The complexity of security patching processes within the OT landscape at a logistic service provider in the liquid bulk industry

A socio-technical case study to extract lessons learned from current practices, governance and complexity factors within security patching processes within an industrial, operational environment

by

Rozemarijn Schraven

15 November 2024

To be defended on Friday November 22nd 2024 in obtaining the degree of Master of Science in

Complex Systems Engineering and Management

First supervisor TU Delft:	Dr. S.E. Parkin
Second supervisor TU Delft:	Dr. J.A. Annema
External supervisor:	Dhr. F. Jiskoot
Chair:	Dr. J.A. Annema
Thesis duration:	March, 2024 – November, 2024
Faculty:	Faculty of Technology, Policy and Management, Delft
Student number:	5182425
Publication can be found on:	https://repository.tudelft.nl/
Keywords:	Security patching, patch management, socio-technical aspects, case study, lessons learned, operational technologys

Delft
University of
Technology

Preface

This thesis was written to explore the security patching processes within an industrial operational environment, where a socio-technical case study was performed at a logistic service provider in the liquid bulk industry. Both practical and academic insights were combined when writing this thesis. This research is performed to contribute to closing the knowledge gap regarding missing information about current practices of security patching in OT, combined with a lack of insights into governance and contributing factors related to human interactions and the complexity of security patching processes within an industrial, operational environment.

Curiosity was created to investigate social aspects within a technical system, such as security patching in an industrial, operational environment, during the Economics of Cybersecurity course, lectured by my first supervisor, Dr. Simon Parkin. I want to thank Simon for all the brainstorming sessions and regular meetings to discuss the (many) exciting points gathered during the research and for guiding me to generate this final thesis. I would also like to thank my external supervisor, dhr. Frank Jiskoot for the dedication given to supervise me at the case-selected organisation despite your hectic schedule. Thirdly, I want to thank Dr. Jan Anne Annema, Chair of this thesis, and all the participating experts in the internal and external interviews. I would not have achieved this final thesis without your participation in this research. Lastly, I want to thank my family and close friends for the support given during these very busy months and challenging moments. Whereby I want to thank Menno van der Vaart, in particular, for dealing with all my mood swings and supporting me these past months.

Finally, I would like to wish you, as the reader, much success and enjoyment in reading this thesis.

Rozemarijn Schraven

Delft, November 2024

Abstract

Software security patch management refers to *"the process of applying patches to the security vulnerabilities present in the software products and systems deployed in an organisation's cyber environment"* (Dissanayake et al., 2022a). This involves identifying, acquiring, testing, installing and verifying patches for vulnerabilities, requiring intricate coordination among stakeholders (Dissanayake et al., 2022a). Automox and AimPoint Group uncovered that less than 50 percent of organisations can patch vulnerable systems quickly enough to protect against critical threats and zero-day attacks (Automox, 2020a). Fortinet (2024) describes that attacks on OT systems components are increased, with more than 90 percent of organisations that operate within the industry, including one or more damaging security events in two years (Kovacs, 2019). Within the transportation sector, cybersecurity breaches could pose significant safety risks, emphasising the need for efficient collaboration in patch management.

From the literature review, it can be concluded that very little literature can be found regarding the interactions employees have to carry out (human interactions) to address vulnerabilities within cybersecurity (security patching). Socio-technical challenges have been identified; however, there is a lack of information about the roles and effects of these challenges, as well as known vulnerabilities and their intake. Furthermore, most cited references neglect human interactions associated with security patching or patch management in their research. It can be seen that these found gaps within the academic research world are dedicated to security patching in IT, without further research towards security patching within an OT environment. Information about current practices of security patching in OT is lacking, combined with a lack of insights into governance and contributing factors related to human interactions and the complexity of security patching processes, resulting in the main research question: *What lessons can be learned from the current practices, governance and complexity factors within security patching processes in an industrial, operational environment?* An embedded single case study is performed at a logistic service provider in the liquid bulk industry to answer this main research question. An exploratory research design is used to shape this case study, where the socio-technical system theory of Mumford (2000) is used as a basis for the analytical framework. Based on this framework, three sub-research questions (SRQ) were derived:

- *SRQ1: What is the current state of the security patching processes at the selected case study organisation?*
- *SRQ2: How are the security patching processes governed within the operational domain?*
- *SRQ3: Which factors give insight into the complexity of the security patching processes in an industrial, operational environment?*

Three types of research methods were used to gain the data for each sub-research question: direct observations (SRQ1), internal document analysis (SRQ2) and semi-structured interviews (SRQ2 and SRQ3). Direct observations were executed during multiple rounds of performed security patching by one of the selected case study organisation's most important OT suppliers and during an internal cybersecurity audit at one of the selected locations. Four internal documents regarding OT security were analysed. Three semi-structured interviews were organised with the selected case study organisation's experts within the OT domain, and twelve semi-structured interviews were organised (out of thirty-one) OT suppliers of the selected case study organisation. The data was analysed via a SWOT analysis for SRQ1, whereas for SRQ2 and SRQ3, reflexive thematic analysis was performed to retrieve final themes as results, where Atlas.ti was used as a qualitative research tool. In answering the main research question of this research, lessons learned can be drawn from the current state of the selected case study organisation's security patching processes based on the identified strengths, weaknesses, opportunities, and threats for sub-research question one. Lessons learned based on the

identified strengths can be seen to incorporate OT security assessments to define the criticality of OT systems, that OT systems are (mostly) standalone systems without a connection towards the internet, preventing the risk of unwanted malware, and perform Last Minute Risk Assessment, before issuing work permits to OT suppliers who perform security patching at the locations. Lessons learned based on the identified weaknesses include incorporating earlier gained knowledge of cyber incidents towards an organisation's business contingency plan, generating overviews of update statuses of OT systems at locations or when this is not possible, controlling the responsible OT supplier on this, implementing preferred OT suppliers and define solutions for equal OT systems at locations within an organisation's Business Units, resulting in fewer differences of OT suppliers and therefore fewer frequency cycles of performed security patching. Lastly, if security patches are installed more frequently on OT systems, this may result in fewer technical malfunctions, which can cause *location downtime*, where a lot of production time might be lost to find the cause. Lessons learned based on opportunities can be seen in incorporating more recommendations via audits into the current states of security patching processes, avoiding OT suppliers bringing USB sticks to locations for transferring data and software towards OT systems, letting them use safe data transfer systems, deploy earlier gained knowledge for more mature stakeholders within the industry, and develop strategies to make current security patches more efficient when operations are paused (planned *location downtime*). Threats resulted in lessons learned to create safer strategies for password management and rotation of the OT systems at locations, arranging security patching timely to avoid unplanned *location downtime*, and investing in knowledge levels of location employees regarding security patching, risk management and problem-solving within this environment to avoid supplier dependency.

More lessons can be learned in addressing an organisation's governance, revealing poor centralised control over OT suppliers, incorporating standards into policies without expertise surrounding these certifications and weak interdepartmental coordination. Governance is also lacking in implemented performance metrics (e.g. missing KPIs), limiting the efficiency of the OT security policy in practice.

The last type of lessons learned are dedicated to five key factors regarding supplier dependency, ignorance of the OT environment, missed certification in the OT landscape, human knowledge remaining necessary, and complexity within the OT domain causing delays in security patching. With underlying contributing factors of this resistance towards security patching by OT suppliers, misalignment of terminology of security patching, inconsistent patch log processes with many organisational differences between OT suppliers, and lost information due to email traffic surrounding no central point for the documentation of reported problems.

Within the discussion section, a diversion can be seen into the reflection on OT-specific considerations (as industry perspective) as first, where little information is available about security patching in OT, the enormous impact of patching behaviour by OT experts, and missed governmental guidance within the industrial, operational environment. Secondly, the reflection on the selected case study organisation's perspective regarding the lack of incorporated KPIs in the SLA addendum and closing with limitations of the research. The knowledge gap of lacking information regarding security patching processes, combined with socio-technical aspects in an industrial operational environment, has been made smaller via this research. It can be concluded that practical insights of lessons learned are identified regarding the knowledge gap, including reasons for delays in implementing security patches and contributing factors of resistance towards security patching within this complex, industrial, operational environment of the specific case study organisation. However, the identified knowledge gap is not yet closed. Therefore, two types of recommendations are given for the industry. Further research is needed regarding security patching in an industrial, operational environment, and four practical recommendations are provided for the selected case study organisation.

Index

Preface 2

Abstract 3

Concept list 8

Abbreviations list 9

Chapter 1: Problem introduction 10

1.1 Background information 10

1.2 Introduction Cyber Security Act 10

1.3 Difference between IT and OT 11

1.4 Relation with Complex Systems Engineering and Management program 11

1.5 Thesis structure 12

Chapter 2: Academic knowledge gap and research question 13

2.1 Search and selection process 13

2.2 Literature review 14

2.2.1 Socio-technical challenges in patch management 14

2.2.2 Time effect of patching and publishing 14

2.2.3 Patching strategy 15

2.2.4 Prioritizing patching processes 15

2.3 Knowledge gap and main research question 15

Chapter 3: Research design and sub-research questions 16

3.1 Research design: Embedded single case study 16

3.2 Socio-technical system theory as the analytical framework 17

3.3 Sub-research questions 18

Chapter 4: Research methods and research flow diagram 19

4.1 Research methods 19

4.1.1 Direct observations 19

4.1.2 Internal document analysis 20

4.1.3 Semi-structured interviews 21

4.2 Data requirements 23

4.3 Data analysis methods and Atlas.ti as tool 23

4.4 Research flow diagram and time schedule 24

Chapter 5: Sub-research question 1: What is the current state of the security patching processes at the selected case study organisation? 26

5.1 Internal audit for cybersecurity for Location 2 26

5.1.1 Strengths of the security patching processes 26

5.1.2 Weaknesses of the security patching processes 27

5.2 Performed security patching by OT supplier at Location 1 ... 28

5.2.1 Opportunities of the security patching processes ... 28

5.2.2 Threats of the security patching processes ... 29

5.3 Conclusion sub-research question 1 ... 30

Chapter 6: How are the security patching processes governed within the operational domain? ... 32

6.1 Internal document analysis ... 32

6.1.1 The selected case study organisation OT Security Policy ... 33

6.1.2 The selected case study organisation OT Security Requirements ... 34

6.1.3 The selected case study organisation OT Security Standard ... 36

6.1.4 SLA addendum: OT Security Requirements ... 39

6.1.5 Comparison OT Security documents ... 40

6.2 Policy foundation of security patching governance at the selected case study organisation 41

6.3 Semi-structured interviews with the selected case study organisation's employees ... 42

6.3.1 Outsourced responsibilities ... 43

6.3.2 Lacking communication at the selected case study organisation ... 44

6.3.3 No regular quality checks on OT suppliers by the selected case study organisation ... 44

6.3.4 Contradicting governance ... 45

6.4 Conclusion sub-research question 2 ... 47

Chapter 7: Which factors give insight into the complexity of the security patching processes in an industrial, operational environment? ... 49

7.1 Theme 1: Supplier dependence ... 49

7.2 Theme 2: Ignorance of the OT environment ... 50

7.3 Theme 3: Certification is missing within the OT landscape ... 52

7.4 Theme 4: Human knowledge remains necessary ... 54

7.4.1 Human knowledge or experience in diagnoses, testing and operating the OT systems . 54

7.4.2 Human interactions in preparation and compatibility of security patching ... 55

7.4.3 Specialised local OT knowledge and system customisation ... 55

7.5 Theme 5: Complexity within the OT domain causing delays for security patching ... 57

7.5.1 Ignorance of OT suppliers about terminology ... 57

7.5.2 No uniformity in patch (log) processes of OT suppliers ... 57

7.5.3 No central point for documentation of the reported problems ... 59

7.6 Conclusion sub-research question 3 ... 61

Chapter 8: Conclusion ... 63

Chapter 9: Discussion ... 65

9.1 Reflection on OT-specific considerations (industry perspective) ... 65

9.1.1 Little information available about security patching in OT 65
9.1.2 Patching behaviour has an enormous impact 66
9.1.3 Governmental guidance is missing 67
9.2 Reflection on the selected case study organisation’s perspective 68
9.3 Limitations of the research 68
Chapter 10: Recommendation for future research or practice 70
10.1 Recommendation for the industry within the operational domain 70
10.2 Recommendations for the selected case study organisation 70
References 71
Appendices 76
Appendix 1: Time schedule research 76
Appendix 2: SLA Addendum regarding OT security requirements 77
Appendix 3: Questionnaire for semi-structured interview with the selected case study organisation’s expert employees 78
Appendix 4: Informed consent form interviews OT-suppliers 80
Appendix 5: Codebook Thematic analysis internal document analysis 85
Appendix 6: Codebook Thematic analysis transcript internal experts 86
Appendix 7: Codebook Thematic analysis transcripts OT-suppliers 87

Concept list

Table 1.1: Concept list

Concept	Definition
OT supplier	Third parties who deliver and manage the OT systems at the selected case study organisation’s locations, sometimes including the performance of security patching.
OT systems	Operational technology systems, such as DCS or SCADA systems, which are crucial for the locations’ ongoing operations.
Patches	Additional pieces of code developed to address problems in software. Patches are also known as bugs, whereby they enable additional functionality or address security flaws within a program (Mell et al., 2005).
Patch logs	Records that document the details and processes of software patch management activities, where they serve as a history of patch-related actions to update, fix, or improve software systems in cases where vulnerabilities or issues have been identified.
Software security patching	The process of applying patches to the security vulnerabilities in the software products and systems deployed in an organisation’s cyber environment (Dissanayake et al., 2022a).
Vulnerabilities	Flaws that a malicious entity can exploit to gain greater access or privileges than authorised on a computer system (Mell et al., 2005).

