Juuso Viljamaa

# OT SECURITY AND TELECOMMUNICATIONS NEEDS AND REQUIREMENTS IN SMART FACTORY ENVIRONMENT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

# TIIVISTELMÄ

Viljamaa Juuso
Operatiivisen Teknologian (OT) Turvallisuus ja Tietoliikenne Tarpeet ja Vaatimukset Älytehdasympäristössä
Jyväskylä: Jyväskylän yliopisto, 2022, 92 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaajat: Seppänen Ville, Takala Arttu

Tämä pro gradu -tutkielma tutkii operatiivisen teknologian (OT) turvallisuuteen ja tietoliikenteeseen liittyviä tarpeita ja vaatimuksia älytehdasympäristössä. Tutkielma noudattaa Design Science Research (DSR) tutkimus metodologiaa, jonka tarkoituksena on tuottaa päätöksentekoa avustava opas yritysten käyttöön, jossa esitetään tärkeimpiä vaatimuksia OT turvallisuus ja tietoliikenne perspektiivistä. Tutkimusprosessiin kuuluu kirjallisuuskatsaus, jonka pohjalta tunnistetaan tärkeimpiä vaatimuksia älytehdasympäristöön liittyen. Tätä tietoa jalostetaan tekemällä kvalitatiivisia haastatteluja yrityksessä x haastatellen teknisiä asiantuntijoita. Tämän ensimmäisen haastattelukierroksen jälkeen tuotetaan raakaversio oppaasta, joka menee toiselle haastattelukierrokselle arvioitavaksi. Tämä arviointi kierros koostuu kahdesta osasta, jotka ovat oppaan vaatimusten kvantitatiivinen prioriteetti ja kompleksisuus arviointi sekä kvalitatiivinen palautteen anto tuotetusta oppaasta johtaja/päällikkö tason näkökulmasta. Näiden perusteella tuotetaan lopullinen versio päätöksentekoa tukevasta oppaasta, mutta annetaan myös osa palautteessa mainituista kehitysideoista suuntaviivoina tulevaisuuden tutkimukselle aihealueeseen liittyen.

Asiasanat: Operatiivinen Teknologia, OT turvallisuus, OT tietoliikenne, Älytehdas, Digitalisoitu teollisuus

# ABSTRACT

Viljamaa Juuso
OT Security and Telecommunications Needs and Requirements in Smart
Factory Environment
Jyväskylä: University of Jyväskylä, 2022, 92 pp.
Information Systems, Master's Thesis
Supervisors: Seppänen Ville, Takala Arttu

This master's thesis researches operational technology (OT) security and telecommunications needs and requirements in smart factory environment. This thesis obeys Design Science Research (DSR) research methodology, which aims to produce a supportive guide for decision making in companies. This guide consists of most important requirements from OT security and telecommunications perspective. The research process contains a literature review which recognizes important needs related to smart factory environment. This information is extended with the qualitative interviews which are made in company x involving technical experts. After this the draft version of the guide is created. The draft version will be evaluated on the second interview round in two parts. The first part consists of quantitative priority and complexity evaluation of requirements and the second part consists of qualitative evaluation and feedback from directorial/managerial perspective. Based on these the final version of the guide is created and some of the development ideas received based on the feedback are presented as directions for the future research.

Keywords: Operational Technology, OT security, OT telecommunications, Smart factory, Digitalized manufacturing

# TABLE OF FIGURES

Figure 1 DSR process model (Peffers et al., 2006) .................................................. 12
Figure 2 Operational requirements of IT security versus OT security (Hahn, 2016) .......................................................................................................... 18
Figure 3 Purdue model for control hierarchy (Cook et al., 2017) ......................... 22
Figure 4 Example of a Purdue network architecture (Siemers et al., 2022)......... 23
Figure 5 General layout of a SCADA system (Rakas et al., 2020)......................... 25
Figure 6 High-level example of a SCADA communication architecture (WAN highlighted) (Upadhyay & Sampalli, 2020) ........................................................... 28
Figure 7 Visualization of the added priority and complexity values to the guide (Attachment 5)......................................................................................... 58

# TABLE OF CONTENTS

TIIVISTELMÄ
ABSTRACT
TABLE OF FIGURES

1 INTRODUCTION ........ 8

2 RESEARCH METHODOLOGY ........ 11

3 LITERATURE REVIEW ........ 14
3.1 Hardware and systems of OT ........ 15
3.1.1 Lifecycle of OT components and patching in general ........ 16
3.2 Definition of OT Security ........ 17
3.2.1 Compliance of OT security ........ 18
3.3 OT Telecommunications ........ 19
3.3.1 Differences between business and OT networks ........ 20
3.3.2 Network segmentation ........ 21
3.3.3 Models for segmentation ........ 21
3.3.4 OT segments, communication, and protocols ........ 26
3.3.5 Local and remote factory environment communications ........ 27
3.4 Cyber-attacks and vulnerabilities in OT environment ........ 28
3.4.1 Real-life attacks and vulnerabilities ........ 29
3.4.2 Attack prevention and solutions ........ 29
3.5 Benefits for companies implementing smart factory environment ........ 30
3.5.1 Business and process related benefits ........ 31
3.5.2 Environmental benefits ........ 31
3.5.3 Human resource related benefits ........ 31
3.6 Summary of literature review ........ 32

4 FIRST ROUND INTERVIEWS - INFORMATION GATHERING FOR THE GUIDE ........ 33
4.1 Topic areas for interview ........ 34
4.1.1 OT hardware and systems ........ 34
4.1.2 OT security in organization culture ........ 34
4.1.3 OT standards ........ 34
4.1.4 OT telecommunications ........ 35
4.1.5 Cyber-attacks and prevention ........ 35

5 INTERVIEW RESULTS & DRAFT VERSION OF THE GUIDE ........ 36
5.1 Results of interviews ........ 37
5.1.1 OT hardware and systems ........ 37
5.1.2 OT security in organization culture ........ 38
5.1.3 OT standards ........ 40
5.1.4 OT telecommunications ........ 40

5.1.5 Cyber-attacks and prevention ........................................ 42
5.2 Quality of interviews ........................................ 44
5.3 Creation of guide – draft version ........................................ 45
5.3.1 Heading – What this guide is? ........................................ 45
5.3.2 Description – Why this guide exists? ........................................ 45
5.3.3 Scope – For who the guide is intended to? ........................................ 45
5.3.4 Contents of the guide ........................................ 46
5.4 Overview of the draft version ........................................ 47

6 SECOND ROUND INTERVIEWS – EVALUATION AND FEEDBACK OF THE GUIDE ........................................ 48
6.1 Questions for interview 2-1 ........................................ 49
6.2 Questions for interviews 2-2 ........................................ 50

7 INTERVIEW RESULTS & FINAL VERSION OF THE GUIDE ........................................ 51
7.1 Results of interview 2-1 ........................................ 52
7.1.1 Ownership of assets – OT hardware and systems management52
7.1.2 CMDB for asset information (asset register) ........................................ 52
7.1.3 Lifecycle management ........................................ 52
7.1.4 Patch and update management ........................................ 52
7.1.5 OT security as a term – OT security in organization ........................................ 53
7.1.6 OT security awareness ........................................ 53
7.1.7 Roles and responsibilities in OT security ........................................ 53
7.1.8 Usage of OT security standards ........................................ 53
7.1.9 Auditing of OT environment ........................................ 53
7.1.10 Business versus OT network recognition – OT telecommunications ........................................ 54
7.1.11 Network segmentation ........................................ 54
7.1.12 Choosing the segmentation model ........................................ 54
7.1.13 Protocols in multi-vendor environment ........................................ 54
7.1.14 Appropriate WAN solution in remote factory ........................................ 55
7.1.15 AIC instead of CIA – OT cyber preparedness ........................................ 55
7.1.16 Disaster recovery and business continuity ........................................ 55
7.1.17 Security solutions in smart factory environment ........................................ 55
7.2 Results of interviews 2-2 ........................................ 56
7.2.1 Structure ........................................ 56
7.2.2 Contents ........................................ 56
7.2.3 Functionality ........................................ 57
7.3 Analysis and finalization of the guide ........................................ 58
7.3.1 Development in this thesis ........................................ 59
7.3.2 Development directions for future ........................................ 60

8 SUMMARY AND COMMUNICATION ........................................ 62

REFERENCES ........................................ 64

ATTACHMENT 1 STRUCTURE OF THE INTERVIEW (ROUND 1) ..................68

ATTACHMENT 2 DRAFT VERSION OF THE GUIDE..........................................72

ATTACHMENT 3 STRUCTURE OF THE INTERVIEW (ROUND 2-1) ...............79

ATTACHMENT 4 STRUCTURE OF THE INTERVIEW (ROUND 2-2) ...............84

ATTACHMENT 5 FINAL VERSION OF THE GUIDE...........................................85

# 1 INTRODUCTION

OT security's role is developing besides the more familiar IT security in current organizations and manufacturing environments since the digitalization of manufacturing processes is one of the current trends. Digitalized manufacturing and the environment where the activities are carried out can be described as a smart factory environment. This environment is part of the fourth industrial revolution (Industry 4.0) which includes the aspect of Cyber Physical Systems (CPS) and Internet of Things (IoT) and can be also seen as OT/IT convergent environment which involves different systems and technologies (Vaidya et al., 2018). The environment is different from traditional IT environment since the aspect of physical manufacturing processes is involved and usually these processes must be kept available everyday around the clock. In worst case scenario security incidents in this environment can lead for example to major financial losses or even to human fatalities.

It is important for employees and organizations to understand what OT security in smart factory environment is and what does it consider. In companies the decision making related to new investments can be based on commercial actors' offerings and what is suggested per organization's environment to be implemented related to OT security from their perspective. These offerings can be proper and might be backed up for example with evidence from other companies which have implemented similar environments. This can be still recognized as a big problem related to decision making if the employees making the decisions do not have overall understanding what is procured. The academic proof and support for decision making is a huge benefit in these situations so that investments can be made in a proper manner based on knowledge of the required implementations. This thought leads to the research question: "What are the OT security and telecommunications needs and requirements in smart factory environment?". Telecommunications related requirements in the environment can be seen as part of OT security since for example network segmentation is a method for securing the networks but the topic area of telecommunications is necessary to consider as own topic to make understanding of it clearer. It is also important to understand that this thesis does not consider facility security related aspects, for example how physical access control affects the environment, although these are important topics related to overall security of smart factories.

In response to the identified problem a supportive guide for decision making in smart factory environment is created as a solution by using Design Science Research (DSR) (Peffers et al., 2006) research methodology which starts from problem identification and leads to an artifact which is developed by carrying out research related to the topic area. The guide is developed by doing literature review to recognize important topics related to OT security and telecommunications. These important topics are extended with the knowledge of technical experts by organizing qualitative interviews. Based on the combination of the literature review and interviews a draft version of the supportive guide is created. The draft version is demonstrated for the interviewees of the second round which is done in two parts. The first part consists of specialist's evaluation of priority and complexity of each requirement which is done by using numerical scales in a quantitative manner with qualitative justifications. These evaluations are added to the draft guide which is demonstrated for the second-part interviewees of the second interview round. The second part interviewees are from the directorial/managerial level which evaluate and give feedback of the developed draft guide in a qualitative manner from decision making perspective concentrating on the structure, contents, and functionality. Based on these the guide is developed to its final form and directions for future research related to topic area are stated. The research is done in cooperation with company x which is a large manufacturing company. The company uses digitalized manufacturing in its business. All of the interviewees are chosen from this company. The company and its employees are anonymized.

The structure of this master's thesis consists of seven main content paragraphs in addition with introduction which are:

- Research methodology
- Literature review
- First round interviews - Information gathering for the guide
- Interview results & draft version of the guide
- Second round interviews – Evaluation and feedback of the guide
- Interview results & final version of the guide
- Summary and communication

Attachments -list is located in the end of this thesis after references. In research methodology the DSR process (Peffers et al., 2006) is introduced for the reader and why it is used in this research. The different steps of the DSR are introduced by tying these to the different phases of this research. Following this the literature review is carried out by concentrating on OT, OT security, and OT telecommunications related topics. The topics are divided under topic areas from where the important topics are chosen for the development of the guide. The first-round interviews follow the literature review in which the important topics are extended with the experience and knowledge of technical experts from company x. The interview structure is attached to the end of this thesis (Attachment 1). The results of this interview round are considered in the following paragraph included with analysis of the answers. Based on the combination of literature review and these first-round interview results the draft version of the supportive guide is created (Attachment 2).

After the draft guide is ready it is introduced for the specialist of second interview round's first part. This part consists of the evaluation of priority and complexity of the requirements. The interview structure is attached to the attachments -list (Attachment 3). The priority and complexity values are added to the draft guide, and it is delivered for the directorial/managerial interviewees of the second part of second round. This part consists of evaluation and feedback of the guide in a "free word" manner and the structure of this interview round is as well in the attachments -list (Attachment 4). After the second round of interviews is finished the results are considered at the same time under own specific topics (results 2-1 and results 2-2) since both of the parts can be considered as the evaluation and feedback of the guide. The addition of priority and complexity values was done earlier but the results contain the analysis of why some requirement has certain values. Also, the analysis is done for the part 2 and development for the guide is made based on these. This paragraph includes the directions for the future research based on the part 2 evaluation and feedback and these are listed under this. Final version of the guide is included as the last attachment of this thesis (Attachment 5).

Summary and communication -paragraph consists of analysis of the overall process of what was made and noticed during the research. This contains observations about the research methodology (DSR) and how it was modified and used related to this thesis. This paragraph includes information about shortages related to the research and what was the response to these. Summary and communication also includes suggestions for future research and how this can benefit the academic field and companies in future. Company x is commented as a cooperative actor in the made research.

# 2 RESEARCH METHODOLOGY

The structure of this master's thesis obeys the Design Science Research (DSR) process which can be described as a step-by-step process from problem identification and motivation to communication. As this thesis aims to introduce a guide for manufacturing companies which describes the most important OT security and telecommunications components in smart factory environment, DSR will suit this goal in an appropriate way. Hevner et al. (2010) mention related to information systems research that design science supports the idea of creating innovative artifacts to solve real-world problems which was later specified with the context of business problems (Hevner et al., 2010). In this thesis the lack of academic guidance of specified needs and requirements for smart factory environment is identified as a problem for OT, IT, and business decision makers and DSR is used to create a response for this.

Based on previous, entry point for this research can be described as problem centred approach as Peffers et al. (2006) mention in their DSR process model (Peffers et al., 2006). DSR process models are not the same and these usually have differences based on the author. For example, Hevner et al. (2004) model does not include the step of demonstration which on the other hand is included in the Peffers et al. model (Peffers et al., 2006). Despite the demonstration step, these two models have a lot in common and the path of the research is similar. This thesis obeys the DSR process model (figure 1) described by Peffers et al. (2006) because it suits the problem, why this research is made (problem centred approach), and the structure of this thesis from introduction to summary (Peffers et al., 2006).

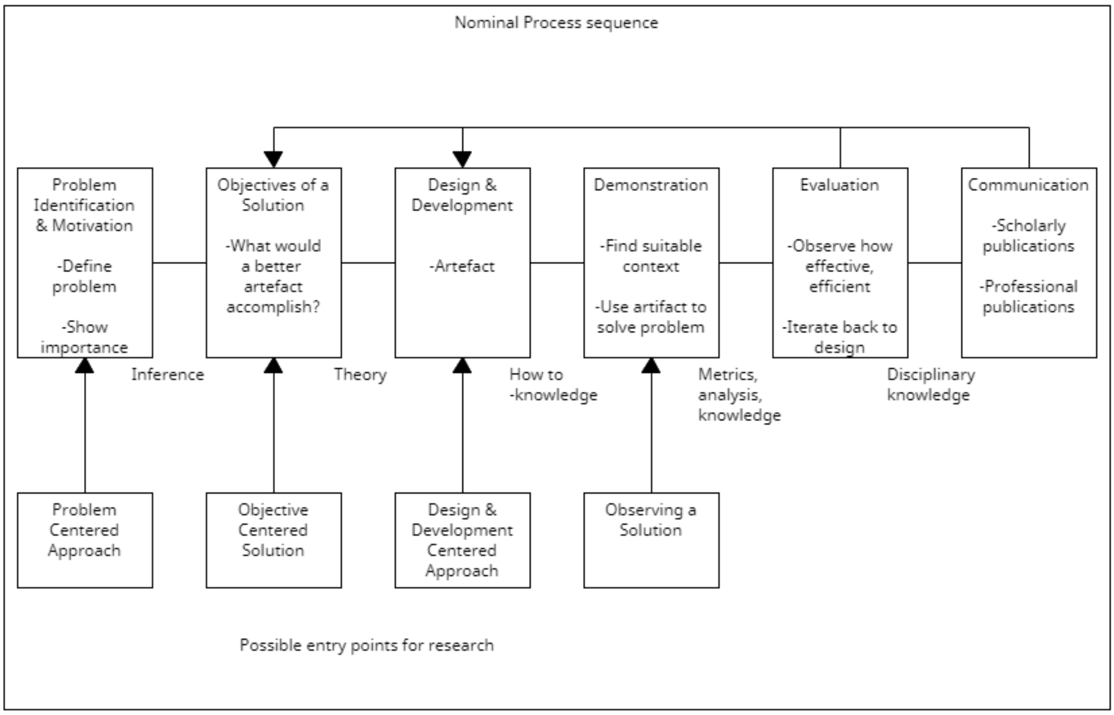

Nominal Process sequence
Problem Identification & Motivation
-Define problem
-Show importance
Objectives of a Solution
-What would a better artefact accomplish?
Design & Development
-Artefact
Demonstration
-Find suitable context
-Use artifact to solve problem
Evaluation
-Observe how effective, efficient
-Iterate back to design
Communication
-Scholarly publications
-Professional publications
Inference
Theory
How to -knowledge
Metrics, analysis, knowledge
Disciplinary knowledge
Problem Centered Approach
Objective Centered Solution
Design & Development Centered Approach
Observing a Solution
Possible entry points for research

Figure 1 DSR process model (Peffers et al., 2006)

The DSR process model (Peffers et al., 2006) in this research case starts from problem centred approach and continues with the following steps:

- Problem identification and motivation
- Objectives of a solution
- Design and development
- Demonstration
- Evaluation
- Communication

As the approach to this research is problem centred, the first step in the DSR process is the **problems identification and motivation** (Peffers et al., 2006). This step defines the specific problem and justifies the value of the created solution (Peffers et al., 2006). In this thesis, this understands the lack of "academic guides" for OT security and telecommunication in smart factory environment and that the decisions related to previous are justified with academic proof so that the business can also adapt. This can be seen as the qualitative **objective of the solution** besides the "decisions made easier" -idea for OT decision making personnel. Peffers et al. (2006) mention that the objectives should be made from the problem specification step (Peffers et al., 2006). These steps are described in the introduction of this thesis.

**Design and development** is the step of creating the solution (Peffers et al., 2006) keeping the described research goal in mind. In this thesis this appears by developing a guide using the information gathered by literature review and organizing interviews in company x to get real-world experience for reasoning the requirements in the guide. It is important to remember that the solution is made in two phases. First round of interviews will consist of more technical questions which are answered by "technical experts". The first version of the guide is made after this. The first version is the draft which is developed even further based on second interview round. The second-round interviewees are more business-oriented employees who have experience in OT/IT decision making and business. These interviewees will evaluate the draft guide and give feedback from decision making perspective. The previous process means that the design and development stay beside various steps in this DSR process.

The solution is **demonstrated** several times during the thesis after design and development phases. Demonstration is described as how the solution solves the identified problem (Peffers et al., 2006). In this case, the solution is demonstrated for the first time for second interview group to get required feedback for final solution creation. The final solution is demonstrated in this thesis for public audience and why certain changes were made for the draft version. This demonstration is better to be considered more as communication since the final version of the guide is provided for the company and academic world at the same time related to publishing of this thesis. The **evaluation** is made for the draft version based on how well the suggestions of the guide could be considered in a company, but also related to the structure and functionality of the guide. The evaluation is described as how well the solution created supports the solving of the identified problem (Peffers et al., 2006). It is important to understand that the developed guide is not taken into use in a company, but it is evaluated by IT and business-related personnel that how well it could be obeyed.

The final step, **communication**, is described as the step of communicating about what was the problem, what was made and in which way, how it can be used and what is the effectiveness (Peffers et al., 2006). The most important matter in this step is to communicate about the problem and solution for companies with or who are planning to deploy smart factories. It is also as important to communicate about this process for academic world to understand the importance of academic proof in OT related decision making. On the other hand, this thesis communicates about the effectiveness of this DSR process in research.

# 3 LITERATURE REVIEW

The information for this literature review is gathered by using google scholar as the main database for relevant academic research, but also extending the search to trustworthy academic publishers' databases. The preferred publishers are IEEE, SpringerLink, Elsevier, or similar since these can be described as trustworthy based on their JUFO-rating (Julkaisufoorumi). Also, globally recognized actors related to standards and best practices qualify as relevant sources of information. The references are chosen mainly from the time window of past five years, but also older references can be chosen based on how well these comply with the current OT and smart factory environment. The databases are searched by using recognized relevant keywords for example "OT security" or "OT networks" and extended further by using keywords which tend to appear related to the academic field of OT in earlier relevant research.

Operational Technology (OT) can be described as hardware and software that through direct monitoring and/or control of physical devices, processes and events detect or cause a change in a corporation environment (Hahn, 2016). OT often refers to Industrial Control Systems (ICS), which are used in manufacturing environment to control industrial manufacturing and/or production processes (Shilenge & Telukdarie, 2022). Examples of these kind of systems are Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Remote Terminal Units (RTU) and Supervisory Control and Data Acquisition (SCADA) systems (Shilenge & Telukdarie, 2022).

The difference between Operational Technology (OT) and Information Technology (IT) is important to understand related to this research. The technology which involves the development, maintenance, and usage of computer systems, software, and networks to process and distribute data is described as IT (Hahn, 2016). Typical IT systems, which concentrate on processing corporate data, are for example Enterprise Resource Planning (ERP) systems, Customer Relationship Management (CRM) systems, and Product Lifecycle Management (PLM) systems (Shilenge & Telukdarie, 2022). When talking about information technology especially in industrial environment, it covers corporate systems, office networks, and software which handles the data from production environment (Hollerer et al., 2021). Related to ICSs, both OT and IT can be seen as part of the overall systems, depending on functionalities, but OT is described as "the heart of the ICSs" (Hahn, 2016). One of the key differences between OT and IT is that OT focuses on monitoring and controlling of physical processes (Hahn, 2016).

The fourth industrial revolution (Industry 4.0) concentrates on Cyber Physical Systems (CPS) and Internet of Things (IoT) as part of manufacturing (Vaidya et al., 2018). Internet of Things (IoT), Industrial Internet of Things (IIoT), cloud based manufacturing, and smart manufacturing are considered as the four main drivers of Industry 4.0 which help the manufacturing process to transform into fully digitalized and intelligence one (Vaidya et al., 2018). OT can be seen as part of Industry 4.0 for example related to IT/OT cybersecurity and also as part of manufacturing facility's architecture and network design (Shilenge & Telukdarie, 2022). As smart manufacturing is described as one of the most important drivers of Industry 4.0 in different sources (Vaidya et al., 2018) (Shilenge & Telukdarie, 2022), it is important to understand the OT Security and telecommunications needs and requirements in smart factory environment and to which this research aims to provide an academic solution for manufacturing companies.

## 3.1 Hardware and systems of OT

It is important to understand related to this research what are the functionalities of different OT devices and systems. It is not necessary to understand the technical specifications of the devices. Main idea is to understand what something does and why some components of OT are in a certain connection. OT environment can be described in many different ways and there is no certain correct way of architecture. OT devices and systems can be classified on different levels based on their action and can be seen as part of SCADA system in Ghosh and Sampalli's (2019) demonstration (Ghosh & Sampalli, 2019). Three levels of architecture in this demonstration are (Ghosh & Sampalli, 2019):

- Supervisory level
- Process control level
- Field instrumentation control level

On **supervisory level**, SCADA system includes Master Station Unit (MSU) or Master Terminal Unit (MTU) which works as a control center in SCADA networks. This level also includes Human-Machine Interface (HMI) and database, but these are considered rather as IT components than pure SCADA/OT hardware components. **Process control level** has a possible Sub-MSU or Sub-MTU. It is not always necessary since the upper lever has the "main MTU" which is able to connect to the Remote Station Units (RSU) directly. RSU's are on the same architecture level and include Remote Terminal Units (RTU), Intelligent

End Devices (IED), and Programmable Logic Controllers (PLC). These devices are in connection with **field instrumentation control level's** devices and monitor the sensors and actuators to collect data from these. (Ghosh & Sampalli, 2019)

As from this classification can be seen, physical processes are related with previous levels of architecture and the hardware and systems control and/or monitor the processes. This was also mentioned in the description of operation technology in Hahn's (2016) article (Hahn, 2016). The field devices around the environment are also responsible for monitoring and controlling of processes (Pliatsios et al., 2020). For example, the earlier mentioned sensors are responsible of data gathering when on the other hand actuators perform control actions (Pliatsios et al., 2020). There is a wide list of different SCADA communication protocols (Pliatsios et al., 2020) which is an important component of OT architecture, but this topic is considered under telecommunications.

### 3.1.1 Lifecycle of OT components and patching in general

The lifecycle of OT and IT differ a lot since the usage of these devices is different. IT devices are usually used in well-controlled environments, such as office networks or server rooms, which are usually also isolated from major physical changes in environment (Upadhyay & Sampalli, 2020). OT systems, for example a SCADA system, are mostly located in factory environment or in its near environment and usually contain the effect of physical environment which can be caused by dust or different liquids (Upadhyay & Sampalli, 2020).

When designing an OT environment, the reliability of hardware is in a big role since the environment requires long-lasting products. The lifecycle of IT system is described from 3 to 5 years when on the other hand a SCADA system (OT) is required to last over 25 years. As related to OT systems physical environment requirements, systems are required to work in hot temperature from +40 to +70 degrees Celsius. This describes that the components of this environment must be heavy duty related to original IT components in different environment. (Upadhyay & Sampalli, 2020).

