al. [30] there are two main problems with the Purdue model presented in subsection 2.2.1 when using IIoT components. Communication between the levels will be necessary to accommodate the information flow that will be required for the IIoT devices, and this is not encouraged by the model at the moment. This will make it more difficult to maintain clear zones and boundaries if not careful when implementing the solutions.

ENISA provides a solution to these problems with their High-level reference model for Smart Manufacturing, as shown in figure 4.3. The model is divided into six layers. The first level, level 0, is the lowest level designed for devices such as machines and robots. Level 1 includes a SIS system with IIoT devices for measuring system parameters in the form of sensors and executing specific system actions with IIoT actuators. This level transmits the data to levels 2 and 3. Level 2 controls the processes on level 0 based on the information it gets from the IIoT devices on level 1. This level contains PLCs, RTUs, DCS, and SCADA systems. The third level is where the OT side connects with the IT side. This contains systems that are used in the manufacturing process, such as Manufacturing Execution Systems and Historians. Separating this level...
makes it possible to communicate between IT and OT without direct communication. This layer also has an IIoT platform that manages and processes the data from the IIoT device in the system.

This makes it easy to provide systems in the level above with the correct IIoT data. Level 4 includes the Enterprise level. This means production management and supply chain management systems. Level 5 is constructed for third-party services such as Software as a Service (SaaS) and Platform as a Service (PaaS).
Figure 4.3: Proposed High-reference model from ENISA. Based on figure from [36]
Constraints

The High-level reference model is quite new, and there is little information about successful implementations of the exact model. This might be due to the fact that the model requires a lot of new equipment, and many small to medium-sized companies may not have the knowledge or equipment yet.

The model will most likely be taken into consideration when setting up new industrial environments in the future and, until then, remain a great inspiration on how to build architecture models suited for Industry 4.0. As the thesis aims to provide recommendations on how to securely transfer into Industry 4.0, it sure should be mentioned. However, the thesis also aims to give recommendations on how to use what one has right now, and there should also be mentioned a more realistic example. Included is, therefore, also a solution from the case study.

Model in case study

How one chooses to segment the network with or without the IIoT component will depend on other factors in the company. It will be restricted by legacy systems, earlier solutions, and knowledge within the company as well as the economy. In the industrial company from the case study, one saw the need to build on what one already had. Based on the Purdue model, they had segregated IT and OT networks. The physical and logical separation between the IT and OT network and the air gap made it difficult to send data from the lower OT levels to the IT levels, and one saw the need to upgrade to a better-fitted model that could accommodate the new cloud service they wished to implement.

Another reason to restructure the network was discovered during the Covid-19 pandemic. Many of the vendors the industrial company uses are not stationed in Norway. When the pandemic hit and the borders closed, getting service and
help with the industrial equipment was hard. Some vendors offered remote help, but the network architecture was not rigged for this, and the risk was too high to accept this. The urgent problem lead to unsecure solutions.

"Due to the air gap between the IT and OT level, we had difficulties when we suddenly needed to push some information from the lower levels to the higher levels. This resulted in rather randomly installing routers, giving remote access, and so on without any proper plan. This means that we established services that are not ours, that we are not in charge of, that we can not monitor, and it was very easy to access the heart of the inner production area."

They decided to keep the Purdue model with some modifications to best fit the existing operational and technical solutions, as shown in figure 4.4. Due to the rapid changes with more and more assets connecting to the internet, the need for a dynamic and flexible model was evident. The infrastructure that has the same requirement of security will belong to the same security level but be segmented based on the different operational and functional needs. The security levels are all to be separated by a firewall. As the industrial system has legacy systems that are hard to replace or update, they decided to isolate this as well as possible.

Another requirement was for the architecture to be redundant whenever possible. This might be a very common practice in IT, but OT has more specialized equipment in the industrial systems, making redundancy more difficult and expensive. Sometimes, parts of the system is redundant, but not the system as a whole. As the industrial company has more than one plant, it is necessary to have secure communication between the plants. With the new model, this is ensured. The new architecture will not only provide better security but also open up new systems such as network monitoring and network logging.
Security Levels

Security levels were used in order to indicate the criticality of the operations of each level. Critical operations have more security and communication restrictions compared to less critical levels. To represent this in the model, the security levels increase when moving downward in the model.

Segmentation

When having defined the security levels, the work to segment inside the levels is done. This is to ensure predictable, stable, and controllable traffic through the levels and zones. Constructing specific IP segments based on processing activity and making sure all traffic with different segments passes through a firewall is important.

Firewalls

To segment the infrastructure into different security levels, there is a need for mechanisms that can control the traffic. In TCP/IP networks, this is mainly done by inserting firewalls. The firewalls can allow or deny communication between machines based on preconfigured rules. To get a good segmentation, one looks into the components and groups them based on whom they need to communicate with. Within the grouping, the communication can flow freely. If one is to communicate with someone outside the group, the firewall checks whether this communication is allowed or not. This enforces precise control of the communication between different segments. Typically, a security level contains more than one group, though having the same security requirements, the firewall might be configured to control the communication in order to separate different processes or environments.
"We used to have the same physical firewall at two of our plants. It was logically separated but the same physical device. This was difficult because if we needed to change something, we had to stop the production at both sides, which is not optimal at all"

To change this, different zones were separated by Next Generation Firewalls (NGFW). The northern firewall in the iDMZ is used to protect and control all traffic coming from the enterprise environment. The communication is monitored and logged. In addition to this, the firewall has the possibility to configure an Intrusion detection System, blocking suspicious activity is detected. The southern firewall is for inspecting, monitoring, and logging all activity that is coming from the iDMZ and monitoring the industrial network.

**iDMZ**

To separate the Enterprise network from the industrial network, an Industrial Demilitarized Zone (iDMZ) was used. As the availability requirement is very important in OT, the production should not be affected by any external events in the IT environment. Another important design requirement was that none of the functions and solutions the iDMZ is facilitating (remote access, monitoring, and so on) should affect the production and OT environment in any way if they were to compromised.

When implementing an iDMZ, one ensures that communication between the OT level and the IT level is not directly permitted but has to go through a system where the communication is verified before sending it further up in the model. It is also possible to change protocols in the iDMZ to ensure that there are no protocol vulnerabilities that can be used from the enterprise zone and all the way down in the industrial environment.

The industrial zone is constructed to only be a zone for forwarding communication and is therefore not set up for storing any information. The iDMZ zone is
logically separated from the IT and OT through firewalls, mainly called north (IT) and south (OT). The firewalls inspect the communication, as all communication is by default terminated in the iDMZ. This is done by gateways and proxy solutions. Requesting access as an internal user or vendors to, e.g., HMI devices, is possible but is controlled by different Privileged access management (PAM) solutions. In addition to this, any update or patching will go through a proxy server in the iDMZ to ensure secure updates.
Figure 4.4: Network architecture design with remote access solution.
Monitoring

Monitoring the enterprise network has long been a common security control. When breaking down the barrier between the operational network and the enterprise network, monitoring should be a great part of the security.