Abbreviations list

Table 1.2: Abbreviations list

Abbreviation	Definition
CCTV	Closed-Circuit Television or more commonly known as video surveillance, where broadcasts are transmitted to a limited (closed) number of monitors (Paessler, n.d.).
CVE	Common Vulnerabilities and Exposures is a publicly accessible database that identifies and catalogues known security vulnerabilities in software and hardware. Each vulnerability is assigned a unique ID, making it easier for organisations to share information, prioritise fixes, and protect their systems (Goodman, 2024a).
CVSS	Common Vulnerability Scoring System is a standardised framework for measuring the severity of security flaws in information systems, which assigns each vulnerability a score between zero and ten, where higher scores mean more severe issues (Goodman, 2024b).
DCS	Distributed Control System is a digital automated industrial control system that uses geographically distributed control loops throughout a factory, machine or control area, where industrial processes are controlled to increase their safety, cost-effectiveness and reliability (Gillis, 2023).
IACS	Industrial Automation and Control System are measurement and control systems that ensure, for example, that locks and bridges function, energy and gas are distributed, drinking water is cleaned, nuclear material is processed, trains arrive at their destination, containers are being transported, and elevators are functioning. They are comparable with OT (Ministry of Justice and Security, 2021).
IT	Information Technology is the development, management, and application of computer equipment, networks, software, and systems. These are crucial to modern business operations because they enable people and machines to communicate and exchange information (Fortinet, 2024).
KPI	Key Performance Indicators can be used to measure and monitor operational performance and progress across an organisation toward specific, measurable goals (Twin, 2024).
NMi	The Netherlands Measuring Institute (Dutch: *Nederlands Meet Instituut*) measures instruments, which will be installed in the field, as referred to in the Dutch Metrology Act, where after the approval of the management system, the certificate holder may carry out activities as an accredited (accepted) verifier. Whereby the system's quality have to be verifying and re-verifying that measuring instruments comply with Dutch regulations (NMi, n.d.).
OT	Operational Technology is the hardware and software to manage industrial equipment and systems, controlled by high-tech specialist systems, like those found in the energy, industrial, manufacturing, oil and gas industries (Fortinet, 2024).
PLC	Programmable Logic Controller is a small, modular, solid-state computer with customized instructions for performing a particular task (Zola, 2024).
SCADA	Supervisory Control and Data Acquisition is a system of software and hardware elements that allows organisations to control and monitor industrial processes by directly interfacing with plant-floor machinery and viewing real-time data (Inductive automation, 2018).
SIS	Safety Instrumented Systems help to reliably protect assets and improve process availability (Emerson, 2024).
SLA	Service Level Agreement defines the level of service expected from an OT supplier, laying out metrics by which service is measured (Greiner et al., 2024).

Chapter 1: Problem introduction

The problem introduction for the performed research is discussed in this first Chapter. The background information will be provided to explain the concept of software security patching in Chapter 1.1. Moreover, the Cyber Security Act, with its motivation, will be introduced in Chapter 1.2. After this, the difference between the IT and OT landscapes will be highlighted in Chapter 1.3, followed by the described relation to the Master's program in Complex Systems Engineering and Management (Chapter 1.4) and the thesis structure in Chapter 1.5.

1.1 Background information

Software security patch management refers to *“the process of applying patches to the security vulnerabilities present in the software products and systems deployed in an organisation’s cyber environment”*, according to Dissanayake et al. (2022a). According to Mell et al. (2005), these vulnerabilities are *“flaws that a malicious entity can exploit to gain greater access or privileges than authorised on a computer system”*. Dissanayake et al. (2022a) state that the process involves identifying existing vulnerabilities in managed software systems and acquiring, testing, installing, and verifying software security patches. Mell et al. (2005) and Dissanayake et al. (2022a) use security patching or patches as *“additional pieces of code developed to address problems in software. Patches are also known as bugs, whereby they enable additional functionality or address security flaws within a program”*. However, performing these activities involves managing interdependencies between multiple stakeholders and several technical and socio-technical tasks and decisions that make software security patch management complex (Dissanayake et al., 2022a).

Moreover, according to the research of Islam et al. (2019), cybersecurity breaches lead to severe organisational and socio-economic consequences, such as loss and theft of proprietary data. A lack of efficient collaboration, coordination, and communication during the software security patch management process can significantly negatively influence the timely vulnerability remediation of security patching (Dissanayake et al., 2022a).

Automox, the cloud-native cyber hygiene platform provider, uncovered in partnership with AimPoint Group that less than 50 percent of organisations can patch vulnerable systems quickly enough to protect against critical threats and zero-day attacks (Automox, 2020a). Whereby 81 percent have suffered at least one data breach in the last two years. Automox (2020b) surveyed 560 IT operations and security professionals and enterprises with between 500 and 25.000 employees across more than fifteen industries to benchmark the state of endpoint patching and hardening. When asked about causes within this research, respondents placed phishing attacks (36%) as the top cause (Automox, 2020a) (Automox, 2020b), followed by missing operating systems patches (30%), missing application patches (28%) and operating system misconfigurations (27%).

1.2 Introduction Cyber Security Act

In light of all digital developments, the European Union has been working on the Network and Information Security (NIS2) directive since 2020 (National Cyber Security Centre, 2024a). This directive is focused on improving the digital and economic resilience of European member states and will be implemented in The Netherlands as the Cyber Security Act (Dutch: *Cyberbeveiligingswet*). When this Cyber Security Act is adopted, it will replace the current Network and Information Systems Security Act (Dutch: *Wet Beveiliging Netwerk-en Informatiesystemen*) (National Cyber Security Centre, 2024a). The European implementation date for the NIS2 directive has been set at 1 July 2025. At this date, the European member states must comply with the new NIS2 directive, where important actors in Dutch society, called ‘Providers of Essential Services’, have to act now to be compliant with obligations which the Cyber Security Act prescribes (National Cyber Security Centre, 2024b):

- *Duty of care* that obliges organisations to carry out a risk analysis themselves as the basis on which they take appropriate measures for securing the network and information systems they use to provide their business services.
- The *reporting obligation* requires organisations to report significant incidents within 24 hours to the Computer Security Incident Response Team and the supervisory authority.
- The *registration obligation* requires organisations under the Cyber Security Act to register in the entity register.
- Organisations under the Cyber Security Act are subjected to receive *supervision*, which involves looking at compliance with the obligations under the Cyber Security Act.

1.3 Difference between IT and OT

Within cybersecurity, there is a distinction between Information Technology (IT) and Operational Technology (OT). Fortinet (2024) defines IT as *"the development, management, and application of computer equipment, networks, software, and systems"*, where IT is crucial to modern business operations because it enables people and machines to communicate and exchange information. On the other hand, Fortinet (2024) describes that OT *"uses hardware and software to manage industrial equipment and systems"* where OT controls high-tech specialist systems, like those found in the energy, industrial, manufacturing, oil and gas industries. An example of one of the most prominent systems within OT is a Distributed Control System (DCS), which is a digital automated industrial control system that uses geographically distributed control loops throughout a factory, machine or control area, where industrial processes are controlled to increase their safety, cost-effectiveness and reliability (Gillis, 2023). Another type of OT system is Supervisory Control and Data Acquisition (SCADA), a system of software and hardware elements that allows organisations to control and monitor industrial processes by directly interfacing with plant-floor machinery and viewing real-time data (Inductive automation, 2018). According to Fortinet (2024), cybersecurity has long been critical in IT to:

- Keep sensitive data safe
- Ensure users connect to the internet securely
- Detect and prevent potential cyberattacks

More importantly, cybersecurity is also vital to OT systems to protect critical infrastructure. As explained by Fortinet (2024), any unplanned downtime can cause manufacturing plants, power plants, or water supply systems to shut down. Protecting OT systems becomes more critical due to the many interwoven systems within each plant's industrial environment. As a result, new vulnerabilities may occur when cybercriminals gain access to interwoven industrial networks with all those OT system components. Fortinet (2024) describes that these attacks have increased, with more than 90 percent of organisations that operate within the industry and OT systems having experienced one or more damaging security events in two years (Kovacs, 2019).

1.4 Relation with Complex Systems Engineering and Management program

Security patch management is a complex issue due to managing interdependencies between multiple stakeholders within the OT environment of the industrial domain. Several technical and socio-technical tasks must be performed, and decisions must be made since human interactions operate these processes and systems. The master's program in Complex System Engineering and Management (CoSEM), focus on complex systems that examine the dynamics of interconnected elements within a system. An interdisciplinary element is intertwined within this research due to combining insights from human interactions (social sciences) and security patch management within the OT environment of the industrial domain (engineering and management). Therefore, this research highlights how it adopts a system thinking approach by researching this complex interplay of socio-technical aspects.

1.5 Thesis structure

After the introduction of Chapter One, the literature review results are shown in Chapter Two, resulting in the academic knowledge gap and the main research question of this research. Within Chapter Three, the research design of the embedded single case study is stated, where the analytical framework is shaped based on the socio-technical system theory of Mumford (2000), and the derived sub-research questions can be found. This is followed by Chapter Four, where the research methods are described for each sub-research question, including data requirements, data analysis methods, data analysis tool and research flow diagram. Chapter Five outlines the results of the first sub-research question, Chapter Six outlines the results of sub-research question two, and Chapter Seven outlines the results of sub-research question three. The conclusion of this research, including the answer to the main research question, can be found in Chapter Eight. Chapter Nine highlights the discussion, where reflections can be found on OT-specific considerations, as the industry perspective, and on the selected case study organisation's perspective, closing off with the limitations of the research. Chapter Ten describes the recommendations for future research for the industry within the operational domain and future practice for the selected case study organisation, followed by the References and Appendices at the end of this thesis.

Chapter 2: Academic knowledge gap and research question

Within this chapter, the academic knowledge gap and main research question are formulated based on the findings of the literature review. The search and selection process for the literature review can be seen in Chapter 2.1, whereas the results of the literature review can be seen in Chapter 2.2. In Chapter 2.3, the knowledge gap can be found, including the main research question for this research.

2.1 Search and selection process

The literature on security patch management and its socio-technical aspects was reviewed to establish the academic knowledge gap. The Google Scholar database was used to select the applicable articles. The following combination of keywords and Boolean Operators were used to retrieve the first relevant articles: software AND security AND patch OR patching AND management. The first three academic articles (Dissanayake et al., 2021; 2022a; 2022b) were retrieved from Google Scholar, which fit the security patch management research area and was the starting point for the literature review. Each article is studied in detail, and the search technique 'snowballing' is used to search further for the to-be-included articles. Wohlin (2014) state that snowballing refers to *"using the reference list of a paper or the citations to the paper to identify additional papers"*. The benefit of using snowballing as a review approach is that this approach complements the search process with *"a systematic way of looking at where papers are referenced and where papers are cited, where references and citations are used respectively and are referred to as backward and forward snowballing"* (Wohlin, 2014). Within Table 2.1 below, the included articles can be seen, combined with the applied search method or review approach for each article. The selected articles are scoped down to the research areas, whereby the included articles had to be written in English and had a maximum publication year of 2003.

Table 2.1: Included articles within the literature review

Author(s)	Year	Research area	Key contribution	Search method/review approach
Dissanayake et al.	2021	Security patch management	Delays within security patch management due to socio-technical intricacies that complicate decision-making.	Google Scholar / Boolean Operators
Dissanayake et al.	2022a	Security patch management	Socio-technical challenges and solutions.	Google Scholar / Boolean Operators
Dissanayake et al.	2022b	Security patch management	Consequential outcomes and causes of patching delays	Google Scholar / Boolean Operators
Mell et al.	2005	Security patch management	Time effect of patching and system vulnerability disclosure.	Backward snowballing
Islam et al.	2019	Security orchestration	Challenges among stakeholders within security patching.	Backward snowballing
Rebensky et al.	2021	Cyber security	Role of human factors in cybersecurity.	Backward snowballing
Arora et al.	2004	Vulnerability disclosure and patch availability	Lacking information on successful attacks, with corresponding countermeasures, and the severity of damages incurred.	Forward snowballing

Feng et al.	2022	Vendor patching strategies	Negative security externalities, when positive networks are low.	Forward snowballing
Porcedda	2018	Efficacy of six EU instruments addressing security breaches	Uncovered deficiencies in the framework's ability to address security breaches.	Backward snowballing
de Smale et al.	2023	Prioritising patching processes	Missing link between the overall software vulnerability ecosystem as well as the patching processes within organisations.	Forward snowballing

2.2 Literature review

2.2.1 Socio-technical challenges in patch management

Dissanayake et al. (2021) describe security patch management as *"a complex process involving the identification, acquisition, installation, and verification of patches"*, marked by socio-technical intricacies complicating decision-making. They emphasise that delays primarily result from socio-technical elements, particularly coordination challenges among individuals, groups, and technical systems, intertwined with organisation processes, policies, skill management, and resource allocation (Islam et al., 2019). In their subsequent work (Dissanayake et al., 2022a), fourteen socio-technical challenges and eighteen corresponding solutions in software security patch management are identified, emphasising the need for further research on socio-technical factors' impact and dynamics. Rebensky et al. (2021) highlight a 50 percent decline in incident reports through enhanced cybersecurity measures. They advocate for improved application development and employee education to fortify data protection within organizations, within their research of human factors in cybersecurity and privacy.

2.2.2 Time effect of patching and publishing

Mell et al. (2005) underscore the critical importance of timely patching for maintaining IT systems' operational confidentiality, integrity and availability. Mell et al. (2005) and Dissanayake et al. (2022a) use security patching or patches as "*additional pieces of code developed to address problems in software. Patches are also known as bugs, whereby they enable additional functionality or address security flaws within a program"*. Despite the prevalent issue of neglecting patches for operating systems and application software, not all vulnerabilities, *"flaws that a malicious entity can exploit to gain greater access or privileges than authorised on a computer system",* have corresponding patches, according to Mell et al. (2005). System administrators must stay informed about vulnerabilities and available patches and be proficient and proactive in alternative remediation methods (e.g., employee training). Furthermore, security experts face challenges handling a growing influx of security alerts from diverse tools, hindering prompt incident response. Islam et al. (2019) introduced security orchestration to enhance the efficiency of monitoring and addressing security incidents, an area where academic research lags behind practical adaptation. Thirdly, Arora et al. (2004) explored the impact of vulnerability disclosure and patch availability on attackers' behaviour and vendors' responsiveness, revealing the complexities of these dynamics. However, there remains a shortage of information on successful attacks, corresponding countermeasures, and the damage's severity. Dissanayake et al. (2022b) highlighted the consequences of delayed patch applications, attributing delays to technological, human, and organisational factors, particularly coordination issues during the deployment phase, emphasising the need for a more comprehensive understanding of practical reasons behind delays.

2.2.3 Patching strategy

Feng et al. (2022) designed three vendor patching strategies: PS1 (rebates for all users), PS2 (rebates only for free users), and PS3 (rebates for no users). These strategies involve trade-offs between benefits and costs. Their research emphasises how the patching incentive can prompt universal user adoption of optimal patching, enhancing network security. This highlights the role of negative security externalities, especially when positive networks are low, in selecting the most suitable approach. Furthermore, Porcedda (2018) investigate the efficacy of six European Union instruments addressing breaches, questioning their effectiveness in preventing or mitigating breaches and addressing network insecurity. Their research uncovers deficiencies in the regulatory framework's ability to facilitate mutual learning, raise awareness among authorities and the public about data protection, and compel entities to manage information to improve their practices (Porcedda, 2018).