It is important to understand related to previously mentioned OT-IT convergence as the OT environment contains IT devices and systems, that these must fit to the requirements of the environment. As the physical effect of the environment plays a big role related to the lifecycle and reliability of the devices and system, also the length of the lifecycle plays role when connecting OT and IT devices together. The environment and connections must be able to work even though a device is replaced due to the age or malfunction. This will create a problem in an environment where field devices, for example different controllers, are from an older era when cyber-attacks were not considered as relevant threats for the environment (Upadhyay & Sampalli, 2020). Related to previous perception of the current environments, the OT devices and systems are going to be replaced at some point which is a question of time. Different scenarios related to previous are discussed in a later part of this thesis.

IT devices in organizations environment are usually updated remotely by organizations rules and are easy to install to a big number of devices. The

SCADA (OT) systems patch management is commonly done by the original equipment manufacturer and requires long periods of time to install. In IT network environment for example security updates can be handled by scanning the network and devices connected to it. Usually, companies have automated tools for these actions. The same method cannot be implemented for example to a SCADA network since the PLC's and RTU's network interface can be so fragile and weak that the scanning process could affect to the entire network, and in worst case, could shut it down and make it unavailable. (Upadhyay & Sampalli, 2020)

## 3.2 Definition of OT Security

Earlier OT and its systems were counted as "more isolated" environment and equipped with low connectivity since these different systems were operated manually or by proprietary controls (Sonkor & García, 2021). In the past, no cyber threats were identified against OT, but this has changed because of OT-IT convergence which is linked to networked industrial environment (Sonkor & García, 2021). One of the main reasons for this change is the business's demand for information from industrial control systems to be integrated with company's business network (Conklin, 2016). As many of the OT components are designated to work in an isolated environment, one important OT security related question is, how the OT systems can be protected from the outside world and its threats (Conklin, 2016). The OT-IT convergence is one component of Industry 4.0 description (Shilenge & Telukdarie, 2022) and is related straight to Industrial Internet of Things (IIoT) (Sonkor & García, 2021) which can be understood as a smart factory environment with connectivity between devices in this thesis context.

IT security focuses on data and its confidentiality, integrity, and availability (CIA-triad) (Hollerer et al., 2021). Hahn (2016) describes the CIA-triad also as part of OT security related to data in the OT systems, but also mentions the protection of physical process which includes safety, environment, dependencies, and regulation (Hahn, 2016). As Sonkor and García (2021) mentions the OT-IT convergence (Sonkor & García, 2021) and Conklin (2016) mentions the demand of business for information from production environment (Conklin, 2016), it is imminent that CIA-triad is part of OT security description. Figure 2 includes Hahn's (2016) division based on operational requirements between IT and OT security (Hahn, 2016).

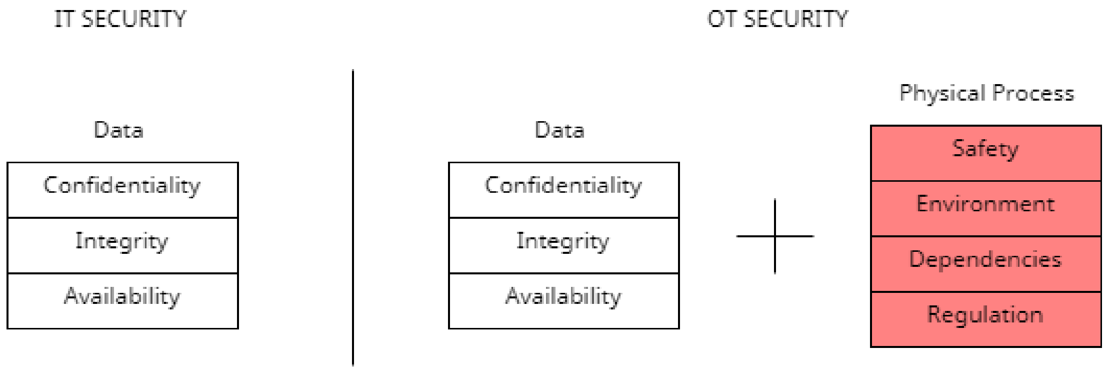


Figure 2 Operational requirements of IT security versus OT security (Hahn, 2016)

Negative impact in **safety** is described as an impact which has an effect to the safety of employees and/or neighboring communities which could result for example from kinetic forces or electrocution. Failure in systems could lead to a negative impact towards **environment** which could be a result for example of chemical releases or radiation. Often physical components of ICS are considered as critical infrastructure and a failure in system could directly or indirectly impact interdependent infrastructures which would have a negative impact related to **societal dependencies**. OT **regulations** affect the environment since ICS failures can potentially cause damage to expensive physical systems (e.g. boilers and motors) which could lead to high capital costs and long system outages. (Hahn, 2016)

OT security can be also seen as "OT environment security" since the OT-IT convergence idea connects the systems which are in place in the environment for different purposes. OT level threats are considered more as safety threats which could affect for example the availability of the environment (Hollerer et al., 2021). IT level threats can be considered as security threats (Hollerer et al., 2021), but in this thesis term "OT security" considers the OT-IT convergence related risks and threats since the main focus is on the connected smart environment.

### 3.2.1 Compliance of OT security

As mentioned, related to the description of OT security, OT is regulated to ensure the availability and safety of the controlled physical process (Hahn, 2016). There are different OT related technical standards which describe the security related requirements for OT to ensure the compliance of environment and systems. Examples of main standard providers for automation and manufacturing are International Society of Automation (ISA) and International Electrotechnical Commission (IEC) which introduce the standards ISA 62443-1-1 and IEC 62443-3-3 (Kulik et al., 2019). These standards provide the security requirements for cloud-connected industrial control systems and the IEC 62443-3-3 is beneficial to be introduced in this research with examples to understand the purpose of an OT related standard and how it considers security of OT in practice (for example SCADA system) (Kulik et al., 2019).

The IEC 62443-3-3 security standard describes the compliance requirements on technical level for OT networks and systems and the main audience of the standard is from asset owners to compliance authorities (IEC, 2013). It is important to understand that the standard does not provide detailed specifications for building a compliant security architecture (IEC, 2013). The main goal of the standard is to provide minimum set of requirements to progressively reach improved security levels (IEC, 2013). Although this standard is from year 2013 and the OT has improved during the years as technology has developed, the standard mentions about its flexibility and how the framework of IEC 62443 facilitates the addressing of current and future's vulnerabilities and application of necessary mitigations in correct manner (IEC, 2013).

An example of IEC system requirement (SR) which is described with an example by Kulik et al. (2019) is the SR 1.6 RE 1. Every requirement (SR) includes the requirement enhancement (RE) to increase the security level of the system (ISO, 2013). The system requirement states:

> The control system shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication. (IEC, 2013)

Kulik et al. (2019) consider this in their research in example environment as connection between the client and the cloud. It is also considered as connection between gateway (router) and cloud. These are the points in their cloud-OT environment where the security requirement applies. (Kulik et al., 2019)

## 3.3 OT Telecommunications

In current smart factory environments advanced systems are used to control industrial processes which are used either locally or remotely in the infrastructure (Ahakonye et al., 2021). The control systems have a high importance level since the data gathering and monitoring is done in real-time and these systems include other OT related devices which are connected to each other (Ahakonye et al., 2021). The communication between the devices and systems must be secured by using different solutions, but also the availability is an important factor since for example SCADA systems control critical physical components, for example different motors and sensors (Ahakonye et al., 2021).

The systems are connected to each other by using different telecommunications solutions depending on the intention and usage. The environment mostly sets requirements for the connectivity and network devices since the OT environment near the processes can be challenging related to for example temperatures and physical stress (Upadhyay & Sampalli, 2020). It is clear that OT environment has different requirements compared to a basic IT office environment where the devices are in more stable conditions. The IT telecommunication perspective comes to the discussion with the OT-IT convergence when different networks are integrated in an environment and for example in situations when the need of data for business from OT environment and processes is recognized.

OT telecommunications is obviously a part of OT security since the devices and networks are part of the OT environment. For example, the attacks against the systems can be committed using the connections included in the infrastructure and the existence of business network beside the smart factory environment creates needs for risk management. OT telecommunications is relevant to be considered as an individual topic in this research to create a clearer view about the infrastructure. The OT security and telecommunications connects when considering about OT targeted attacks and prevention later in this thesis.

### 3.3.1 Differences between business and OT networks

There are many ways of describing the network architecture of a company which uses OT devices and systems in their business. These models have some basic similarities which include the separated segments for different types of devices and systems, and these are separated by using firewalls between the segments. These different models are introduced in a more detailed manner later in this thesis, but at this point, it is important to understand what kind of devices and systems are in business network segments and in OT related network segments in general. The reason for segmentation is also described later in this thesis.

Business network segments typically contain employee workstations and servers which are used to operate business related activities (Zimba et al., 2018). These can be for example laptops, printers, and file servers to operate with everyday business data. For example, in smart factory context, enterprise resource planning (ERP) systems are used in these network segments to report and share business related data with other systems (Lin et al., 2019). Different everyday applications operate in these network segments like company’s email and intranet (Cook et al., 2017). The business network segments are typically connected to internet or cloud by using switches, and this traffic is filtered with firewalls (Zimba et al., 2018).

OT network segments contain devices earlier mentioned in this thesis, for example SCADA systems and PLC’s (Zimba et al., 2018). These devices are used to perform either supervisory, process control or field actions (Ghosh & Sampalli, 2019). The level of OT network segment depends on the usage and for example SCADA systems and PLC’s can be in different segments depending on the architecture (Zimba et al., 2018). Firewalls are used between the network segments to filter the network traffic like in business network segments (Zimba et al., 2018). These network segments can technically have access to internet but are in many cases separated as isolated networks (Cook et al., 2017). It is important to understand that the OT network segments handle with physical factory processes when on the other hand business network segments handle with data which is important for business. The current infrastructure models related to OT-IT convergence and Industry 4.0 are usually built inline that the network segments are in communication related to the businesses demand of information from industrial control systems (Conklin, 2016).

### 3.3.2 Network segmentation

Network segmentation in practice is dividing a network into different network segments which is done to control the communication between the segments and the Internet (Wagner et al., 2016). Generally, network access is required for cyber-attacker to carry out cyber-attacks remotely in target systems. Network segmentation is a defensive method to reduce cyber attacker's abilities to move inside a network and to reduce cyber-attack's possibilities in common (Wagner et al., 2016). Network segmentation's main goal is to protect the network resources (Wagner et al., 2016) which can include for example the availability of the network devices or from business perspective, confidentiality of data. Network segmentation brings many beneficial effects from security perspective for a corporation, which are for example (Wagner et al., 2016):

- Reducing the number of entry points for attacker to the network
- Limiting the access of the attacker inside the network when the access is already gained
- Reducing the lateral movement of the attacker inside the network to prevent access and ability to other network devices
- Making the monitoring of communications in the network easier to detect and stop cyber intrusions

It is mentioned that there is not only one correct way of segmenting network, and current best practices and recommendations offer guidance which can be seen as a more general guidance in overall (Wagner et al., 2016). For example, in pure business network, segmentation can be done inside this environment which includes workstations and servers, and specialized demilitarized zones (DMZ) can be built to separate certain assets from internal network. In this thesis the concentration is on OT network segmentation, but the overall infrastructure also contains business network segments beside them, which are in communication with each other. It is important to concentrate on different suggested models from the perspective of a smart factory environment and how the OT security can be ensured in these. The main security idea is the same as the purpose of network segmentation describes. The more fragile nature of OT devices and systems require own requirements for these segments.

### 3.3.3 Models for segmentation

One of the most common OT related segmentation models is the Purdue model, which has developed by time to respond the current needs. The model was introduced in its original form by T.J. Williams in the 1990's (Williams, 1993) and the model was referred as Purdue Enterprise Reference Architecture (PERA) (Williams, 1993). PERA was introduced as a new method to define the place of human in a computer integrated manufacturing environment (Williams, 1993). The current implementations of the model share the same idea in the background, but these can be seen more as an example of an OT related infrastructure with different segments which can be used as a guidance for companies. Cook et al. (2017) present the Purdue model as a control hierarchy which consists of six different Purdue levels (Cook et al., 2017). The model is a high-level visualization which describes the main focus of each level, and the levels are filled with examples of assets from a typical OT-IT manufacturing environment (Cook et al., 2017). The six levels are visualized in figure 2 which are enterprise network (business network), site business planning and logistics network, site manufacturing operations and control, area supervisory control, basic control, and process (Cook et al., 2017).

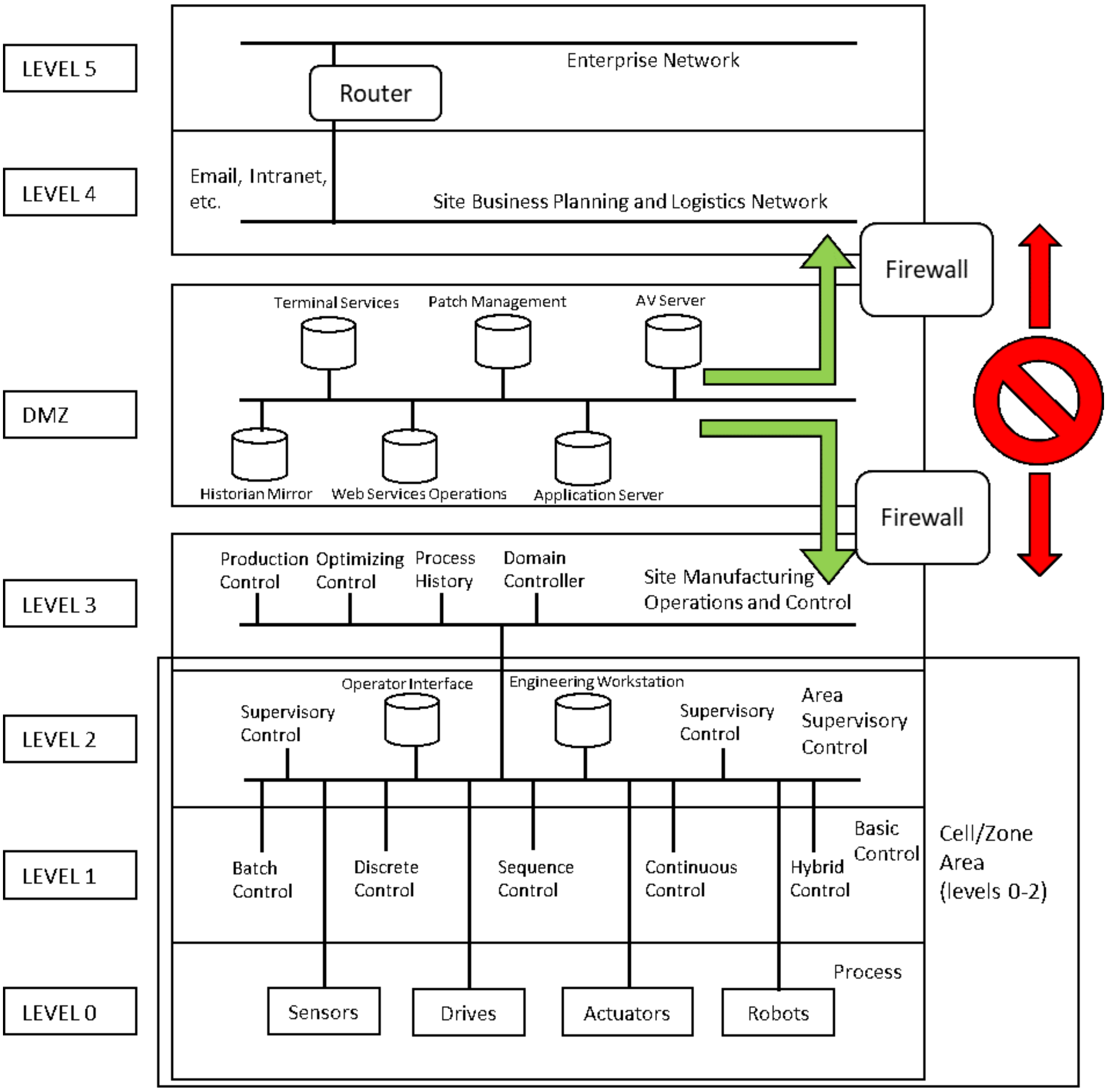


Figure 3 Purdue model for control hierarchy (Cook et al., 2017)

Siemers et al. (2022) present an example Purdue network architecture with a visualization of Purdue levels in practice (Siemers et al., 2022). The visualization in its original form also includes information about cyber-attack paths and detection (Siemers et al., 2022), but these are not considered in this part of the thesis. Idea is to understand the similarities between the Purdue model for control hierarchy (Cook et al., 2017) and the example of a Purdue network architecture, which is presented in figure 4 (Siemers et al., 2017). This visualization includes "combined" Purdue segments compared to the figure 3 (Cook et al., 2017) and these segments are enterprise network and server (business network), operation, and control zone (Siemers et al., 2022).

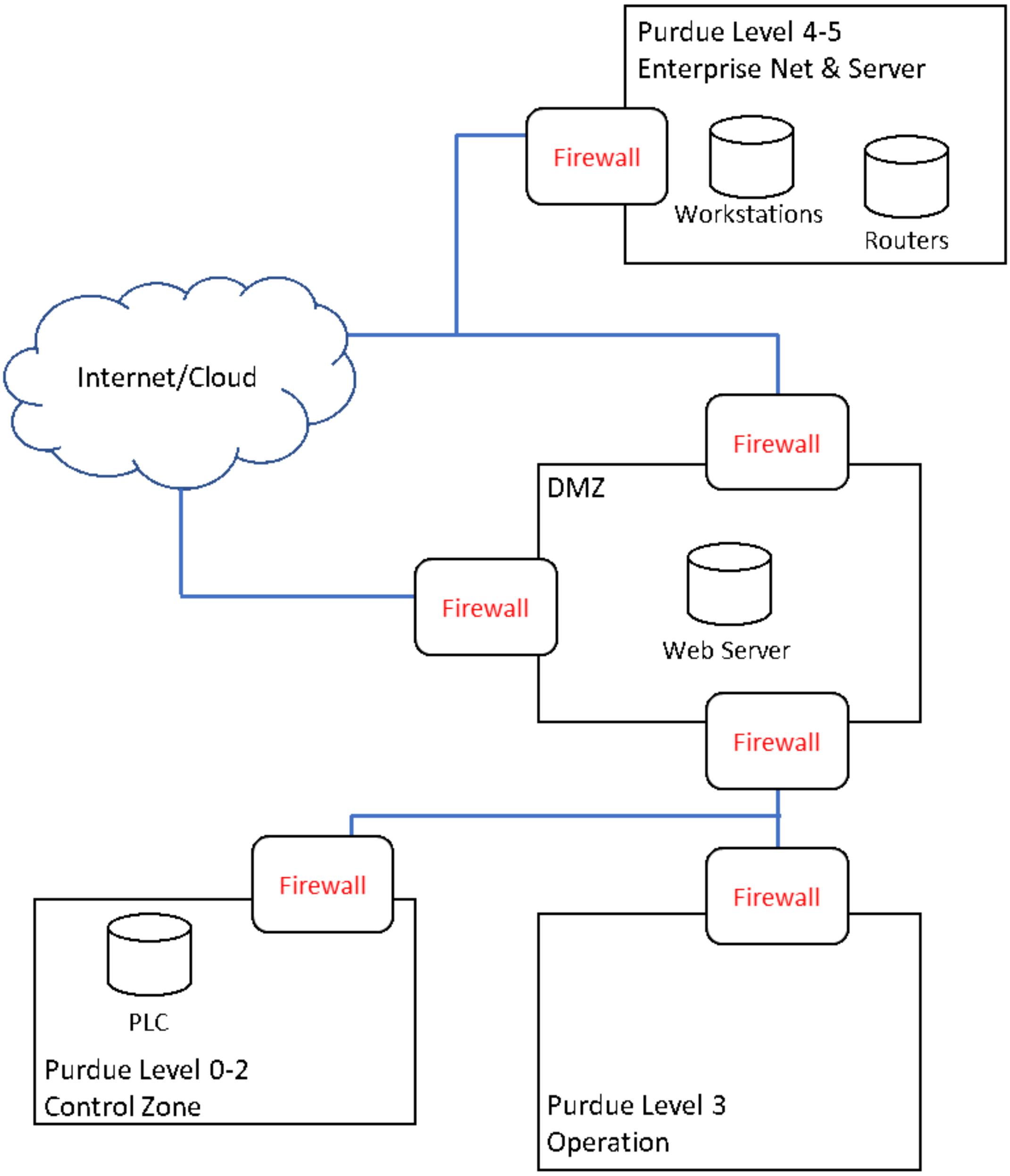


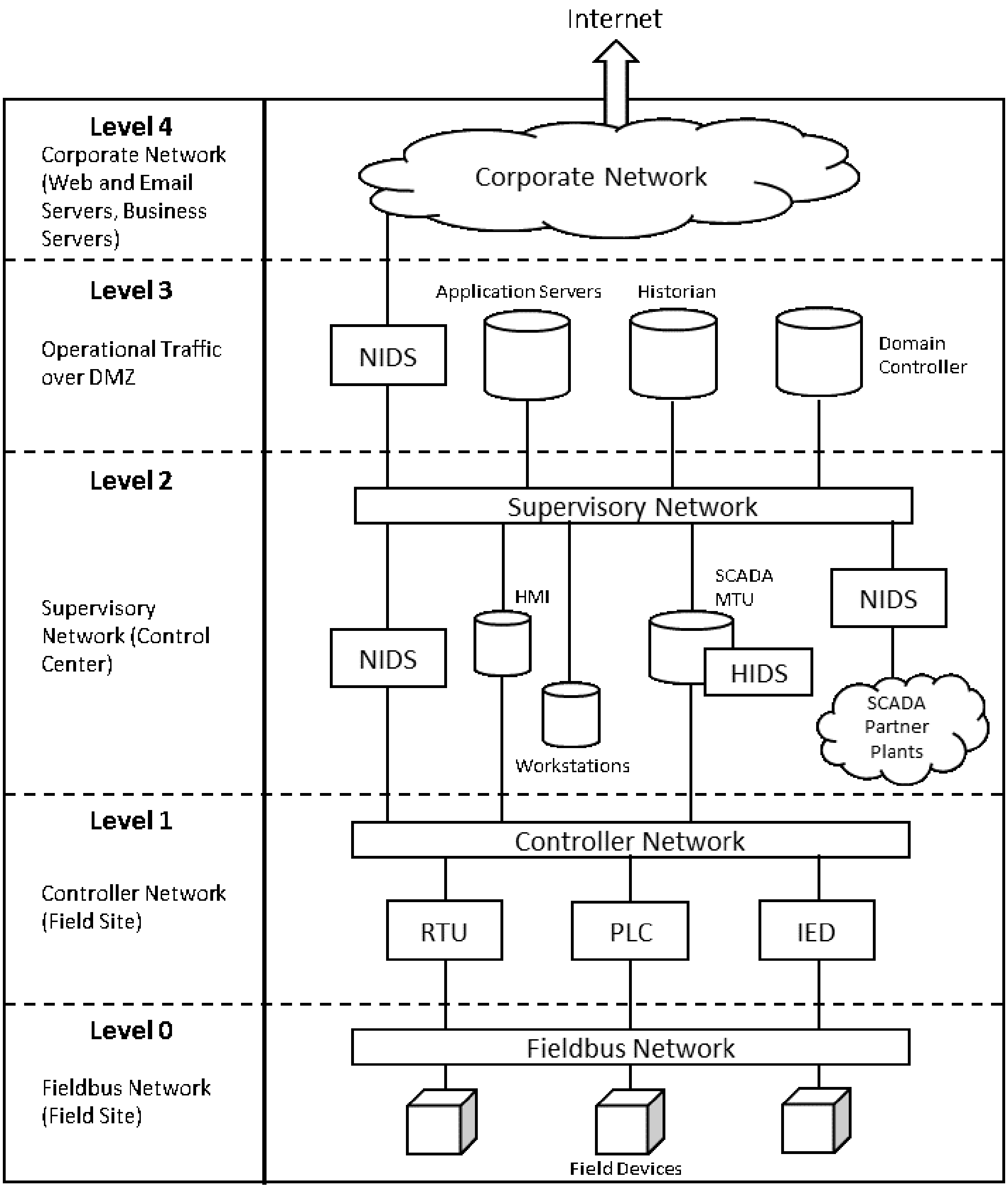
Figure 4 Example of a Purdue network architecture (Siemers et al., 2022)

Level 5 and 4 are intended for business usage and contain employee devices, for example workstations. The level includes the company email and intranet and the division between levels 5 and 4 can be made by dividing these to company network (level 5) and site business planning and logistics network (level 4). In general, these levels include similar devices and are on the top level of the control hierarchy. The division depends on the level of detail in the infrastructure, and it might be necessary to see the top levels as "one level". This level has its own firewall which filters the traffic from and to this segment based on certain rules. (Cook et al., 2017) (Siemers et al., 2022)

Between the top levels and level 3 the infrastructure includes a DMZ which can be seen as an outward-facing zone toward internet. This zone's network traffic is filtered with firewalls and usually has as many firewalls as there are ways into the segment. The DMZ includes different internet facing assets, for example application servers or web servers. As can be seen from figure 4, the internet/cloud facing areas of the infrastructure are the level top level(s) and the DMZ. The figure 3 and 4 does not contain internet connectivity straight to the levels 3 and below which can be seen as a preventative action for ensuring the physical processes in smart factory environment. (Cook et al., 2017) (Siemers et al., 2022)

Level 3 is the site manufacturing operations and control level (figure 3) which is mentioned as operation level in the figure 4. The level includes for example process control and domain controller. Domain controller is generally used as a "authentication server" and the role of this device can be to respond to authentication requests coming towards this network area and systems. Level 3 can be seen as a separate area in both figures on top of the levels 0, 1, and 2. It can be seen from figure 4 that level 3 can be set behind a firewall as well to filter the traffic. Figure 3 shows levels 0, 1, 2, and 3 behind one specified firewall when figure 4 separates levels 0,1, and 2 to an own segment. (Cook et al., 2017) (Siemers et al., 2022)

Levels 0, 1, and 2 include OT devices and can be seen as a control zone or cell zone as a whole. The figure 4 describes these levels as control zone, when on the other hand, figure 3 sees this zone as Purdue levels 0, 1, and 2. The level 2 contains the supervisory control (SCADA) and operator/engineering interfaces. Level 2 can be seen as the supervisory control of the cell zone. Level 1 contains the basic controls of the cell zone which are for example continuous control and sequence control. Level 0 is intended for the physical process and is the lowest level of the Purdue hierarchy and the cell zone. Level 0 is the zone where field devices, for example different sensors and robots, are. The following figure (figure 5) is introduced to show earlier mentioned OT devices per level from SCADA perspective (Rakas et al., 2020). The following visualization generally obeys similar structure than the Purdue model of hierarchy (figure 3), but it includes a more detailed view from device perspective tied to the different network levels (Rakas et al., 2020). The model includes for example SCADA on level 2 and Remote Terminal Unit (RTU) and Programmable Logic Controller (PLC) on level 1 (Rakas et al., 2020). (Cook et al., 2017) (Siemers et al., 2022)



NIDS = Network-based Intrusion Detection System
HIDS = Host-based Intrusion Detection System

Figure 5 General layout of a SCADA system (Rakas et al., 2020)

The OT included segmentation obeys certain redline from the top of the architecture to the lowest levels. Thus, there are different research articles which include the segmentation in a way or another, many of the examples of infrastructure obey the Purdue model of hierarchy on some level. The usage of this certain segmentation in many different sources gives a picture of the effectiveness and popularity of it and how it is generally accepted related to the guiding of modern OT environment implementation. The three figures introduced in this thesis contain similarities on different levels although these have a different level of detail (Cook et al., 2017) (Rakas et al., 2020) (Siemers et al., 2022). The OT segments are the most interesting ones from the perspective of this thesis, and these are considered next on a more detailed level.