“There will be a long time before security in devices is good enough. Until then, we have to rely on building baselines for the equipment and make frequent comparisons”

When starting the project, one of the main goals was to establish a Security Operation Center collaboration between the industrial company and Telenor. This is a task Telenor is now taking on, monitoring, and following up with companies that are too small or have few resources to create a SOC for themselves. As pointed out above, the IIoT devices and new solutions will need proper monitoring in real-time to detect anomalies. There will be a long time before all devices are connected to the internet due to long lifecycles. Active and passive monitoring should therefore be used in order to monitor all devices.

Related Challenges

The challenges good network architecture can suppress are many. Insecure protocols (C7) in the new IIoT devices as well as in legacy ICS equipment (C6) will remain a challenge, so the need for good segmentation, strong firewall rulesets, and continuous monitoring is present. The IT/OT convergence (C4) will increase the need to send data from the higher levels and the internet and down to the lower levels, and this is difficult to do securely without proper segmentation. Increased connectivity (C3) between systems and collaborations across plants will not be secure if the network is not segmented with levels, firewalls and iDMZ for each plant. Lastly, security updates (C11) over the network will be more secure if it is terminated in a iDMZ before being implemented.
Related Attack Scenarios

Defining a secure-based network architecture can help mitigate many of the stated attack scenarios. Monitoring and inspecting all traffic can be the first step in order to detect Malware (AS8), DDos (AS9), and Stepping-stones attacks (AS10). It will certainly not be enough in case of a well-structured attack. AS4 Attack on the information transferred over the network, is not an easy attack to mitigate, however proper network segmentation might lead to unusual data values being recognized earlier.

To overcome the challenge and reduce the risk of the overstated attack scenarios, the following recommendations are given.

Recommendations

• Create a proper plan for segregating and segmenting the network. Ask for help if there is little competence in the company

• Use a reference model to separate the enterprise network from the operational network. Minimize the paths that allows communication from enterprise to OT

• Focus on segmenting and creating security levels with respect to critically

• Put work into creating proper firewall rules. All traffic should be terminated in a firewall

• Build an iDMZ zone where all traffic is terminated

• Make sure patching and updating goes through the iDMZ as well as remote connections

• Use both active and passive monitoring if possible
• Establish a SOC solution, either within the company or outsource it to a trusted company

### 4.3.2 Industrial Internet of Things

The possibility to gather, analyze and present real-time data from the industrial processes will be a game changer for industrial companies. One of the key concepts to realize this is through the Industrial Internet of Things (IIoT). Though it might contribute to the production, it also increases the attack surface.

> *Many of the IIoT components does not have proper security mechanisms, though they are new. Security is not always in focus when designing IIoT devices.*

The quote is from one of the Telenor informants and describes one of the main problems with the new devices. This concern is supported by a report conducted by the Norwegian Water Resources and Energy Directorate (NVE) from 2020. The aim of the report is to map out the use of IoT and IIoT in the energy sector in Norway. Research regarding standards and frameworks used in the companies designing and manufacturing the IIoT components was also carried out.

The findings show that there are initiatives to try to follow specific security standards like NIST and ISA/IEC when making the components, but that implementation of security controls is rather sparse. As these components are relatively new, many of the products were not tested yet and, therefore, not in production. The report points out the lack of specific security standards for the products and services. Another main problem is that the requirements given by the customer are comprehensive and, in many cases, very difficult to meet. Many of the devices are designed with speed, low price, and small dimensions
in mind, meaning that the memory and processing capabilities are low. This affects the ability to, for example, implement strong encryption. [35].

**Authentication and Authorization**

As the devices are likely to communicate directly with each other without human interaction, strong authorization and authentication are needed. The devices must be certain that they communicate and exchange sensitive data with whom they think they are connecting. Each device needs to be assigned a unique identity in order to authenticate. Authentication can take the form of certificates, keys, security tokens, or passwords. Looking to the IoT field, the use of Public Key Infrastructure (PKI) to authenticate through digital certificates is rising [4].

PKI opens for authentication through public-key cryptography, where the public key is signed by a certificate authority (CA). This requires all devices to have a digital certificate, and as there are many IIoT devices, there will be great amounts of certificates. In order for the PKI to work, there needs to be an efficient way of generating, distributing, and revoking the certificates, which is a challenge. As the process is rather resource-consuming, this will be a problem for IIoT devices with low memory and processing capabilities [2].

There are initiatives to adapt digital certificate solutions to fit IIoT environments, and this is to evolve over the next years. It will therefore be important to address this topic in SLAs and push IIoT manufacturers to design devices with security in mind. When buying IIoT components, the authentication possibilities should be a highly prioritized requirement.
Communication

“The best security solution is not always straightforward. You must look into what is compatible with what you already have and make choices based on what is fitting with each other”

When discussing how to ensure secure communications between the IIoT devices over the network, this quote from one of the Telenor employees must be taken into account. The IIoT devices can be implemented with different network protocols with various built-in security. According to ENISA [36], the best is to avoid using protocols with known vulnerabilities and instead use well-known protocols that have proven to stand attacks like TLS. However, they also recommend shortening the amounts of protocols used within an environment and making sure that the protocols are interoperable and have the same security capabilities. To not lose control over the devices, protocols, and technologies, it will be better to strip down the amount. This will ensure better security as one can concentrate on using many of the same techniques to secure a broader aspect of the system.

Configuration

Before the devices are to be integrated into the industrial system, it is important that they are configured with the possible security mechanisms the device comes with, e.g., running in safety mode. Testing the device in an enclosed environment before allowing it to connect to the production network is an important step and can rule out any misconfigurations.

Related challenges

Relevant challenges include C1 Vulnerable components, C7 Insecure protocols, and C9 Unused functionalities. Many of the devices lack secure protocols, and
they are often difficult to update. A possibility would be not to implement such devices, but in order to produce and manufacture in the future, this is an unlikely possibility. Having security in mind when buying and implementing these devices will therefore be important. Configuring the devices with the security controls that they do have is also crucial in order to secure these IIoT devices. C11 Security updates is a very related challenge as the devices are hard to patch. For this to be solved, the designers will have to work with the industry in order to figure out how patch management and updates can be done efficiently.

**Related Attack Scenarios**

Related attack scenarios include attacks on AS4 Attacks on the information transferred over the network and AS5 IIoT gateways and AS6 Control of remote controllers. As the devices lack device security and security protocols when communicating, this might give the attacker a chance to infiltrate the network through the device.

To overcome the challenge and reduce the risk of the overstated attack scenarios, the following recommendations are given.