2.2.4 Prioritizing patching processes

De Smale et al. (2023) explored the disconnection between the broader software vulnerability ecosystem and organisational patching processes. Their investigation revealed that none of the respondents comprehensively acquired information on software vulnerabilities, even in aggregated forms like the National Vulnerability Database. Their study identified implicit and explicit coping mechanisms organisations employ to limit vulnerability information intake, posing three trade-offs. The disconcerting finding was the lack of comprehensive knowledge acquisition about published vulnerabilities, underscoring the need for a more deliberate evaluation and formal risk management process in acquiring vulnerability information (de Smale et al., 2023).

2.3 Knowledge gap and main research question

From the literature review, it can be concluded that very little literature can be found regarding the interactions employees have to carry out (human interactions) to address vulnerabilities within cybersecurity (security patching). Socio-technical challenges have been identified; however, there is a lack of information about the roles and effects of these challenges, as well as known vulnerabilities and their intake. Furthermore, most cited references neglect human interactions associated with security patching or patch management in their research. It can be seen that these found gaps within the academic research world are dedicated to security patching in IT, without further research towards security patching within an OT environment. Information about current practices of security patching in OT is lacking, combined with a lack of insights into governance and contributing factors related to human interactions and the complexity of security patching processes within an industrial, operational environment. This emerged knowledge gap has to be (partially) addressed, accompanied by the following main research question:

What lessons can be learned from the current practices, governance and complexity factors within security patching processes in an industrial, operational environment?

Chapter 3: Research design and sub-research questions

As stated in Chapter 2.3, the derived research question for this research is: *What lessons can be learned from the current practices, governance and complexity factors within security patching processes in an industrial, operational environment?* This chapter elaborates on the selected research design and starts in Chapter 3.1 by substantiating the research design of an embedded single case study at the selected case study organisation. This is followed by the analytical framework for this research in Chapter 3.2, where a socio-technical system theory of Mumford (2000) is used to shape this. The derived sub-research questions can be seen in Chapter 3.3.

3.1 Research design: Embedded single case study

Exploratory research, as advocated by Casula et al. (2020) and Marlow (2005), offers preliminary insights into an issue, guiding questions for deeper investigations, focusing on the 'What' aspect. This aligns well with the thesis' 'What' main research question (see Chapter 2.3). Creswell (2009) classifies research designs into qualitative (exploring social or human problems), quantitative (testing objectives), and mixed methods (combining both forms), each serving distinct purposes. Creswell (2009) outlines strategies for diverse research designs, including using case studies in qualitative research. These studies involve an in-depth exploration of a program, event, activity, process, or individual to attain a detailed understanding. Ary et al. (2006) emphasise comprehensive case descriptions, bound by time and activity, with data collected over an extended period. Eisenhardt (1989) notes the potentially time-consuming nature of case studies and warns against overly complex theories as outcomes. Yin (2011) suggests performing a single case study as a research design when studying human interactions. An embedded single case study applies to this research's exploratory research design since the complex interplay of human interactions (social elements) within security patching processes (technical elements) in an industrial, operational environment is analysed.

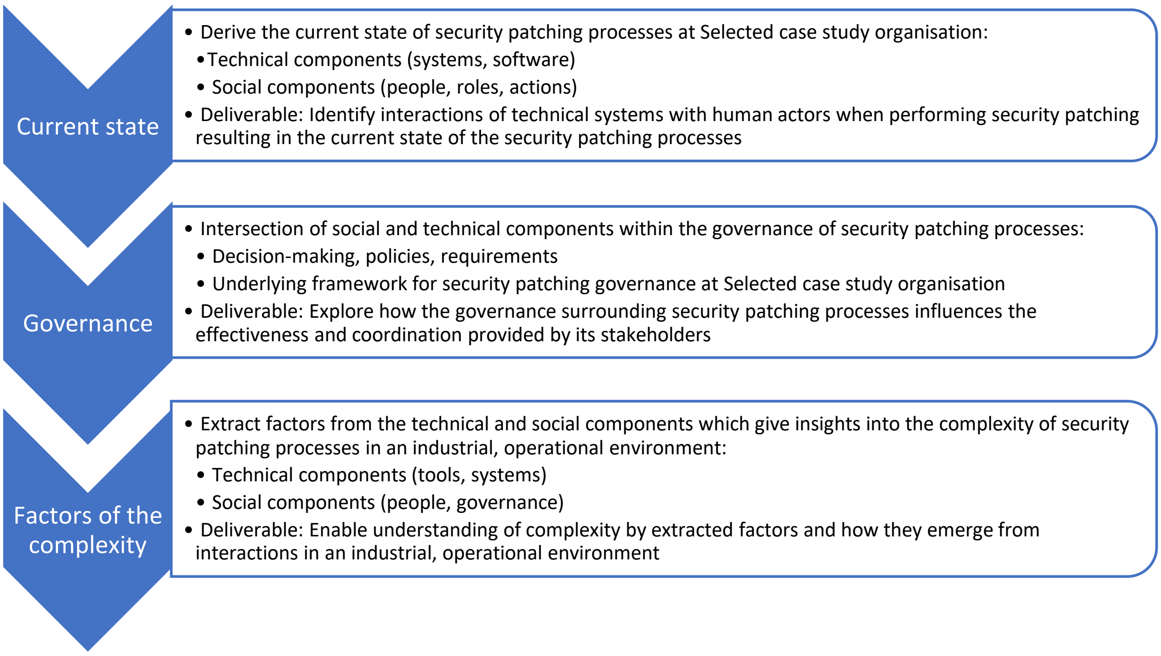
The selected case study organisation is a logistic service provides in the liquid bulk industry, and an important actor in Dutch society, the organization is selected as a Provider of Essential Services (Dutch: *Aanbieders Essentiële Diensten*). Nowadays, the selected case study organisation has to perform according to the Network and Information Systems Security Act (Dutch: *Wet Beveiliging Netwerk-en Informatiesystemen*). This act aims to increase The Netherlands's digital resilience. It requires Providers of Essential Services to take measures to protect their information and communication technology against cyber incidents, who are obligated to report serious incidents (Ministry of Economic Affairs, Agriculture and Innovation, 2023). Furthermore, this law aims to limit the consequences of cyber incidents among these groups and thus prevent unplanned *location downtime* (shutdown of operations), social disruption or even environmental disasters.

Providers of Essential Services must comply with the NIS2 directive before the European Union's implementation date, as stated on 1 July 2025 (National Cyber Security Centre, 2024a). When looking at the established knowledge gap in Chapter 2.3, research is lacking regarding security patching within an OT environment, where information is missing about current practices of security patching in OT, combined with insights into governance and contributing factors relating to human interactions and the complexity of security patching processes within an industrial, operational environment. Due to this reason, the scope of this research is limited to the research security patching of operational systems (OT systems), which are active on the selected case study organisation's locations within the Business Unit The Netherlands.

3.2 Socio-technical system theory as the analytical framework

Many years after the introduction of socio-technical system theory, introduced firstly by Trist and Bamforth (1951) based on coal mining after World War II, several empirical studies formed the starting point for design principles for socio-technical systems. According to Bauer and Herder (2009), the socio-technical approach emphasises the close interdependence of the social and technical subsystems, where socio-technical systems are constituted at single plants, firms or even the entire industrial sector. These subsystems or components are so intertwined that "*their design requires the joint optimisation of technological and social variables"* as Bauer and Herder (2009) stated. Moreover, Norman (2016) introduces socio-technical systems in software engineering, emphasising the intricate interplay between these social and technical elements. Given the research's association with social and technical elements, it is interesting to identify interactions of technical systems with human actors (as social components) when performing security patching within an industrial, operational environment. For this reason, socio-technical system theory is applied as the analytical framework within this research.

Mumford (2000) identifies system design as a problem-solving activity that requires a multidisciplinary approach. This approach examines the current and new problems of complex systems design and describes how a socio-technical approach can assist in creating humanistic and effective systems in the future (Mumford, 2000). Mumford (2000) describes three stages in problem-solving within the socio-technical approach, whereby in Figure 3.1 below, the analytical framework for this research is visualised based on the approach of Mumford (2000), combined with the socio-technical system components (technical systems with human actors when performing security patching). The first stage is *'Seeing the total picture'*, where the researcher focuses on understanding the phenomenon under study. Translated for this research, the current state of the security patching processes, including the technical and social components, had to be determined. The second phase of the approach is called *'Developing strategies'*. Since governance regarding security patching processes has already been developed, this had to be analysed within the operational domain. Finally, the last phase of the approach is *'Taking action'*, where Mumford (2000) describes the design task as a six-stage hierarchy of activities. In terms of this research, all come together to extract factors which give insights into the complexity of the security patching processes in an industrial, operational environment and how these emerge.



Current state

- Derive the current state of security patching processes at Selected case study organisation:
  - Technical components (systems, software)
  - Social components (people, roles, actions)
- Deliverable: Identify interactions of technical systems with human actors when performing security patching resulting in the current state of the security patching processes

Governance

- Intersection of social and technical components within the governance of security patching processes:
  - Decision-making, policies, requirements
  - Underlying framework for security patching governance at Selected case study organisation
- Deliverable: Explore how the governance surrounding security patching processes influences the effectiveness and coordination provided by its stakeholders

Factors of the complexity

- Extract factors from the technical and social components which give insights into the complexity of security patching processes in an industrial, operational environment:
  - Technical components (tools, systems)
  - Social components (people, governance)
- Deliverable: Enable understanding of complexity by extracted factors and how they emerge from interactions in an industrial, operational environment

Figure 3.1: Analytical framework for this research based on the STS-approach of Mumford (2000)

3.3 Sub-research questions

Based on each phase of the socio-technical system theory approach of Mumford (2000), the following sub-research questions, with each deliverable, are composed to accompany the main research question (Chapter 2.3):

1) What is the current state of the security patching processes at the selected case study organisation?
    a. Deliverable: Identify interactions of technical systems with human actors when performing security patching resulting in the current state of the security patching processes.
2) How are the security patching processes governed within the operational domain?
    a. Deliverable: Explore how the governance surrounding security patching processes influences the effectiveness and coordination provided by its stakeholders.
3) Which factors give insight into the complexity of the security patching processes in an industrial, operational environment?
    a. Deliverable: Enable understanding of complexity by extracted factors and how they emerge from interactions in an industrial, operational environment.

Chapter 4: Research methods and research flow diagram

Since the research design and the analytical framework for this research are established in the corresponding Chapter 3.1 and Chapter 3.2, together with the sub-research questions stated in Chapter 3.3, the research methods for each sub-research question are selected. Within Chapter 4.1, the selection of each sub-research question is distinguished based on the common sources of evidence of Yin (2011) when conducting case studies. Chapter 4.2 indicates the data requirements for each sub-research question. Next, SWOT analysis (for sub-research question one) and reflexive thematic analysis (for sub-research questions two and three) are selected as data analysis methods, where Atlas.ti is selected as data analysis tool, as seen in Chapter 4.3. This all comes together in the research flow diagram as a research summary in Chapter 4.4.

4.1 Research methods

Yin (2011) states that *"case study research is not limited to a single source of data, as in the use of questionnaires for carrying out a survey"*. Therefore, multiple research methods are used, whereby each sub-research question (Chapter 3.3) contributes to the case study via a separate research method. Table 4.1 below describes which source of evidence applies to each sub-research question and which specification is relevant for this embedded single-case study at the selected case study organisation, based on the six common sources of evidence of Yin (2011) when conducting case studies.

Table 4.1: Sources of evidence with each contribution and specification per sub-research question (Yin, 2011, p.10)

Source of evidence based on the research of Yin (2011, p.10)	Contribution to the research in	Specification for embedded single-case study at the selected case study organisation
Observations	Sub-research question 1	Direct observations of the current state of security patching processes including technical and social components within these processes.
Documents	Sub-research question 2	Document analysis of the internal documents regarding the OT Security Policy, Requirement, Standard, including the SLA addendum regarding the OT Security Requirements to the contracts with the OT suppliers
Interviews	Sub-research questions 2 and 3	Semi-structured interviews with the selected case study organisation employees as expert interviews and semi-structured interviews with experts of OT suppliers

4.1.1 Direct observations

Direct observations are used to analyse the current state of the security patching processes at the selected case study organisation based on the interactions between the technical elements (security patching) and social elements as human actors (stakeholders, locations, and OT suppliers). These interactions revealed strengths, weaknesses, opportunities, and threats. The strengths and weaknesses were derived from the observations during the internal audit at Location 2. The opportunities and threats were derived from multiple observations during the execution of security patching by an OT supplier at Location 1. When looking at the active OT systems at the selected locations within Business Unit The Netherlands as the scope of this research, the selected OT supplier for the direct observations of performed security patching is most crucial since this OT supplier delivers multiple OT systems at these locations that are crucial for the ongoing operations. Conversations and questions may occur when performing the observations, which will be included in the results of this sub-research question. The deliverable of the first sub-research question was to derive the current state of the security patching processes at the selected case study organisation, including identifying interactions of technical systems with human actors (as social components) when performing security patching. The outcomes of the observations were used as input for directly selecting the internal documents and indirectly used for formulating the questionnaire for the semi-structured interviews with the selected case study organisation's experts, both within sub-research question two. These outcomes were also partly used to formulate the questionnaire for the semi-structured interview with the OT suppliers in the third sub-research question.

4.1.2 Internal document analysis

According to Bowen (2009), document analysis is *"a systematic procedure for reviewing or evaluating documents, printed and electronic material"*, where these documents contain words and images that have been recorded without the researcher's intervention. For this embedded single case study, internal documents related to the governance of security patching at the selected case study organisation will be analysed. Therefore, the internal document analysis will examine the documents presented in Table 4.2. The outcomes of the observations from sub-research question one are used to select the documents below.

Table 4.2: Selected documents for internal document analysis in sub-research question two

Document	**Specification for embedded single-case study at the selected case study organisation**
OT Security Policy of the selected case study organisation	Insights into the OT Security Policy of the selected case study organisation regarding security patching
OT Security Requirements of the selected case study organisation	Insights into the OT Security Requirements of the selected case study organisation regarding security patching
OT Security Standard	Insights into the OT Security Standard of the selected case study organisation regarding security patching
SLA addendum OT Security Requirements	Insights into the SLA addendum of OT Security Requirements of the selected case study organisation regarding security patching

Document analysis helps to understand and indicate the conditions that conflict with the subject under study (Bowen, 2009). Bowen (2009) describes document analysis as often used with other qualitative research methods, such as triangulation. Denzin (1970, p.291) states that triangulation is *"the combination of methodologies in the study of the same phenomenon"*. The deliverable for the second sub-research question is to explore how the governance of security patching influences the effectiveness of the security patching processes and coordination amongst the OT suppliers. The internal document analysis will add value to the deliverable of this sub-research question by generating insights into the governance surrounding security patching processes. The outcomes of the internal document analysis will contribute to finalising the questionnaires for the semi-structured interviews with the selected case study organisation's experts, later in sub-research question two, and the semi-structured interviews with the OT suppliers in sub-research question three.