### 3.3.4 OT segments, communication, and protocols

In the early days, OT networks were usually air-gapped by separating these from other network infrastructure due to the vulnerable nature of the devices in these (More et al., 2020). This explains, why the OT networks are on the lowest level of Purdue hierarchy, and this method is called as multi-layering of architecture, also known as defence in depth (Upadhyay & Sampalli, 2020). The usage of DMZ between IT and SCADA networks is recommended to ensure secure communication inside the network architecture (Upadhyay & Sampalli, 2020). As the devices in OT network segments are different compared to the IT network segments, and the communication is technically carried out in a different way inside the network between the devices, OT environment requires its own communication protocols. OT environment has relations to traditional IT related protocols, for example to Internet Protocol (IP), but OT protocols have their own additions to function in factory environment (Rakas et al., 2020).

Rakas et al. (2020) introduces a listing of protected SCADA related protocols which are common for OT networks. Many of the protocols are created or extended to work over Transmission Control Protocol/IP networks, which are typical protocols for native IT communication. On the field level (fieldbus), many of the protocols are Ethernet-based. OT environment includes a wide list of different communication protocols, but the ones listed in the article are commonly in use. The protocols introduced are Modbus, IEC 60870-5 series, Distributed Network Protocol (DNP3), and Ethernet/IP. (Rakas et al., 2020)

Modbus is a protocol which is based on the client-server model (Rakas et al., 2020). The functionality of this protocol is based on communication between the Modbus master device and Modbus slave (Rakas et al., 2020). Modbus over TCP creates a request-response connection amongst the master device, slave, and field level devices (Upadhyay & Sampalli, 2020). Modbus has different variations in different function, but for example in this case, Human-Machine Interface (HMI) can be seen as the master device, PLC or RTU as the slave, and a process related device as a field device (Upadhyay & Sampalli, 2020).

IEC 60870-5 series protocols are in common use related to SCADA devices' basic telecontrol tasks (Rakas et al., 2020). The 104 protocol of the series establishes a TCP/IP based network access for the 101 protocol to carry out mentioned tasks between control centers and substations (Rakas et al., 2020). The protocols of this IEC series are used especially in the industry of Europe (Rakas et al., 2020). The DNP3 protocol is widely used in North America as an alternative for the 60870-5 series (Rakas et al., 2020). The protocol is used in communication between the control center and field devices for example through Transmission Control Protocol (TCP), User Datagram Protocol (UDP) or Hypertext Transfer Protocol (HTTP) (Upadhyay & Sampalli, 2020). 60870-5 series and

DNP3 protocol are an example of extending the usage of typical IT related protocols in factory environment.

Ethernet/IP is a set of industrial network protocols which allow the usage of Common Industrial Protocol (CIP) over Ethernet and TCP/IP (Rakas et al., 2020). CIP is described as a media independent and object-oriented protocol to support automation applications (Rakas et al., 2020). The CIP object can be for example the data which can be gathered from the factory environment (Rakas et al., 2020). Ethernet/IP protocols are vendor-dependent protocols which can have different functions. For example, Upadhyay & Sampalli (2020) mention the function of Rockwell automation's Ethernet/IP protocol which is used to upload and download an application to a PLC and reading and writing the register values in PLCs or RTUs (Upadhyay & Sampalli, 2020).

It is important to understand that communication protocols are the enablers for the network communication between the industrial devices in OT environment. As it is mentioned, industrial vendors tend to have own versions of protocols in use depending on the functionality of communication. OT environment uses traditional IT network protocols which step in place when considering the entire infrastructure, for example from the Purdue model's aspect (Cook et al., 2017). Also, traditional IT related protocols are in use as they are in factory environment, for example HTTP & HTTP Secure (HTTPS) in factory floor web usage (Upadhyay & Sampalli, 2020), which creates additional actions related to the OT-IT convergence and OT Security.

### 3.3.5 Local and remote factory environment communications

Factory environment and OT devices can be locally implemented which requires short-range communications between the local RTU's, instruments and operating equipment (Sayed & Gabbar, 2017). These communications can be made by using short distance wired or wireless connections which carry digital and analog signals using electronic properties (Sayed & Gabbar, 2017). This is an example of an environment where the SCADA system and field devices are on the same site. If the factory is implemented remotely, the communication between the factory devices and SCADA network needs other solutions, since the short-range communications are not an efficient solution.

In a remote factory environment field devices can be for example RTU's and PLC's which monitor and gather data from the processes and communicate it to a remote location host server (Sayed & Gabbar, 2017). The connection between the factory and remote location is established by using long-range communications either in wired or wireless way (Sayed & Gabbar, 2017). This communications zone can be also called as Wide Area Network (WAN) (Upadhyay & Sampalli, 2020). Communication typically uses leased telephone lines, microwave, satellite, frame relay network and cellular data as a method (Sayed & Gabbar, 2017). Long-range communication (WAN) methods are usually in public use and are owned by different governmental actors, which set certain regulations for communication. The following figure (figure 6) describes an example OT environment, where WAN is involved in the architecture.

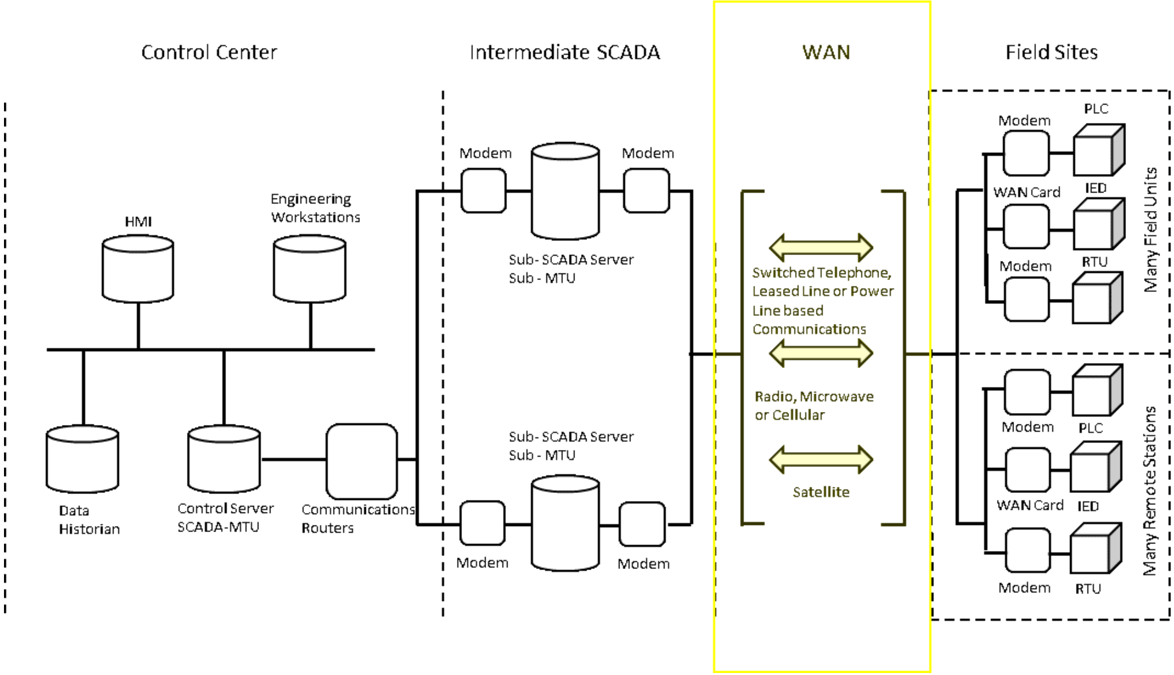


Figure 6 High-level example of a SCADA communication architecture (WAN highlighted) (Upadhyay & Sampalli, 2020)

## 3.4 Cyber-attacks and vulnerabilities in OT environment

A cyber-attack against ICSs and OT environment can cause a lot of damage from business and physical perspective. A good example of this is the Stuxnet which was carried out by using Remote Access Trojans (RATs) in industrial environment (Alladi et al., 2020). It has been evaluated that average impact of a cyber-attack against ICS costs around $5 million for the company and causes approximately 50 days of downtime and IT losses (Alladi et al., 2020). Since the OT in the industries is commonly older generation, it causes an increased risk of cyber-attacks against the environment when the devices are integrated with the IoT and the digital environment (Alladi et al., 2020). It is mentioned that the common adoption of IT defences as a response to OT cyber-attacks is not enough since these cannot protect the physical systems at the process level (Sundaram et al., 2020). In cyber-attacks against the OT environment, important points of view for analysing the impact of cyber-attack against the environment are financial loss caused by the attack, damage caused against the physical equipment, and damage caused against the humans (Alladi et al., 2020). This is in connection with the description of OT security, which was earlier described (CIA + physical process) (Hahn, 2016). Usually, CIA triad is considered in order, confidentiality > integrity > availability, related to IT environment and the importance of business data, but since the OT environment considers the critical infrastructure and its vital processes by different actors, the triad can be considered in order availability > integrity > confidentiality (AIC) (More et al., 2020).

### 3.4.1 Real-life attacks and vulnerabilities

German steel mill was attacked in 2014 by hackers who were able to take control of the production software of the mill which resulted to large damages in the production infrastructure. The vulnerable component was the user of the company's network combined with the poor network architecture. Attackers used phishing emails, which contained attachments with malware, to get into the company's network. The attackers reached the management software and ICS network which were the control systems of the mill. The control systems were used to destroy the Human Machine Interface (HMI) components of the mill which led to the prevention of operation of the mill's furnace since the security settings were disabled. This chain of activities caused serious damage to the physical infrastructure of the mill. (Alladi et al., 2020)

In 2015, a water treatment plant was attacked by hacktivists in the USA which caused changes in the chemical quantities in water treatment process. The vulnerable component in this attack was the network segmentation in which an outdated SCADA system was used to manage PLC's which managed the industrial valves and ducts at the plant. The outdated SCADA system was accessed by extracting login credentials from the front-end web server and gaining access to the plant's water treatment control software which also ran on the same outdated SCADA system. The system was the central for the plant's IT operations which gave the attackers privilege to control other industrial equipment at the plant as well. The attackers did not seem to have much knowledge about the SCADA system which prevented the plant from suffering major critical consequences either to the infrastructure or people. (Alladi et al., 2020)

Both examples of real-life attacks are relevant related to the topic of this thesis since both have the perspective of OT-IT convergence in them. Both attacks had OT and IT systems in the same environment and segments, which lead to the malfunction and unavailability inside the infrastructure. The attacks are possible in the current OT environments either in companies or national critical infrastructure since the OT devices tend to be older generation and the Industry 4.0 concept sets new environment for actors to think of related to OT-IT convergence. In these attacks the actions were carried out remotely, but the local attack possibility is still necessary to be considered. As an example, Stuxnet and its consequences were made possible since the attacker had hands on contact with the environment where the USB-stick was inserted (Alladi et al., 2020).

### 3.4.2 Attack prevention and solutions

Related to both German steel mill and American water treatment plant attacks, the consequences of the attack could have been prevented with a proper model for network segmentation (Alladi et al., 2020). Attacker was able to move inside the company’s network in both cases which was the factor for gaining more and more access (Alladi et al., 2020). It is suggested that the OT and business network should be separated from each other by using for example firewalling between the segments, as mentioned related to the Purdue model (Siemers et al., 2022), to block and filter unnecessary traffic from them (Alladi et al., 2020). Also, the number of interfaces between the OT and business network must be minimized to prevent unauthorized access (Alladi et al., 2020).

Network security monitoring is mentioned as important part of the OT environment since these services can be used to highlight anomalies in the network infrastructure (Alladi et al., 2020). It is mentioned that most of the state of art OT Intrusion Detection Systems (IDS) operate on network level (Bécue et al., 2021). Also, implementing OT environment based on OT related standard IEC 62443 (IEC, 2013) is seen as important preventative action related to cyber-attacks (Alladi et al., 2020). Since the environment might include legacy OT devices, the ownership of the devices must be described inside the organization in disaster recovery and business continuity manner. The lifecycle of OT can cause additional actions related to the updates of the devices, since the lifecycle is much longer compared to the traditional IT devices (Upadhyay & Sampalli, 2020) and the updates might have to be installed manually.

Related to current trends, Machine Learning (ML) can be seen as a big part of OT security and intrusion detection (Bécue et al., 2021). Old OT devices and systems can be described as predictable and stable actors in which the ML-based anomaly-detection would function properly (Bécue et al., 2021). On the other hand, the IoT oriented factory environment (IIoT) is seen as a challenge for ML (Bécue et al., 2021) since the devices and systems are getting more complex combined with new network environments. An aspect which has to be taken seriously related to the smart factories and security is the nature of multi-vendor environment. Since the OT in the factories might be acquired from different vendors, it is important that the environment works fluently without compromising the OT security. For example, vendor related communication protocols come into consideration when implementing anomaly detection inside the networks.

## 3.5 Benefits for companies implementing smart factory environment

Industry 4.0 concept might require big changes in the environment and infrastructure due to the digitalization of the manufacturing process. For example, older devices might have to be replaced with newer ones because of their manual nature, and network segmentation and telecommunications might have to be planned again from the scratch. It is mentioned related to the Industry 4.0 concept that the true challenge in the OT-IT convergence is the alignment of the security objectives of each system with the business objectives of the system

(Conklin, 2016). Earlier in this literature review, we have described some of the OT security and telecommunications related details which have to be considered to tackle challenges and avoid problems in the smart factory environment. The smart factory environment might be an attractive target for cyber-attackers due to the digital nature of it, but with correct actions the risks can be managed and minimized. It is important to spotlight and understand some of the benefits for the company, that can be achieved by implementing smart factory environment. The benefits can be business and process related, environmental, and human resource related (Ghobakhloo, 2020).

### 3.5.1 Business and process related benefits

Implementing smart factories can lead to improved profitability of the company which is associated for example with optimization of material flow, better timing in market related to products, optimization of manufacturing facilities, and lower inventory costs (Ghobakhloo, 2020). It is mentioned that smart manufacturing can lead to sustainable economic development of countries by for example creating more digitalization-related job opportunities to the field and improving the circular economy (Ghobakhloo, 2020). Transparency of data on different levels of organization, and quick and correct decision making is named as notable advantages (Garimella, 2018). Related to manufacturing process, Industry 4.0 concept can offer a controllable non-stop production with real-time monitoring with accident prevention, lower human errors, and resource efficiency (Ghobakhloo, 2020).

### 3.5.2 Environmental benefits

Smart factory environment can lead to reduced carbon and harmful gasses when the IIoT and Artificial Intelligence (AI) based production is able to increase the efficiency and flexibility of the production, reduce the waste from manufacturing, and minimize the caused carbon emission index per each produced product (Ghobakhloo, 2020). Smart manufacturing can lead to customization and individualization of products for consumer which improves the low-carbon idea related to lowering unnecessary production (Ghobakhloo, 2020). Development of environmental responsibility is also mentioned as a benefit related to smart manufacturing since the technology enables the usage of environmental management practices such as environmental performance benchmarking in a more powerful way (Ghobakhloo, 2020).

### 3.5.3 Human resource related benefits

Ghobakhloo (2020) mentions that enhanced decision-making which is result of process automation and simplification can boost human resource efficiency (Ghobakhloo, 2020). It is mentioned related to the Industry 4.0 concept that AI and data analytics tools can enable for example the creation of personalized career development schemes and learning programs based on employees' attributes (Ghobakhloo, 2020). Smart manufacturing will remove many different low- to medium-skilled jobs since the technologies will replace many humans for example in inventory tracking and quality control, but on the other hand, many new employment opportunities will rise for example in the areas of informatics and process engineering (Ghobakhloo, 2020). Risk management is one of the main benefits in the environment since the real-time monitoring and automation of processes improves the reaction to malfunctions and downtime, but also reduces the risks which are related to the safety of employees (Ghobakhloo, 2020).

## 3.6 Summary of literature review

The focus of this literature review was to concentrate on important topics related to OT assets, OT security, and OT telecommunications which are the key components of smart factory environment. Also, the business perspective was considered in this part, and what benefits the smart factory implementation can bring for companies. One of the main points was to understand the term OT security and how the physical process is part of it beside the CIA triad. Also, OT security and telecommunications can be considered "as one", but as earlier mentioned related to this thesis, it is necessary to handle them as two individual topics to make the structure clear, but also to help the development of the guide for decision making.

The topics considered in this literature review will be the information base of the qualitative research besides the information from the interviews which are carried out in company x. The structure of the first-round interview is going to be based on the topics of literature review. The interviewees for the first round are chosen from the technical side of the company x. Important action point for the first-round interview is to tie the topics to a company environment and extend the knowledge about OT assets, OT security, and OT telecommunications with real-life experience. Based on this, the draft solution for OT-IT decision making will be created. It is important to understand that literature review is also considered as part of the DSR design and development phase (Peffers et al., 2006) since the topics which are recognized as important from the motivational perspective of this thesis are extended and developed further.

# 4 FIRST ROUND INTERVIEWS - INFORMATION GATHERING FOR THE GUIDE

To build up the structure for the interview based on made literature review it is important to remember the goal of the guide, which is created based on the gathered information. The guide is made to be a supportive tool for higher level decision making related to smart factory environment which includes OT/IT implementations. It is important to remember that OT-business decision making does not need to know every technical detail of the environment. It is important to understand the requirement, what is the meaning of it, and how it affects the environment. In other words, why something is important to be done or implemented in smart factory environment. Topic areas in the interview are the ones which were recognized as important areas related to smart factory environment, and which require feedback from the experts related to the current real-life OT environment.

As earlier mentioned, the interviews are carried out in a qualitative semi-structured manner by asking detailed questions related to the topics of literature review, but also letting the interviewees express their own opinion related to the topic area in a manner of “free word”. The interviewees are going to be technical experts, who have experience in OT environment generally and are experienced in infrastructure, security, and telecommunications field. The number of interviewees in the first round is three. Interviewee’s role in the company and involvement with OT is asked in the beginning of the interview. The interviews are held inside company x by using Microsoft Teams as an interview platform and the interviews are carried out in Finnish. Finnish is used with interviewees since the native language is Finnish and the dialog is more fluent in this way. Answers are written in English to the structured interview form. The interviews are recorded and are going to be carried out in a time window of one and a half hours per interview. Although the interviews are recorded, it is necessary to use a structured interview form beside it, to write down clear and precise answers. It is important to avoid interpret related mistakes and writing the answers down also helps when creating the draft guide. Interviewees are anonymized and referred as Employee 1 (E1), Employee 2 (E2), and Employee 3 (E3).

## 4.1 Topic areas for interview

### 4.1.1 OT hardware and systems

In literature review, this topic was considered to understand what kind of hardware and systems can be in OT/smart factory environment. Also, important details were considered related to the nature of the OT and for example what kind of differences are between OT and IT. It is important to understand generally in company context, that are the OT assets counted as infrastructure, which is owned or managed by the company, or should these assets have employees who are responsible of managing the device. Owner/manager relationship is an important part of disaster recovery and business continuity in case of emergency. Since OT hardware and systems are much older in general and the lifecycle is longer, it is important to extend the information from literature review related to lifecycle and patch management. It is important that the devices are managed and monitored to ensure the OT security (CIA + physical process) from this perspective.

### 4.1.2 OT security in organization culture

OT security can be confused with IT security since these assets are in the same environment in Industry 4.0 concept. The digitalization has an effect which requires the company to get employees familiar with the OT. The IT security aspect is considered in companies related to learning and different training programs since cyber-attacks have increased in number in past years. It is important to get information from the interviews related to OT security's role in organization culture and how it should be considered among the employees. Also, the description of OT security (Hahn, 2016) requires feedback from technical expert's perspective and could it be used as a commonly used description in future. Since Industry 4.0 and smart factory idea is the environment of OT-IT convergence, it is important to extend the information, that should OT and IT security be considered as one or are these better to be handled as two own topics.

### 4.1.3 OT standards

In literature review, ISO 62443-3-3 (IEC, 2013) was introduced to get an idea, what OT security related technical standard says and what it has to give for the company. It is important to get evidence from interviews about implementing the environment based on OT related standards and what benefits for example from OT audits can be achieved. Based on literature review, it is clear that creating the environment based on globally accepted recommendations is a positive thing related to the compliance, but it is important to get feedback from company's perspective.

### 4.1.4 OT telecommunications

From OT telecommunications perspective, it is important to understand more technical level topics to develop higher level recommendations to the guide. Differences between business and OT networks were discussed in literature review, and both of these are part of the Purdue network segmentation model. It is important to understand, what are the differences from technical experts' perspective, and is the Purdue model the most suitable one since new networking technologies have developed in past few years. Communication protocols have to be considered in the interviews since these are a big part of communications in multi-vendor OT environment based on literature review. Since smart factory can be physically implemented either as a remote environment or close to the business unit, WAN has to be considered under this topic area and what WAN solution suits the smart factory environment.

### 4.1.5 Cyber-attacks and prevention

Some of the possible cyber-attacks were considered in literature review and how these could have been prevented. Also, some of the current solutions and practices were introduced to understand, how cyber-attacks are prevented in smart factory environment. It is important to get feedback, that should the CIA triad be considered in opposite direction (AIC) in OT environment since the availability of the physical process is vital for manufacturing. Disaster recovery and business continuity aspect has to be considered since the processes have to be clear if something causes negative impact and consequences for the environment. OT cybersecurity solutions were handled in literature review and some of the relevant implementations were introduced. The importance of network level in OT environment was mentioned related to workspace of cybersecurity solutions. It is important to get feedback from technical experts that do the security solutions have value when used in smart factory environment and what are the meaningful solutions at the time. Machine learning and AI are also discussed as possible preventative methods in future smart factory environment.

# 5 INTERVIEW RESULTS & DRAFT VERSION OF THE GUIDE

The interviews were held by obeying the interview structure for technical experts (Attachment 1). The answers to the questions were written down to the interview from (Attachment 1) beside the interview and the answers were confirmed with the interviewee to prevent interpret related mistakes. This was confirmed to be the best solution for the research part since the questions were technical and required detailed answers to benefit the development of the guide for decision making. Interviewees were chosen from the IT organization of company x since this organization has been the most involved in the smart factory environment in their current and previous work history. The employees from this organization were chosen based on their current role and by questioning about their experience with OT and smart factory environment. The employees who attended the first round of interviews (technical experts) were Senior Cybersecurity Manager (E1), Global Technology Manager (E2), and IT Solution Architect, Networking (E3) from the company x. The structure of the interview was kept the same in all of the interviews since the first interview (E1) gave evidence, that the questions are relevant from the development perspective of the guide and the questions were able to get extended information related to the recognized important topics of the literature review. Related to interviewees involvement in OT, E1 had worked with Security Operations Centre (SOC) monitoring, inspection, and internal cybersecurity services which include the OT aspect. E2 had been involved with OT related to concepting and building digitalized services and capabilities towards company x manufacturing operations. OT security controls, data collection and secure remote access capabilities had been part of this work. E3 had been working with OT related to company x smart factory project regarding company's production sites. E3 had worked with network related topics in this project. Earlier, E3 had been working for network vendors related to OT installations, for example in health care sector. Based on the background of the interviewees, all of them have had experience in the main topics of this thesis, which are OT security and OT telecommunications. Also, involvement in digitalization and smart manufacturing (E2

& E3) is important from the main goal's perspective since it is to develop a guide to support decision making related to OT and smart factory environment. IT experience was the major experience of all interviewees, as their current roles in company x tells, but it is important to remind that IT is part of smart manufacturing related to the OT/IT convergence and Industry 4.0 concept. The interviewees had been involved with OT besides their IT related roles.

## 5.1 Results of interviews

### 5.1.1 OT hardware and systems

The meaning of having an owner or manager for OT assets is seen as an important thing to do. The responsibility of owner is to take care of assets security control configuration and security posture but also of the lifecycle management. In addition, it is mentioned that physical location is an important attribute which has to be included related to asset information. Also, the ownership of an asset has an effect to the business continuity.

> It is crucial to be able to identify and notify the asset owner during possible security incidents involving the assets for quick incident resolution and to minimize the impact on business continuity (E2).

When describing the lifecycle management of OT assets, it is mentioned that the physical lifecycle is longer than the software in these assets. For example, a certain device can have a reliable process which keeps on going, but the software in it can be outdated from the security perspective and it cannot be updated. Comparing OT assets to IT assets, the variety of Operating Systems (OS) is very wide in OT environment, and these are not easy to standardize. From the cost perspective, device replacement in business environment compared to the OT environment causes a big difference since the OT devices are typically higher in monetary value.

> Environment and devices around a certain device can develop which gives new requirements for the outdated software from connectivity and security perspective (E1).

OT patch management and updates are closely related with the lifecycle management, and this was witnessed in the interviews since both of the topics were considered mixed under Q4 and Q5. OT environment is typically designed as a more static environment where the adaptation to software changes related to system patching and updates has not been taken into account. The nature of the OT environment is fragile and some of the updates have to be tested and verified before carried out in the production environment. The downtime of the environment cannot be long since the physical processes must go on, but certain shutdowns are required for the systems to be updated. The OT systems require high availability with minimal downtime so that the business continuity does not suffer from this. There are so called "patch Tuesdays" in OT environment to commit timetabled patching and updates in the environment to predict system outages.