**Recommendations**

- When possible, choose trusted manufacturers of IIoTs where security is a priority
- Make sure to configure the asset with all build-in security controls
- Test the devices before connecting
- Have proper authentication and authorization for each device in use, e.g., through digital certificates
- Use secure protocols whenever possible
4.3.3 Cloud

"We need a system that can gather all the data and present them in a simple way, so it is easy to see the production and follow up on security aspects"

The quote is from an employee in an industrial company. When the company is now transferring towards a more digitalized production, this is possible. This can be done by implementing a cloud system and letting the components feed the cloud with information. Once the information is gathered in one place, multiple solutions on how to display it are possible. Learning from the industrial company, this information had earlier been gathered manually in an Excel sheet that was sent around in the company making everyone fill in the information regarding their area of responsibility. The method was insufficient and not very reliable as the information could simply be mistyped. Sending the sheet around was not secure, and it could easily have fallen into the wrong hands.

When considering pushing all the information from the assets to the cloud, this might lead to a bigger threat picture. Yet, this may be a safer option for many industrial companies compared to how they operated earlier if the cloud is secured properly. As cloud solutions emerge and become more and more popular in ICS systems, security is destined to follow. This will be necessary in order to provide strong security solutions to ICS-specific cloud systems, not only trying to adopt security solutions from enterprises.

When choosing a cloud solution, many factors must be taken into account. What the company chooses should reflect the amount of data to be stored, the processing activity, and other solutions and devices that must interact with the cloud. More importantly, the decision should be based on how the cloud solution will impact the overall security of the system.
Being sure who can access the server, what security controls the providers have, and if they have been certified to any standard is important. Data in rest, transit, or use should be secured through strong encryption and should not be accessible in plain text to the cloud provider. When consulting with the cloud provider, topics like backup and disaster recovery should be addressed, and there should be both internal company strategies as well as cloud provider strategies for the scenario of needing to restore data.

**Related Challenges**

The cloud solution will struggle with vulnerable components and insecure protocols (C7) when the device security is yet not strong enough. Human factors (C8) like bad password hygiene will also affect the security around the cloud. Securing just the cloud itself will, therefore, not be enough. Developing layers of security and having good policies and procedures will be necessary to tackle these challenges.

**Related attack scenarios**

Attacking vulnerable Internet-connected devices such as IIoT (AS5), controllers (AS1), sensors (AS2), and (AS3) actuators that send information can compromise the cloud. Authenticating all devices before sending information, monitoring the network, and having good backup and recovery policies can help decrease the damages from an attack. Configuring the cloud with barriers between receiving and handling data is also an important mitigation technique to avoid the overstated attacks.

To overcome the challenge and reduce the risk of the overstated attack scenarios, the following recommendations are given.
**Recommendations**

- Reflect on how the cloud solution will affect the security of the rest of the system
- Be specific in the SLA and ask for security controls
- Discuss backup and recovery possibilities with the provider but do also have an internal routine for this
- Let the devices who are to push data into the cloud authenticate themselves, and thus do not let anything else upload data to the cloud

**4.3.4 Remote Access**

For a long time, the option to get support on ICS devices and systems was limited to on-site work only. This was difficult to coordinate and expensive. When one got the possibility of VPN connections during the 2000s, many industrial companies took advantage and implemented solutions. As the systems and infrastructure were not designed for this in the first place, the security was weak. Due to the fact that industrial attacks were yet not a problem, the security was not an issue \[10\].

"*We have a VPN solution to the most critical system that the vendors can use to troubleshoot, but it is not a system that we can monitor and have control over. You connect from the vendor site, but we cannot control who connects, monitor what they do, or see that they disconnect again.*"

According to NIST \[41\], there needs to be strong authentication in use, preferably using a token-based multi-factor authentication method in order for it to be secure. If connecting to the Enterprise network before connecting to the operational network, the second round of authentication should be performed before accessing the control network.
This is supported by the security architecture in Telenor. Working with remote access in ICS environments, they saw the need for proper Identity Access Management (IAM). Vendors, technicians, or other people of interest asking for access to the system should have personal user accounts with multi-factor authentication to prevent identity spoofing.

Granting no more than the absolute necessary level of access may seem evident, but due to lack of segregation, access policies, and little knowledge, giving full access is not uncommon in ICS. Rules and policies for how to group users based on access level should therefore be implemented based on the least privilege method. This will also make it easier to have lifecycle control of the user, meaning that they will have to re-authenticate to still be a part of the user database occasionally, as well as removing the user when the person is no longer supposed to have access.

Addressing the second part of the concern from the informant from the industrial company, the importance of having just-in-time access (JIM). Having enough time to fulfill the task or troubleshoot the system is crucial, but having access after the task is done is not necessary. Just-in-Time access grants each user a time slot before they are logged out. There is possible to extend this, but that has to be clarified before it is granted. This will ensure that no user forgets to log out or have unlimited time to modify the system. Auditing the modifications and troubleshooting is also important in order to have the possibility in order to go back and check the log if the system or devices start to behave in an unexpected way. If the industrial system is connected to a Security Operation Center (SOC), having real-time logging to their monitoring system is also recommended.
Related Challenges

The C4 IT/OT convergence challenge will question how one looks at connections from outside of the plant in connection to vendors configuring devices, SOC troubleshooting, or people working remotely from home. The increased connectivity and supply chain complexity will require an architecture designed for secure remote connections.

Related Attack Scenarios

Having remote access options will increase the attack surface. Having a controlled and secured way to connect will, however, help in mitigating attacks such as Control of remote controllers (AS6) and Attacks against the IIoT gateways (AS5). Having to authenticate with a personal user before accessing any of the devices or the different networks will increase the steps to be taken in order to create an attack using remote access solutions.

To overcome the challenge and reduce the risk of the overstated attack scenarios, the following recommendations are given.

Recommendations

• Use Identity Access Management (IAM) or similar to have control over users, user groups their different access rights

• Use multi-factor authentication when possible

• Create personal accounts for everyone asking to access the system

• Have clear access policies and do not give out more access than absolute necessary

• Maintain lifecycle control over users and delete users who should no longer have access frequently
• Implement a just-in-time approach for users to only have access in a specific amount of time