4.1.3 Semi-structured interviews

Gill and Baillie (2018) underscore the significance of research interviews as a fundamental qualitative method, allowing researchers to gain in-depth insights into participants' perspectives, experiences, beliefs, and motivations. Gill and Baillie (2018) describe in their research that structured interviews offer clarification on specific topics but provide less in-depth analysis. Meanwhile, unstructured interviews enable the collection of comprehensive data on participants' experiences, but they can consume many hours on a single occasion. Semi-structured interviews are commonly used in research and allow the researcher to ask predetermined questions; nevertheless, there is room to add or leave out questions. The outcomes of the direct observations of sub-research question one and the internal document analysis of (partly) sub-research question two resulted in starting questions for interviews with the selected case study organisation's experts. Semi-structured interviews were organised with the selected case study organisation's experts because, depending on the answers provided by the participants during the interview, questions were added or left out.

When assessing which experts of the selected case study organisation had to be selected to perform the semi-structured interviews, Yin (2011) highlighted that important insights into the case can be retrieved if participants are key persons in the organisation and those insights are based on the participants' construction of reality. With this in mind, three experts were selected for the semi-structured expert interviews, as shown in Table 4.3 below. Within Table 4.3, each relation to this research can be seen and is defined by their responsibilities. The added value of these semi-structured expert interviews to the deliverable of this second sub-research question is by generating insights into the effectiveness of security patching processes and the coordination provided by its stakeholders.

Table 4.3: Selected experts of case study organisation for semi-structured interviews in sub-research question two

Internal experts of the selected case study organisation	**Relation to embedded single case study at the selected case study organisation**
Internal Expert 1	Responsible for the information security policy of both the IT and OT domains at the selected case study organisation globally
Internal Expert 2	Responsible for the implementation and maintenance of the OT systems at the locations within the Business Unit The Netherlands
Internal Expert 3	Responsible for applying OT knowledge to the Global IT/OT team for policy-making, consultation or giving advice, sharing best practices, creating awareness

To have an overall view of the security patching processes at the selected case study organisation, insights from the perspective of the OT suppliers into the security patching processes had to be derived as well. Therefore, semi-structured interviews were organised with the OT suppliers since they deliver and manage the OT systems (business services) at the selected case study organisation's locations and interact within the selected case study organisation's OT landscape. When looking at the locations within the scope of this research, the following locations are included in this research: Location 1, Location 2, Location 3, and Location 4 (including Location 5 and Location 6 since the management of Location 4 supervises them).

After several brainstorming sessions with the selected case study organisation employees at each described location, several lists of active OT systems for each location were derived, where the scope was narrowed down towards OT suppliers who deliver OT systems with a business criticality of level 'Gold', as they are the most critical OT suppliers for these locations and where 'monitoring is required' of their specific OT system. Table 4.4 below shows the OT suppliers included in this research, specified with the type of OT system provided at which location. Before the semi-structured interview with an expert of each OT supplier was conducted, every participant had to consent to the interview by filling in the informed consent document, including the questionnaire, which can be seen in Appendix 4. Questions were added or left out during the semi-structured interviews with the OT suppliers, depending on the answers provided by the participant. The deliverable for sub-research question three is to extract factors that give insights into the complexity of security patching processes in an industrial, operational environment. The added value of the semi-structured interviews with the OT suppliers is that these interviews may also explain how these factors emerge from the interactions within the operational environment.

Eventually, eleven direct OT suppliers and one indirect OT supplier were included in this research, which can be seen in Table 4.4. below. The four highlighted OT suppliers in Table 4.4 are included in the research but not interviewed since they did not want to participate in the research with a semi-structured interview. The direct OT suppliers supply to the selected case study organisation locations directly. OT supplier OT 12 is the indirect OT supplier, which approved participating in this research, but does not supply directly to the selected locations of the selected case study organisation. Other OT suppliers, such as OT supplier 1, OT supplier 13, and OT supplier 15 use OT supplier 12' OT systems. OT supplier 13 and OT supplier 15 did not want to participate but are still included. This also applies to the OT supplier 14, where the OT system of an OT supplier 3 is used, but this OT supplier is not interviewed, and for OT supplier 16, OT systems of interviewed OT suppliers 7 and 4 are used, but that one also not interviewed.

Table 4.4: Selected OT-suppliers for semi-structured interviews in sub-research question three

#	OT supplier	Location	OT system
1	OT supplier 1	Location 1	Waste incinerator (Dutch: *verbrandingsoven*) – OT supplier 12
2	OT supplier 2	Location 4	SIS
3	OT supplier 3	Location 1/Location 2/Location 4 /Location 3	DCS and SIS (Location 1 and Location 3), PLCs (Location 4) and DCS and Tank Gauging (Location 2)
4	OT supplier 4	Location 3/Location 6	SCADA
5	OT supplier 5	Location 4	PLCs
6	OT supplier 6	Location 2	Weighbridge
7	OT supplier 7	Location 4	PLCs
8	OT supplier 8	Location 4	DCS
9	OT supplier 9	Location 4/ Location 1	Tank Gauging
10	OT supplier 10	Location 4/ Location 4	Fire alarm control panels
11	OT supplier 11	Location 1	CCTV – Fourth party 4
12	OT supplier 12	Location 2/Location 1/ Location 3	Supplier of OT supplier 1, OT supplier 13, and OT supplier 15
13	OT supplier 13	Location 3	PLC – OT supplier 12
14	OT supplier 14	Location 3	Tank Gauging – OT supplier 3
15	OT supplier 15	Location 2	Boiler house (Dutch: *ketelhuis*) – OT supplier 12
16	OT supplier 16	Location 4	PLC – OT supplier 7 and OT supplier 4

4.2 Data requirements

The data requirements for the direct observations (sub-research question one) and semi-structured interviews (sub-research questions two and three) necessitate primary data originating directly from the research effort (Deakin University, 2023). According to Gill and Baillie (2018), the semi-structured interviews have to be recorded to retrieve an accurate transcription of each interview. The semi-structured interviews can be conducted in a physical environment or online. Microsoft Teams will be used when the semi-structured interviews are conducted online. Before the semi-structured interviews with the OT suppliers (in the third sub-research question), all participants must sign a consent document, which will be handed out via e-mail to the participant, as seen in Appendix 4. Afterwards, all participants of the semi-structured interviews of both selected case study organisation's Experts in sub-research question two and the OT suppliers in sub-research question three must check if the retrieved anonymous transcript is correct and approve their anonymous transcript before including and using the transcript as data within this thesis. Additionally, internal document analysis in sub-research question two demands secondary data. The data is derived from primary sources related to the selected case study organisation's governance regarding security patching processes.

4.3 Data analysis methods and Atlas.ti as tool

Within sub-research question one, the direct observations result in interactions between technical elements (security patching) and social elements as human actors (stakeholders, Locations, and OT suppliers), revealing strengths, weaknesses, opportunities, and threats. Gürel (2017) described that organisations interact with their environments and comprise various sub-systems, where the organisation exists in two environments, one in itself and the other outside. According to Gürel (2017) is *"the process of examining the organisation and its environment is termed as SWOT analysis"*. Strengths and weaknesses are internal factors (direct observations during the internal audit at Location 2). In contrast, opportunities and threats can be seen as external factors (direct observations during performed security patching by one of the selected case study organisation's most important OT suppliers at Location 1). Gürel (2017) describes that a SWOT analysis can be used as a strategic planning framework to evaluate an organisation, a plan, a project or a business activity. Within this case study research, SWOT analysis frames these interactions in the four described categories.

For sub-research questions two and three, the data will be analysed using thematic analysis. Fereday & Muir-Cochrane (2006) state that thematic analysis is *"a form of pattern recognition within the data, with emerging themes becoming the categories for analysis"*. Bowen (2009) describes that the process involves *"a careful, more focused re-reading and review of the data",* whereby the researcher takes a closer look at the selected data and performs coding and category construction based on the characteristics to uncover themes to a phenomenon.

Braun and Clarke (2020) describe a six-phase process for data engagement, coding, and theme development within their research. The process is as follows: 1) data familiarisation and writing notes; 2) systematic data coding; 3) generating initial themes from coded and collated data; 4) developing and reviewing themes; 5) refining, defining, and naming themes; and 6) writing the report. Specific to this research, the primary data which is generated from the semi-structured interviews (in sub-research questions two and three) and the secondary data within the internal document analysis (sub-research question two) will be coded. Braun and Clarke (2020) state that data coding in the thematic analysis is conceptualized as *"an analytical unit or tool, used by researcher to develop (initial) themes. Here, codes can be thought of as entities that capture (at least) one observation, display facets"*. Braun and Clarke (2020) describe three general types of thematic analysis: *Coding reliability TA, Codebook TA, and Reflexive TA. Coding reliability TA* captures the approach of objective and unbiased coding. The use of a codebook for the analytical process is critical to ensuring accurate and reliable coding, where themes are developed early on, even before analysis. *Codebook TA* captures a cluster of methods in a qualitative paradigm. They use some structured coding framework for developing and documenting the analysis; however, consensus between inter-rater reliability is not usually a quality measure. Themes are initially developed early on, but in some methods, they can be refined, or new themes can be developed through inductive data engagement and the analytical process. Lastly, Braun and Clarke (2020) described *reflexive TA*, which captures approaches that fully embrace qualitative research values and the subjective skills of the researcher brings to the process. The analysis can be more inductive or theoretical/deductive as a situated interpretative reflexive process whereby the coding is open and organic. Themes are the final outcome of data coding and iterative theme development. For this case study research, *reflexive TA* is chosen, where the coding through the outcomes of the internal documents and transcripts of the semi-structured interviews are open and organic. To retrieve the final themes as outcomes, the codes are grouped into code groups to subtract these final themes.

Atlas.ti is a qualitative research tool used for reflexive thematic analyses within this qualitative case study research. Atlas.ti is used to systematically code and categorize specific aspects of the content in the data to uncover trends and patterns of words or characteristics (Hecker & Kalpokas, 2023).

Moreover, as Yin (2011) suggests, it is vital to ensure consistency among findings from various sources. Convergence is most desired when three or more independent sources align on the same events, facts, or interpretations, resulting in triangulation or *"establishing converging lines of evidence"*, enhancing the findings' robustness (Yin, 2011).

4.4 Research flow diagram and time schedule

Within Figure 4.2, a research flow diagram is generated to visualize the research design of this research, based on the earlier described research questions (Chapter 3.3), research methods (Chapter 4.1) and data analysis method and tool (Chapter 4.3). Within the research flow diagram, the research flow is indicated, as well as the knowledge flow of the research.

Next to the research flow diagram, a Gantt chart is used to develop a schedule for the planning of this research, which can be seen in Appendix 1. Maylor (2001) states that the Gantt Chart is the most widely used technique to develop a planning bar chart since it encourages a one-step approach to planning the research, allowing the researcher to control the project and its timeline (Maylor, 2001). The overarching research elements are as follows: start of the thesis, kick-off meeting, data collection period, data analysis period, green light meeting, and thesis defence meeting, whereby a distinction is made between the duration of the step and the time to complete.

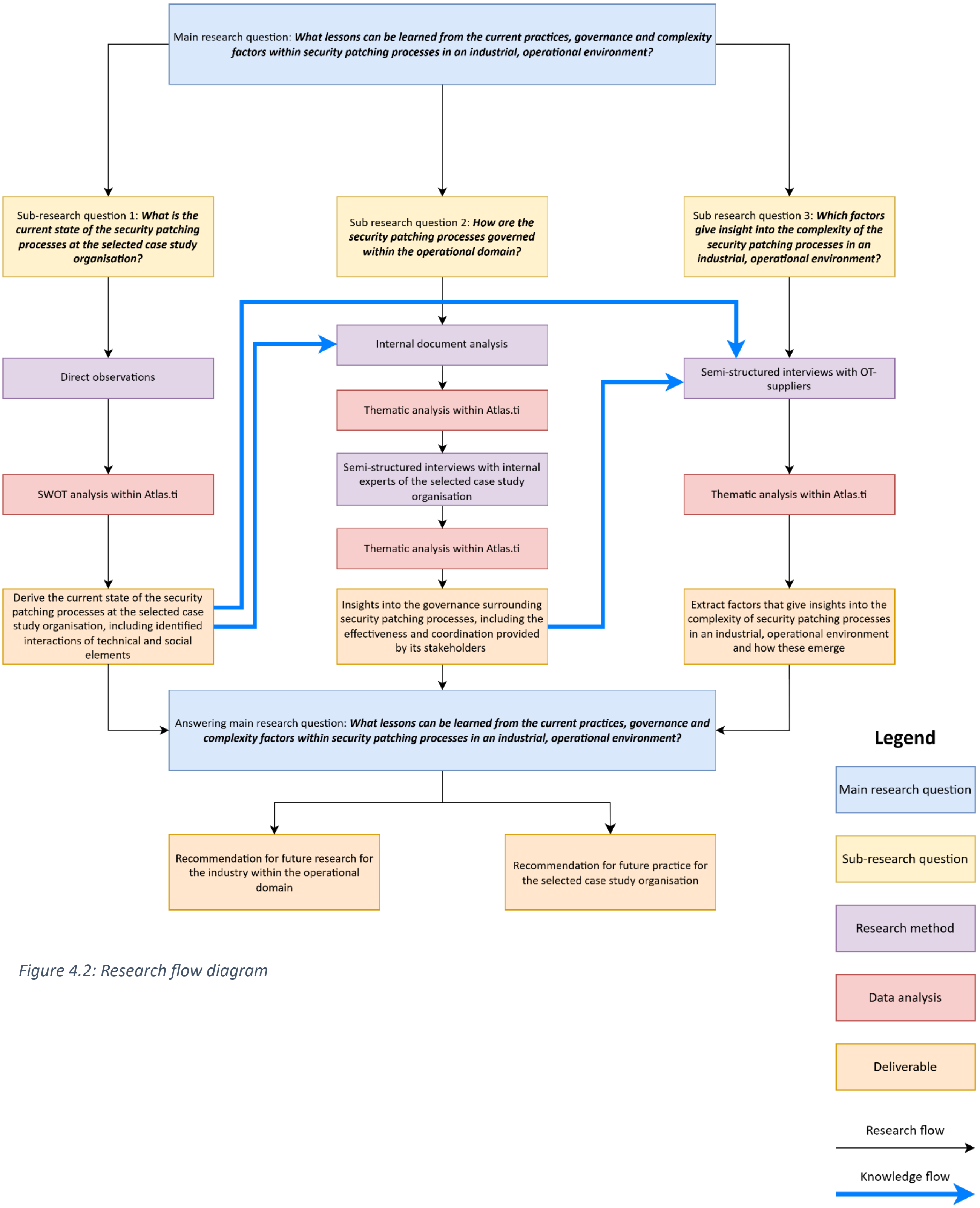

Main research question: ***What lessons can be learned from the current practices, governance and complexity factors within security patching processes in an industrial, operational environment?***
Sub-research question 1: ***What is the current state of the security patching processes at the selected case study organisation?***
Sub research question 2: ***How are the security patching processes governed within the operational domain?***
Sub research question 3: ***Which factors give insight into the complexity of the security patching processes in an industrial, operational environment?***
Direct observations
SWOT analysis within Atlas.ti
Derive the current state of the security patching processes at the selected case study organisation, including identified interactions of technical and social elements
Internal document analysis
Thematic analysis within Atlas.ti
Semi-structured interviews with internal experts of the selected case study organisation
Thematic analysis within Atlas.ti
Insights into the governance surrounding security patching processes, including the effectiveness and coordination provided by its stakeholders
Semi-structured interviews with OT-suppliers
Thematic analysis within Atlas.ti
Extract factors that give insights into the complexity of security patching processes in an industrial, operational environment and how these emerge
Answering main research question: ***What lessons can be learned from the current practices, governance and complexity factors within security patching processes in an industrial, operational environment?***
Recommendation for future research for the industry within the operational domain
Recommendation for future practice for the selected case study organisation
Legend
Main research question
Sub-research question
Research method
Data analysis
Deliverable
Research flow
Knowledge flow