> With normal IT system patching and updating policies and deployment cycles the OT systems can easily break and cause severe outages (E2).

It is mentioned that the capability to recover from these issues is a very cumbersome process which might require the involvement of special OT system experts. Production side personnel have not got the biggest acceptance to patching and updates due to the outages caused by these which makes the patching and updating harder. Also, the culture in OT environment is totally different compared to IT related to patching and updates and OT side might not see the importance of this in a same way than the IT.

> I have many times discovered now that OT side doesn't have good understanding of IT and same thing is in the opposite way. Both of these needs understanding from OT and IT field. (E3)

Important topic related to OT hardware and systems is the OT assets Configuration Management Database (CMDB) information management and how it is incorporated with the OT asset owner's responsibilities. A centralized OT asset CMDB information could be organized together with OT and IT organizations in cooperation. OT environment includes many different protocols, many different old devices, and different electrical related requirements for devices which makes the accomplishment of OT security harder.

### 5.1.2 OT security in organization culture

It is mentioned that OT security should be integrated to organization culture especially if the OT is part of the core business. The security culture overall should be integrated to all organization levels. This way the personnel working around OT and IT environment are able to understand the value of security in the company. The awareness of security related to this environment can be increased via trainings and info sessions which should be organized in cooperation with IT and OT organisations. Important thing to remember is that for example education should be role based inside the organizations. When something is connected to the network, IT security principles affect the action also in OT environment. One of the mentioned important topics for education is the identity management of OT environment and how the practices can be brought to consider so called "shared devices" which are used by several employees.

> Also, in the future world the OT and IT environments are getting more and more mixed, especially due to new digitalized capabilities introduced to the OT space (E2).

The suggestions for OT and IT security roles are mixed, but the different point of views which rose in the interviews are important to consider. Security personnel can be seen as employees in both OT and IT areas at the same time to increase overall security competence of the security topics. This could also reduce the diverging of OT and IT security. The more specific description for roles is that there should be personnel who work between OT and IT to solve challenges between these. It is necessary to have separate specialist roles in both OT and IT, but for example a certain OT security person with extended OT knowledge could help with the product development related tasks. This person should be in communication to the IT security direction as well.

> All of the OT engineers should be carrying out OT security in their work (E1)

One point of view is to have IT security expert with extended knowledge of OT environment. Separated roles between OT and IT security could be necessary, but these could work in a same security organization or team. These role related challenges depend a lot of the size of the company and on which level the security is part of its actions.

> Basic IT security role in a smaller company might not have any experience for example related to securing PLC's or so (E3).

In literature review OT security as a term was considered as a combination of CIA triad and physical process (Hahn, 2016). In interviews CIA triad is seen as very stabilized standard in IT environment for understanding, assessing, and mitigating the risks. It could be useful to extend the same standard to OT environment to unify the understanding of the security related definitions in all company's environments. Process element of the OT is more unique for OT security than IT security so the highlighting of it might be useful inside organization. This will require more extended awareness and training for IT security personnel to adopt it.

> It could be an accepted term (CIA + physical process), but CIA can be hard in automation side to understand since automation people might not have the IT security (CIA) understanding. It should be opened that what these letters mean (E3).

From OT security perspective, it is suggested that CIA triad would be better to consider as AIC triad, which describes the importance order of availability, integrity, and confidentiality in the environment. Safety, reliability, and productivity (SRP) is stated to be important to include to the OT security description and this is closely related to the physical process (safety, environment, dependencies, regulation) which is mentioned in the description in literature review (Hahn, 2016). In overall, OT security related things in organization culture require more cooperation inside the company. Important part of this is the individual level of understanding the OT security.

> OT security's function has to be understood on individual level. If it isn't understood why, it is in place, individuals try to go around it if it speeds up their tasks. For example, generally related to safety, some protection is not used physically because it is not understood why it is used. (E1)

### 5.1.3 OT standards

Implementing the OT environment based on certain standard is seen as a good practice and how the obeyance improves consistency and gives better understanding of how the OT environment should be implemented. IEC 62443 standard series is mentioned to be the preferred one in OT environment, but it might not be necessary to blindly follow it from recommendation to recommendation. IEC 62443 series should be utilized but keeping in mind that what is necessary to implement related to security compared to the cost it causes for the company. Cost versus reward thinking should be connected with risk versus reward thinking. Control cannot be more expensive than the risk it tackles.

Auditing the OT environment helps keeping the OT environment in line with agreed standards and risk mitigation. It is important to understand, what should be audited, and this is in connection with the asset register (CMDB) which should be maintained of the environment. Auditing the environment can also help to discover assets from the environment which are not documented for example in the asset register.

> Benefit from OT auditing is that we can map the changes and discover new environments which are not documented. Also, IT can be made conscious of the environments. Automated monitoring of the environment can be used for "auditing" related to the OT. (E3)

If the asset register is in place related to the OT environment, audits can be carried out. It is mentioned that the auditing process is still heavy in OT environment since the OT related personnel might not be used to this kind of auditing in big companies and the amount of assets in the entire environment is so big that it causes friction related to the auditing process.

### 5.1.4 OT telecommunications

One of the main points related to differences between OT and business networks is the nature of the networks. OT networks are not seen as cyber resilient as IT networks and OT devices are not designed from the same security perspective as IT devices. In business networks IT organization has typically a very high control over assets attached to the network. In business networks the active devices can be identified and directed to connect to only needed services.

> Also, the devices itself are typically under IT management controls & practices which helps mitigating the possible security incidents. The IT networks are typically segmented for different use cases (workstations,

> servers, printers, etc.) and traffic control rules between segments are in place. (E2)

In OT networks the security controls are much more weaker compared to IT networks from asset control and segmentation perspective. Networks are typically designed as flat networks, and these do not have any inner segmentation for different OT use cases or asset types. Also, the lack of clear lifecycle management inside OT networks is mentioned as a negative thing.

Network segmentation is generally identified as a critical and important thing to do related to smart factory environment. Segmentation model should be obeyed in every infrastructure architecture regardless of if it is for OT or IT environment. Proper network segmentation makes the isolation of workloads and assets from each other possible based on their use case type and access requirements. Lateral movement inside the network can be limited and made harder during security related incidents.

> The impact to business continuity can be more easily controlled and recovery times from possible outages can be shortened (E2).

Segmentation can be simplified as a thought, that there are two devices in the network which do not have to communicate with each other in any scenario. This will further lead to the idea of micro segmentation inside bigger network segments, which controls the components inside the segments which are intended to communicate with each other. Segmentation makes the security mechanisms, for example firewalling, possible inside the OT environment. From organizational perspective, use of agreed segmentation model increases organization awareness of how to operate within the OT and IT networks and what needs to be considered from this perspective when implementing new solutions in these environments.

Purdue model is considered as a relevant network segmentation model since it helps to understand the control hierarchy and relations inside the network architecture. The biggest challenge for Purdue model is the development of new wireless technologies and IIoT in general since the model was developed during the age when OT environment was seen as a very controlled and isolated environment. The model does not necessarily take into account modern IIoT solutions and cloud services.

> In Purdue model you have to go through levels to get Internet connection. Challenge is that what if the OT device is directly connected to Internet (for example IIoT devices)? (E1)

IEC 62443 standard series uses a similar model as Purdue, which reasons the usage of the model in current environments. Purdue model is still pretty heavy from management perspective since every segment and device inside it must be understood. Purdue model might have some unnecessary levels since the architecture can be built different, but it can be used as an instructive model and modify it to answer company’s needs. The model itself might not consider earlier mentioned micro segmentation in an example case where vendor y and vendor z devices have to be divided into own micro segments inside a Purdue level. Technically, this can be implemented by modifying the model and this is suggested related to support of future requirements related to rising networking and telecommunications solutions.

> We can have an OT device which uses cloud services, but the model can be modified to suit this. The basic principle is still the same. Conduits (corridors) can be made between the segments to communicate. (E3)

The communication in multi-vendor environment has to be implemented so that the OT systems and devices support industry standard protocols which will enable fluent communication between different types of devices in a standardized manner. For example, Open Platform Communications United Architecture (OPC UA), which is an industrial data exchange standard, is mentioned related to this and could at least partly answer to the challenge. Automation systems can communicate with their own protocols, but when the communication is carried out to other segments, standardized protocols are required. In multi-vendor environment, vendor specific protocols can cause difficulties from security perspective since these might not fully enable monitoring.

Related to WAN solutions in remote factory environment, dedicated connectivity methods are typically used, for example Multiprotocol Label Switching (MPLS), which can provide connections with good quality and high availability levels. This might not be possible to implement in all remote locations due to the connectivity capabilities. It would be important to implement multiple connectivity methods to increase the availability, but also develop fail-safe mechanisms into both network and application layer. WAN solution and usage in remote factory environment is important to divide in to two parts, which are underlay and overlay. Underlay is the physical network infrastructure and overlay, for example in this case Software Defined Wide Area Network (SD-WAN), is a communication network on top of underlay networks which handles with the traffic of these.

> Underlay which is the access mechanism must be flexible. Underlay could be for example Internet, MPLS, 5G, etc. Overlay is more important which should be software defined (SD-WAN). This makes overlay security and encryption of traffic possible and flexible use of different underlay networks. (E3)

### 5.1.5 Cyber-attacks and prevention

It was earlier mentioned in these interview results that A>I>C could be the relevant order for IT familiar CIA triad in OT environment. Also, the involvement of SRP or physical process besides the AIC would be a better fit. Availability and business continuity are seen as the most critical in OT environment since the processes must keep on going without disturbance. It has been witnessed by the interviewees that confidentiality for example has not been in an important role inside the OT environment.

When talking on a more detailed level of disaster recovery and business continuity in OT/IT integrated environment, plans and processes must be in place inside the organization. The plans and processes have to consider the hardware, software, people, organization, and communication topics. Business continuity and disaster recovery process includes the earlier mentioned documentation of assets to a CMDB. Backups of systems must be taken regularly, and recovery processes must be rehearsed if something negative happens. Risk management mapping should be carried out in the process related environment and how malfunctions and unavailability affect the business continuity of the company.

> These plans should be periodically tested in live environments to ensure that recovery from disaster recovery incidents can be executed in time frame set for the particular environment (E2).

Practice of proper securing of environment is an important topic related to business continuity. For example, standardized network segmentation and firewalling are part of this on a more technical level. Backups are more related to the disaster recovery, but also spare devices are required from this perspective if something physically breaks in the environment.

> All cannot be reached immediately. Competences have to be built step by step. For example, IT security hasn't got to its current stage in one year. (E1)

Generally, different security solutions should be implemented into the smart factory environment to improve OT security. Related to OT networks, the nature should be static on some level so the baseline should be the ability to create an alert from anomalies.

> Different security solutions should be implemented to increase the visibility of what kind of assets are connected to OT networks, what kind of vulnerabilities they might have, how the assets communicate within the OT networks and in/out of OT networks, and also preventative measures for blocking unauthorized or unwanted traffic (E2).

Network monitoring is mentioned as an important security solution for the smart factory environment. It is important to understand that network monitoring is different from active network scanning, which could have an effect to the availability of the devices since the nature of the OT environment can be fragile. If the active scanning is done, it should be carried out when the factory is not in production mode to avoid negative consequences. Passive asset detection and detection of unusual communication partners are mentioned as effective solutions. AI and machine learning are considered related to these.

> The AI and machine learning solutions can help understanding what is considered as normal network traffic pattern and identifying anomalies from the OT network traffic (E2).

> When the factory is in "production", passive solutions should be used and for example how PLCs communicate and to where. Machine learning and AI could be used in this kind of passive monitoring (who communicates to who, what does it look like). Reacting to changes of communication patterns in the network environment. (E1)

Network monitoring of the smart factory environment might require special licenses for the vendor specific protocols. The solutions mentioned related to the environment are common solutions nowadays and can be easily taken into use. Network segmentation was mentioned earlier related to OT telecommunication topic area and how it can be heavy to use from management perspective. This problem can be eased by using automation and monitoring to detect anomalies in the environment. Workloads of human employees can be decreased by using different technologies beside the OT security work.

## 5.2 Quality of interviews

The interviews extended the topics from the literature review which were recognized as important from OT security and telecommunications perspective. It can be seen from the results of interview that the interviewees have expertise related to the topic areas and were able to give detailed answers to the questions. All of the topic areas received many-sided input and any of these were not left blank or did not make sense for the interviewees. It was necessary to ask more detailed questions under the topic areas since the important needs and requirements were mapped preliminarily based on the literature review. If the interviews were held in a "free word" way and opinions would have been asked of higher-level topics, for example: "What do you think about OT security?", the qualitative interviews probably would have not given as detailed information of the recognized important aspects and the DSR design and development phase (Peffers et al., 2006) would have achieved an unformed state. It was important to structure the interview topic area wise in a similar way as these were considered in the literature review to categorize the information for the creation of the guide. Most important aspect related to the guide for supporting decision making in smart factory environment is that the academic and scientific input is connected with the input of real-life experience and these two combined will justify the contents what are included in the guide which is the next step of this research.

## 5.3 Creation of guide – draft version

At the beginning of the guide creation process it is important to describe what this guide is, why this guide exists, and for who the guide is intended to. These will be included in the official guide document before the actual content part of the OT security and telecommunications needs and requirements. The guide is developed to an appropriate document template to suit possible official usage in companies generally. The guide is not made from any certain company's perspective, and it can be taken into use in various companies.

### 5.3.1 Heading – What this guide is?

The heading of the guide must give the first understanding for the user, that what information does this guide include. The heading must be clear, that the user can find it easily and does not mix it up with other guides on the field. The main goal for the guide was to support decision making on higher level related to OT security and telecommunication needs and requirements in smart factory environment. Based on this, the heading for this guide should be: "Supportive guide for decision making in smart factory environment – OT security and telecommunications".

### 5.3.2 Description – Why this guide exists?

The guide must include a description to give an understanding, why this guide exists and what it is used for. The description is also based on the main goal of the guide. The description must include that the guide is intended for higher level decision making related to the OT security and telecommunications needs and requirements in smart factory environment. It must be described that the guide gives requirements for the environment for decision makers to understand, why something has to be implemented in the environment. Description also mentions that the requirements are described in language which can be understood for example from directors or managers perspective so that the implementations can be moved to technical level to be carried out. It must be made clear that the guide does not offer technical instructions of how something is concretely inserted to the environment. The main focus is to understand what something is and what it does in bigger picture.

### 5.3.3 Scope – For who the guide is intended to?

Scope is included in this guide to describe to the users, who needs this guide in their actions. Since companies can have a large amount of different documentation and many of the documents can be closely related to each other, scope must be defined to deliver it to appropriate user crowd inside the company. Scope does not have to include specific roles from the organization hierarchy, but it should include the information, that the guide is intended to decision makers in smart factory environment, who for example negotiate about contracts and decide about the budget allocation related to implementations. It should be defined in the scope that the guide can be used in an educative manner for employees who do not have expertise related to OT security and telecommunications but have interest of getting familiar with the current requirements.

### 5.3.4 Contents of the guide

The content part of this guide consists of the requirements which were recognized as important through literature review and qualitative research (results of technical expert interviews). The requirements are described in a "brochure way" where the recognized requirement is the topic. Under the topic the requirement is explained what it means in practice, why it is important, and what does it bring for the company when implementing it. The explanations do not concentrate on technical details or instructions of certain implementations. As earlier mentioned, these concentrate on what something is and what it does in bigger picture. The contents are categorized under subtopics based on the made research to make the guide systematic and its contents easier to understand. The subtopics for contents are OT hardware and systems management, OT security in organization, OT telecommunications, and OT cyber preparedness. The following requirements are recognized as important based on the made research and are in the following structure under subtopics in the guide:

- OT hardware and systems management
    - Ownership of assets
    - CMDB for asset information (asset register)
    - Lifecycle management
    - Patch and update management
- OT security in organization
    - OT security as a term
    - OT security awareness
    - Roles and responsibilities in OT security
    - Usage of OT security standards
    - Auditing of OT environment
- OT telecommunications
    - Business versus OT network recognition
    - Network segmentation
    - Choosing the segmentation model
    - Protocols in multi-vendor environment
    - Appropriate WAN solution in remote factory
- OT cyber preparedness
    - AIC instead of CIA
    - Disaster recovery and business continuity
    - Security solutions in smart factory environment

## 5.4 Overview of the draft version

The draft version of the guide is in the attachment section of this thesis (Attachment 2). The guide is written on a certain Microsoft Word-document template which is optimal for writing a company guide. As earlier mentioned, the requirements written to the guide are picked from the earlier research made in this thesis and based on topics that are considered, but also seen as important in literature review and interviews. The descriptions of requirements are also based on the research. The draft guide is included in its original form to visualize how it would look in a format of company level document. Although the guide is a draft at this point, the final version is planned to use the same template since it is clear and easy to understand format wise.

Some of the subtopics were modified compared to literature review and technical expert interviews to create clear structure for the requirements. The requirements are divided under appropriate subtopics, and what a certain requirement can bring for the company is listed by using bullet points. For example, CMDB for asset information was recognized as important topic in the interviews and it is listed under "OT hardware and systems management", because it is related to asset management. OT standards were considered as own topic area in the interviews but is included under subtopic "OT security in organization" since standardization affects the compliance of the company, and the company is the target in audits. The division of requirements under subtopics helps the user to understand them in bigger picture and what these have in common.

Following this draft version, the possible modifications are made to the guide during and in the end of the next interview round based on the evaluation and feedback. The final version of the guide is published in this thesis after it and is added as an attachment to this thesis. Additions to this draft guide are considered in the interview results of next round but are all published officially in the final version of the guide at the same time.

# 6 SECOND ROUND INTERVIEWS – EVALUATION AND FEEDBACK OF THE GUIDE

The second round of the interviews is carried out in the same company, but the interviewees are new. The main focus of the second round of interviews is to get the draft guide evaluated with feedback so that the guide can be developed to its final form and published. Most important aspect to figure out, is that can the supportive guide be taken into use and are the suggested requirements relevant from the decision-making perspective. These interviews are also carried in a qualitative manner as in the first round. This second round of interviews is done in two parts. The first part is semi-structured, and the second part can be seen more as unstructured.

In the first part of the second-round interviews a smart factory specialist (E4) from company x who owns a specific solution related to the concept is interviewed. The goal of this interview is to get evaluation in quantitative manner of priority and complexity related to each requirement introduced in the guide. This information is necessary for the guide from decision-making perspective so that the priority order of implementations can be described but also the resources can be planned for each implementation related to the complexity. Priority is evaluated by using numerical chart from 1-5 in which 1 is least priority and 5 is critical priority. Complexity is evaluated also by using the chart from 1-5 in which 1 is easily implemented and 5 is hard to implement. The interview is carried out in a semi-structured way where the interviewee gives an answer from the chart but also comments the choice in a personalized way. The numerical evaluations of priority and complexity are inserted to the guide after this interview and are presented for the interviewees in the second part of this interview round. This part of the interview can be classified from DSR perspective as demonstration, since the draft guide is demonstrated for the interviewee, as evaluation, since the interviewee will do this related to priority and complexity, and as design and development since the draft guide returns back to this phase in the name of priority and complexity which are added to the guide before the second part of this round (Peffers et al., 2006).

The second part of interviews includes 3 persons from directorial and managerial level of company x. The interviewees are or have been involved with OT or IT decision making and are chosen to this part because of this. The roles of the interviewees in company x are Manager, IT Operations (E5), Director, Enterprise Architecture and Transformation (E6), and CIO (E7). The main focus of the second part of second interview round is to get the draft guide evaluated related to its format, contents, and can it support smart factory related decision making. This information is important since the draft guide must be evaluated and commented from the actual decision-making perspective before publishing the final version. The interviews are carried out in a more unstructured way since the interviewees have the possibility for "free word" of their opinions related to the guide. This will give the possibility for different point of views to rise related to the guide. This part of the interview round can be considered from DSR perspective as demonstration since the draft guide is presented in this part as well, and as evaluation since the guide will receive evaluation and feedback from the interviewees (Peffers et al., 2006).

## 6.1 Questions for interview 2-1

The structure of this interview consists of the similar background section, as in the first interview round, and of the priority and complexity evaluation of the draft guides requirements. The answers to the questions are written down to a separate Microsoft Word interview form to avoid misunderstandings when later analysing the answers. The interview is recorded by using Microsoft Teams platform. The interview is done in English since the interviewee is international and English is the most fluent language in this dialog.

The priority is described in the interview form that what is the priority for a certain implementation to be carried out. Implementation is the same as the earlier mentioned requirement in the guide. Complexity is described in a way that how complex a certain implementation is to carry out. The interview structure is the same as the subtopics and the requirements under them in the draft guide (Attachment 2). Same questions are asked for every requirement. The first one is the priority evaluation from the scale of 1 to 5. This is justified by the "free word" of interviewee that why the evaluation is like this. Similar is done for the complexity evaluation.

The interview is held in a time window of one hour. This is proper reservation for the interview since the guide has been presented for the interviewee earlier. It is necessary for the interviewee to get familiar with the guide before the interview since the evaluation requires knowledge and understanding of the requirements. If the interview requires more time, flexibility of time window is possible. The interview form is in the attachments list (Attachment 3).

## 6.2 Questions for interviews 2-2

The interview structure of the second part obeys the same principles as the first part structure, except the priority and complexity evaluation is replaced with evaluation and feedback of the guide in overall, including the priority and complexity evaluation made in first part. Also, the interview language is Finnish since all of the interviewees are native Finnish speakers. Answers are documented in English to the interview form.

In this interview the decision maker’s perspective is the most important and it is necessary to figure out that could the supportive guide work in a real-life environment. To receive the most honest evaluation and feedback from these interviews it is important to give the interviewee possibility for “free word”. The opinion is asked about the whole guide which can include every aspect of it from format to contents. The ability of the guide to support decision making is asked in the same question. The reason why this interview part is done in a manner of “free word” is to get as many-sided answers related to the guide which can be summarized before changing the draft guide to its official form. It is understood that interviewees might concentrate on totally different details of the guide, but all of this is important since the interviewees can be seen as potential users of the guide.

Interview form of the second part of second round is also in the attachments list (Attachment 4). The results of this interview round (part 1 and 2) are considered in the next part of this thesis. The results of each part follow each other to create a clear understanding of what was evaluated and added in the first part, and how the guide was seen in its intended role in the second part. It is important to understand that although the second part of this round concentrates on evaluation and feedback, it can possibly give development ideas for the draft guide which should be taken into consideration. These are analysed based on their nature and evaluated, should these be included in this supportive guide or possibly included in the future research or a different OT environment related guide. Some of possible development ideas can be out of context which means that these are not relevant to be considered in this guide, but these must be also mentioned in general.

# 7 INTERVIEW RESULTS & FINAL VERSION OF THE GUIDE

The interviewee of the first part of second round, smart factory specialist (E4), has been involved with OT related to long experience on plant floor organization. Interviewee has worked with IT support, management tasks, different assets, factory processes, and automation related to context. Currently the interviewee is working with the smart factory service in company x. The interviewee was chosen and classified as the most suitable one for this priority and complexity review from company x. The interviewee has handled with the requirements of the guide in work tasks and decision making related to smart factory environment is a familiar task for the interviewee. The evaluations can be considered as trustworthy since these can be justified with interviewees experience related to smart factory environments requirements.

The interviewees of the second part of second interview round have been involved with OT related to current smart factory project tasks and OT/IT architect's role in other company (E5). Interviewee 6 has been launching the factory digitalization development in company x and is familiar with the field for example infrastructure security service wise (E6). The last interviewee has not been involved with OT directly, but in company x OT is part of the current IT which is under interviewees responsibility as well as information security and privacy (E7). Interviewee also mentions that security, development and invests are related with this and OT is usually faced in security related discussions (E7). Interviewees can be described as valid responders for the evaluation and feedback round since all of these are or have been involved with either OT or IT decision making and work currently in a directorial/managerial role in company x. Great decision was to carry out the interview by asking single question related to the guide and its function since this enabled the interviewees to concentrate and mention the different details which they found out considerable related to the evaluation and feedback of the guide. The answers were many-sided and included different point of views.

## 7.1 Results of interview 2-1

### 7.1.1 Ownership of assets – OT hardware and systems management

The priority of this requirement was evaluated as 3. It was mentioned related to this that the ownership of assets in the environment is important, and a certain single point of contact is required for the assets. The evaluation is not higher on the scale since some of the OT environments assets might already have an owner. Complexity of this requirement was as well evaluated as 3 since the naming of owners can be complex depending on the number of different environments and volume of the organization. Also, in larger organizations the number of locations affect this and in where the ownerships have to be implemented.

### 7.1.2 CMDB for asset information (asset register)

This requirements priority is described as 3. The registering of assets and all documentation related to these is considered as indispensable implementation. Requiring asset owners and support groups is mentioned as an unnecessary action if the information related to these is not documented. The information related to assets can and should be documented which will help in the cases of incidents in future.  The complexity of this requirement is 3. This is justified by highlighting the easiness of registering assets and gathering information about these. It is stated that the complexity evaluation could be higher, if proper CMDB tools are not available or there are no standard framework for data collection of assets.

### 7.1.3 Lifecycle management

Implementation of lifecycle management is evaluated priority wise as 3. OT devices usually have to be in process 24 hours every day and different partners and vendors are involved. It is important that replaceable devices and outdated software is recognized related to assets' lifecycle. Complexity of this requirement is 4 since modifications in assets lifecycle can cause downtime which leads to process unavailability. Modifications in environment usually involve different teams in activities, for example maintenance, IT, and vendors, which increases the complexity related to cooperation.

### 7.1.4 Patch and update management

This is considered as critical priority 5. Patch and update management is carried out to keep track of the OT device security. These practices lower the overall business risk and are business continuity related tasks. Also, the complexity is evaluated as 5 since in case of security incidents in the environment, the availability is affected. OT/IT teams and factory teams usually can have conflicts since the processes have to be shut down for the recovery activities in OT environment.