• Audit and log all modifications and configurations are done in the system

4.4 Overview Table

This section presents a table with all the categories, their subcategories, related challenges, related attack scenarios, and recommendations.
<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>Challenges</th>
<th>Attacks Scenarios</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Management</td>
<td>• C2 Management of process</td>
<td>• AS11 Social Engineering</td>
<td>• As a leader, take the responsibility to educate oneself through online courses and webinars. OT specific if possible, but general information security courses are also important</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C4 IT/OT convergence</td>
<td>• AS12 Highly personalized attacks using AI</td>
<td>• Build an organizational culture which includes cybersecurity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Budget for cybersecurity controls. It will cost, but an incident will most likely be more expensive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Let everyone participate in the cybersecurity work. A knowledgeable workforce is the first line of defense when mitigating an incident.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Do not think that you can give out the security responsibility to everyone else. You are still the person who has the responsibility.</td>
</tr>
<tr>
<td>Category</td>
<td>Subcategory</td>
<td>Challenges</td>
<td>Attacks Scenarios</td>
<td>Recommendations</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>------------------------------------------</td>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>People</td>
<td>IT/OT security team</td>
<td>• C4 IT/OT convergence</td>
<td>• AS11 Social Engineering</td>
<td>• Create a cybersecurity team with both IT and OT personnel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C8 Human Factor</td>
<td>• AS12 Highly personalized attacks using AI</td>
<td>• Spend time on culture caps. Good collaboration start with understanding each other</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Assess the team with specific tasks where the need for collaboration is important</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Set up a list of tasks and activities throughout the year in order to have frequent meetings and discussions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Address topics like social engineering and information gathering in order to prevent information disclosure</td>
</tr>
<tr>
<td>Category</td>
<td>Subcategory</td>
<td>Challenges</td>
<td>Attacks Scenarios</td>
<td>Recommendations</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>People</td>
<td>Security Awareness Training</td>
<td>• C8 Human factor,</td>
<td>• AS1 Attacks on the connection between controllers</td>
<td>• How to detect and react to suspicious behavior in operational assets like PLCs, DCSs, and IIoT devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C4 IT/OT convergence</td>
<td>• AS2 attacks targeting sensors</td>
<td>• Get familiar with new technology used at the plant and their protocols, functions and security controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C2 Management Process</td>
<td>• AS3 attacks targeting actuators</td>
<td>• Learn about specific attacks like malware and DDoS attacks and how to react in such situations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AS8 Malware attacks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Subcategory</td>
<td>Challenges</td>
<td>Attacks Scenarios</td>
<td>Recommendations</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Process</td>
<td>Asset Management</td>
<td>• C1 Vulnerable components</td>
<td>• AS8 Malware</td>
<td>• The benefits of having proper asset management are many - address this when discussing with management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C3 Increased connectivity</td>
<td>• AS9 DDoS Attacks</td>
<td>• Prioritize the most critical assets if there are too many</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C5 Supply chain complexity</td>
<td>• AS10 Stepping Stones Attacks</td>
<td>• Having a good plan for how to define and detect assets as well as how to manage and upgrade the database is crucial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C11 Security updates</td>
<td></td>
<td>• Use both passive and active sources when detecting assets if possible.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Defining who is responsible for which assets and how this group or person should react in case of an incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Have frequent routines for how often one takes backup and updates the asset register. New assets should be added when connected to the system</td>
</tr>
<tr>
<td>Category</td>
<td>Subcategory</td>
<td>Challenges</td>
<td>Attacks Scenarios</td>
<td>Recommendations</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>------------</td>
<td>------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Process</td>
<td>Risk Manage-</td>
<td>• C10 Safety aspects</td>
<td>• AS7 Safety Instrumental</td>
<td>• OT, IIoT, and Industry 4.0 threats and attack scenarios must be taken into account when doing risk assessments</td>
</tr>
<tr>
<td></td>
<td>ment</td>
<td></td>
<td></td>
<td>• When doing risk assessments on OT, make sure there is OT personnel helping out with the assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Use a pre-defined framework to make sure there is a common understanding of what needs to be done</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• The definition of what an acceptable risk varies between IT and OT. Be prepared for trade-offs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Address the safety and environmental aspect in light of cyber security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Conduct risk assessment annually if possible, especially in the most critical parts of production</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• If possible, implement both a top-down as well as a bottom-up approach when doing risk management</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td><strong>Subcategory</strong></td>
<td><strong>Challenges</strong></td>
<td><strong>Attacks Scenarios</strong></td>
<td><strong>Recommendations</strong></td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| Process      | Vendor and Third Party Agreements | • C1 Vulnerable components  
• C6 Legacy industrial control systems  
• C12 Secure product lifecycle | • AS1 Attacks on the connection between controllers  
• AS2 attacks targeting sensors  
• AS3 attacks targeting actuators  
• AS5 Attack against the IIoT gateways | • Check existing SLAs and see if it is possible to upgrade the security part  
• Establish good and frequent communication with vendors  
• Ensure IT and OT collaborate on the security when signing new SLAs  
• Push security in all SLAs, even if it turns out to be "should-have" instead of "must-have." |
<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>Challenges</th>
<th>Attacks Scenarios</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>Network Architecture</td>
<td>• C3 IT/OT Increased connectivity</td>
<td>• AS4 Attack on the information transferred over the network</td>
<td>• Create a proper plan for segregating and segmenting the network. Ask for help if there is little competence in the company</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C4 IT/OT convergence</td>
<td>• AS8 Malware</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C7 Insecure protocols</td>
<td>• AS9 DDoS Attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C6 Legacy industrial control systems</td>
<td>• AS10 Stepping Stones Attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C11 Security updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Use a reference model to separate the enterprise network from the operational network. Minimize the paths that allows communication from enterprise to OT
- Focus on segmenting and creating security levels with respect to critically
- Put work into creating proper firewall rules. All traffic should be terminated in a firewall
- Build an iDMZ zone where all traffic is terminated
- Make sure patching and updating goes through the iDMZ as well as remote connections
<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
<th>Challenges</th>
<th>Attacks Scenarios</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>Industrial Internet of Things</td>
<td>• C1 Vulnerable components</td>
<td>• AS4 Attack on the information transferred over the network</td>
<td>• When possible, choose trusted manufacturers of IIoTs where security is a priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C7 Insecure protocols</td>
<td>• AS5 IIoT gateways</td>
<td>• Make sure to configure the asset with all build-in security controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C9 Unused functionalities</td>
<td>• AS6 Control of remote controllers.</td>
<td>• Test the devices before connecting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C11 Security updates</td>
<td></td>
<td>• Have proper authentication and authorization for each device in use, e.g., through digital certificates</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Use secure protocols whenever possible</td>
</tr>
<tr>
<td>Category</td>
<td>Subcategory</td>
<td>Challenges</td>
<td>Attacks Scenarios</td>
<td>Recommendations</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Technology</td>
<td>Cloud</td>
<td>• C7 Insecure protocols</td>
<td>• AS1 Attacks on the connection between controllers</td>
<td>• Reflect on how the cloud solution will affect the security of the rest of the system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• C8 Human factors</td>
<td>• AS2 attacks targeting sensors</td>
<td>• Be specific in the SLA and ask for security controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• AS3 attacks targeting actuators</td>
<td>• Discuss backup and recovery possibilities with the provider but do also have an internal routine for this</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• AS5 IIoT gateways</td>
<td>• Let the devices who are to push data into the cloud authenticate themselves, and thus do not let anything else upload data to the cloud</td>
</tr>
<tr>
<td>Category</td>
<td>Subcategory</td>
<td>Challenges</td>
<td>Attacks Scenarios</td>
<td>Recommendations</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>-------------------------------------------------</td>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Technology</td>
<td>Remote access</td>
<td>• C4 IT/OT convergence</td>
<td>• AS6 Control of remote controllers</td>
<td>• Use Identity Access Management (IAM) or similar to have control over users, user groups their different access rights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AS5 IIoT gateways</td>
<td></td>
<td>• Use multi-factor authentication when possible</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Create personal accounts for everyone asking to access the system</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Have clear access policies and do not give out more access than absolute necessary</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Maintain lifecycle control over users and delete users who should no longer have access frequently</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Implement a just-in-time approach for users to only have access in a specific amount of time</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Audit and log all modifications and configurations are done in the system</td>
</tr>
</tbody>
</table>