Figure 4.2: Research flow diagram

Chapter 5: Sub-research question 1: What is the current state of the security patching processes at the selected case study organisation?

The first sub-research question investigates the current state of the security patching processes at the selected case study organisation, using direct observations. These direct observations result in interactions between the technical elements (security patching) and social elements as human actors (stakeholders, locations, and OT suppliers), revealing strengths, weaknesses, opportunities, and threats. Gürel (2017) describes that a SWOT analysis can be used as a strategic planning framework to evaluate an organisation, a plan, a project or a business activity. The SWOT analysis frames these interactions in the four described categories within this case study research. The direct observations during the internal audit at Location 2 resulted in strengths and weaknesses as internal factors, as seen in Chapter 5.1. On the external side, direct observations during security patching performed by one of the selected case study organisation's most important OT suppliers at Location 1, resulted in opportunities and threats, as seen in Chapter 5.2. The determination of the current state of the security patching processes at the selected case study organisation is shown in the conclusion of sub-research question one, provided in Chapter 5.3.

5.1 Internal audit for cybersecurity for Location 2

Based on the gathered data from the observation round of the internal audit for cybersecurity for Location 2, strengths and weaknesses of the interactions between technical systems and social elements as human actors were identified as the internal side of the SWOT analysis. The results of the identified strengths within the current state of the selected case study organisation's security patching processes are shown in Chapter 5.1.1. In contrast, the identified weaknesses of these processes are shown in Chapter 5.1.2.

5.1.1 Strengths of the security patching processes

The first identified strength is found regarding the internal OT security assessment. In 2022, an OT security assessment was performed to determine the criticality of the OT assets at Location 2. The assessment guidelines of these OT systems were tested to determine if they match the business's criticality and current Service Level Agreement (SLA). The SLA defines the level of service expected from an OT supplier, laying out metrics by which service is measured (Greiner et al., 2024).

A second strength based on the interactions of the current state of the security patching processes is established on the observation that most OT systems are standalone systems, where they cannot be connected towards the internet. Only a local connection is being made with the selected case study organisation's network. An additional advantage of this strength is that the risk of unwanted harmful data, malware, or other breaches via this internet connection is prevented.

The third identified strength is that OT suppliers must have a signed work permit at all times before the specific OT supplier can perform work on the location, in this case, related to security patching. Within the work permit, a risk analysis is carried out based on the activities to limit and mitigate all possible risks, where personal safety is considered. Before the work permit is issued to the OT supplier, it is read aloud so the OT supplier can confirm the assessment within the risk analysis of the work permit. A second part of the work permit is the Last Minute Risk Assessment (LMRA), where all performed activities with its risks have to be stated, in consultation with the location's process operators from the selected case study organisation's Operations department. It has been shown during the observation that all active work permits are monitored by the selected case study organisation continuously, and personal safety is considered the most important.

5.1.2 Weaknesses of the security patching processes

The first identified weakness of the current security patching processes at the selected case study organisation can be seen as a lack of information about lessons learned from cyber incidents within the selected case study organisation's business contingency plan. The business contingency plan (Dutch: *bedrijfsnoodplan*) has to be applied in case of an unexpected location shutdown. This business contingency plan focuses more on fundamental safety (how to make the location safe in terms of operations) than getting the location up to speed after *location downtime* caused by a cyber incident. Although it has been said that cyber incidents are included within this plan, it could not be retrieved which cyber incidents are included and which improvements were added based on these previously experienced incidents.

A second weakness is identified regarding the observation that it cannot be retrieved from the internal system *Service Now,* which software updates are installed at which OT system since this type of information has to be entered manually by the selected case study organisation's experts for each OT system, of each OT supplier at each location. The definition provided by the selected case study organisation of the internal system *Service now* is as follows: *"Service now is the logging system for maintenance of all the assets with cables and plugs, where assets are registered, including their maintenance and life-cycle management"*. The active SLAs for each OT supplier can also be found within *Service Now*. However, all assets without cables and plugs, such as valves and pumps on a location, are registered within the selected case study organisation's internal system *Infor*. *Infor* is the selected case study organisation's enterprise asset management system, where also other specifications are registered towards these assets, such as malfunctions or technical issues. Within *Infor*, active work permits with potential follow-up actions can be retrieved. These cannot be retrieved from *Service Now* for the specific OT systems. It can be seen that some asset-specific lessons learned are included within *Infor*, but business disruptions, such as leakages, are registered and monitored within the selected case study organisation's system *Enablon*. However, in *Enablon*, cybersecurity cannot be chosen as a category for reporting a business disruption due to cyber incidents. In addition to this, every OT supplier has its own maintenance system where follow-up actions are logged. For example, the selected case study organisation can access an OT supplier's digital platform to address end-to-end lifecycle needs for automation, control software, or asset performance management solutions. Still, the selected case study organisation cannot access this OT supplier's malfunction or maintenance system. Therefore, generating an overview of installed updates, actions, and lessons learned on each OT system, OT supplier, and location is very challenging, making it unclear how the selected case study organisation monitor performed security patching on each OT system of these OT suppliers.

A third observed weakness is that many OT suppliers are contracted within Business Unit The Netherlands. Every location has its own type of product storage or handling, which results in another type of OT system, resulting in variances of OT suppliers amongst the locations and, therefore, in other frequencies of security patching. Due to the ongoing operations, it is more difficult to install updates or perform security patching, whereas, for other locations with less ongoing operations, this is easier to perform. For example, when a location is equipped as a storage location, security patching may be performed more frequently, contradicted with a location with continuous transshipments of goods or other types of operations, where saving historical data and measurements of weights and loads is more important. However, it can be seen that even for one type of OT system (for example, CCTV monitoring system), five OT suppliers are contracted within the same Business Unit (e.g. four locations within Business Unit The Netherlands). This results in every location reinventing the wheel instead of incorporating already existing knowledge of other locations.ss

The last identified weakness is regarding technical malfunctions of the OT systems. Technical malfunctions can result in (safety) risks or errors of the OT systems due to the end-of-life assets of the OT system, causing being unable to update the digital environment (e.g. Windows) on the specific asset of the OT system (e.g. when an OT system is operating based on a Windows 7 environment). More extreme consequences of the unavailability of OT systems are causing risks of *location downtime* since the OT system cannot be used and ongoing operations are disrupted. It is observed that the lifecycle of IT/OT assets is not prioritised since they do not produce turnover and, therefore, do not directly result in profit. It was discussed that location management does not approve of replacing all these assets of OT systems at one time, and mitigating measures have to be drawn up first. If security patches are installed more frequently on OT systems, with fewer end-of-life assets, fewer technical malfunctions, which can cause *location downtime*, will occur. Due to these technical malfunctions, much production time might be lost in finding the cause.

5.2 Performed security patching by OT supplier at Location 1

Three observation rounds were organised when an important OT supplier for the selected case study organisation performed security patching at Location 1. Based on the gathered data from these three observation rounds, opportunities and threats of the interactions between technical systems and social elements as human actors were identified as the external side of the SWOT analysis. The results of the identified opportunities within the current state of the selected case study organisation's security patching processes can be seen in Chapter 5.2.1. In contrast, the identified threats of these processes are shown in Chapter 5.2.2.

5.2.1 Opportunities of the security patching processes

The first identified opportunity relates to the observation that more lessons learned can be incorporated into the current state of the selected case study organisation's security patching processes via the stated recommendations of internal (or external) audits. Within the selected case study organisation's internal system *Enablon*, business disruptions, such as leakages, are registered and monitored. It was observed that *Enablon* includes an audit module, where audit findings can be rewritten as actions with due dates and linked to specific employees as action owners for audits within the selected case study organisation's Operations department. It was stated that the selected case study organisation's IT department does not use *Enablon*; since the Internal Expert 1's team organised and directed these types of audits and fall under the selected case study organisation's IT department, *Enablon* is not being used for audit findings related towards security patching or cybersecurity. An example of an included lesson learned in the selected case study organisation's security patching processes is that recently, all USB sticks brought along by the OT suppliers are currently being scanned before issuing the work permit and before the actual performance of maintenance, security patching or another type of work on each location. It was discussed that a couple of years ago, these USB sticks, with all the to-be-installed data by the OT supplier on OT systems at the selected case study organisation's locations, were not scanned at all, resulting in the risk of unwanted installations of dangerous malware.

A second identified opportunity can be seen when the usage of secure file transfer systems (e.g. *Datasluis*) is incorporated within the selected case study organisation's security patching processes. Nowadays, the to-be-installed data is brought to the location by the OT suppliers via USB sticks for transferring and installing data and software towards OT systems. Risks arise from unwanted data (malware or viruses) installed on the OT systems at the selected case study organisation's locations. Incorporating secure file transfer systems (e.g. *Datasluis*) allows users to download the to-be-installed data and other files easily and safely. The reason why *Datasluis* is not used currently is because information on how to use this system is unavailable at the selected case study organisation. However, it can be seen that the selected case study organisation is determining the usability with one of the selected case study organisation's newer OT suppliers at one of the locations within the Business Unit The Netherlands, for implementing *Datasluis*, which needs to be taken up further.

A third identified opportunity is to deploy the knowledge of important OT suppliers regarding security patching processes to other OT suppliers at the selected case study organisation, by incorporating insights of general processes or operations regarding security patching or cybersecurity into the SLAs with other OT suppliers. It can be seen that the OT supplier who performed security patching during the observation rounds pays much attention to security patching and software development, including preparation to avoid possible risks or vulnerabilities and cyber breaches within the OT systems, which could result in potential business disruptions. In addition, it has been observed that this OT supplier assesses security vulnerability databases, such as CVE, in detail and makes all their updates cumulative, including earlier-solved vulnerabilities, errors or other bugs, to mitigate the risk that an update is missed at their OT systems. The result of investing heavily in the OT suppliers' cyber environment and resilience can be seen in the fact that the assets of their OT systems are updated with the newest software versions on a preventive basis. The OT supplier mitigates the risk of business disruptions due to missed software installations within the software of their OT systems. Moreover, the OT supplier indicates that the published vulnerabilities by CVE do not always apply to every situation. For example, the CVE published a low-level vulnerability, where a patch had to be installed to download it via an internet connection at the OT system's server. However, this vulnerability is not applicable since the OT system's server has no internet connection.

The last identified opportunity is related towards the observation that security patching can be more efficiently performed during planned *location downtime*. More OT systems' assets could be updated simultaneously when ongoing operations are paused during the *location downtime* if the OT supplier schedules more experts to perform security patching. Security patching is time-consuming, with much idle time when the OT supplier expert cannot perform any other work and has to pay attention to perform actions related to security patching. It was observed that multiple experts of the specific OT supplier could perform security patching simultaneously, resulting in more to-be-installed installations within the same (small) time window of *location downtime*. During security patching, OT systems' assets have to reboot, which consumes much time, and the asset cannot be used for other actions. Meanwhile, the OT experts have to wait until the reboot of the asset is completed. Due to the complexity of the virtual environment, installing more than two virtual assets simultaneously, provided by one OT supplier expert on one physical asset, seems impossible without the risk of making (human) errors or mistakes. In addition, much expertise is needed to perform the software installations at each asset, which not all OT suppliers' experts have since *"training new colleagues consumes a tremendous amount of time so that they can install the software updates themselves"*, as stated by the OT supplier expert during one of the observation rounds.

5.2.2 Threats of the security patching processes

The first identified threat based on the interactions within the security patching processes relates to password management of the OT systems' assets. Risks of cyber breaches are lurking, where vulnerable information about OT suppliers' log-in credentials for OT systems at the selected case study organisation's locations can be exploited due to a cyber hack. This also applies to password rotation in cases where OT suppliers' employees could forget these passwords and when OT suppliers' employees are uncertain about the availability of these OT systems when passwords are changed since passwords have to be inserted after the reboot of an OT system during security patching. It is unclear if the OT systems will be available after changing the credentials of these OT systems. If not, a more significant risk arises, where the operational systems of the specific location won't be accessible, resulting in potential business disruptions. It has been said by the OT supplier expert that: *"these operation systems are not often used to install new software with these specific credentials. Therefore, adequately saving these credentials is very important"*.

A second threat has been identified: OT suppliers cannot arrange to perform security patching within the agreed time window to solve the vulnerability of the OT system. Since the OT suppliers are responsible for performing the security patching, delays may arise, including the risk that a vulnerability can compromise the OT system at the selected case study organisation's locations, resulting in unexpected *location downtime*. Contributing factors to this threat are that 1) OT suppliers have to organise appointments on each location to perform security patching with approved timeslots by the local operation department of the selected case study organisation's locations, 2) not all experts of these OT suppliers have the required knowledge level to perform security patching at the locations, where issues with employee visas (for travelling towards these locations) may also contribute to these delays.