### 7.1.5 OT security as a term – OT security in organization

Since the awareness of employees is important, this is evaluated as 3 priority wise. The importance increases especially when the company has locally bigger teams related to OT and usually the OT environment has a long list of different OT terminology. Complexity is 2 since the terminology is easy to train for the employees when the plans for it are in place. These should obey the organization standards.

### 7.1.6 OT security awareness

This requirement has priority of 4. Related to this the concentration is on employees who really work with on the subject of OT, and these should have a knowledge of accepted terms and practices in their everyday work. OT security can be seen to be far from basic IT security topics which are familiar for many compared to OT security. The complexity is 3 since its basic knowledge transfer, but in a bit more detailed manner. This is justified by the terminology which is different to IT security.

### 7.1.7 Roles and responsibilities in OT security

Priority 4 is stated related to this since the naming of persons and teams related to this requirement is a must have. In smart factory environment communication between the OT and IT is very critical. The complexity is 4 because the roles and responsibilities are quite different compared to normal IT ones. It is also highlighted related to this that OT personnel must have a good knowledge of the security in environment.

### 7.1.8 Usage of OT security standards

The requirement is evaluated as 4 in priority. Usage of OT security standards is a must have since this practice improves the consistency in the environment. The OT environment receives updates all the time which requires the companies to adapt to this by obeyance of standards. These can be also considered as reliable since these are tested and accepted already before. The complexity of this is 3 since this is a basic thing in companies to carry out. There has to be a certain plan in the background before implementing globally in certain locations to make this process easy.

### 7.1.9 Auditing of OT environment

This is mentioned as a must have which sets the priority to 4. Regular auditing is important in the OT environment, but the size of the environment and what is in it affects this a lot. Auditing is mentioned as a practice of lowering business risk and carrying out business continuity at the same time. As mentioned, that this depends lot on the environment, the complexity is evaluated as 4. Some OT environments can be hard to approach, and the production cannot be interrupted or stopped in some cases. The complexity evaluation is increased due to the complex nature of the OT systems.

### 7.1.10 Business versus OT network recognition – OT telecommunications

This requirement is evaluated priority wise as 4. It is mentioned that business and processes might be harmed if only basic IT related policies and segmentation are implemented in the factory environment. Specialized OT perspective must be kept in mind when implementing and describing the networks. This requirement is standard task from implementation perspective and the complexity is evaluated as 3. If correct awareness and document is in place this is an easy task to implement.

### 7.1.11 Network segmentation

The priority is evaluated as absolute 5. Network segmentation must be carried out in terms of accepted security standards. This requirements involves a lot of planning and developing the knowledge of what assets the company has in the environment. Strong and secure network segmentation is the goal. The segmentation might require advanced segmentation and that is why the complexity is evaluated as 4. This depends a lot on different devices and processes in the environment and the smart factory environment is in nature much more cooperative from communications and process perspective. Network segmentation is described to be a “complex thing to do from management perspective” (E4).

### 7.1.12 Choosing the segmentation model

When choosing the correct segmentation model this should be planned carefully which evaluates the priority as 4. It is mentioned that a lot of background work has to be done before the real segmentation and the business perspective and its requirements play a big role since the segmentation model should be decided in cooperation with these. Segmentation model should obey accepted standards. Complexity is also evaluated as 4 referring to the aspects of priority evaluation.

### 7.1.13 Protocols in multi-vendor environment

Implementing this requirements is a basic activity, so the priority is evaluated as 3. Replacing the older devices with new and more technological ones in the smart factory environment require industry standard protocols to enable fluent communication in multi-vendor environment. It is also important to understand what protocols are used in the environment, but there might rise problems related to older devices compared to new ones if the data collection process is complex. The complexity is 4 and it depends on the aging of the devices in the environment. If the environment is full on newer devices, the complexity would be lower since the data collection is much more easier from these.

### 7.1.14 Appropriate WAN solution in remote factory

Priority wise this is 4. The location of the environment affects this since the location can be far away from everything and there might be no good network solutions for this. Proper WAN solutions mean proper connectivity, and this is important to acknowledge. Also, alternative solutions from fail-safe perspective is important in terms of reliability. The complexity is higher if there are not many WAN solutions available depending on the location, but this requirement is evaluated as 3. It is mentioned that most of the sites have nowadays more than one solutions available, but the geographical aspect affects this sometimes.

### 7.1.15 AIC instead of CIA – OT cyber preparedness

The priority of this requirement is 4 since the difference in AIC and CIA can create problems in future when trying to implement security standards. It is important to clarify the prior role of availability in the smart factory environment and that it is understood. The awareness of priority of availability can be hard to implement since there are different understandings of the criticality of the processes which evaluates the complexity as 4. This creates a new perspective of focus in the smart factory environment compared to the more familiar CIA triad.

### 7.1.16 Disaster recovery and business continuity

The processes and plans related to this requirement must be in place if something bad happens which evaluates the priority as 5. The interviewee has personal experience of these situations, and it is mentioned that if the good plans were not in place there would have not been any business continuity (E4). This requirement is developed with awareness and support in companies. This requirement can be really time-consuming implementation which requires several stakeholders to be involved which evaluates the complexity as 4.

### 7.1.17 Security solutions in smart factory environment

This requirements priority is 4. The security is truly increased, and the business risks are lowered if security solutions are implemented to the OT environment and automation solutions. These are described as preventative processes for OT security. The monitoring connected with alarms in the environment with automation and AI can be considered as important things to have. This requirements is a very complex action to carry out and that is why the complexity evaluation is 5. Since the smart factory environment can include a huge variety of different assets this cannot be approached as “plug and play” because these solutions will not work immediately with all of the assets. The implementation of security solutions requires that the foundation work is done for example related to network segmentation and security standards before more advanced solutions are taken into consideration. The statement related to this is that “lots of things have to be in place before reaching this level” (E4).

## 7.2 Results of interviews 2-2

### 7.2.1 Structure

The structure of the guide is seen as logical in which the important topics are categorized under larger sub-topics (E7). It is mentioned that the guide is clear and easy to follow, and it is described to be better documentation from this perspective than earlier which has considered similar topic areas (E5). In summary, the interviewees see the guide’s structure as good and that it would be in line with the company environment since this kind of a guide is needed (E6).

### 7.2.2 Contents

The contents of this guide have similarities with important topics experienced in OT/IT convergent environment and its requirements (E5). The contents are mentioned to be the ones which should be implemented in the considered environment (E6). It is suggested that the beginning of the guide could include a short description of smart factory environment and what is its function in case the reader of this guide is not so familiar with the topic area (E7).

In interviews the importance of support model was highlighted and what is the connection between this and the guide for example in situations when support tickets are opened (E6). This is suggested to be added to the contents of the guide. The priority evaluation of the requirements described in the guide is mentioned to have correlation with the role of service desk and support model in company (E6).

It is suggested that the business’s needs and requirements could be considered in this guide related to smart factory environment (E6). It is also mentioned that the OT/IT security and telecommunications implementations should be planned based on the functionality and requirements of the factory (E5). The interviewee mentions that if for example PLC configurations are wanted to be done straight from the factory, what has to be considered when doing the security and telecommunications implementations (E5). This approach from the requirement perspective might not suit this guide (E5) because this guide is made from the perspective of what are the important requirements in the environment more generally.

The importance of recognizing and describing non-standard environments from lifecycle management and updates perspective related to smart factories is highlighted in the interviews (E6) and this was also considered earlier in this thesis. It is also mentioned that patching is considered more as firmware updates in OT environment and that patching often refers to Windows or IT related tasks (E5). Both patching and firmware updates can be seen as part of smart factory environment (E5).

The segmentation part of the guide is seen as a clear a descriptive part, but it is suggested that the firewall and third-party connection related aspect could be handled in the guide (E6). This could include information about the approval and workflows related to the processes and how this should be organized in bigger picture since OT, IT, and business stakeholders are involved in this (E6). It is mentioned related to segmentation and security that management should get an understanding that the strictest level is not required in these, but the lowest level is not either an option (E5). In other words, the required levels should be described based on the company (E5). Metrics could be added to the requirements list of the guide since these can be seen as important part when measuring the maturity and security levels of certain factory (E5). It is important to understand what the current level of these metrics in a factory is and what is the desired level which should be reached since this information is required from the management level to follow up (E5).

It is suggested that service perspective and "making a service" -thought could be added to this guide and what services are related to these requirements (E6). Important topics related to this are that is the service developed from old one to the smart factory environment or is the service totally new, and who or what area is the manager for these different services (E6). The relation between the service idea and for example management models and budgeting would be necessary information (E6). Related to roles in smart factory environment the cooperative goals could be described and opened in the guide (E5). Information related to resourcing per requirement is stated to be an important addition to this guide from decision making perspective (E5).

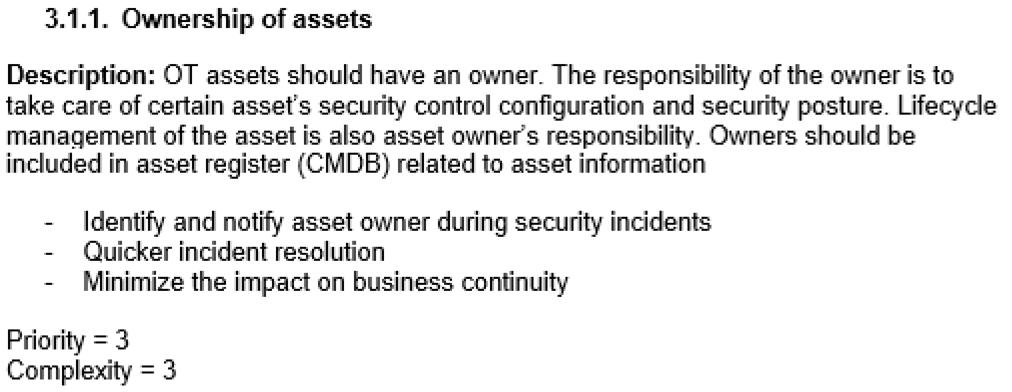
The cyber preparedness is considered as well-made topic area, but it could include information of how to for example tackle OT security in old factory automation or company integrations (E6). Also, OT related requirements, for example ISO-standard requirements, could be mentioned related to investments and vendors (E6). Related to the impact of each requirement it is mentioned that could this include information about what happens if something fails to succeed, but this can be solved by approaching the benefits of each requirement from opposite direction (E7).

### 7.2.3 Functionality

The functionality of the supportive guide can be summarized from the answers of all interviewees that the guide can really support the decision making, but possibly some additions could be made to make it more usable especially for business orientated decision making. If the guide would be tested in practice, more development ideas would rise based on the functionality (E7). It is mentioned that this guide is a step to right direction and the content is good quality wise in overall (E6). The possible additions to the guide to improve its functionality were considered from interviewees perspective under 7.2.2 Contents.

## 7.3 Analysis and finalization of the guide

Referring to the first part interview of the second round (E4) the priority and complexity evaluation were added to the draft guide below every requirement in following way:



**3.1.1. Ownership of assets**

**Description:** OT assets should have an owner. The responsibility of the owner is to take care of certain asset's security control configuration and security posture. Lifecycle management of the asset is also asset owner's responsibility. Owners should be included in asset register (CMDB) related to asset information

- Identify and notify asset owner during security incidents
- Quicker incident resolution
- Minimize the impact on business continuity

Priority = 3
Complexity = 3

Figure 7 Visualization of the added priority and complexity values to the guide (Attachment 5)

The added values were described in short words in the description of the guide to give the reader an understanding about what priority and complexity mean in this context. The results of the priority and complexity interview and why some requirement was evaluated in a certain way are not necessary to be opened in the guide since the guide is intended to be used as a guide document in companies and this kind of documents have to be simple and understandable. The justifications for the priority and complexity values can be found from this thesis. Following text was added to the description of the guide:

> Every requirement includes priority evaluation of what is the priority for the implementation to be carried out (1 = least priority, 5 = critical priority) and complexity evaluation of how complex is the implementation to be carried out (1 = easily implemented, 5 = hard to implement). (Attachment 5)

The guide was delivered with previous additions for the interviewees of the second part of this interview round to give evaluation and feedback about it (Attachment 4). It is important to understand at this point that the further development of the guide must be justified in a proper manner and what changes have to be made for the guide related to this thesis. It must be understood that the development process of the guide would continue for undefined time if every perspective would be considered in it. The goal of this thesis is necessary to be reminded. What are the OT security and telecommunications related important requirements in smart factory environment and how these can be informed for the decision making? The feedback of the second part can be filtered under two topics which are **development in this thesis** and **development directions for future**. The received feedback which will lead to changes in the guide is classified under the first and the received feedback which would need additional research or is not necessary to be considered in this thesis is classified under the second. The feedback which is considered as "development directions for future" is considered as suggested topics which are concluded from the second part interview results. These topics will describe how the research and development should continue after the publishing of this thesis based on the opinions of the researcher.

### 7.3.1 Development in this thesis

This development can be considered again as design and development in the DSR process (Peffers et al., 2006) since development is required for the guide based on the second part evaluation and feedback. The DSR process will continue after this phase straight to the communication (Peffers et al, 2006) since the desired state of the guide is reached and the directions for future are communicated for the companies and academic research.

It was suggested that the description of smart factory could be added to the description of the guide to make the term clear for people who are new to the topic. It can be admitted that the term smart factory is probably familiar to people involved with OT/IT convergent manufacturing, but the guide can be used as well as educative material related to requirements which describes the need for defining the smart factory as a term with few words. This can be described as a manufacturing environment related to forth industrial revolution (Industry 4.0) which concentrates on Cyber Physical Systems (CPS) and internet of things (IoT) (Vaidya et al., 2018). The main focus is on digitalized manufacturing which is done in OT/IT convergent environment. The term is based on the literature review of this thesis and is added to the description of the guide (Attachment 5).

> Smart factory can be described as an environment of digitalized manufacturing which is related to Industry 4.0. Smart factory concentrates on Cyber Physical Systems (CPS) and Internet of Things (IoT) in OT/IT convergent environment. (Attachment 5)

"Firmware updates" was mentioned to be a more standardized term in OT environment for its IT alternative "patching". Firmware updates are carried out to OT hardware and systems. Smart factory environment will include both of these terms since both OT and IT are involved in digitalized manufacturing. It is important to add firmware updates as a term to the requirement "Patch and update management" to clarify the meaning for more OT oriented personnel. It is not clear that is there going to be a standardized term in smart factory environment which includes both OT and IT updates related activities. The previous "Patch and update management" (Attachment 2) is changed to "Patch / Firmware updates management" (Attachment 5).

Since the contents in the guide are based on the contents of this master's thesis, it is important to add this as a reference to the header. This master's thesis is going to be available on the Internet which can be used as a supportive document for the guide itself for example when finding out the justifications for certain priority / complexity evaluations or why something ended up listed as requirement for the smart factory environment. As earlier mentioned, these are not included in the guide itself since it would confuse the reader if the contents and structure would include a lot of information per requirement from different directions. The final version of the developed guide can be found from the attachments list (Attachment 5).

### 7.3.2 Development directions for future

It can be concluded from the results of the second part that the development ideas for the guide were mostly related to extending the requirements and considering these from different perspectives in company environment. None of the interviewees suggested something to be removed from the guide which is a good sign from acceptance perspective. Still, the evaluation and feedback are necessary to consider and what it could bring for the future research and development related to supportive documentation of smart factory environment. From the second part results following main directions can be concluded for the future R&D in which the guide's requirements are involved:

- Support model involvement
- Business and factory needs and requirements
- Approval and workflows of processes
- Metrics for the requirements
- Services from the requirements ("making a service")
- Resourcing related to the requirements
- Standardization of made investments and vendors

These development ideas are recognized from the results which need additional research to be integrated with the guide. For example different stakeholders should be interviewed and further investigation from certain organization should be carried out to gather trustworthy information. For example the topic related to support model's connections with the requirements of the guide could be carried research wise in a qualitative manner by involving service desk and service management in the research. On the other hand, the metrics of evaluating the maturity and security levels in factories has to be made in a quantitative manner for example concentrating on case studies on some real-life environment. Also, if these would be considered in the guide, it would be on a more specialized level of documentation and it would be in conflict with the obeyed idea of introducing important OT security and telecommunications needs and requirements. Of course the more specialized documentation would also include information about the earlier mentioned, but the current form enables the future development of the guide to different directions either academically or inside companies. It can be used in its current form as supportive guide as it was stated in the interviews.

# 8 SUMMARY AND COMMUNICATION

A supportive guide for decision making in smart factory environment was achieved based on the research process of this thesis. The guide was developed in cooperation with the employees of company x which enabled the research process to involve different employees with different backgrounds which enabled a many-sided approach from the perspective of this master's thesis. The research was made and described as transparent as possible from academic perspective to understand what was considered and in which phase. To remind why all of this was carried out it is important to reflect on the main goal and motivation which was to create a supportive guide for decision making based on the combination of academic material and experience from a certain company. This guide tackles the problem related to relying solely based on commercial actors' suggestions and that the considered environment can be approached with academic proof. The final version of the guide is a proper solution which responds to the requirements which describe why this research was made. Also, based on feedback the guide was seen as potential choice from the company's perspective to take into use which is the most important thing since this research process really succeeded to develop a solution for an identified problem.

The Design Science Research (DSR) process (Peffers et al., 2006) which was used as a research methodology for this thesis can be described as a qualified methodology for the research which is made in the way as in thesis related to research in information systems science. The process was not carried out in a step-by-step manner as described in the beginning of this thesis related to research methodology and some of the phases of DSR were carried out multiple times. These were considered in an order in which the design and development phase (Peffers et al., 2006) was repeated during the empirical data gathering process in the name of interviews. This thesis gives trustworthy feedback for the academic world related to DSR research methodology although the concentration was not on researching the methodology itself. DSR process can be modified to the needs of the made research and the process is very flexible from the perspective of repeating earlier phases. Also, the DSR process enables the usage of qualitative and quantitative methods related to research which was necessary in this thesis.

The directions for future research were considered in the analysis and finalization of the guide -part and these can be considered either from academic, company or both perspectives. The guide created in this thesis can be for example taken to company use and develop it to suit the possible specialized needs, for example when mapping the businesses needs and requirements and how these requirements affect the environment which is described by the business. Also, this guide can be approached from more academic perspective and for example test it in practice related to a case study or similar which could bring even more feedback and development ideas for future. The topic areas introduced in the guide can be taken into more technical inspection which would enable the creation of technical level documentation for example of OT cyber preparedness. It must be understood related to smart factory environment that the digitalized factory solutions develop from security and telecommunications perspective which possibly affects the requirements list described in the guide. The guide is made based on current trends and how the smart factory environment is seen in late 2022.

Related to the research, some shortages can be described related to data gathering. The first-round interviews could have involved more interviewees which would have given a wider range of information related to the topics, but the number of interviewees was based on the timeframe of this thesis and that the information can be extended in future. The first part of second-round interviews (priority and complexity) could have also involved more interviewees which would have given more feedback for the evaluation. Since the company x was the company from where the interviewees were chosen, this was not a choice since the finding and qualifying process of interviewees would have been too long from time perspective. Same can be admitted related to the second part of the second-round interviews. The important topics chosen from literature review to be developed could be different from other researchers' perspective and some requirements could be added to the guide, but the list would be never ending. It is important to understand that the requirements described in the guide (Attachment 5) are important from the perspective of this thesis with the support of technical experts and evaluators from company x.

In overall, the master's thesis process was efficient, and the clear plans of every phase helped to achieve what was pursued. Although, the solution is not for example a concrete system or improvement in it related to information systems, DSR can be admitted being a suitable choice for this kind of research. Company x as a big manufacturing company was a proper choice from the perspective of choosing interviewees since the desired knowledge and profession related to the topic area was on a high level. The research process was carried out mainly in the way as described in the beginning of this master's thesis which tells about the fact that the research process was planned correctly to suit the aim of this thesis.

# REFERENCES

Ahakonye, L. A. C., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2021). Efficient Classification of Enciphered SCADA Network Traffic in Smart Factory Using Decision Tree Algorithm. IEEE Access, 9, 154892-154901. IEEE.

Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. Computer Communications, 155, 1-8. Elsevier.

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review, 54(5), 3849-3886. Springer.

Conklin, W. A. (2016). IT vs. OT security: A time to consider a change in CIA to include resilience. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 2642-2647). IEEE.

Cook, A., Janicke, H., Smith, R., & Maglaras, L. (2017). The industrial control system cyber defence triage process. Computers & Security, 70, 467-481. Elsevier.

Garimella, P. K. (2018, October). IT-OT integration challenges in utilities. In 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS) (pp. 199-204). IEEE.

Ghobakhloo, M. (2020). Industry 4.0, digitization, and opportunities for sustainability. Journal of cleaner production, 252, 119869. Elsevier.

Ghosh, S., & Sampalli, S. (2019). A survey of security in SCADA networks: Current issues and future challenges. IEEE Access, 7, 135812-135831. IEEE.

Hahn, A. (2016). Operational technology and information technology in industrial control systems. In Cyber-security of SCADA and other industrial control systems (pp. 51-68). Springer, Cham.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS quarterly, 75-105. JSTOR.

Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. In Design research in information systems (pp. 9-22). Springer, Boston, MA.

Hollerer, S., Kastner, W., & Sauter, T. (2021). Towards a threat modeling approach addressing security and safety in OT environments. In 2021 17th IEEE International Conference on Factory Communication Systems (WFCS) (pp. 37-40). IEEE.

International Electrotechnical Commission. (2013). Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels (IEC 62443-3-3). IEC.

Kulik, T., Tran-Jørgensen, P. W., & Boudjadar, J. (2019, June). Compliance verification of a cyber security standard for Cloud-connected SCADA. In 2019 Global IoT Summit (GIoTS) (pp. 1-6). IEEE.

Lin, Y. J., Wei, S. H., & Huang, C. Y. (2019). Intelligent manufacturing control systems: The core of smart factory. Procedia manufacturing, 39, 389-397. Elsevier.

More, S., Jamadar, I., & Kazi, F. (2020, July). Security Visualization and Active Querying for OT Network. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V. & Bragge, J. (2006). The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. In 1st International Conference, DESRIST 2006 Proceedings. (pp. 83-106). Claremont Graduate University.

Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Communications Surveys & Tutorials, 22(3), 1942-1976. IEEE.

Rakas, S. V. B., Stojanović, M. D., & Marković-Petrović, J. D. (2020). A review of research work on network-based scada intrusion detection systems. IEEE Access, 8, 93083-93108. IEEE.

Sayed, K., & Gabbar, H. A. (2017). SCADA and smart energy grid control automation. In Smart energy grid engineering (pp. 481-514). Academic Press.

Shilenge, M. C., & Telukdarie, A. (2022, June). Optimization of Operational and Information Technology Integration Towards Industry 4.0. In 2022 IEEE 31st International Symposium on Industrial Electronics (ISIE) (pp. 1076-1081). IEEE.

Siemers, B., Fischer, L., & Lehnhoff, S. (2022, May). A Trust Model in Control Systems to Enhance and Support Cybersecurity. In 2022 IEEE 7th International Energy Conference (ENERGYCON) (pp. 1-6). IEEE.

Sonkor, M. S., & García de Soto, B. (2021). Operational technology on construction sites: a review from the cybersecurity perspective. Journal of Construction Engineering and Management, 147(12), 04021172. Research Gate.

Sundaram, A., Abdel-Khalik, H. S., & Ashy, O. (2020). A data analytical approach for assessing the efficacy of Operational Technology active defenses against insider threats. Progress in Nuclear Energy, 124, 103339. Elsevier.

Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666. Elsevier.

Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0–a glimpse. Procedia manufacturing, 20, 233-238. Elsevier.

Wagner, N., Şahin, C. Ş., Winterrose, M., Riordan, J., Pena, J., Hanson, D., & Streilein, W. W. (2016, December). Towards automated cyber decision support: A case study on network segmentation for security. In 2016 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-10). IEEE.

Williams, T. J. (1993). The Purdue enterprise reference architecture. IFAC Proceedings Volumes, 26(2), 559-564. Elsevier.

Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. Ict Express, 4(1), 14-18. Elsevier.

# ATTACHMENT 1 STRUCTURE OF THE INTERVIEW (ROUND 1)

## Interview – Round 1 (Technical Experts)

### Background

Q1: What is your role in this company?

A:

Q2: How have you been involved with the OT?

A:

### OT hardware and systems

Q3: Should OT assets have an owner/manager? Why?

A:

Q4: Does OT lifecycle management require something different than IT (other than the longer lifespan)? What?

A:

Q5: Does OT patch management and updates require something different than IT? What?

A:

Free word related to the topic area:

### OT security in organization culture

Q6: OT security (CIA + Physical Process) can be confused with IT security (CIA). Should OT security be integrated to organization culture (e.g. learning related to OT security)? Why and how?

A:

Q7: OT security can be considered together with IT security since these are in the same environment related to digitalized concepts. Should the personnel consider with both areas or be separated under each? Why?

A:

Q8: What is your opinion of the description OT security = CIA + physical process and could it work as an accepted term?

A:

Free word related to the topic area:

## OT standards (e.g. IEC 62443 series)

Q9: Should OT environment be implemented based on certain standard? Why?

A:

Q10: Should the OT environment be audited yearly? What is the benefit from this?

A:

Free word related to the topic area:

## OT telecommunications

Q11: What are the biggest differences between business and OT networks?

A:

Q12: Is it necessary to use segmentation models for the architecture of infrastructure? Why?

A:

Q13: Purdue model is a network segmentation model which is widely used related to OT/IT network architecture. Do you see the model as a relevant version?

A:

Q14: Is Purdue model the best possible model for network segmentation since new network and telecommunications are rising (e.g. cloud solutions, 5G, etc.)? Why?

A:

Q15: OT hardware and systems use different OT related communication protocols (e.g. Modbus, DNP3, extended IT protocols) to communicate inside the environment. Many vendors have own vendor-specific protocols. How a possible multi-vendor environment has to be implemented related to protocols?

A:

Q16: What is the best solution for using WAN in remote factory environment? Why?

A:

Free word related to the topic area:

## Cyber-attacks and prevention

Q17: CIA triad is considered in IT security in order C > I > A. It is suggested that OT is in order A > I > C. Is this relevant hierarchy? Why?

A:

Q18: Attacks against OT environment have caused major physical damage in history. What are the important things in OT/IT integrated environment to consider related to disaster recovery and business continuity?