Table 4.1: Table for challenges, attack scenarios and recommendations
Chapter 5

Evaluation

5.1 Evaluation

In order to see how well these recommendations are, as well as the usefulness of the connection with the challenges and related attack scenarios, the main part of the thesis was reviewed and discussed with the industrial company. As some of the recommendations are based on their work with Telenor, one can discuss how this influences their ability to neutrally look at the recommendations. However, they were also asked to give feedback on structure, usefulness and how easy the language was to understand.

In general, the company was satisfied with the final product. They liked the structure with people, processes and technologies as it covers the main areas of issue. They also find satisfaction in that it is not as obscure as many of the frameworks and that the recommendations are given based on the findings, and not only listed as a point without any further explanation.

With that being said, they did state that it cannot be read and understood by someone with no knowledge about cybersecurity beforehand. This is due to the fact that there are many field-specific terms that one is expected to
know. There was also raised a discussion about whom the recommendations and tables are targeted towards. Someone in the company addressed that this could be reviewed by specific groups inside the company, while others meant that if it was targeted towards leaders the text was too difficult to understand.

5.1.1 People

Commenting on the people section, it was pointed out that the management part was recognizable. The issue of unknowable leaders persists and will be a challenge for the next years. They agreed on building a strong organizational security culture, especially involving the workers in the OT field.

Designing the IT/OT security team was easily understood and highly recognized. As the thesis aims to give general advice, the team’s structure is not specifically stated, neither is how one creates time and budget for such teams. This is due to the fact that it depends immensely on the organization’s size, management, resources and knowledge. This was understood by the industrial company, but a little advice on how to construct such team was something they would have wanted.

It could have been more clear how one is to train for specific incidents like malware and social engineering attacks. The focus should be on yearly training, in a recognized environment. Hopefully, specific courses on these topics will emerge and become available in the next years.

One of the participants pointed out that they would have liked recommendations on how to address the need for budgeting for cybersecurity to the management. As security controls can be expensive, having a good dialogue on what is necessary to protect the company is important. Hoping that increased knowledge among the leaders will be sufficient enough for them to see the need for great security, it was left out on purpose.
5.1.2 Processes

The asset management part was considered important, and they recognized their situation as described by the quotes. They would start to look into how to implement asset management, and especially how they can communicate that this will be beneficial for the rest of the security work in the company.

An important part of security work in industrial systems is incident handling. In case of an unwanted incident, everyone should know what to do and whom to contact. This can reduce the effects of the incident, but more important keep workers at industrial plants out of danger.

This was left out from the thesis, as it is extremely important that the industrial company tailor the incident response to their specific systems. Having a general incident response plan will not work, and thus giving general recommendations did not seem appropriate.

The risk management part was appreciated, and it was a common agreement that risk management for ICS is hard. Having explained two different frameworks that can be used was valuable. There was however a common understanding that these needs to be developed further in order to help industrial companies protect themselves against cyber threats.

5.1.3 Technologies

For the technology part, it was mostly good feedback. One could have added more specific controls, and written more about PAM and IAM solutions. Due to the time frame and scope of the thesis, it was chosen not to add information about 5G security. It will be an important part of Industry 4.0, however, as the topic is very broad, it would have consumed a lot of this thesis. How each company chooses to implement 5G solutions will also vary. That being said,
more focus on 5G in industrial systems and how this will contribute to the
security of the systems will be beneficial.
Chapter 6

Conclusion

This thesis has examined a Norwegian industrial company on its way to a more secure future enabling technologies from Industry 4.0. Based on the experiences from this work, and state-of-the-art literature, one has tried to give recommendations for how to securely transfer from Industry 3.0 to Industry 4.0. In addition to this, the recommendations have been connected to challenges and attack scenarios most relevant for Industry 4.0. This chapter will provide a conclusion for the thesis and the stated research questions.

6.1 Conclusion

The recommendations have been categorized into three main categories, People, Processes and Technologies. Each category has subcategories with excerpts from interviews and in-depth explanations behind the recommendations. In addition to this, the recommendations have been connected to challenges and attack scenarios most relevant for Industry 4.0. This is to prove that one can minimize the risks of many of these challenges and attack scenarios through the presented recommendations.
**RQ1: How can industrial companies secure themselves against threats related to Industry 4.0?**

For the first research question, the recommendations that have been given in each subcategory can be helpful when trying to secure against threats for Industry 4.0. Moreover, the method of thinking about securing multiple aspects of the company like People, Processes and Technologies with their subcategories is important. The recommendations are to some extent general, and needs to be specified and tailored to each company. They are also not exhaustive, meaning that implementing the recommendations will not secure against all attack scenarios or help with all challenges.

**RQ2: How can one link security recommendations to relevant challenges and attack scenarios for Industry 4.0?**

Each subcategory has its own Related Challenges and Related Attack Scenarios part, describing what challenges and attack scenarios can be relevant for that subcategory. To create an overview, a table has been presented in section 4.4 with all the information. The aim is to show that it is possible to mitigate some of the risks using the recommendations. In accordance, it also shows that one can cover a rather large set of risks and challenges by focusing on some key categories.

In addition to answering the research questions, the thesis has provided insight from an industrial company in Oslo trying to secure themselves for the fourth industrial revolution. The analyses have presented some general perceptions from Telenor when securing industrial companies and compared this with the situation in the industrial company. This shows that manufacturers, in many cases, lack the knowledge to secure both the IT and the OT sides of the company. Management is not prepared to secure the OT side and is therefore not ready to move into Industry 4.0. Before installing IIoT devices, cloud solutions, and remote access, the OT security will have to increase.
6.2 Future Work

In the future, it will be important to gather knowledge of different industrial sectors. Manufacturing can learn a lot from the oil, gas and power industries, but this collaboration will require more specific work. There are incentives to do this, but this needs to be recognized. There will be a need to fund the collaboration and let more companies take part in the cooperation.

There will also be a need to support the industrial companies in the shift from Industry 3.0 to Industry 4.0 in terms of designing secure devices aimed at industrial systems. This will be crucial when companies start adopting new technology like IIoT. There will also be a need to better figure out one can do proper risk management in IT/OT environments, taking safety into consideration.