A third identified threat is that the selected case study organisation depends on the knowledge of OT suppliers' experts who perform security patching on their OT systems at the selected case study organisation's locations. Each location is a highly integrated, complex landscape of multiple OT systems of different OT suppliers, which cannot permit malfunctioning systems due to missed patches. It appeared during the observation that it is unclear how the selected case study organisation's employees monitor which assets of which OT systems of which OT supplier update the software, and which OT supplier of which OT system of which asset has to update their software. Even when multiple experts of the same OT supplier perform security patching at each location, misunderstandings and miscommunication may occur between OT suppliers' experts and the selected case study organisation. There is lacking information about the overview of the already installed updates of these assets for the selected case study organisation, supplemented when an OT supplier performs an update on one of the assets, and further knowledge levels regarding security patching, risk management and problem-solving within this environment.

5.3 Conclusion sub-research question 1

Determining the current state of the security patching processes at the selected case study organisation is based on the performed interactions with both the technical elements (security patching) and social elements as human actors (stakeholders, locations, and OT suppliers). These interactions are framed via a SWOT analysis in four different categories: strengths, weaknesses, opportunities, and threats, resulting in the overview of the current state.

Three strengths were identified:

1. OT security assessments are held at the selected case study organisation to define the criticality of OT assets and test whether the assessment guidelines of OT systems match the business continuity and SLA.
2. OT systems are (mostly) standalone systems without a connection towards the internet to prevent the risk of unwanted or harmful data, malware, or other breaches via this connection. Only a local network of the selected case study organisation is connected towards the OT systems.
3. Before an OT supplier performs security patching, a work permit has to be signed by both the selected case study organisation and the OT supplier. This work permit includes a risk analysis (Last Minute Risk Assessment) to limit and mitigate all possible risks where personal safety is considered.

Four weaknesses were identified:

1. Lacking information about lessons learned from cyber incidents within the selected case study organisation's business contingency plan. The business contingency plan ('*bedrijfsnoodplan'*) focuses more on fundamental safety (how to make the location safe for operations) instead of how to get the location up to speed after *location downtime* caused by a cyber incident. However, although it is said that cyber incidents are included within this plan, it could not be retrieved which cyber incidents are included and which improvements were added.
2. It cannot be retrieved from *Service Now* which updates are installed at which OT system since this type of information has to be entered manually by the selected case study organisation's experts. In addition to this, every OT supplier has its own maintenance system where actions are logged. Therefore, it is challenging to generate an overview of installed updates on each OT system.
3. Many OT suppliers are contracted within Business Unit The Netherlands, where every location has its own type of product storage or handling, resulting in other OT systems with many variances of OT suppliers, including other frequencies of security patching. Where the ongoing operations make it more challenging to install updates or perform security patching. However, even for one type of OT systems (for example, CCTV monitoring system), multiple OT suppliers are contracted within the same Business Unit. Resulting in the fact that every location is reinventing the wheel and needs to incorporate already existing knowledge of other locations.
4. Technical malfunctions can result in (safety) risks or errors within the OT system due to the end-of-life assets within the OT system, causing an inability to update the digital environment (e.g. Windows) on the specific asset of the OT system (e.g. when an OT system is operating based on a Windows 7 environment). More extreme consequences of the unavailability of OT systems are causing risks of *location downtime* since the OT system cannot be used, and ongoing operations are disrupted. Much production time might be lost in finding the cause of technical malfunctions or the unavailability of the OT systems.

Four opportunities were identified:

1. Incorporate more recommendations into the current state of the security patching processes of the selected case study organisation via recommendations of audits internal (or external) audits.
2. Incorporating the usage of a secure file transfer systems (e.g. *Datasluis*) within the selected case study organisation's security patching processes. Nowadays, the to-be-installed data is brought to the location by the OT suppliers via USB sticks for transferring and installing data and software towards OT systems. Risks arise from unwanted data (malware or viruses) installed on the OT systems at the selected case study organisation's locations.
3. Deploying the knowledge of more mature stakeholders within the industry to SLAs with other OT suppliers regarding insights into general processes or operations of security patching or cybersecurity.
4. Develop strategies to make current security patches more efficient when operations are paused (planned *location downtime*). Security patching could be simultaneously deployed to more OT systems' assets when ongoing operations are paused (*location downtime*). Security patching is time-consuming, with much idle time when the OT supplier expert cannot perform any other work and has to pay attention to perform actions related to security patching.

Three threats were identified:

1. Risks of cyber breaches are lurking, where vulnerable information about OT suppliers' log-in credentials for OT systems at the selected case study organisation's locations can be exploited due to a cyber hack. This also applies to password rotation in cases where OT suppliers' employees could forget these passwords and when OT suppliers' employees are uncertain about the availability of these OT systems when passwords are changed since passwords have to be inserted after the reboot of an OT system during security patching.
2. Since OT suppliers are responsible for security patching, it is a threat that they cannot arrange to perform security patching within the appropriate time. Delays for security patching may occur (with the risk that a vulnerability compromises an OT system at the selected case study organisation's locations) when the local operations department does not approve *location downtime*.
3. The selected case study organisation depends on the knowledge of the OT suppliers' experts who perform security patching on their OT systems at the selected case study organisation's locations. Each location is a highly integrated, complex landscape of multiple OT systems of different OT suppliers, which cannot permit malfunctioning systems due to missed patches. There is a lack of information about the overview of the already installed updates of these assets for the selected case study organisation, supplemented by an OT supplier performing an update on one of the assets. Further in-house knowledge levels regarding security patching, risk management and problem-solving within this environment ares missing.

Chapter 6: How are the security patching processes governed within the operational domain?

The current state of the selected case study organisation's security patching processes is examined, where interactions between the technical systems and the human actors when performing security patching are described in Chapter 5, resulting in strengths, weaknesses, opportunities, and threats. The second phase of this research is to explore how the governance surrounding security patching processes influences the effectiveness of security patching processes and coordination provided by its stakeholders. Therefore, an internal document analysis is performed in Chapter 6.1. The analysis of the policy foundation of the selected case study organisation's governance regarding the security patching processes is assessed in Chapter 6.2. Three semi-structured interviews with the selected case study organisation's employees were conducted as expert interviews, and these results can be seen in Chapter 6.3. The chapter finishes with a conclusion of the second sub-research question in Chapter 6.4.

6.1 Internal document analysis

An internal document analysis was conducted based on four internal documents of the selected case study organisation regarding the security patching processes, where interesting insights of each OT Security document can be seen in the designated subchapters: 1) OT Security Policy (Chapter 6.1.1), 2) OT Security Requirements (Chapter 6.1.2), 3) OT Security Standard (Chapter 6.1.3), and 4) SLA addendum for OT Security Requirements (Chapter 6.1.4). The documents were analysed via reflexive thematic analysis within the data analysis tool Atlas.ti to determine how the governance related to security patching processes is implemented and governed within the operational domain. The created codes resulting in code groups during the thematic analysis can be seen within the codebook in Appendix 5. Next, a comparison of these documents is provided in Chapter 6.1.5, which made it easier to implement the insights from the internal document analysis into the questionnaires of both semi-structured interviews with the selected case study organisation's experts (Chapter 6.3) and OT suppliers (Chapter 7).

6.1.1 The selected case study organisation OT Security Policy

The selected case study organisation's OT Security Policy (CIS-P-003) is the starting document for the internal document analysis. This document aims to *"provide guidance and direction regarding security for all OT systems on the selected case study organisation"*, as stated in the document. The selected case study organisation refers to this document as the 'what', which is what mandatory objectives for OT all locations must adopt. The document of the selected case study organisation OT Security Requirements (assessed in Chapter 6.1.2) assesses 'how' this policy will be secured.

The references within the document, leading towards other related documents, are failing. Therefore, the background information towards these references cannot be checked. It is stated in the document itself (OT Security Policy) that only two components of the ISA/IEC62443 are included as the policy foundation (components 2-1 and 3-3). Component 2-1 relates to '*Security program requirements for IACS asset owners',* and component 3-3 relates to '*System security requirements and security levels'*. It is unclear why the other components are not included in the specific sub-sections, such as component 2-3, related to *'IACS Patch Management'*.

Next to this, it can be seen that the selected case study organisation assessed themselves at a level-3 maturity level in their cybersecurity practices for all OT. The document states that these maturity levels are *"used to describe a development roadmap for capabilities within an organisation, where 'maturity' relates to the degree of formality and optimisation of processes and controls"*. Five maturity levels can be seen starting at 'Initial' (level 1), 'repeatable/informal' (level 2), 'structured & formalised' (level 3), 'implemented & periodically assessed' (level 4), and 'optimised' (level 5). According to the document, *"It is the selected case study organisation's ambition to achieve a maturity level that provides for formal and optimised cybersecurity practices for all OT"*, which refers to level 5 'optimised'. However, it is not substantiated why the selected case study organisation currently places themselves in level 3, 'structured & formalised'.

Moreover, the selected case study organisation generated its own Global OT Security Framework and Vendor Requirements, as shown in Figure 6.1 below. It can be seen that Patch Management is included within the 'Prevent' section of the framework. the selected case study organisation states that the 'Prevent' section serves *"to develop and implement appropriate safeguards protecting against and/ or mitigating the impact of cyber security events to OT systems and assets"*. For each 'prevent' sub-section, a more detailed description of practical implementations of the OT Security Policy is described.

This information has been removed within this published external version of the thesis due to sensitive information of the case study organisation.

Figure 6.1: Global OT Security Framework and Vendor Requirements (Selected case study organisation OT Security Policy document, 2021)

It can be seen that the only information related to the OT Security Policy is presented in Figure 6.2 below. There is a reference to the OT Security Requirements document, which will be assessed in Chapter 6.1.2. Still, it can be concluded that the amount of information within the OT Security Policy consists of minimal substantiation. In this document, 'patches' are being used as *"currently installed versions and the released versions of systems that are in use"*, not as *"additional pieces of code developed to address problems in software. Patches are also known as bugs, whereby they enable* *additional functionality or address security flaws within a program"*, as stated by Mell et al. (2005), how the terminology of patches is used within the academic environment.

This information has been removed within this published external version of the thesis due to sensitive information of the case study organisation.

Figure 6.2: OT Security Policy related to security patching (Selected case study organisation OT Security Policy document, 2021)

Then, the document covers all the selected case study organisation locations, joint ventures, and associated third parties, where third parties are included as: "*all suppliers, vendors, integrators or contractors who access, support or manage the selected case study organisation's OT systems or are involved in the implementation and integration of new or legacy OT systems"*. It is stated that third parties "*who access, support or manage the selected case study organisation's OT systems are responsible for ensuring that the requirements are adhered to and that they operate systems in such manner as to ensure security"*, where within this research, third parties are referred to as 'OT suppliers'. However, it is unclear how the selected case study organisation guarantees that the OT suppliers will ensure that the requirements are adhered to, and it is unclear how OT suppliers will ensure this security.

In addition, the document states that management at all levels is responsible and accountable for *"ensuring that users are aware of and adhere to these requirements and associated policies"*. Based solely on the document, it is unclear how the users are aware of and adhere to the requirements and associated policies. Internal Expert 1 should be notified in cases where *"the applicability of the requirement(s) is/are in question for a particular system or asset, Internal Expert 1 must be notified"*, as stated in the document. Information is lacking to determine who is notifying Internal Expert 1, when this situation will occur.

More importantly, the selected case study organisation uses contradictory language. The document describes the following distinction of terminology, but unclarity arises by the use of the distinction of terminology:

- *Shall* and *Must* both mean 'a mandatory requirement'
- *Should* mean 'a preferred method of action (best practice)'
- *May* and *Could* and *Might* mean 'a possible method of action'

As a result of this, in the document, it is stated that the document "*shall be reviewed annually or when required/requested by the document owner"*, it is given that the selected case study organisation's Internal Expert 1 is the owner of this document. And since *Shall* means 'a mandatory requirement', it is odd that the latest revision date of the document, according to the revision history of the document itself, is dated 22 December 2021, which is almost three years ago. So, the little available information regarding the selected case study organisation's OT Security Policy about security patching causes unclarity, contradictory use of language and subordinated review cycles of the document itself.

6.1.2 The selected case study organisation OT Security Requirements

As said in Chapter 6.1.1, the selected case study organisation refers to the OT Security Policy document as the 'what', which is what mandatory objectives for OT all locations must adopt. This document, the selected case study organisation OT Security Requirements (CIS-S-504), assesses 'how' this policy will be secured. According to the selected case study organisation, this document is *"to safeguard the* *selected case study organisation's OT against unauthorised access, modification and to ensure availability, integrity and confidentially of operational processes"*.

Compared with the selected case study organisation's OT Security Policy (Chapter 6.1.1), the following similarities can be seen:

1. The references within this document, leading towards other related documents, are also failing. Therefore, the background information towards these references cannot be checked.
2. The same components (2-1 and 3-3) of ISA/IEC62443 are included as the policy foundation of this document.
3. The underlying framework for this document is equal to the earlier assessed policy document, namely, the selected case study organisation's Global OT Security Framework and Vendor Requirements, see Figure 6.1.
4. The scope of this document is equal to the scope of the earlier assessed policy document.
5. The use of language and the requirement for document review is equal to the earlier asses policy document.
6. The terminology of *patches* in this document is also used differently than academia.

As for other interesting insights, it can be seen that the selected case study organisation included more information within the OT Security Requirements document, which can be seen in Figure 6.3 below, compared with the OT Security Policy document, which can be seen in Figure 6.2. Still, there is only a small amount of information available for the requirements related to patch management. Related references for OT requirements of patch management are based on ISA/IEC62443 component 2-1 (regarding security program requirements for IACS asset owners). Oddly, the component of ISA/IEC62443 about IACS Patch Management (component 2-3) is not included as a basis for these requirements regarding patch management. The selected case study organisation also states that the objective for these requirements is that *"a procedure for patch management shall be established, documented and followed"*. However, it is unclear how this procedure looks like, how it is documented and followed, and by whom. Besides that, the document refers to *Chapter 4.3.4.3 System development and maintenance*, however, this chapter does not exist at all.