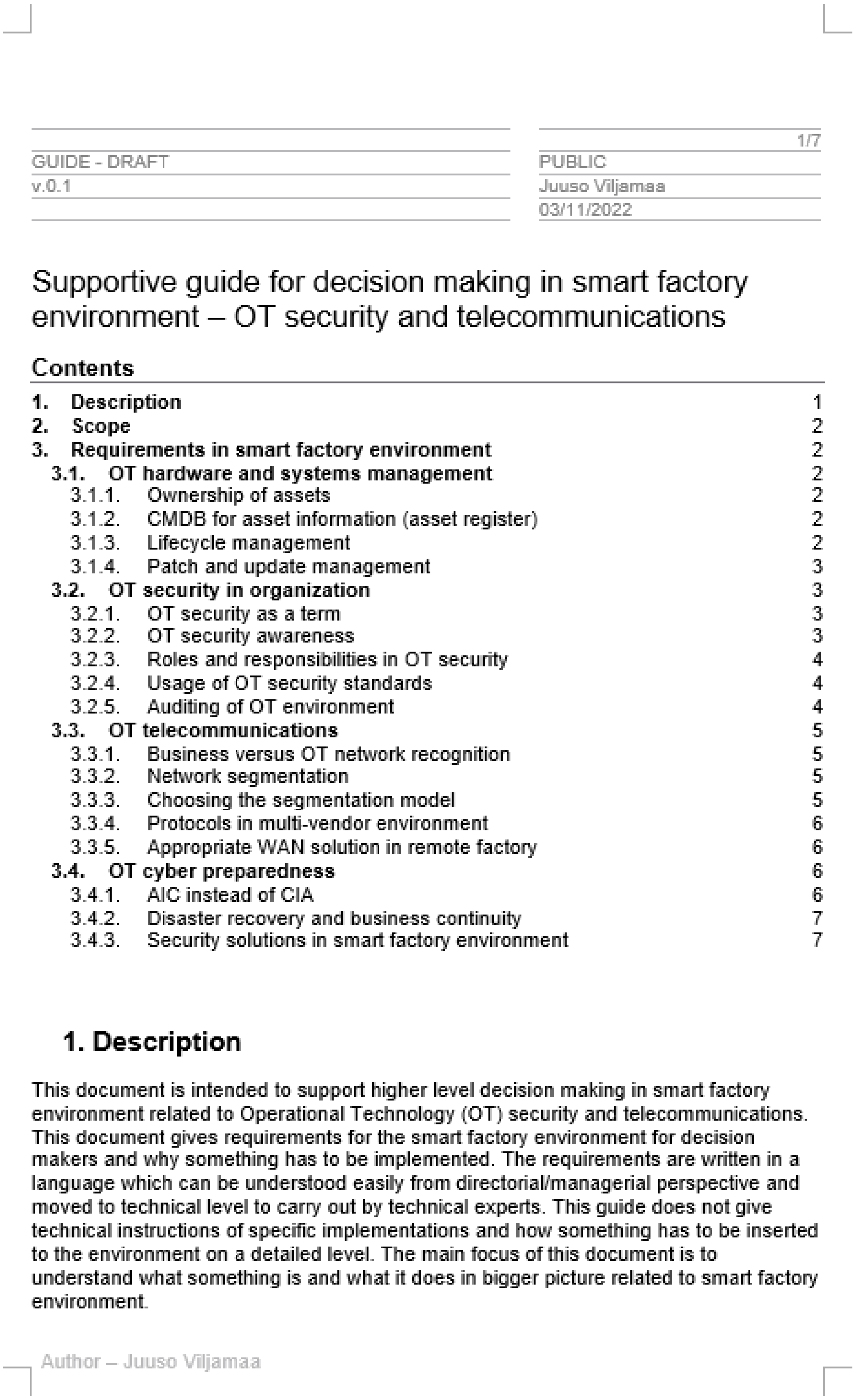
A:

Q19: Different network monitoring solutions and intrusion detection systems are used in OT environment and network level is mentioned as an important surface. Do you see different security solutions relevant, and what has to be implemented? What about machine learning and AI in OT cybersecurity?

A:

Free word related to the topic area:

# ATTACHMENT 2 DRAFT VERSION OF THE GUIDE



| | |
|---|---|
| | 1/7 |
| GUIDE - DRAFT | PUBLIC |
| v.0.1 | Juuso Viljamaa |
| | 03/11/2022 |

## Supportive guide for decision making in smart factory environment – OT security and telecommunications

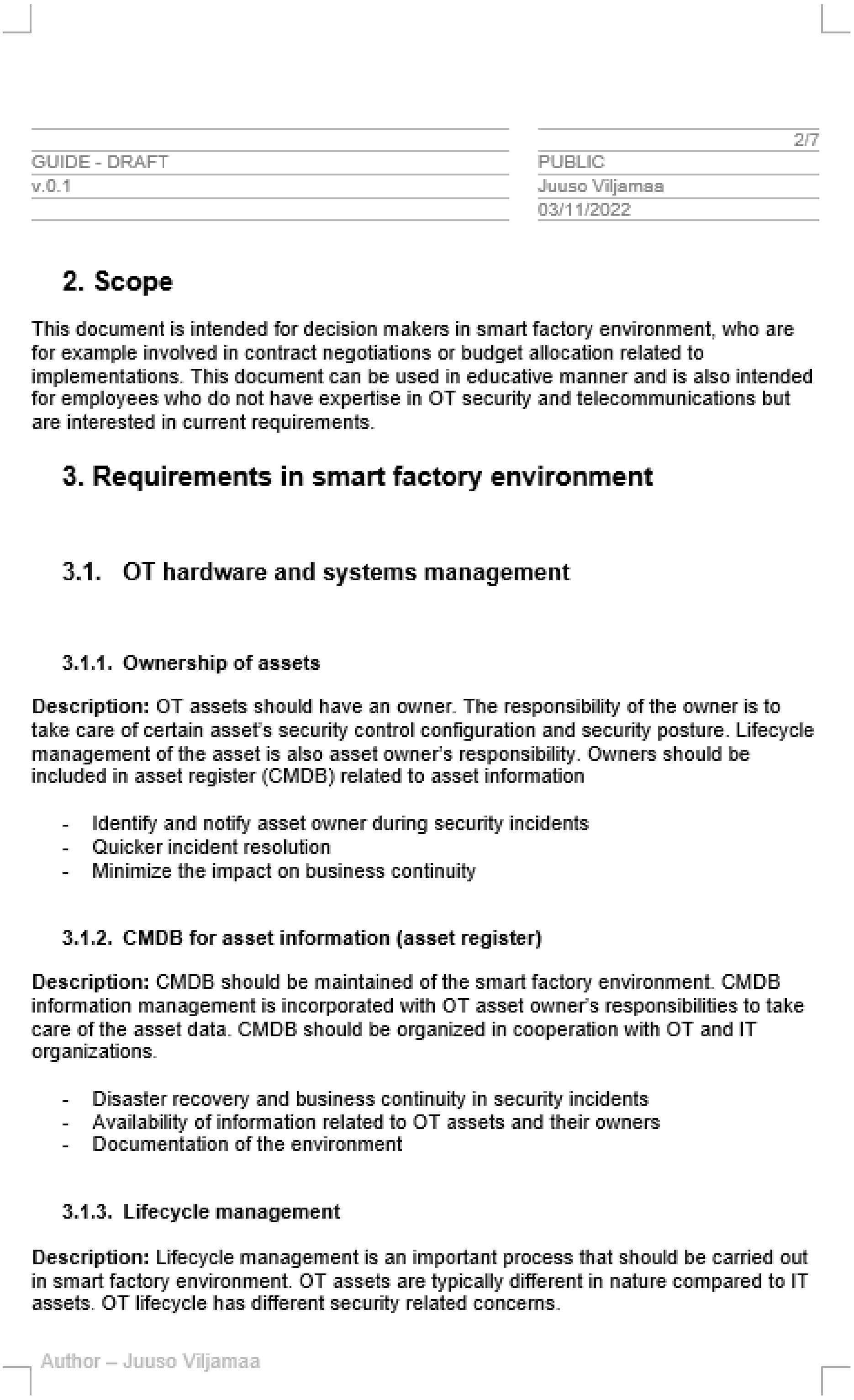
### Contents

1. **Description** 1
2. **Scope** 2
3. **Requirements in smart factory environment** 2

**3.1. OT hardware and systems management** 2
3.1.1. Ownership of assets 2
3.1.2. CMDB for asset information (asset register) 2
3.1.3. Lifecycle management 2
3.1.4. Patch and update management 3
**3.2. OT security in organization** 3
3.2.1. OT security as a term 3
3.2.2. OT security awareness 3
3.2.3. Roles and responsibilities in OT security 4
3.2.4. Usage of OT security standards 4
3.2.5. Auditing of OT environment 4
**3.3. OT telecommunications** 5
3.3.1. Business versus OT network recognition 5
3.3.2. Network segmentation 5
3.3.3. Choosing the segmentation model 5
3.3.4. Protocols in multi-vendor environment 6
3.3.5. Appropriate WAN solution in remote factory 6
**3.4. OT cyber preparedness** 6
3.4.1. AIC instead of CIA 6
3.4.2. Disaster recovery and business continuity 7
3.4.3. Security solutions in smart factory environment 7

## 1. Description

This document is intended to support higher level decision making in smart factory environment related to Operational Technology (OT) security and telecommunications. This document gives requirements for the smart factory environment for decision makers and why something has to be implemented. The requirements are written in a language which can be understood easily from directorial/managerial perspective and moved to technical level to carry out by technical experts. This guide does not give technical instructions of specific implementations and how something has to be inserted to the environment on a detailed level. The main focus of this document is to understand what something is and what it does in bigger picture related to smart factory environment.



## 2. Scope

This document is intended for decision makers in smart factory environment, who are for example involved in contract negotiations or budget allocation related to implementations. This document can be used in educative manner and is also intended for employees who do not have expertise in OT security and telecommunications but are interested in current requirements.

## 3. Requirements in smart factory environment

### 3.1. OT hardware and systems management

#### 3.1.1. Ownership of assets

**Description:** OT assets should have an owner. The responsibility of the owner is to take care of certain asset's security control configuration and security posture. Lifecycle management of the asset is also asset owner's responsibility. Owners should be included in asset register (CMDB) related to asset information

- Identify and notify asset owner during security incidents
- Quicker incident resolution
- Minimize the impact on business continuity

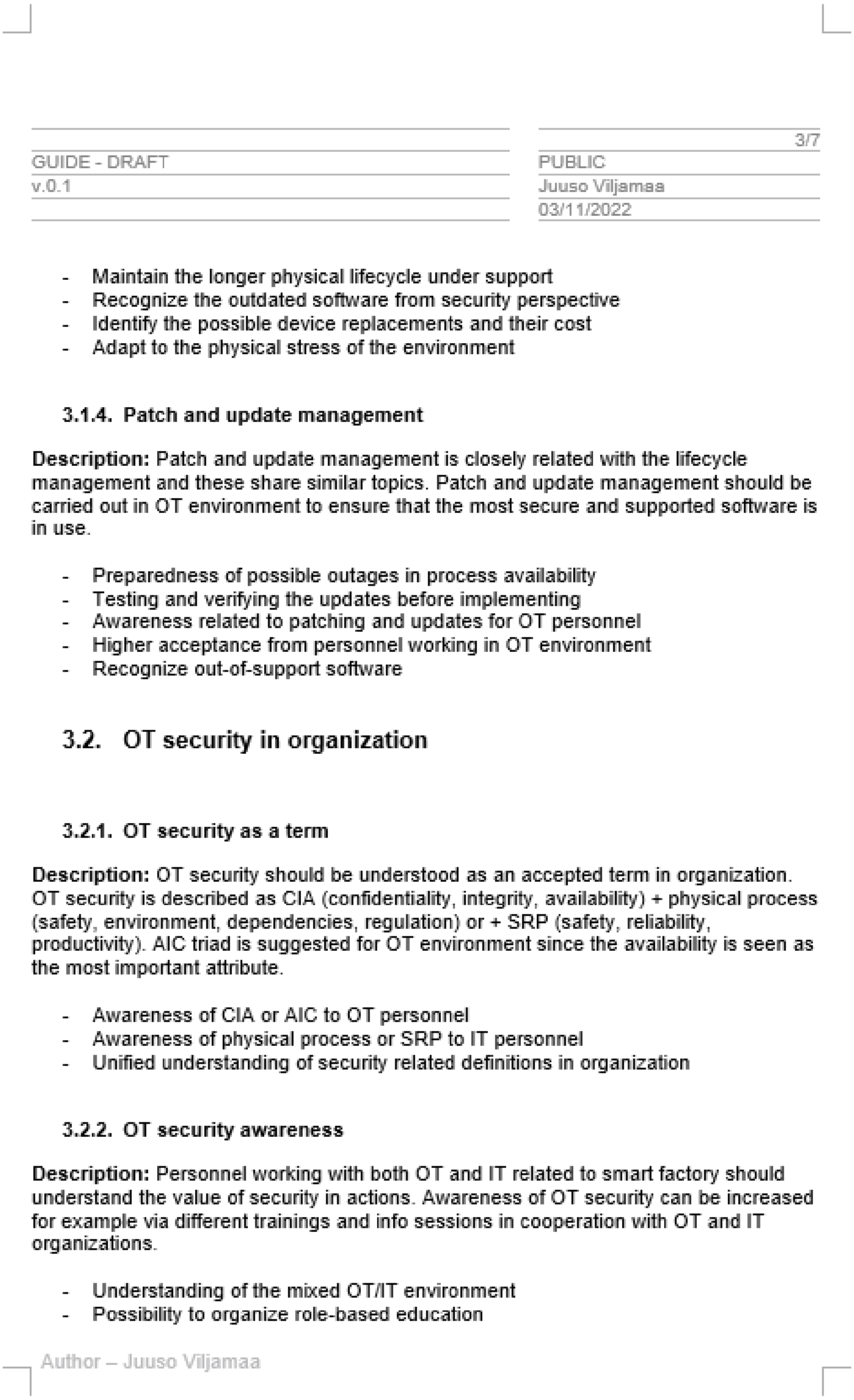
#### 3.1.2. CMDB for asset information (asset register)

**Description:** CMDB should be maintained of the smart factory environment. CMDB information management is incorporated with OT asset owner's responsibilities to take care of the asset data. CMDB should be organized in cooperation with OT and IT organizations.

- Disaster recovery and business continuity in security incidents
- Availability of information related to OT assets and their owners
- Documentation of the environment

#### 3.1.3. Lifecycle management

**Description:** Lifecycle management is an important process that should be carried out in smart factory environment. OT assets are typically different in nature compared to IT assets. OT lifecycle has different security related concerns.



- Maintain the longer physical lifecycle under support
- Recognize the outdated software from security perspective
- Identify the possible device replacements and their cost
- Adapt to the physical stress of the environment

### 3.1.4. Patch and update management

**Description:** Patch and update management is closely related with the lifecycle management and these share similar topics. Patch and update management should be carried out in OT environment to ensure that the most secure and supported software is in use.

- Preparedness of possible outages in process availability
- Testing and verifying the updates before implementing
- Awareness related to patching and updates for OT personnel
- Higher acceptance from personnel working in OT environment
- Recognize out-of-support software

## 3.2. OT security in organization

### 3.2.1. OT security as a term

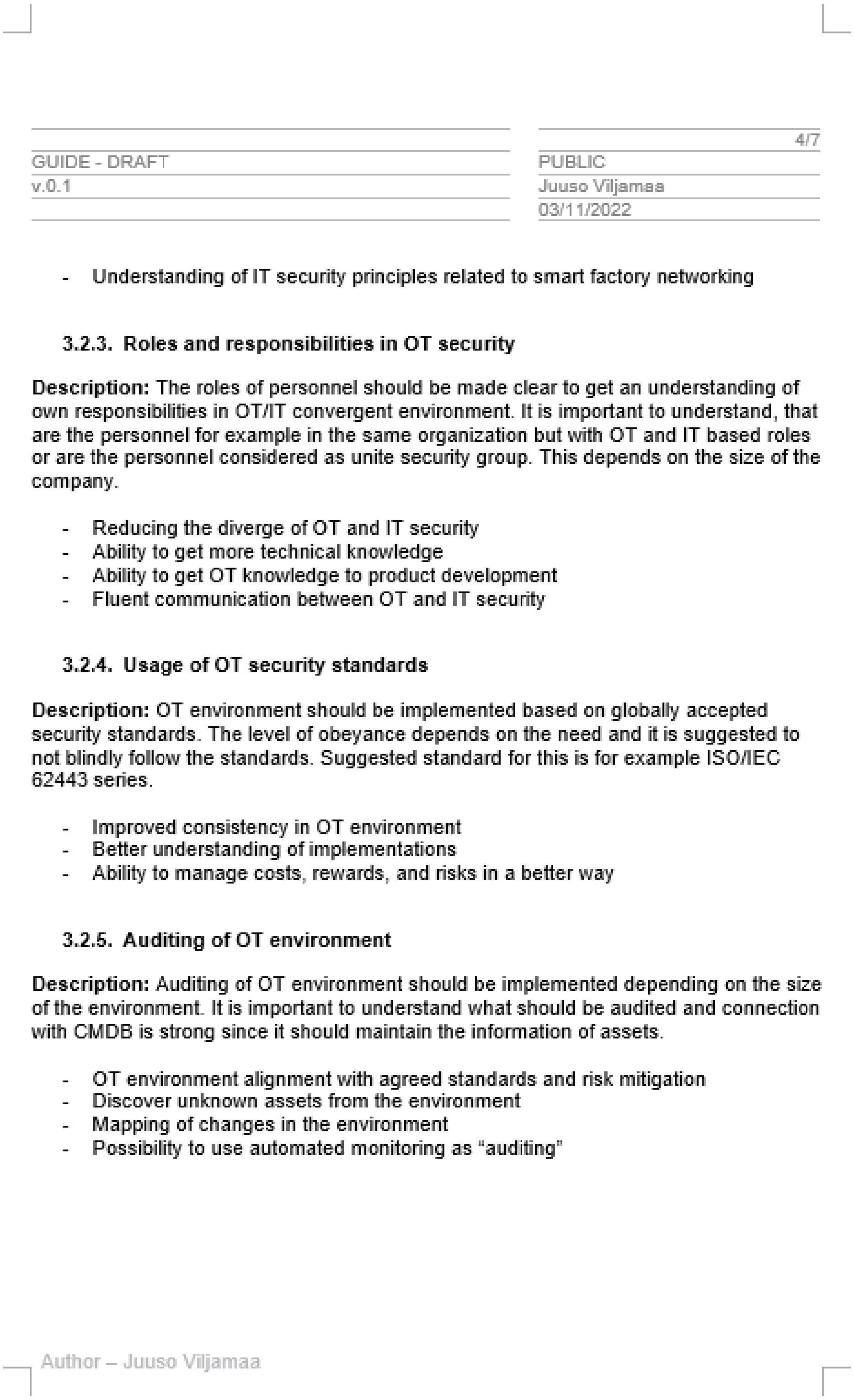
**Description:** OT security should be understood as an accepted term in organization. OT security is described as CIA (confidentiality, integrity, availability) + physical process (safety, environment, dependencies, regulation) or + SRP (safety, reliability, productivity). AIC triad is suggested for OT environment since the availability is seen as the most important attribute.

- Awareness of CIA or AIC to OT personnel
- Awareness of physical process or SRP to IT personnel
- Unified understanding of security related definitions in organization

### 3.2.2. OT security awareness

**Description:** Personnel working with both OT and IT related to smart factory should understand the value of security in actions. Awareness of OT security can be increased for example via different trainings and info sessions in cooperation with OT and IT organizations.

- Understanding of the mixed OT/IT environment
- Possibility to organize role-based education



- Understanding of IT security principles related to smart factory networking

### 3.2.3. Roles and responsibilities in OT security

**Description:** The roles of personnel should be made clear to get an understanding of own responsibilities in OT/IT convergent environment. It is important to understand, that are the personnel for example in the same organization but with OT and IT based roles or are the personnel considered as unite security group. This depends on the size of the company.

- Reducing the diverge of OT and IT security
- Ability to get more technical knowledge
- Ability to get OT knowledge to product development
- Fluent communication between OT and IT security

### 3.2.4. Usage of OT security standards

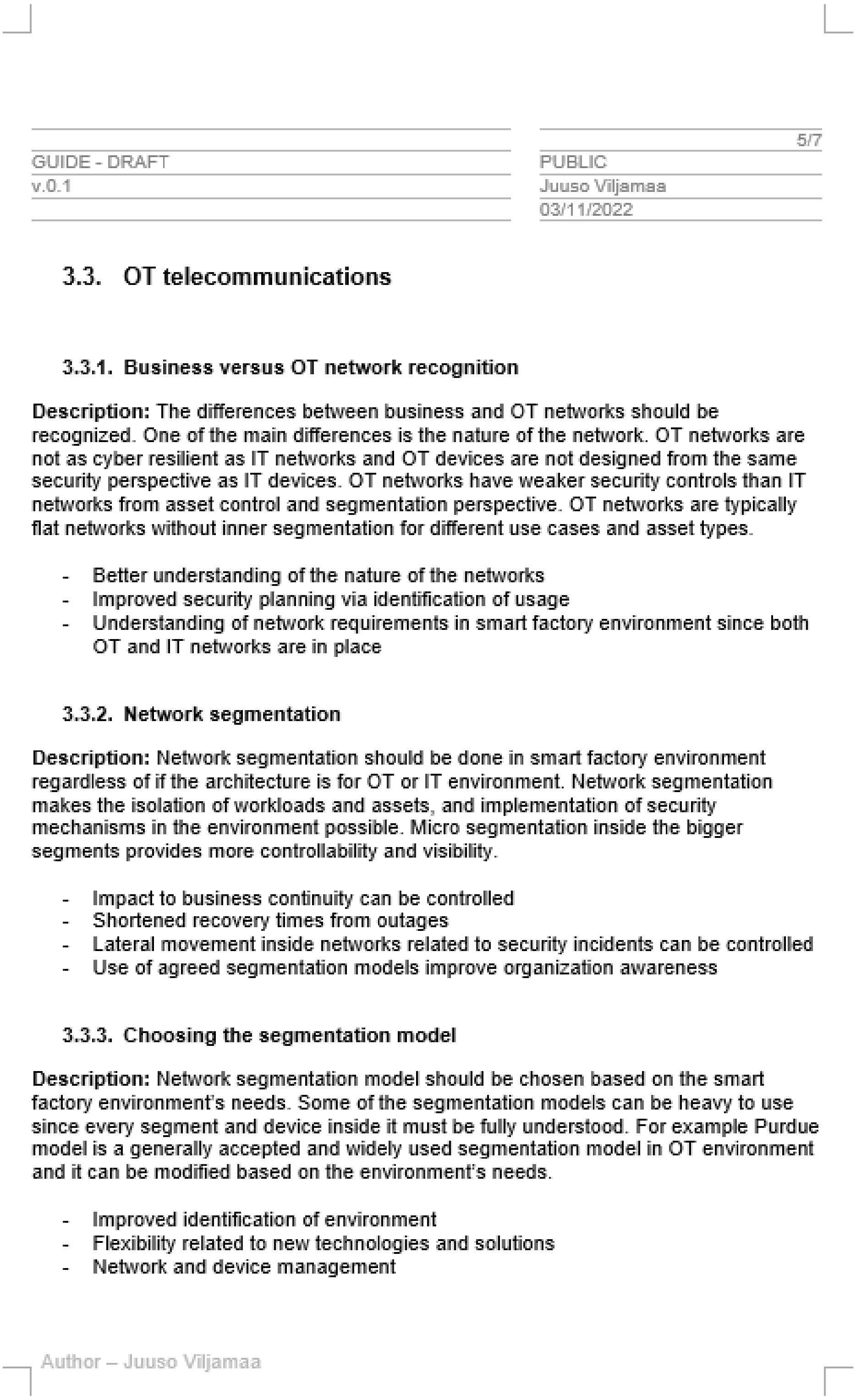
**Description:** OT environment should be implemented based on globally accepted security standards. The level of obeyance depends on the need and it is suggested to not blindly follow the standards. Suggested standard for this is for example ISO/IEC 62443 series.

- Improved consistency in OT environment
- Better understanding of implementations
- Ability to manage costs, rewards, and risks in a better way

### 3.2.5. Auditing of OT environment

**Description:** Auditing of OT environment should be implemented depending on the size of the environment. It is important to understand what should be audited and connection with CMDB is strong since it should maintain the information of assets.

- OT environment alignment with agreed standards and risk mitigation
- Discover unknown assets from the environment
- Mapping of changes in the environment
- Possibility to use automated monitoring as "auditing"



## 3.3. OT telecommunications

### 3.3.1. Business versus OT network recognition

**Description:** The differences between business and OT networks should be recognized. One of the main differences is the nature of the network. OT networks are not as cyber resilient as IT networks and OT devices are not designed from the same security perspective as IT devices. OT networks have weaker security controls than IT networks from asset control and segmentation perspective. OT networks are typically flat networks without inner segmentation for different use cases and asset types.