Lastly, the sector needs competent people with knowledge of both IT and OT security. In order to accomplish this, relevant courses and workshops need to be designed. Schools and universities will have to work closely together with the industry in order to educate people with the correct competence.
Bibliography


URL: https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/.


Appendices
.1 Mandate

Following is the censured mandate made in order to get access to the industrial company’s information and project.
Mandat for samarbeid mellom Oslo REG og Josephine Kjelsrud iht. masteroppgave om sikkerhet i OT-systemer

Bakgrunn

Cyberangrep på industrielle systemer har de siste årene økt kraftig, som et resultat av OTmiljøer gjennom digitalisering åpner opp mot IT. Man ser at operasjonell teknologi ikke har de samme forutsetningene for å beskytte seg mot slike angrep sammenlignet med IT-systemer. Det er derfor ønskelig å se på hvordan man kan heve sikkerheten i industrielle miljøer for å minimere skadene slike angrep kan medføre.

I den forbindelse har det blitt initiert kontakt mellom masterstudent Josephine Kjelsrud (Institutt for Informatikk, UiO) og Oslo Renovasjons og gjenvinningsetaten (REG) gjennom medveileder Jan-Petter Torgersrud fra Telenor i mai 2021. Hensikten med samarbeidet vil være å belyse og avdekke sikkerheten i REGs kritiske infrastruktur, samt bidra inn i akademia med forskningen på hvordan man kan forbedre sikkerheten i OT-systemer ved hjelp av teknikker man i dag kjenner fra IT.

Formål/Målsetninger

Masterstudenten skal utrede virksomhetskritiske tjenester mot kritiske/sårbare komponenter til Reg og dokumentere hvordan denne strukturen bør utvikles fremover med hensyn til den nyopprettede SOCen. Formålet med arbeidet er å:

- Bidra til økt kunnskap om kritiske/sårbare komponenter i REGs teknologisystemer.
- Bidra til en optimalisering av SOCens hovedfokusområder.
- Bidra til økt forståelse for viktigheten av sikkerhet ovenfor Oslo ledelse og ansatte.
- Gjennom masteroppgaven bidra til økt forståelse for OT sikkerhet i akademia.

Hovedleveranser

- Kartlegge og skissere virksomhetskritiske tjenester mot kritiske/sårbare komponenter og subsystemer.
- Fremstille resultatet av kartleggingen gjennom visualisering ved bruk av eksternt visualiseringsverktøy.
- Basert på kartleggingen lage en liste over de mest kritiske komponentene.
- Komme med anbefalinger og fremme forslag til hovedfokusområder til den nyopprettede SOCen på bakgrunn av listen, der det er hensiktsmessig.
Avgrensning


Sammensetning av arbeidsgruppe

- Josephine Kjelsrud, masterstudent
- Jan-Petter Torgersrud, medveileder Telenor
- Jørgen Bakke, Oslo REG
- Leif Søgnen, Oslo REG

Prosessplan

- Tidsplan: Masterstudenten følger prosjektet utover høsten og intensiverer sitt arbeid i desember og frem til mai, i henhold til utviklingen i prosjektet. Ferdigstilt masteroppgave med funn og konklusjon vil være klar medio mai 2022.
- Masterstudenten holder alle i arbeidsgruppen informert om fremdrift i arbeidet via epost og felles møter.
- Prosess: Masterstudenten kartlegger forretningsprosessene med delsystemer og underkomponenter systemet i løpet av høsten gjennom tett dialog/intervju med de involverte fra [REG]. Funnene vil bli analysert og prosessert fra januar til mai 2022.
.2 Interview Guides

The interview guides described in chapter 3 is attached. Interview guide 1-3 was made for participants in Telenor, while 4-7 was made for interviewees from the industrial company.
1. Telenor employee working with security processes

Introduksjon

- Kanskje du kan starte med å fortelle litt om deg selv? (Hvor er du fra, hva har du studert)
- Hvor jobbet du før du begynte i bedriften?
- Kan du fortelle litt om din stilling og hva du jobber med/arbeidsoppgaver?
- Hva er en din rolle i forbindelse med cyber sikkerhet?
- Hvor lenge har du hatt denne stillingen?

Hoveddel

Arbeidsmetodikk

- Når dere går inn i et IT/OT prosjekt, hvordan jobber dere for å få oversikt over eksisterende sikkerhetstiltak?
- Hva er det mest krevende med å jobbe med sikkerhet i industrielle systemer?
- Hvordan føler du ledelse ser på sikkerhet i industrielle bedrifter?
- Hvilke deler av sikkerheten i en bedrift er det som oftest er mest ubehandlet?

Mangler i IT/OT

- Vil du si at det er noen hovedtrekk som går igjen i fht. mangler når det gjelder sikkerhet i industrielle bedrifter?
- Hvordan jobber dere med standarder når dere skal sikre industrielle systemer? Er det annerledes fra IT-systemer?
- Hvordan føler du sikkerhetstiltak er dokumentert?
- Hvilke utfordringer er det med å følge eventuelle standarder når dere sikrer?
- Hvordan jobber dere med risk management?
- Hvilke sider av risk management er de vanskeligste?

Hos bedriften

- Hvilke funn har blitt gjort ang. sikkerheten hos den konkrete bedriften i Oslo?
- Hvordan føler du dette samansvarer med andre bedrifter dere jobber med?
- Hva har vært det mest utfordrende med dette oppdraget så langt?
- Hvilke prosesser og tiltak må igangsettes for at sikkerheten hos bedriften skal bli mest mulig optimal?

Avslutning

- Er det noe du vil tilføye selv?

Takker for deltagelse. Undersøker om det er mulig å komme med oppfølgingsporsomål i etterkant.
2. Telenor employee working with security in industrial systems

Innledning

- Kanskje du kan starte med å fortelle litt om deg selv? (Hvor er du fra, hva har du studert)
- Hvor jobbet du før du begynte i bedriften?
- Kan du fortelle litt om din stilling og hva du jobber med/arbeidsoppgaver?
- Hva en din rolle i forbindelse med cyber sikkerhet?
- Hvor lenge har du hatt denne stillingen?

Hoveddel

Overordet om Telenor

- Hvor lenge drevet med industrielle kunder?
- Hvilke områder er det dere hjelper til på?
- Hva anser du som den største utfordringen til kundene?
- Har dere noen videre plan for «sikkerhetspakker»?
- Hva skulle du ønske kundene gjorde eller hadde før de kom til dere?

Management og policies

- Hvordan opplever du at de ulike lederne i de industrielle bedriftene håndterer overgangen til sikrere løsninger?
- Hvordan tror du man bør konstruere sikkerhetsteam for å få til optimal IT/OT convergence?
- Hvilke rammeverk anbefaler dere at man forsøker å være compliant med når det gjelder IT/OT?
- Hvordan tenker dere når dere guider bedrifter gjennom risk management?