When looking at the stated requirements for patch management, it can be seen that these are divided into three sub-categories: 1) software update management and maintenance, 2) patch testing and verification, and 3) patch installation. While this document should provide information on 'how' the OT Security Policy will be secured, the document is not specific at all. It is not clear from the first sub-category of these requirements regarding 'software update management and maintenance', how the location *shall* establish and maintain for each device an accurate record of the currently installed software versions, nor does it state how locations review if updates are available for the installed software versions are available for the OT systems. It does not state how compensating countermeasures have to be implemented to mitigate security vulnerabilities or what the procedure is for installation of patches qualified as 'emergency patches', where it is not described what the requirement is in order to label a patch as 'emergent'.

Unclarity continues within the second sub-category, 'patch testing and verification'. The document states that the *"supplier of software applications must qualify and test all operating system patches and software application patches for applicability and compatibility with the selected case study organisation system setup for the OT systems use these software applications"*, however, it is unclear how these OT suppliers will perform this and how the selected case study organisation controls the OT suppliers for this requirement. Neither is it stated at what frequency the OT supplier shall provide a list of all patches and their approval status since it is only noted that the OT suppliers *should* inform The selected case study organisation's locations within ten days after the OT supplier of the operating system or software releases a patch.

As for the last sub-category, 'patch installation', these requirements are still not yet concrete, where even within this last sub-category, unclarity has risen. It is stated that *"a risk-based approach shall be used to define the patch update frequency for (critical) systems"*; however, it is not defined which risk-based approach is used and with which risk appetite or global guidelines it should be aligned. The document states that *"OT suppliers shall provide documentation describing the software security patching policy for the products and systems they supply"*, but it is unclear where this documentation can be seen, who has the responsibility to store this documentation, and if the selected case study organisation even assesses, control or manage this for both manually performed security patching, as via a patch management server.

The document mainly states that these OT Security Requirements must be performed, but guidance about how this will be performed is missing. This is odd since the OT Security Requirement document should assess 'how' the policy is secured. Still, concrete guidance regarding the 'how' is missing for implementing quality checks or another form of control. It can also be concluded that it is unclear how the selected case study organisation can ensure that the OT suppliers do as they *shall*, according to the patch management requirements in this document.

This information has been removed within this published external version of the thesis due to sensitive information of the case study organisation.

Figure 6.3: OT Security Requirements related to security patching (Selected case study organisation OT Security Requirements document, 2021)

6.1.3 The selected case study organisation OT Security Standard

The selected case study organisation's OT Security standard is developed to guide location management in obtaining compliance with the selected case study organisation's OT Security Policy and Requirements documents. This is executed by providing the tools and support to assist location management in managing their OT security. The introduced concepts and tools help the location stakeholders to identify cybersecurity risks and gaps in their OT environment, procedures and organisational arrangements. According to the selected case study organisation, the OT Security Standard will help to assess and prioritise the security gaps to define a location plan or roadmap for embedding OT security in the location. Related documents are linked within the document, where a presentation can be found with an introduction to the OT Security Standard, including an intake assessment to start the implementation of the OT Security Standard. The underlying framework of this document is the selected case study organisation's OT Security framework, shown in Figure 6.4 below. Compared with the earlier mentioned Figure 6.1, the framework is expanded by the 'Prepare' phase. According to this document, this phase involves *"developing the organisational understanding of the cybersecurity risks to OT, where identifying and understanding the risks to OT are required to create appropriate safeguarding measures to manage OT security"*.

This information has been removed within this published external version of the thesis due to sensitive information of the case study organisation.

Figure 6.4: Global OT Security Framework and Vendor Requirements (Selected case study organisation OT Security Standard document, 2020).

Furthermore, within the 'Prepare' phase, the roles and responsibilities which are relevant for OT security in the (location) organisation are provided as well, where a division is made between the following stakeholders:

- Location manager/asset owner
- Technical manager/maintenance manager
- Site focal point for OT security
- OT supplier
- Divisional IT/OT manager
- Corporate information security team
- Global IT/OT manager

The roles and responsibilities of the OT supplier can be seen in Figure 6.5 below. It can be seen that the roles and responsibilities towards the OT suppliers are focussing on vulnerability management as: "*Providing the selected case study organisation with timely information about cybersecurity threats and vulnerabilities in supplier supplied systems and services"*, and for patch management: *"Responsible for providing patch updates, back-up and restore capabilities (in collaboration with Site Focal Point) and advice for system hardening)"*. However, no other roles and responsibilities are obligated by the OT supplier.

This information has been removed within this published external version of the thesis due to sensitive information of the case study organisation.

Figure 6.5: Roles and responsibilities OT supplier (Selected case study organisation OT Security Standard document, 2020).

When looking at the 'Prevent' phase, this document describes several preventive measures which involve developing and implementing safeguards to protect and mitigate the impact of cybersecurity events on OT systems and networks. The preventive measures include security awareness, access control, secure remote access, network segmentation, asset management, system hardening, backup and patch management. However, the only included preventive measure for patch management is focused on *"ensuring that risks from new vulnerabilities for OT systems and software do not increase over time, due to missing patches or legacy software platforms"*, but it is not stated how this is to be ensured by the OT supplier when the vulnerabilities or risks are increased over time. It is not stated how missed patches will be identified nor how often the legacy software platforms will be checked for new vulnerabilities. Guidance about patch log processes, including documentation, is also missing in this document.

Within the 'Detect' phase, the document focuses on the timely detection of the occurrence of a cybersecurity event, which is crucial to reducing the potential business impact of the incident. The document states that *"procedures and solutions need to be developed and implemented to help identify cybersecurity events quickly when they occur"*. However, it does not say how these procedures and solutions must be developed and implemented. Moreover, it includes three activities: 1) logging and monitoring, 2) vulnerability management, and 3) endpoint protection. It can be seen that patch management is not included in this phase, while *location downtime* could significantly impact potential business disruptions when security patching is not performed frequently or when no published updates are installed at all.

The 'React' phase gives insights into react measures when adequate mitigation action is required after a cyber security incident is detected. This may involve system-specific action but also require location- or the selected case study organisation-wide mitigation measures. These are crucial to recover quickly and minimise the impact on the ongoing operations of the selected case study organisation's location. This phase focuses on two activities: 1) restoration and 2) incident management. The react measure 'restore' focuses on the backup as a reactive action with an acceptable data loss and testing these backups. The react measure 'incident management' involves predefined incident response- and communication plans which can be used when cyber security events are detected. However, within this document, it is unclear what these plans look like. In addition, patch management is not included in this phase again. Therefore, it is unclear how the location management will react or what steps must be performed when a vulnerability occurs and the OT system has to be patched.

Lastly, some other interesting comments on this document are: 1) the selected case study organisation describes eight definitions: asset, business continuity plan, IT, legacy system, OT, security event, SLA, and vulnerability. However, *security patching*, *patch management,* or *patch* as a concept is not enlightened and could significantly affect location operations. 2) The first step of the location OT security plan is to identify and understand the existing cybersecurity risks and gaps in OT. This is executed by a location assessment of the OT domain, security procedures, and organisational arrangement at the location. The OT security assessment questionnaire must be filled out, which consists of different focus areas in which a specific role (location management, OT focal point, OT supplier and Global IT) is responsible for answering these questions.

Each questionnaire has been thoroughly investigated, and it can be concluded that within this OT security assessment, patch management is not included in the questionnaire for location management; it is only included in the questionnaires for both the OT Focal Point and the OT suppliers, which can be seen below respectively in Figure 6.6 and Figure 6.7. However, very few questions are asked regarding security patching. Furthermore, no questions about the security patching processes, patch logs with follow-up actions or times, or patch log documentation are asked. These questionnaires do not ask the OT Focal Point or the OT suppliers how, when, and if they will identify vulnerabilities that could be exploited to violate the system's integrity.

This information has been removed within this published external version of the thesis due to sensitive information of the case study organisation.

Figure 6.6: OT Security Questionnaire patch management OT Focal Point

This information has been removed within this published external version of the thesis due to sensitive information of the case study organisation.

Figure 6.7: OT Security Questionnaire patch management OT supplier

6.1.4 SLA addendum: OT Security Requirements

The last assessed document within the internal document analysis of this research is the selected case study organisation's SLA addendum: OT Security Requirements. The selected case study organisation introduced security requirements at the end of July 2023 to protect its operational assets against cybersecurity threats via this addendum to the OT security requirements of the SLA. Since the OT suppliers manage their OT systems, the selected case study organisation derived this SLA addendum: OT Security Requirements, which states that OT suppliers must meet these security requirements during the ongoing operations. The security requirements within this document focus on four topics: reporting, anti-virus, operating system updates, and backup/restore, which can be seen in Figure 11.2 in Appendix 2.

In the document, the selected case study organisation restricts that the OT supplier *"shall ensure that the patch levels of the operating systems shall be kept current to within at least 12 months of the security patch being available"*. However, the concept of 'patch levels' within this document is used as terms of update and installation, instead of the use of patching as in: *"Additional pieces of code developed to address problems in software. Patches are also known as bugs, whereby they enable additional functionality or address security flaws within a program"* as stated by Mell et al. (2005). It is also unclear how these patch levels shall be kept current; in other words, how do the OT suppliers know that these patch levels are current?

Furthermore, this document does not indicate concrete measurements regarding security patching. Since these stated requirements are drafted as: *"supplier shall provide vulnerable information about their installed system"*, based solely on this requirement, it is unclear at which period the OT supplier shall provide vulnerable information. Besides that, in cases where OT suppliers do not give any vulnerable information, it is unclear to the selected case study organisation if the OT systems are vulnerable or not. More unclarity arose where answers cannot be found for these generated questions, based on the document:

- How does the OT supplier know when an installed OT system is vulnerable?
- How are vulnerabilities being managed by the OT supplier?
- How must the OT supplier act when vulnerabilities are identified in the selected case study organisation's OT systems' cybersecurity environment?
- Within which amount of time vulnerabilities should be patched?
- What KPIs are used to determine each OT supplier's performance regarding these OT Security requirements?
- Which responsibilities do the selected case study organisation and the OT supplier have regarding patch management?
- Who has ownership of created patch logs in terms of a reported vulnerability?
- Within which amount of time do follow-up actions have to be performed by the OT supplier based on security patching?

- How reliable is this current SLA addendum?
- Which quality checks are performed by the selected case study organisation on each OT supplier?

6.1.5 Comparison OT Security documents

Since all the OT Security documents are analysed individually, it is necessary to assess if they align. As said earlier, the OT Security Policy document (Chapter 6.1.1) should explain what mandatory objects all locations must adopt for the OT Security Policy. The OT Security Requirements document (Chapter 6.1.2) should assess how this policy will be secured. Next, the OT Security Standard document (Chapter 6.1.3) should guide location management in obtaining compliance with the selected case study organisation's OT Security Policy and Requirements documents by providing a questionnaire and an introduction presentation. Lastly, the SLA addendum regarding OT Security Requirements should give the OT supplier additional OT Security Requirements to protect its operational assets against cybersecurity threats. The selected case study organisation derived this SLA addendum since the selected case study organisation outsourced the management of the OT systems to each OT supplier. It is stated that OT suppliers must meet these security requirements during the ongoing operations. Via the outcomes of the reflexive thematic analysis within Atlas.ti, these four documents were compared with each other. Based on the derived codes during the reflexive thematic analysis, a codebook was generated, which can be seen in Appendix 5, and the following conclusions can be drawn:

1. It is unclear why other components of the ISA/IEC62443 (such as components 2-3 for IACS Patch Management) are not included as the policy foundation of the OT Security Policy and Requirements documents, and therefore, neither in the OT Security Standard.
2. The documents lack reasoning as to why the selected case study organisation is currently located at the third maturity level, which describes the roadmap for capabilities within an organisation.
3. It is unclear how the selected case study organisation's management ensures that users are aware of and adhere to the OT security requirements and associated policies, including that OT suppliers will ensure the security of these OT systems.
4. It is unclear how the selected case study organisation communicates amongst the multiple stakeholders at the locations since misalignment about terminologies, such as the terminology about patches, can be seen.
5. It is odd that the latest revision date of the OT Security Policy and OT Security Requirement was 22 December 2021, which is almost three years ago, since the OT Security Policy document states that the document *shall be reviewed annually or when required/requested by the document owner* (the selected case study organisation's Internal Expert 1). According to the document, the review cycle for the OT Security Standard, where the latest revision was in November 2020, is not specified.
6. The documents do not state how the OT supplier ensures preventive measures for patch management, such as when vulnerabilities or risks increase over time, how missed patches are identified, and how often the legacy software platforms are checked for new vulnerabilities.
7. Information about procedures for patch management, including creating patch logs and ownership of the patch logs, along with their follow-up actions and its guidance about these security patching processes, including documentation, cannot be found within these documents.
8. Patch management is not included in the 'detect' or 'react' phase of the OT Security Standard. This is essential since *location downtime* could significantly impact potential business disruptions when security patching is not performed frequently. This makes it unclear how the

location management reacts or what steps must be taken when a vulnerability occurs, and the OT systems must be patched.

9. How procedures and solutions must be developed and implemented to detect the occurrence of cybersecurity events timely is also left behind.
10. Each sub-section of the OT Security questionnaire shows that patch management is not included in the questionnaire for location management; it is included in the questionnaires for both the OT Focal Point and the OT suppliers. These questionnaires do not ask the OT Focal Point or the OT suppliers how, when, and if they will identify vulnerabilities that could be exploited to violate the system's integrity.

It can be concluded that the amount of information regarding patch management consists of minimal substantiation in all assessed documents within this internal document analysis. The documents are not specific or measurable, and timeframes within the stated requirements are also missing. Implementing these documents is very difficult since there is a lack of guidance and communication between the multiple stakeholders. Most importantly, according to these four documents, it is unclear how the selected case study organisation knows that their OT suppliers do as they are required to since there is lacking evidence of concrete, measurable quality checks within a certain timeframe. With the result that the governance and coordination provided by its stakeholders surrounding security patching processes are not effective at all.

6.2 Policy foundation of security patching governance at the selected case study organisation

The policy foundation of the selected case study organisation's OT Security Policy is based on the ISA/IEC62443 Series of International Standards for Industrial Automation and Control System (IACS) Security, as stated in the document, where components 2-1 and 3-3 are included. Since the OT Security Standard is the translation of the selected case study organisation's OT Security Policy and Requirements documents, these two components are also the foundation for the standard. According to ISA Global Cybersecurity Alliance (ISAGCA) (2024), the ISA/IEC62443 Series of International Standards *"define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS)"*. These standards set best practices for security and provide a way to assess security performance (ISA Global Cybersecurity Alliance (ISAGCA), 2024). Their approach is to bridge the gap between operations and information technology as well as between process safety and cybersecurity. Figure 6.8 below shows the most commonly used description, as Cosman (2020) indicated.