- Better understanding of the nature of the networks
- Improved security planning via identification of usage
- Understanding of network requirements in smart factory environment since both OT and IT networks are in place

### 3.3.2. Network segmentation

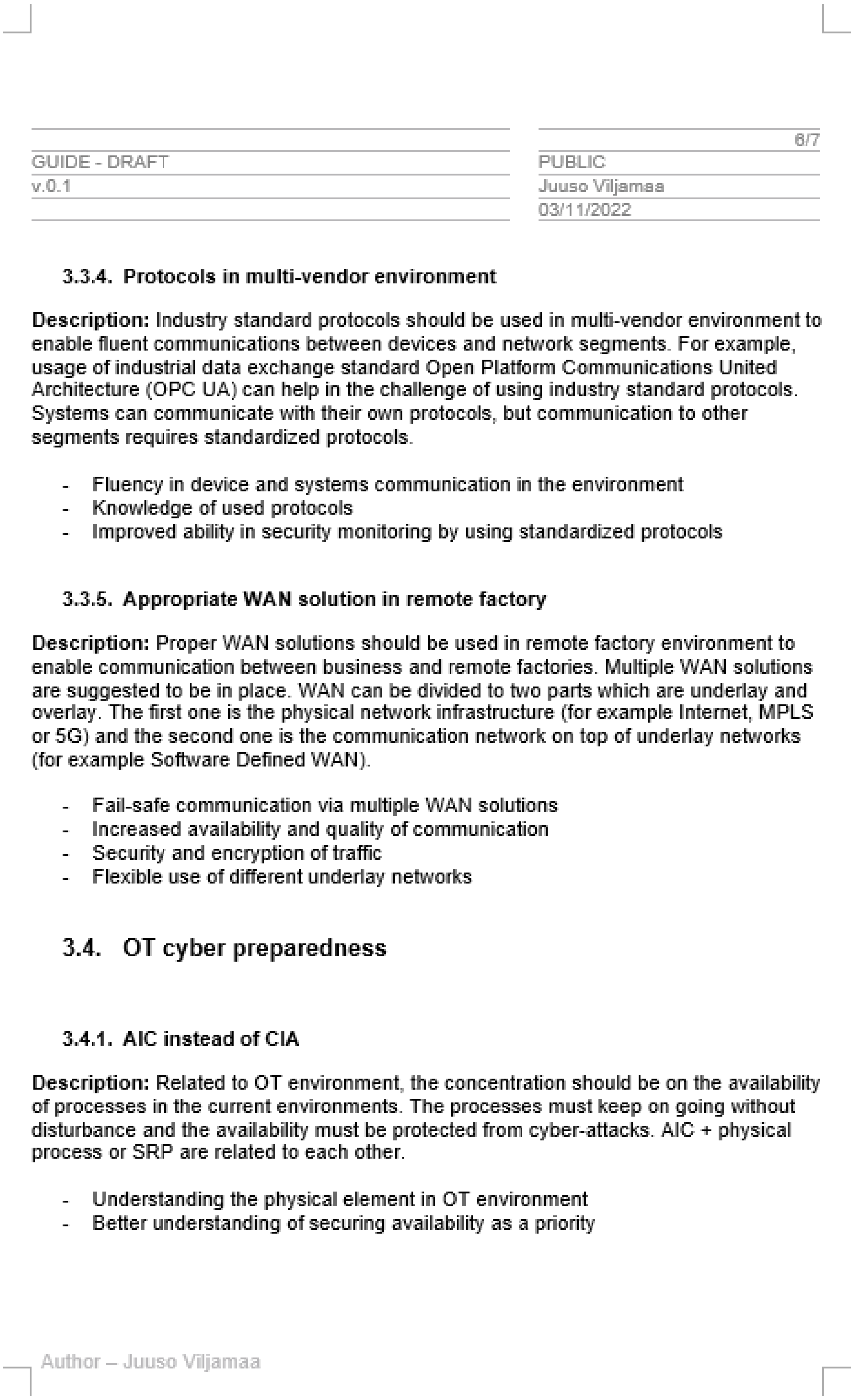
**Description:** Network segmentation should be done in smart factory environment regardless of if the architecture is for OT or IT environment. Network segmentation makes the isolation of workloads and assets, and implementation of security mechanisms in the environment possible. Micro segmentation inside the bigger segments provides more controllability and visibility.

- Impact to business continuity can be controlled
- Shortened recovery times from outages
- Lateral movement inside networks related to security incidents can be controlled
- Use of agreed segmentation models improve organization awareness

### 3.3.3. Choosing the segmentation model

**Description:** Network segmentation model should be chosen based on the smart factory environment's needs. Some of the segmentation models can be heavy to use since every segment and device inside it must be fully understood. For example Purdue model is a generally accepted and widely used segmentation model in OT environment and it can be modified based on the environment's needs.

- Improved identification of environment
- Flexibility related to new technologies and solutions
- Network and device management



### 3.3.4. Protocols in multi-vendor environment

**Description:** Industry standard protocols should be used in multi-vendor environment to enable fluent communications between devices and network segments. For example, usage of industrial data exchange standard Open Platform Communications United Architecture (OPC UA) can help in the challenge of using industry standard protocols. Systems can communicate with their own protocols, but communication to other segments requires standardized protocols.

- Fluency in device and systems communication in the environment
- Knowledge of used protocols
- Improved ability in security monitoring by using standardized protocols

### 3.3.5. Appropriate WAN solution in remote factory

**Description:** Proper WAN solutions should be used in remote factory environment to enable communication between business and remote factories. Multiple WAN solutions are suggested to be in place. WAN can be divided to two parts which are underlay and overlay. The first one is the physical network infrastructure (for example Internet, MPLS or 5G) and the second one is the communication network on top of underlay networks (for example Software Defined WAN).

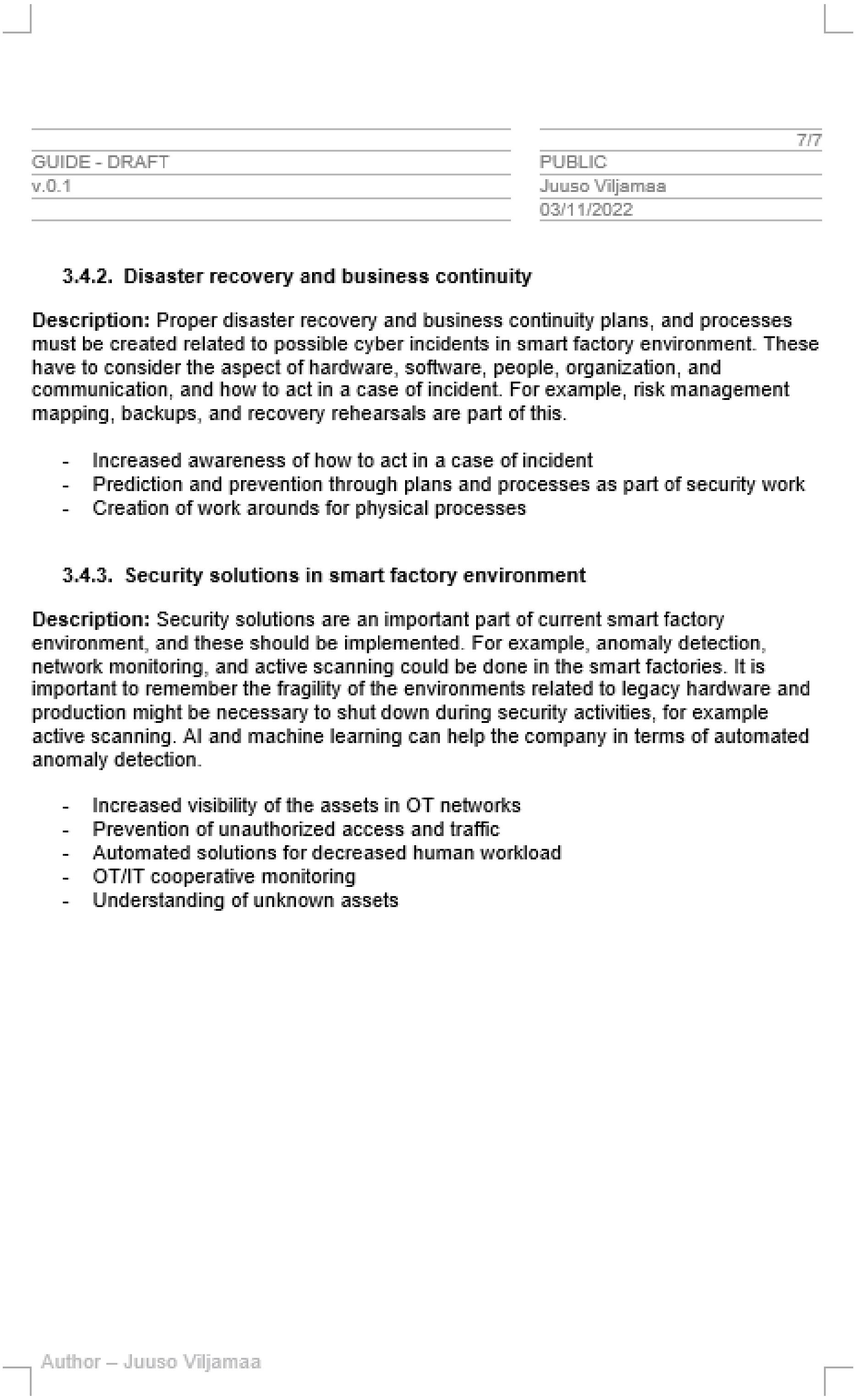
- Fail-safe communication via multiple WAN solutions
- Increased availability and quality of communication
- Security and encryption of traffic
- Flexible use of different underlay networks

## 3.4. OT cyber preparedness

### 3.4.1. AIC instead of CIA

**Description:** Related to OT environment, the concentration should be on the availability of processes in the current environments. The processes must keep on going without disturbance and the availability must be protected from cyber-attacks. AIC + physical process or SRP are related to each other.

- Understanding the physical element in OT environment
- Better understanding of securing availability as a priority



#### 3.4.2. Disaster recovery and business continuity

**Description:** Proper disaster recovery and business continuity plans, and processes must be created related to possible cyber incidents in smart factory environment. These have to consider the aspect of hardware, software, people, organization, and communication, and how to act in a case of incident. For example, risk management mapping, backups, and recovery rehearsals are part of this.

- Increased awareness of how to act in a case of incident
- Prediction and prevention through plans and processes as part of security work
- Creation of work arounds for physical processes

#### 3.4.3. Security solutions in smart factory environment

**Description:** Security solutions are an important part of current smart factory environment, and these should be implemented. For example, anomaly detection, network monitoring, and active scanning could be done in the smart factories. It is important to remember the fragility of the environments related to legacy hardware and production might be necessary to shut down during security activities, for example active scanning. AI and machine learning can help the company in terms of automated anomaly detection.

- Increased visibility of the assets in OT networks
- Prevention of unauthorized access and traffic
- Automated solutions for decreased human workload
- OT/IT cooperative monitoring
- Understanding of unknown assets

# ATTACHMENT 3 STRUCTURE OF THE INTERVIEW (ROUND 2-1)

## Interview – Round 2-1 (Smart Factory Specialist)

### Background

Q1: What is your role in this company?

A:

Q2: How have you been involved with the OT?

A:

### Priority and complexity review of the topics of the guide

**Priority** = What is the priority for the implementation to be carried out?
**Complexity** = How complex is the implementation to be carried out?

Priority scale (1-5) 1 = least priority, 3 = normal priority, 5 = critical priority

Complexity scale (1-5) 1 = easily implemented, 3 = normal implementation, 5 = hard to implement

**OT hardware and systems management**

Ownership of assets

Priority:

Why?

Complexity:

Why?

CMDB for asset information (asset register)

Priority:

Why?

Complexity:

Why?

Lifecycle management

Priority:

Why?

Complexity:

Why?

Patch and update management

Priority:

Why?

Complexity:

Why?

**OT security in organization**

OT security as a term

Priority:

Why?

Complexity:

Why?

OT security awareness

Priority:

Why?

Complexity:

Why?

Roles and responsibilities in OT security

Priority:

Why?

Complexity:

Why?

Usage of OT security standards

Priority:

Why?

Complexity:

Why?

Auditing of OT environment

Priority:

Why?

Complexity:

Why?

**OT telecommunications**

Business versus OT network recognition

Priority:

Why?

Complexity:

Why?

Network segmentation

Priority:

Why?

Complexity:

Why?

Choosing the segmentation model

Priority:

Why?

Complexity:

Why?

Protocols in multi-vendor environment

Priority:

Why?

Complexity:

Why?

Appropriate WAN solution in remote factory

Priority:

Why?

Complexity:

Why?

**OT cyber preparedness**

AIC instead of CIA

Priority:

Why?

Complexity:

Why?

Disaster recovery and business continuity

Priority:

Why?

Complexity:

Why?

Security solutions in smart factory environment

Priority:

Why?

Complexity:

Why?

# ATTACHMENT 4 STRUCTURE OF THE INTERVIEW (ROUND 2-2)

## Interview – Round 2-2 (Directors/Managers)

### Background

Q1: What is your role in this company?

A:

Q2: How have you been involved with the OT?

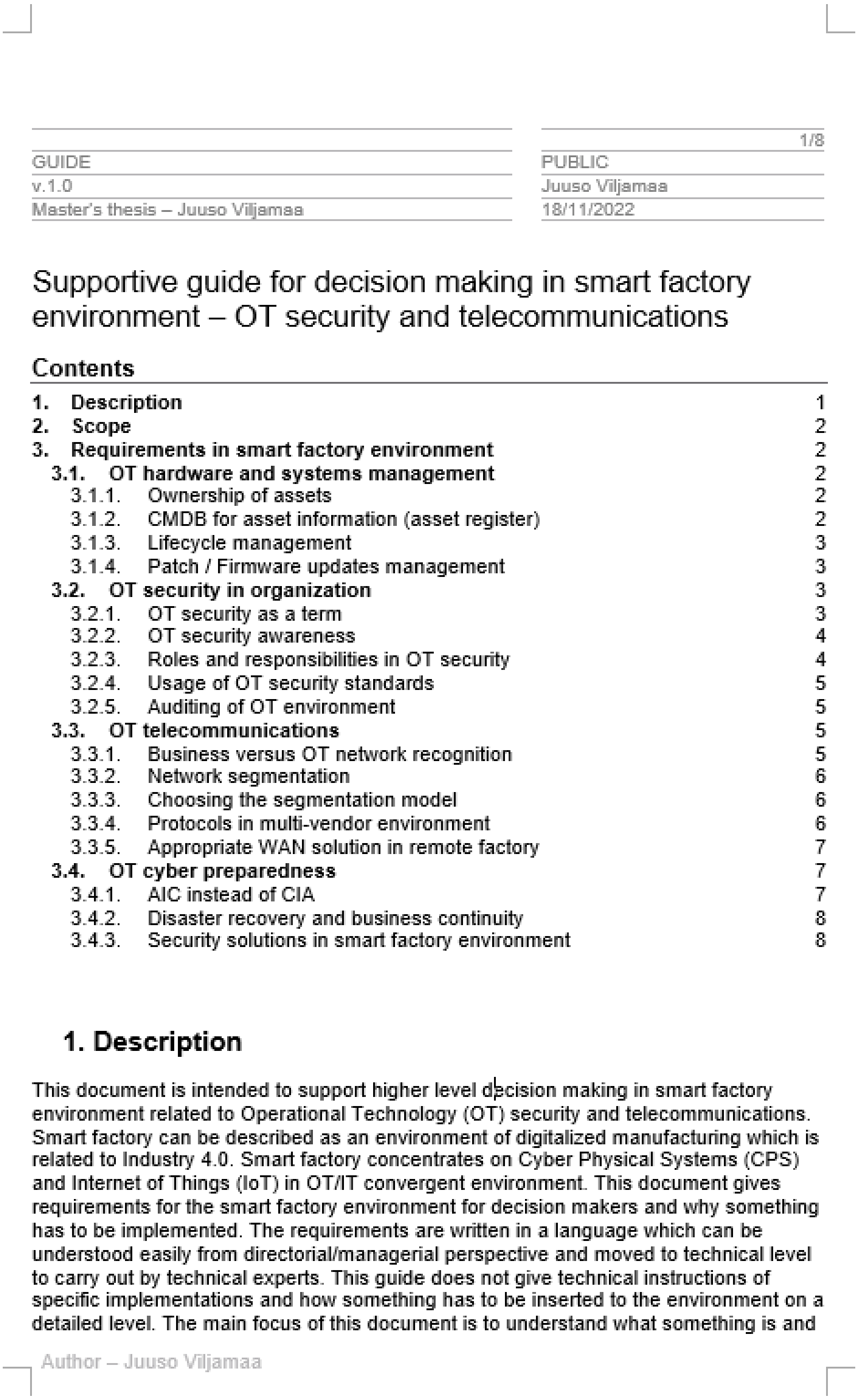
A:

### Evaluation and feedback of the draft guide

Q3: What is your opinion of this guide and its contents, and can it support smart factory environment related decision making?

A:

# ATTACHMENT 5 FINAL VERSION OF THE GUIDE



| | |
|---|---|
| | 1/8 |
| GUIDE | PUBLIC |
| v.1.0 | Juuso Viljamaa |
| Master's thesis – Juuso Viljamaa | 18/11/2022 |

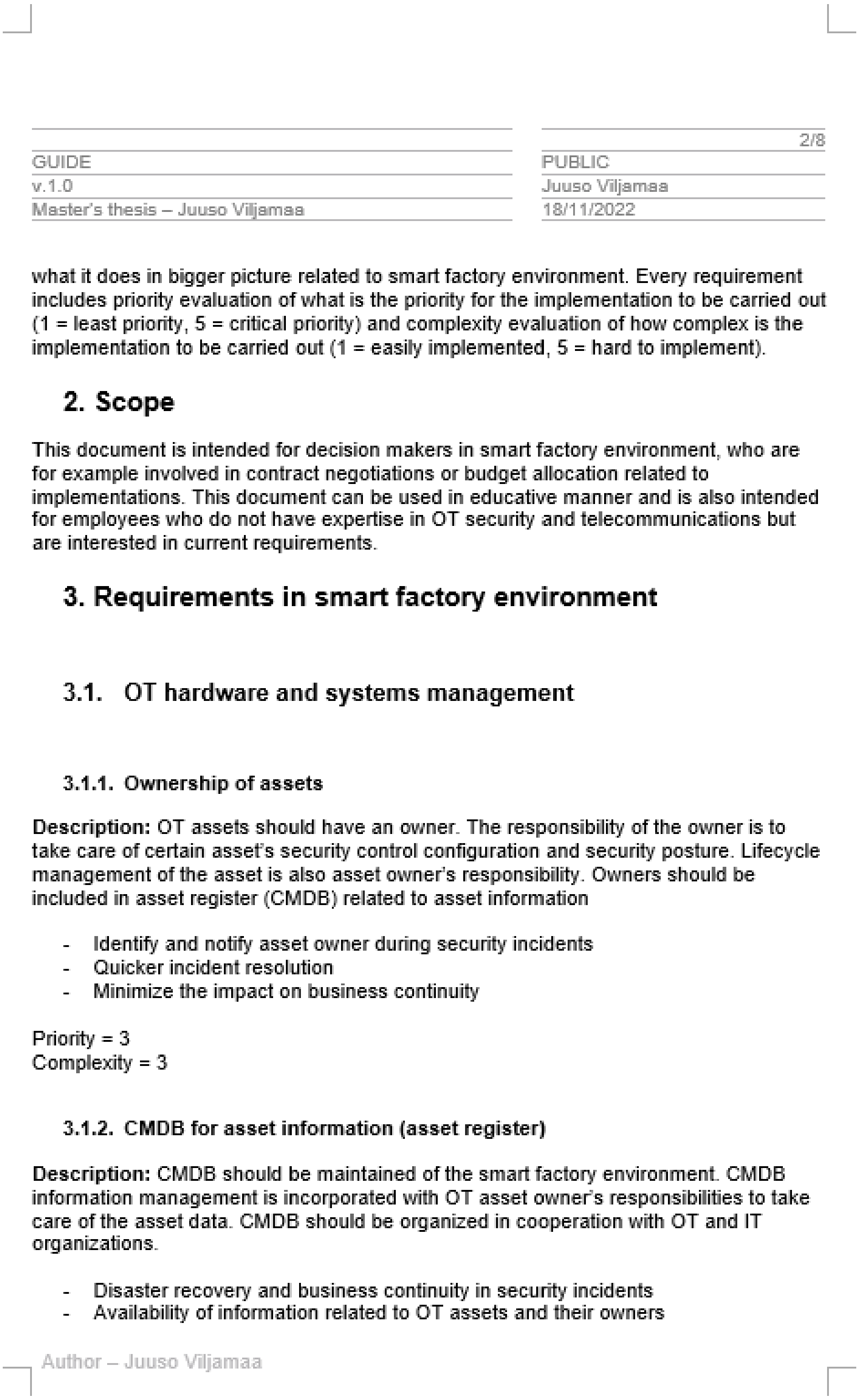
## Supportive guide for decision making in smart factory environment – OT security and telecommunications

### Contents

1. **Description** 1
2. **Scope** 2
3. **Requirements in smart factory environment** 2
   - **3.1. OT hardware and systems management** 2
     - 3.1.1. Ownership of assets 2
     - 3.1.2. CMDB for asset information (asset register) 2
     - 3.1.3. Lifecycle management 3
     - 3.1.4. Patch / Firmware updates management 3
   - **3.2. OT security in organization** 3
     - 3.2.1. OT security as a term 3
     - 3.2.2. OT security awareness 4
     - 3.2.3. Roles and responsibilities in OT security 4
     - 3.2.4. Usage of OT security standards 5
     - 3.2.5. Auditing of OT environment 5
   - **3.3. OT telecommunications** 5
     - 3.3.1. Business versus OT network recognition 5
     - 3.3.2. Network segmentation 6
     - 3.3.3. Choosing the segmentation model 6
     - 3.3.4. Protocols in multi-vendor environment 6
     - 3.3.5. Appropriate WAN solution in remote factory 7
   - **3.4. OT cyber preparedness** 7
     - 3.4.1. AIC instead of CIA 7
     - 3.4.2. Disaster recovery and business continuity 8
     - 3.4.3. Security solutions in smart factory environment 8

### 1. Description

This document is intended to support higher level decision making in smart factory environment related to Operational Technology (OT) security and telecommunications. Smart factory can be described as an environment of digitalized manufacturing which is related to Industry 4.0. Smart factory concentrates on Cyber Physical Systems (CPS) and Internet of Things (IoT) in OT/IT convergent environment. This document gives requirements for the smart factory environment for decision makers and why something has to be implemented. The requirements are written in a language which can be understood easily from directorial/managerial perspective and moved to technical level to carry out by technical experts. This guide does not give technical instructions of specific implementations and how something has to be inserted to the environment on a detailed level. The main focus of this document is to understand what something is and



what it does in bigger picture related to smart factory environment. Every requirement includes priority evaluation of what is the priority for the implementation to be carried out (1 = least priority, 5 = critical priority) and complexity evaluation of how complex is the implementation to be carried out (1 = easily implemented, 5 = hard to implement).

## 2. Scope

This document is intended for decision makers in smart factory environment, who are for example involved in contract negotiations or budget allocation related to implementations. This document can be used in educative manner and is also intended for employees who do not have expertise in OT security and telecommunications but are interested in current requirements.

## 3. Requirements in smart factory environment

### 3.1. OT hardware and systems management

#### 3.1.1. Ownership of assets

**Description:** OT assets should have an owner. The responsibility of the owner is to take care of certain asset's security control configuration and security posture. Lifecycle management of the asset is also asset owner's responsibility. Owners should be included in asset register (CMDB) related to asset information

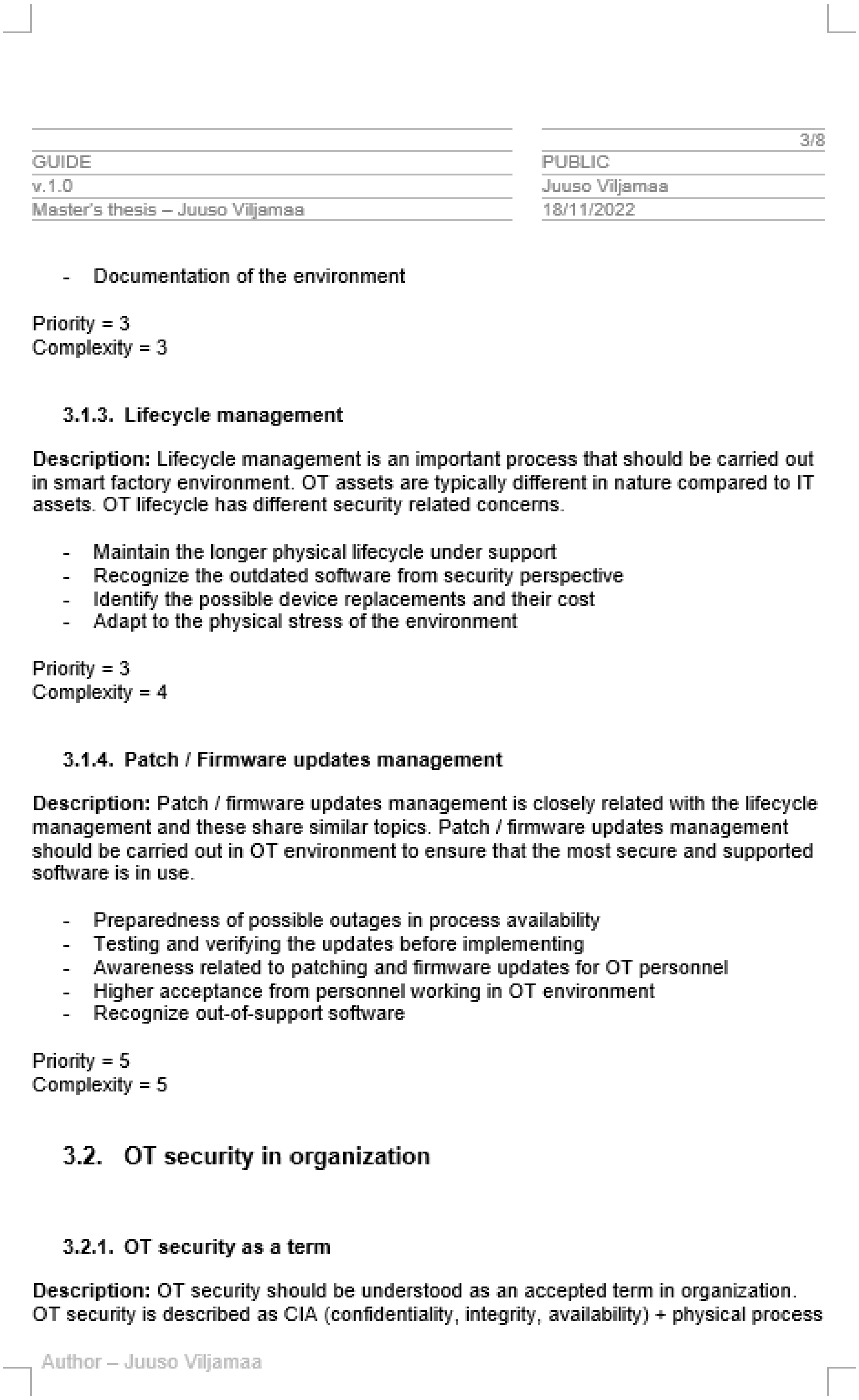
- Identify and notify asset owner during security incidents
- Quicker incident resolution
- Minimize the impact on business continuity

Priority = 3
Complexity = 3

#### 3.1.2. CMDB for asset information (asset register)

**Description:** CMDB should be maintained of the smart factory environment. CMDB information management is incorporated with OT asset owner's responsibilities to take care of the asset data. CMDB should be organized in cooperation with OT and IT organizations.