5G

- Har dere begynt å implementere 5G hos industrielle bedrifter?
- Hvordan konstruerer dere vanligvis dette? Private 5G network?
- Layred security?
- Er det andre sikkerhetsmekanismer i 5G som man må tenke på når man legger det opp for industrielle bedrifter?
- Hva er utfordringen sikkerhetsmessig når man skal legge om til 5G med IIoT og cloud?

Remote Access

- Største forskjell fra tidligere behov?
- Noen standardløsning for industrielle kunder?
- Utfordringen sikkerhetsmessig?
- Krav for en sikker, god remote access løsning?
- Hva blir viktig de neste årene når det gjelder dette?

**IIoT**
- Hvordan bistår Telenor kunder med sikring av IIoT devices?
- Er det formelle kriterier for hvordan man skal velge sikre devices?
- Anbefaler Telenor noen spesifikke protokoller noe mer enn noen andre protokoller?
- Har man opplevd problemer med å integrere disse med legacy systemer? Hvordan påvirker i så fall det sikkerheten?

**Cloud**
- Noen standard provider eller Telenor selv?
- Privat vs. Public. Hva brukes?
- Sikkerhetsutfordringer i Cloud
- Hva skal til for å få en sikker cloud løsning i industrielle systemer?

**Avslutning**
- Er det noe du vil tilføye selv?

Takker for deltagelse. Undersøker om det er mulig å komme med oppfølgingsspørsmål i etterkant.
3. Telenor employee working with network security

Introduksjon

- Kanskje du kan starte med å fortelle litt om deg selv? (Hvor er du fra, hva har du studert)
- Hvor jobbet du før du begynte i Telenor?
- Kan du fortelle litt om din stilling og hva du jobber med/arbeidsoppgaver?
- Hva en din rolle i forbindelse med cyber sikkerhet?
- Hvor lenge har du hatt denne stillingen?

Hoveddel

Nettverk

- Hvordan vil du si at nettverket er strukturert i dag?
- Er dette en vanlig måte for industrielle bedrifter å strukturere på?
- Hvordan er segmenteringen med soner, brannmurer og ip-adresser?
- Hva skal til for å få adgang ned i de nedre lagene i dag?

Sikkerhet

- Hvilke sikkerhetsmekanismer inneholder nettverket i dag?
- Hvordan er ende-komponenter og hosts beskyttet?
- Hvilke oppgraderinger skal Telenor gjøre for å øke sikkerheten?
- Hva mener du må til for at ledere skal forstå truslene i et OT-nettverk?

Framtidige trusler

- Hvordan vil den nye modellen tilrettelegge for sikkerhet for ny teknologi (Cloud, IIoT)?
- Hvilke trusler mot nettet er det Telenor har fokus på når dere nå hjelper bedrifter å oppgradere sikkerheten?
- Dersom det opprettes en SOC fra Telenors side for å bistå bedriften, hvordan vil denne kunne bistå i arbeidet dersom det blir en nettverkshendelse f.eks. malware.
- Hva er dine beste tips for å sikre OT-nettet mot fremtidige trusler?

Avslutning

- Er det noe du vil tilføye selv?

Takker for deltagelse. Undersøker om det er mulig å komme med oppfølgingsspørsmål i etterkant.

Introduksjon

- Kanskje du kan starte med å fortelle litt om deg selv? (Hvor er du fra, hva har du studert)
- Hvor jobbet du før du begynte i bedriften?
- Kan du fortelle litt om din stilling og hva du jobber med/arbeidsoppgaver?
- Hva en din rolle i forbindelse med cyber sikkerhet?
- Hvor lenge har du hatt denne stillingen?

Hoveddel

Standarder

- Hvordan er sikkerhetsføringene fra Oslo kommune? (Blir det lagt føringer fra bystyret, overordnet strategi man må forholde seg til...?)
- Hvilke standarder eller rammeverk er bedriften med?
- Hvor ofte gjennomgår man disse og sjekker at man er compliant?
- Hvor ofte gjennomfører man ROS-analyser eller Risk-asessment?
- Hvordan foregår Risk assessment (hvilke standarder?)

Sikkerhet

- Hvem er ansvarlig for cybersikkerhet? (roller)
- Hvordan blir disse rollene utdelt?
- Får de ansvarlige opplæring? Hva slags?
- Hva legger du i ordet cyber sikkerhetshendelser?
- Hvor ofte blir dere utsatt for cyber sikkerhetshendelser?
- Hvis sjeldent/aldri: Hva tror du er grunnen til det?
- Hvilke cyber sikkerhetshendelser er dere bekymret for?
- Hva tror du er de største risikoene for bedriften per dags dato?
- Dersom du hadde fått mye mer ressurser i form av penger og arbeidskraft, hva ville du ha endret av komponenter, nettverk, struktur, og opplæring?
- Er IT- og OT-avdelingene oppmerksom på hvordan tilgang/uautorisert tilgang i motsatt system kan påvirke egne systemer? F.eks: tilgang til kontrollsystemene, gjennom IT-systemene.

- En hendelse har et tidsperspektiv som kan deles inn i før, under og etter at hendelsen har skjedd. Hvilken fase fokuserer dere på og hvorfor?
- Hvor mener du at fokuset burde ligge?
- Hvilke planer har dere for hvordan dere håndterer sikkerhetshendelser?
• Hvor ofte revideres planen deres?
• Hvilke tiltak har dere gjort for å beskytte dere mot cyber sikkerhetshendelser?

• Har dere trent på dette? Hvordan? Hvor ofte?
• Hvem inkluderes i treningen?

• Har dere hindret sikkerhetshendelser ved hjelp tiltakene deres?
• Hvilke forsvaresmekanismer har dere for å oppdage hendelser? (IDS, logger, overvåkning, osv)
• Følger dere med på disse mekanismene?
• Har dere oppdaget/stanset sikkerhetshendelser ved hjelp av disse forsvaresmekanismene?
• Man må anta at noen er istand til å komme gjennom barrierekontrollen. Hva gjør dere når dere oppdager sikkerhetshendelser? (rett etter)
• Hvor lang tid går det før dere har en respons på plass?

• Hvilke prioriteringer gjør dere? (availability vs confidentiality)
• Hvem er ansvarlig for hendelsesløpet i etterkant?
• Har dere trent på dette scenariet?
• Hvordan føler du resten av ledelsesgruppen ser på sikkerhet?
• Hva skal til for å få mer fokus på sikkerhet blant ledere i bedriften?
• Hva er bedriftens største utfordringer de kommende årene, slik du ser det?

Avslutning

• Er det noe du vil tilføye selv?

Takker for deltagelse. Undersøker om det er mulig å komme med oppfølgings-spørsmål i etterkant.
5. Industrial company employee. OT/IT responsibilities.