- Disaster recovery and business continuity in security incidents
- Availability of information related to OT assets and their owners



- Documentation of the environment

Priority = 3
Complexity = 3

#### 3.1.3. Lifecycle management

**Description:** Lifecycle management is an important process that should be carried out in smart factory environment. OT assets are typically different in nature compared to IT assets. OT lifecycle has different security related concerns.

- Maintain the longer physical lifecycle under support
- Recognize the outdated software from security perspective
- Identify the possible device replacements and their cost
- Adapt to the physical stress of the environment

Priority = 3
Complexity = 4

#### 3.1.4. Patch / Firmware updates management

**Description:** Patch / firmware updates management is closely related with the lifecycle management and these share similar topics. Patch / firmware updates management should be carried out in OT environment to ensure that the most secure and supported software is in use.

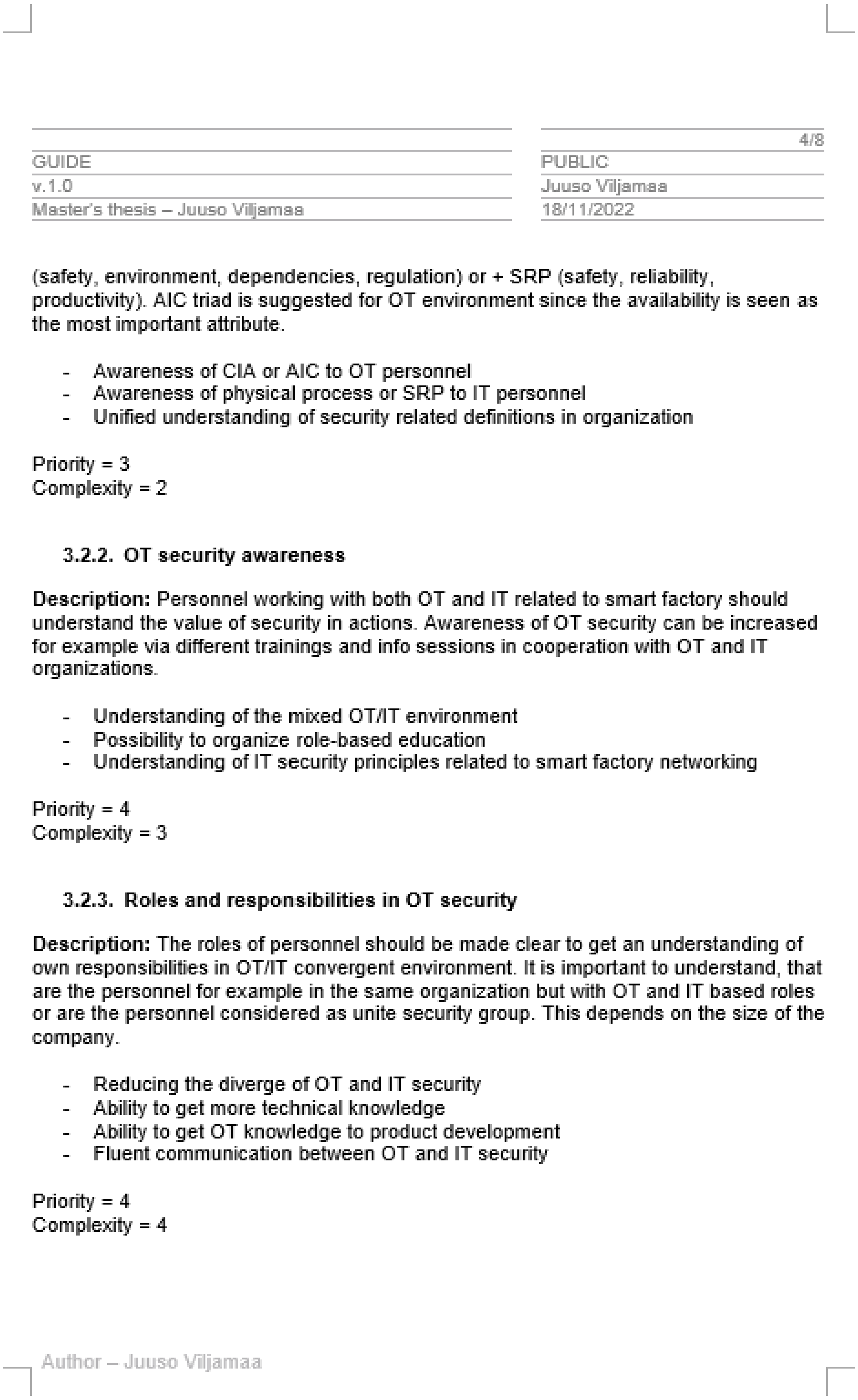
- Preparedness of possible outages in process availability
- Testing and verifying the updates before implementing
- Awareness related to patching and firmware updates for OT personnel
- Higher acceptance from personnel working in OT environment
- Recognize out-of-support software

Priority = 5
Complexity = 5

### 3.2. OT security in organization

#### 3.2.1. OT security as a term

**Description:** OT security should be understood as an accepted term in organization. OT security is described as CIA (confidentiality, integrity, availability) + physical process



(safety, environment, dependencies, regulation) or + SRP (safety, reliability, productivity). AIC triad is suggested for OT environment since the availability is seen as the most important attribute.

- Awareness of CIA or AIC to OT personnel
- Awareness of physical process or SRP to IT personnel
- Unified understanding of security related definitions in organization

Priority = 3
Complexity = 2

### 3.2.2. OT security awareness

**Description:** Personnel working with both OT and IT related to smart factory should understand the value of security in actions. Awareness of OT security can be increased for example via different trainings and info sessions in cooperation with OT and IT organizations.

- Understanding of the mixed OT/IT environment
- Possibility to organize role-based education
- Understanding of IT security principles related to smart factory networking

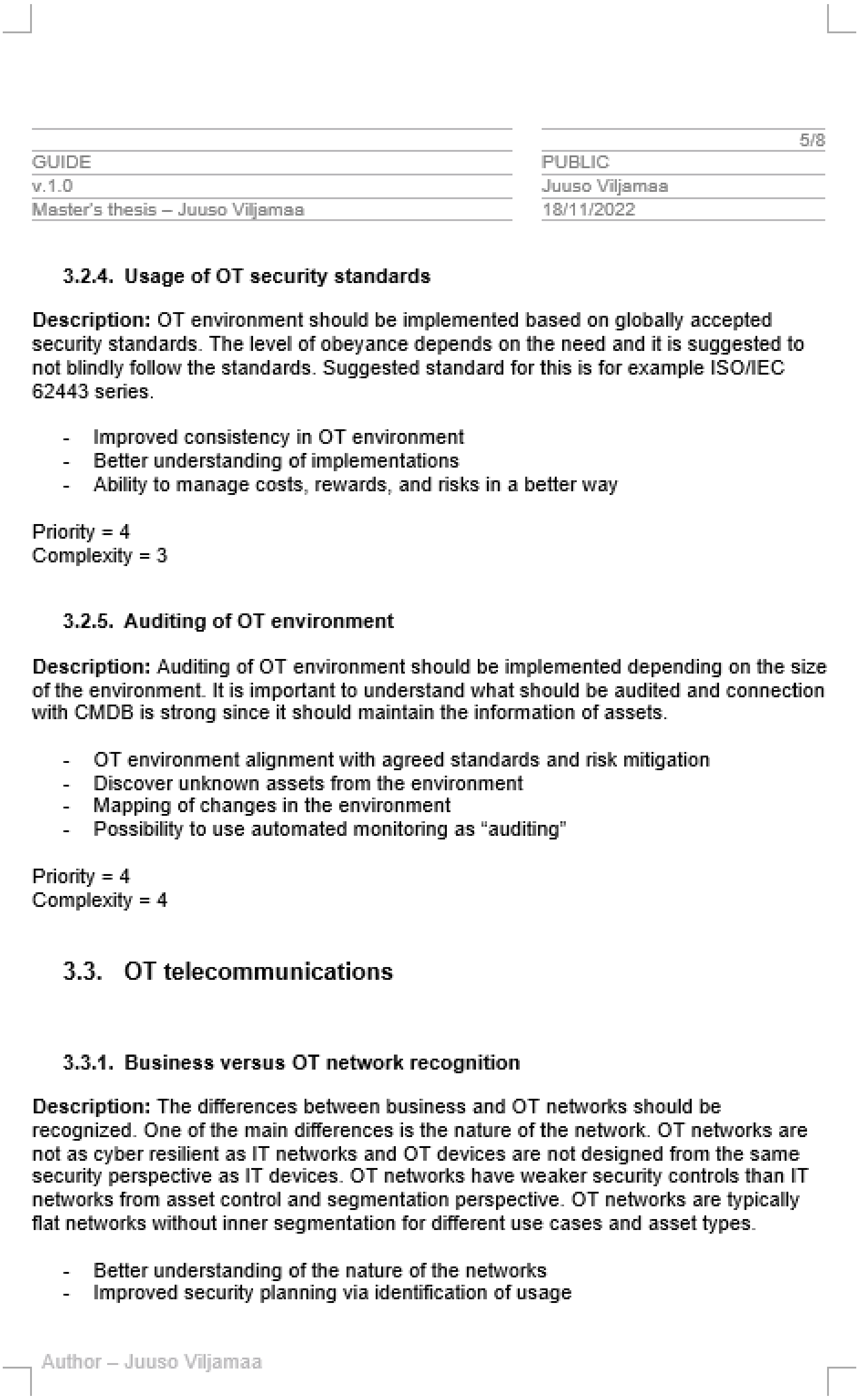
Priority = 4
Complexity = 3

### 3.2.3. Roles and responsibilities in OT security

**Description:** The roles of personnel should be made clear to get an understanding of own responsibilities in OT/IT convergent environment. It is important to understand, that are the personnel for example in the same organization but with OT and IT based roles or are the personnel considered as unite security group. This depends on the size of the company.

- Reducing the diverge of OT and IT security
- Ability to get more technical knowledge
- Ability to get OT knowledge to product development
- Fluent communication between OT and IT security

Priority = 4
Complexity = 4



### 3.2.4. Usage of OT security standards

**Description:** OT environment should be implemented based on globally accepted security standards. The level of obeyance depends on the need and it is suggested to not blindly follow the standards. Suggested standard for this is for example ISO/IEC 62443 series.

- Improved consistency in OT environment
- Better understanding of implementations
- Ability to manage costs, rewards, and risks in a better way

Priority = 4
Complexity = 3

### 3.2.5. Auditing of OT environment

**Description:** Auditing of OT environment should be implemented depending on the size of the environment. It is important to understand what should be audited and connection with CMDB is strong since it should maintain the information of assets.

- OT environment alignment with agreed standards and risk mitigation
- Discover unknown assets from the environment
- Mapping of changes in the environment
- Possibility to use automated monitoring as “auditing”

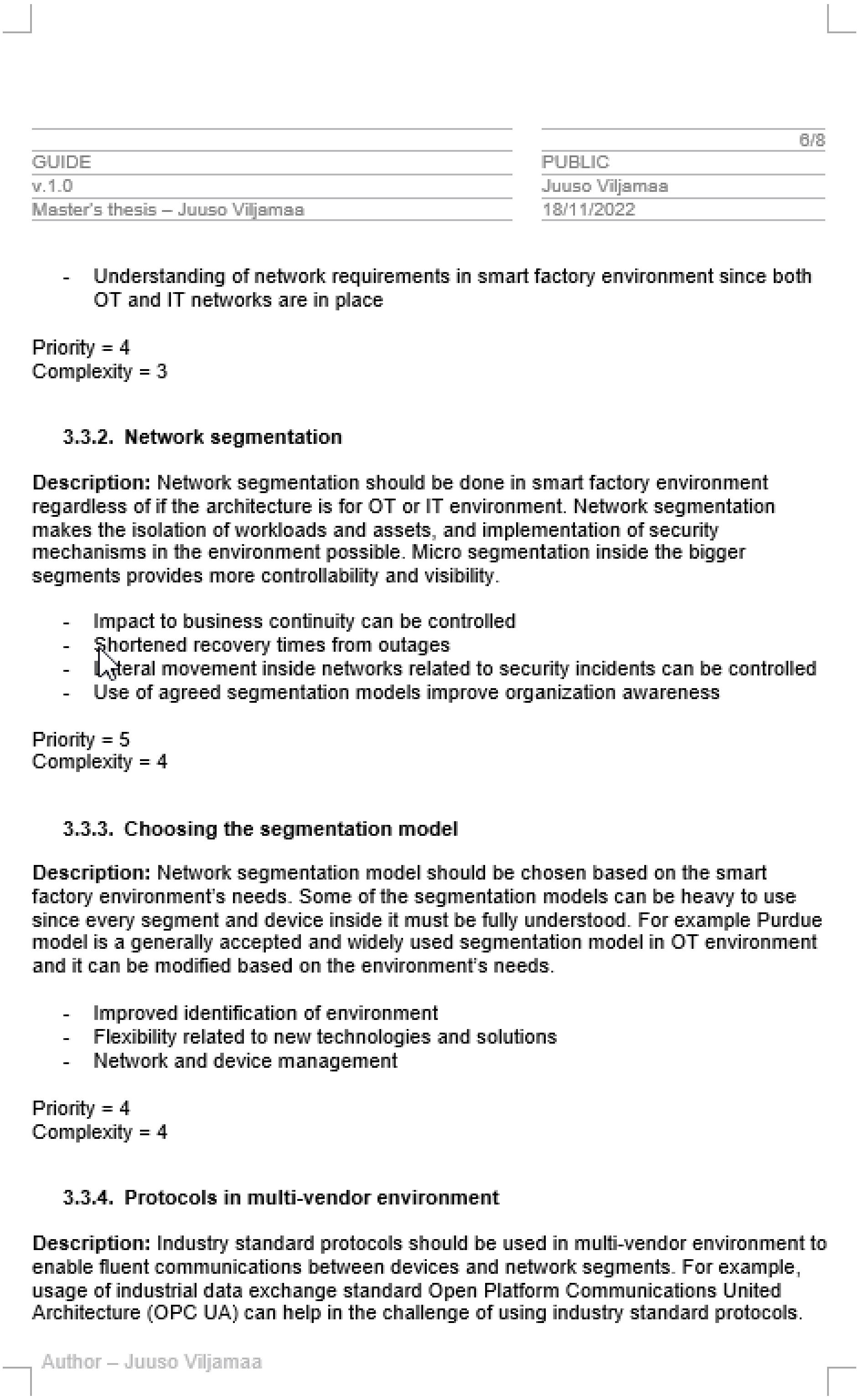
Priority = 4
Complexity = 4

## 3.3. OT telecommunications

### 3.3.1. Business versus OT network recognition

**Description:** The differences between business and OT networks should be recognized. One of the main differences is the nature of the network. OT networks are not as cyber resilient as IT networks and OT devices are not designed from the same security perspective as IT devices. OT networks have weaker security controls than IT networks from asset control and segmentation perspective. OT networks are typically flat networks without inner segmentation for different use cases and asset types.

- Better understanding of the nature of the networks
- Improved security planning via identification of usage



- Understanding of network requirements in smart factory environment since both OT and IT networks are in place

Priority = 4
Complexity = 3

### 3.3.2. Network segmentation

**Description:** Network segmentation should be done in smart factory environment regardless of if the architecture is for OT or IT environment. Network segmentation makes the isolation of workloads and assets, and implementation of security mechanisms in the environment possible. Micro segmentation inside the bigger segments provides more controllability and visibility.

- Impact to business continuity can be controlled
- Shortened recovery times from outages
- Lateral movement inside networks related to security incidents can be controlled
- Use of agreed segmentation models improve organization awareness

Priority = 5
Complexity = 4

### 3.3.3. Choosing the segmentation model

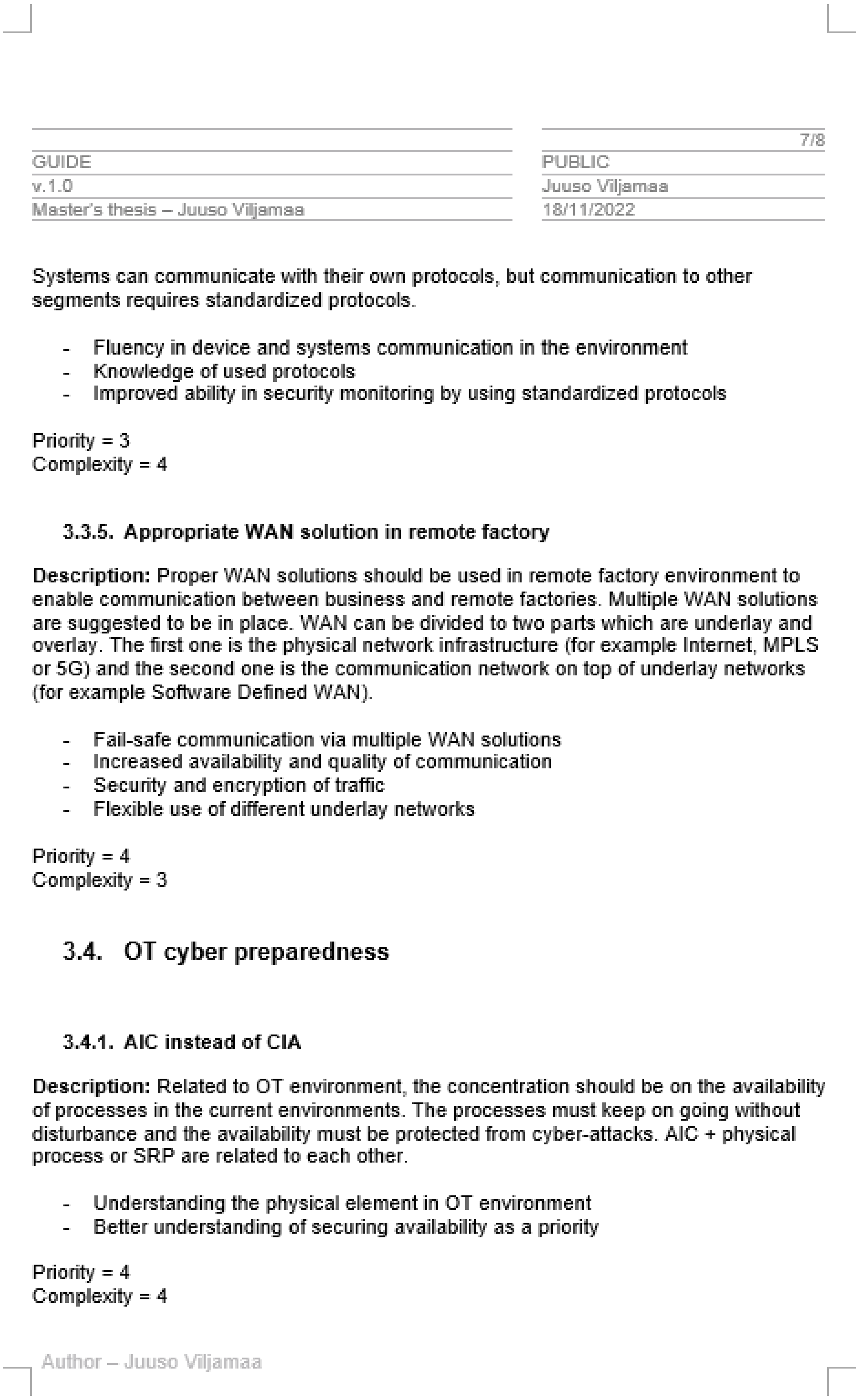
**Description:** Network segmentation model should be chosen based on the smart factory environment's needs. Some of the segmentation models can be heavy to use since every segment and device inside it must be fully understood. For example Purdue model is a generally accepted and widely used segmentation model in OT environment and it can be modified based on the environment's needs.

- Improved identification of environment
- Flexibility related to new technologies and solutions
- Network and device management

Priority = 4
Complexity = 4

### 3.3.4. Protocols in multi-vendor environment

**Description:** Industry standard protocols should be used in multi-vendor environment to enable fluent communications between devices and network segments. For example, usage of industrial data exchange standard Open Platform Communications United Architecture (OPC UA) can help in the challenge of using industry standard protocols.



Systems can communicate with their own protocols, but communication to other segments requires standardized protocols.

- Fluency in device and systems communication in the environment
- Knowledge of used protocols
- Improved ability in security monitoring by using standardized protocols

Priority = 3
Complexity = 4

#### 3.3.5. Appropriate WAN solution in remote factory

**Description:** Proper WAN solutions should be used in remote factory environment to enable communication between business and remote factories. Multiple WAN solutions are suggested to be in place. WAN can be divided to two parts which are underlay and overlay. The first one is the physical network infrastructure (for example Internet, MPLS or 5G) and the second one is the communication network on top of underlay networks (for example Software Defined WAN).

- Fail-safe communication via multiple WAN solutions
- Increased availability and quality of communication
- Security and encryption of traffic
- Flexible use of different underlay networks

Priority = 4
Complexity = 3

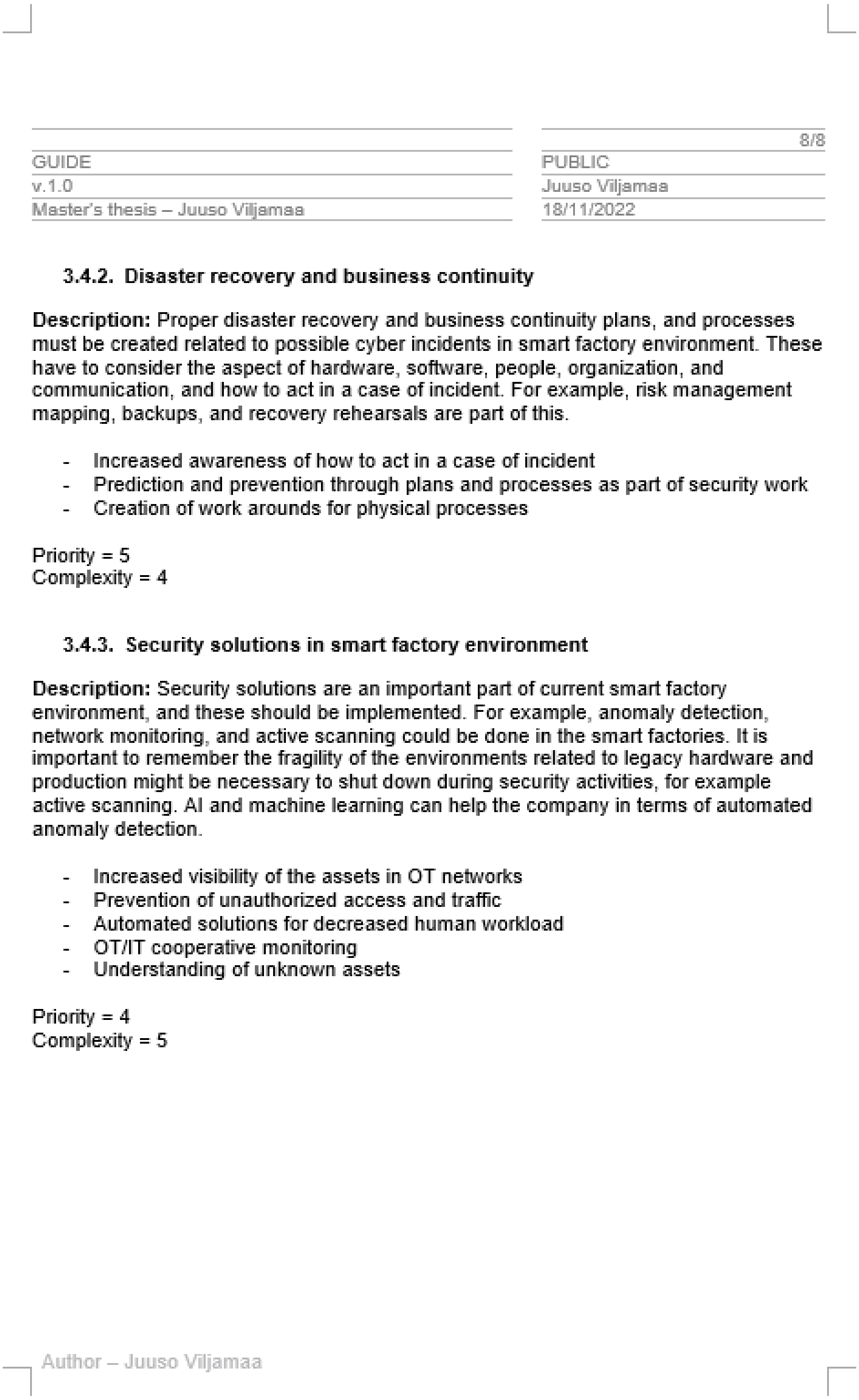
### 3.4. OT cyber preparedness

#### 3.4.1. AIC instead of CIA

**Description:** Related to OT environment, the concentration should be on the availability of processes in the current environments. The processes must keep on going without disturbance and the availability must be protected from cyber-attacks. AIC + physical process or SRP are related to each other.

- Understanding the physical element in OT environment
- Better understanding of securing availability as a priority

Priority = 4
Complexity = 4



### 3.4.2. Disaster recovery and business continuity

**Description:** Proper disaster recovery and business continuity plans, and processes must be created related to possible cyber incidents in smart factory environment. These have to consider the aspect of hardware, software, people, organization, and communication, and how to act in a case of incident. For example, risk management mapping, backups, and recovery rehearsals are part of this.

- Increased awareness of how to act in a case of incident
- Prediction and prevention through plans and processes as part of security work
- Creation of work arounds for physical processes

Priority = 5
Complexity = 4

### 3.4.3. Security solutions in smart factory environment

**Description:** Security solutions are an important part of current smart factory environment, and these should be implemented. For example, anomaly detection, network monitoring, and active scanning could be done in the smart factories. It is important to remember the fragility of the environments related to legacy hardware and production might be necessary to shut down during security activities, for example active scanning. AI and machine learning can help the company in terms of automated anomaly detection.

- Increased visibility of the assets in OT networks
- Prevention of unauthorized access and traffic
- Automated solutions for decreased human workload
- OT/IT cooperative monitoring
- Understanding of unknown assets

Priority = 4
Complexity = 5