Introduksjon

- Kanskje du kan starte med å fortelle litt om deg selv? (Hvor er du fra, hva har du studert)
- Hvor jobbet du før du begynte i bedriften?
- Kan du fortelle litt om din stilling og hva du jobber med/arbeidsoppgaver?
- Hva en din rolle i forbindelse med cyber sikkerhet?
- Hvor lenge har du hatt denne stillingen?

Hoveddel

OT-miljøet

- Kan du snakke litt om hvordan OT-miljøet er konstruert i dag? (PLC, RTU, HMI..)
- Hvordan vil du beskrive sikkerheten til disse komponentene?
- Hvordan er redundansen til de ulike systemene?
- Dersom det skulle bli full stans i produksjonen, hva vil det ha å si for mennesker og miljø?
- Hvis en hendelse inntreffer, hva er da prosedyre for varsling?
- Hvor kritisk er systemet? Hvor lenge kan det være nedetid?
- Hvilke komponenter vil du betegne som de mest sårbare /kritiske?

IT-miljøet

- Hvordan er infrastrukturen til nettverket bygget opp i dag?
- Hva vil du si er de mest kritiske punktene i nettet?
- Hvordan tillater man fjerntilgang i dag?
- Hvordan er brannmurer benyttet for å segmentere nettet?
- Hvordan henger nettverket på de ulike anleggene sammen? Hvordan påvirker de hverandre?
- Hvilke mekanismer finnes i dag for å overvåke nettet?

Sikkerhetsprosjektet

- Hva var det some gjorde at sikkerhetsprosjektet med Telenor ble iverksatt?
- Hva er scopet på prosjektet?
- Hvordan ble dette adressert av ledelsen? Budsjett, diskusjoner osv.
- Hvilke endringer vil Telenor gjøre/bistå med?
- Hvordan vil dette heve sikkerheten i bedriften?
- Hva slags kompetanse er det Telenor sitter med som gjør at dere velger å bruke dem?

Avslutning

- Er det noe du vil tilføye selv?
Takker for deltagelse. Undersøker om det er mulig å komme med oppfølgingsspørsmål i etterkant.
6. Industrial company employee. OT responsibilities.

Introduksjon

- Kanskje du kan starte med å fortelle litt om deg selv?
  (Hvor er du fra, hva har du studert)
- Hvor jobbet du før du begynte i bedriften?
- Kan du fortelle litt om din stilling og hva du jobber med/arbeidsoppgaver?
- Hva en din rolle i forbindelse med cyber sikkerhet?
- Hvor lenge har du hatt denne stillingen?

Hoveddel

IT/OT

- Hvordan vil du si at samarbeidet mellom IT og OT fungerer i bedriften i dag?
- Hvis samarbeid, hva samarbeides det om?
- Hvordan er samarbeidet organisert? Er det en felles IT/OT gruppe?

Sikkerhet generelt

- Hvordan sikkerhetsfokuset vært de siste årene?
- Hvordan vil du beskrive kompetansen blant de ansatte?
- Hva har ledelsen bidratt med hva gjelder sikkerhet?

Sikkerhet i OT-miljøet

- Hvordan vil du beskrive fjerntilgangsmuligheten til det operasjonelle miljøet i dag?
- Dersom systemet eller deler av systemet bryter sammen, hvordan er redundansen?
- Hvor mye av dagens komponenter er koblet opp mot internett?
- Vil du si at sikkerhet blir prioritert når det skal kjøpes inn nytt OT-utstyr?
- Dersom det skulle skje en sikkerhetshendelse i dag, hvor godt vil OT siden av bedriften være forberedt på dette?

Forbedringspunkter

- Hva vil du si er hovedproblemene til bedriften i dag ang. sikkerhet?
- Hvordan kan man forbedre sikkerhet i det operasjonelle miljøet i følge deg?
- Hva ser du for deg at ledelsen kan gjøre for å forbedre sikkerheten?

Avslutning

- Er det noe du vil tilføye selv?

Takker for deltagelse. Undersøker om det er mulig å komme med oppfølgingsspørsmål i etterkant.

Introduksjon
- Kanskje du kan starte med å fortelle litt om deg selv?
  (Hvor er du fra, hva har du studert)
- Hvor jobbet du før du begynte i bedriften?
- Når begynte du i bedriften?

Hoveddel

Samarbeid
- Hvordan er forholdet mellom bedriften og Oslo kommune?
  (Bli det lagt føringer fra bystyret, overordnet strategi man må forholde seg til...?)
- Hva slags erfaringsutveksling og samarbeid er det med andre liknende etater som vann & avløps etaten?
  (Konferanser, diskusjonsforum, beredskap?)
- Er det noen overordnede strategier eller dokumenter som bedriften må forholde seg til?
  (Nasjonal, kommunalt, sektor?)

Mål og KPI
- Finnes det en strategi eller handlingsplan som er skrevet av og for bedriften?
- Hva ligger til grunn for hva som kommer med i årsrapporten?
- Hva er det bedriften skal levere til Oslo kommune og befolkningen?
- Hva er de viktigste strategiske målene for de kommende årene bedriften?
- Hvilke KPIer har bedriften i dag?
  (Utslipp, dokumenter, arbeidsmiljø, sikkerhet)
- Finnes det en oversikt over hva vi måler på de ulike anleggene (PLC)?
- Hvordan sikrer vi at vi leverer på det vi skal levere på?
  (Revisjon, årsmøte?)

Sikkerhet
- Vil du si at bedriften har en samfunnskritisk funksjon, og i så fall hvorfor?
- Hvilket sikkerhetsperspektiv ligger til grunn når det skal oppgradere/kjøpes noe nytt?
- Finnes det noe råd eller forum som diskutere sikkerhetsstrategi, innkjøp, prosjekter osv?
- Hvordan vil du beskrive den tekniske sikkerhetskulturen i bedriften?
- Hvor mange jobber med sikkerhet i bedriften?
- Har du måtte håndtere sikkerhets hendelser i løpet av din tid i bedriften?
  (Hva synes du er vanskeligst når det kommer til å håndtere sikkerhets hendelser?)
- Dersom bedriften skulle blitt utsatt for et dataangrep, hva er planen?
(Hvilke anlegg/funksjoner sikres, hvem kontaktes, hvordan er backup/redundans, IDS/logger)

- Hvem har hovedansvaret under et eventuelt angrep?

Økonomi og ledelse

- Hvordan er sammenhengen mellom økonomi og sikkerhetsarbeid?
- Er det satt av ekstra midler til sikkerhet de kommende årene?
- Hvordan føler du resten av ledelsesgruppen ser på sikkerhet?
- Hva skal til for å få mer fokus på sikkerhet blant ledere i bedriften?

Avslutning

- Hva er bedriftens største utfordringer de kommende årene, slik du ser det?
- Hvordan tror du systemene og teknologien kommer til å utvikle seg de neste årene?
- Hvilken kompetanse vil bli viktig å sikre seg for å være oppdatert?
- Er det noe du vil tilføye selv?