When looking at the included component 2-1, *"Security program requirements for IACS asset owners",* Cosman (2020) describes that components in that layer 'Policies and procedures' focus on the policies and procedures associated with IACS security. In detail, component 2-1 describes what is required to define and implement an effective IACS cybersecurity management system, where the intended audience includes end-users and asset owners responsible for designing and implementing such a program (Cosman, 2020). Component 3-3, *"System security requirements and security levels"*, lies in the layer 'System', where this third layer addresses requirements at the system level. The component provides the foundations for assessing the security levels provided by an automation system, where the principal audience includes suppliers of control systems, system integrators, and asset owners (Cosman, 2020).

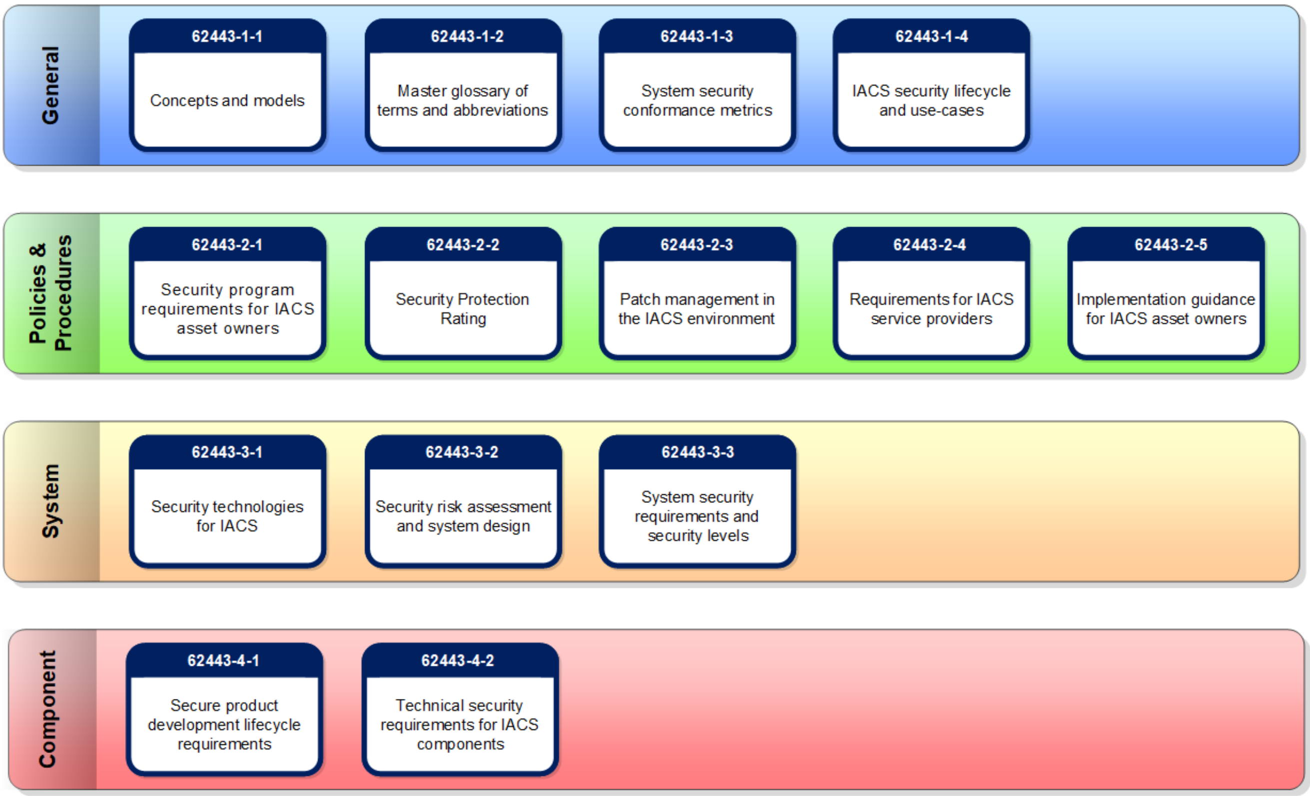

General
62443-1-1
Concepts and models
62443-1-2
Master glossary of terms and abbreviations
62443-1-3
System security conformance metrics
62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
62443-2-1
Security program requirements for IACS asset owners
62443-2-2
Security Protection Rating
62443-2-3
Patch management in the IACS environment
62443-2-4
Requirements for IACS service providers
62443-2-5
Implementation guidance for IACS asset owners
System
62443-3-1
Security technologies for IACS
62443-3-2
Security risk assessment and system design
62443-3-3
System security requirements and security levels
Component
62443-4-1
Secure product development lifecycle requirements
62443-4-2
Technical security requirements for IACS components

Figure 6.8: Diagram ISA/IEC62443 Series of Standards (Cosman, 2020).

When looking at the ISA/IEC62443, a separate component dedicated to patch management in the IACS environment is available (component 2-3) but is left out of the selected case study organisation's OT Security documents. The reason why this component is left out is unclear and not retrievable within the documents. Component 2-3 provides guidance on patch management for IACS, according to Cosman (2020). The intended audience includes anyone responsible for the design and implementation of patch management discipline within the second layer of 'Policies and procedures' (Cosman, 2020).

6.3 Semi-structured interviews with the selected case study organisation's employees

As a result of the direct observations (Chapter 5) and the internal document analysis (Chapter 6.1), multiple questions have arisen about why and how the selected case study organisation has regulated its cybersecurity governance relating to security patching processes. Because of this, three semi-structured interviews were conducted with the selected case study organisation's employees: Internal Expert 1 of the selected case study organisation, Internal Expert 2 of the selected case study organisation and Internal Expert 3 of the selected case study organisation. Based on the insights of the observations and the internal document analysis, the generated questionnaire for the three semi-structured interviews with the selected case study organisation's expert employees can be seen in Appendix 3. Based on the three transcripts, a reflexive thematic analysis was performed to indicate themes amongst the participant's answers (Chapters 6.3.1 to 6.3.4), whereby the created codes during the thematic analysis can be seen within the codebook in Appendix 6.

6.3.1 Outsourced responsibilities

The responsibilities of the interviewed the selected case study organisation experts are as follows:

- Internal Expert 1 is responsible for the information security policy of both IT and OT domains globally at the selected case study organisation. That responsibility also includes cyber resilience, follow-up of incidents and ensuring that the selected case study organisation remains compliant with local laws and regulations, specifically regarding information security and its policy.
- Internal Expert 2 is responsible for implementing and maintaining the OT systems at the locations within the Business Unit The Netherlands.
- Internal Expert 3 is responsible for bringing OT-specific knowledge to the team to make policy, give advice, share best practices and lessons learned, and raise awareness.

During the interview, Internal Expert 1 said that an important feedback loop is to advise on how to act instead of indicating how many mistakes people have made. Within the selected case study organisation, it is essential to create awareness, promote acceptable use, indicate non-acceptable use, and share near misses and incidents. Lessons learned or improvements are collected and implemented within a working document of these policy documents. According to Internal Expert 1, Internal Expert 3 will update these documents as soon as something has to be added. In addition, Internal Expert 3 adds the following topics, which are also to be included within these documents for improvements: industrial best practices, findings on how to protect towards (cyber) attacks and best methods for resolving vulnerabilities. However, it is unknown when the new versions of these policy documents will be made accessible or can be used since the documents are currently being improved.

Internal Expert 1 said during the interview that the entire scope of managing each contract with an OT supplier, about a specific OT system, is divided towards the contract owner. The contract owner is an employee of the selected case study organisation at the specific location. Since the contract with the OT supplier is locally procured, the local contract owner is also responsible for cybersecurity, where sometimes a global component is involved, in terms of preferred OT suppliers, for example. On this local level, the performance of the specific OT supplier is discussed to ensure the quality of the OT systems. It is also possible that OT systems from one OT supplier are applied within the whole Business Unit (not globally). In that case, the contract owner is responsible for the contract with that OT supplier for multiple locations.

The selected case study organisation entirely depends on the OT suppliers regarding vulnerability and patch management. The selected case study organisation *should* be informed when the OT supplier discovers a vulnerability in the IT and OT domains. However, when a vulnerability occurs, the local contract owner has to mitigate the vulnerability with appropriate measures. Internal Expert 2 said in the interview that*: "the OT landscape is very diverse with a lot of OT suppliers and OT systems; I think we need to move more towards a more standardised landscape so that we can organise cybersecurity better and more efficiently."*. The reason why these responsibilities are outsourced towards the OT suppliers are stated as follows by Internal Expert 2: *"The selected case study organisation's strategy is that we want to be unburdened by the OT suppliers. We buy a system; we conclude an SLA, assuming that the OT supplier will manage the OT system for us, including cybersecurity"*. Regarding the OT supplier's responsibility, Internal Expert 3 responded to this topic as follows: *"there is no role of OT supplier responsibility if you don't assign this with actions to the OT supplier"*. Therefore, it can be concluded that the OT suppliers are not under the selected case study organisation's control, as they are granting the responsibilities in this way.

6.3.2 Lacking communication at the selected case study organisation

The Global IT/OT team (of Internal Expert 1) mainly focuses on IT governance, and only one the selected case study organisation Employee (Internal Expert 3) is available to guide OT-specific topics at the selected case study organisation. There is very little cooperation between the Global IT/OT team and the team of Internal Expert 2. According to Internal Expert 1, *"The cooperation is very simple; this is less formally recorded. Eventually, only one person is accountable for the policy itself, not the implementation or operations. I rapport to CFO, via the CIO, where the CFO is also responsible for the operations. Via that route, some policy can be changed and implemented within Operations"*. Internal Expert 2 directly rapport to the management team of Business Unit The Netherlands. When questions are asked towards Internal Expert 2 about sharing lessons learned or knowledge, no formalised procedure of knowledge sharing is currently active. Internal Expert 2 connects the selected case study organisation employees when best practices or lessons learned have to be shared. Criticism of this knowledge-sharing method is that something could be forgotten within the selected case study organisation's high-complexity OT landscape.

Before the interview, department procurement was asked to deliver an overview of all the OT suppliers who maintain a business service at the locations of Business Unit The Netherlands. Unfortunately, this overview could not be given by the department procurement. During the interview with Internal Expert 2, it became clear that the department procurement of the selected case study organisation is not focused on OT suppliers. The department works with a Procurement Management System, where OT suppliers are not classified. OT systems and OT suppliers can be retrieved from another internal system called *Service Now*, where assets are registered, including their maintenance and life-cycle management. Conclusions can be drawn that communication between department procurement, department operations and the Global IT/OT team at the selected case study organisation is lacking.

6.3.3 No regular quality checks on OT suppliers by the selected case study organisation

During the interviews with the selected case study organisation's experts, an important topic was discussed: the SLA addendum of the OT Security Requirements (Chapter 6.1.4). This document was introduced to protect the OT systems against cybersecurity threats via the described OT security requirements (Appendix 2). When questions were asked of Internal Expert 1 about how the selected case study organisation knows that their OT suppliers do as they are required to, since there is lacking evidence of concrete, measurable quality checks within a certain timeframe, no concrete answer could be provided by Internal Expert 1. It can be seen that no KPIs are used within this document. Internal Expert 1 responded towards this observation that: *"that is not a security question, but a procurement question"*, and *"these should be placed locally at each location, at each contract owner"*.

According to Internal Expert 1, the current SLA addendum is a template, not an active document, where, at the same time, this SLA addendum is active at the locations. Internal Expert 2 states that this document was created by an employee of the Global IT/OT team of the selected case study organisation, supervised by Internal Expert 1. So, it is odd that Internal Expert 1 doesn't know that this SLA addendum exists and/or is operative for all OT suppliers within Business Unit The Netherlands. Where Internal Expert 1 states, "*it doesn't tell me anything about the document's validity"*.

In addition, the selected case study organisation Global has no established KPIs for OT. As Internal Expert 2 stated, this is *"because the OT Security Standard is not yet implemented globally. Many Business Units are struggling with implementing that, so, reporting on KPI is not yet applicable. We are focussing now on completing the implementation of the OT Security Standard."*, where later KPIs will follow. Looking at the SLA addendum, the stated OT Security Requirements are not concrete at all, and assessing the performance of these requirements is challenging. When questions are asked towards Internal Expert 2, about assessing the OT suppliers' performance, the answer is as follows: *"There are* *no concrete plans about that yet; it will happen since the laws and legislations have changed"*. However, Internal Expert 3 stated that *"KPIs are 100% applicable on the OT, such as security, reliability and productivity KPIs"*. Internal Expert 3 also explains that checking the performance of OT suppliers is *"a new topic for the industry"* since, in earlier days, OT suppliers only engineered and tested the OT systems. Cybersecurity had no part in it. Moreover, this same person states: *"now, security levels are generated, security requirements are developed, and the security is tested"*. However, it appeared that not all locations can assess the OT suppliers' performance due to limitations in available labour or knowledge of the selected case study organisation's local employees.

Another fascinating insight, based on the expert interviews, is that the selected case study organisation doesn't check CVE, according to Internal Expert 1. This is in contrast to when this question was asked towards Internal Expert 2: *"The Global IT/OT team should monitor if vulnerabilities occur within the industry"*. Whereas Internal Expert 3 said that checking CVE is part of the SLA with the OT supplier where *"for new vulnerabilities, which are recorded via CVE, the OT supplier will inform the selected case study organisation and immediately install the patch if the vulnerability was applicable for OT systems at the selected case study organisation's locations".* Conclusions can be drawn that neither the selected case study organisation's experts monitor the publication of CVEs, and OT suppliers *should* monitor this. However, whether OT suppliers check the CVE is being questioned.

Internal Expert 1 explained that possible vulnerabilities are only investigated by the selected case study organisation through the use of audits (internal or external). Based on these audits' observations, recommendations are composed to resolve the potential vulnerabilities, where these recommendations are transformed into actions, and these actions have to be followed up. Regarding cooperation between Internal Expert 1 and Internal Expert 2, Internal Expert 1 organises and directs the audits, and Internal Expert 2's team is audited by the organisation that performs the audit (internal or external). In the opinion of Internal Expert 2, audits should reveal whether the locations, including the OT suppliers, are performing as they are required to, based on the OT Security documents (policy, requirements, standard and SLA addendum).

Other quality checks at the selected case study organisation's locations are performed by independent bodies or government agencies that perform those quality checks, as explained by Internal Expert 2. For example, the National Digital Infrastructure Service (Dutch: *Rijksdienst Digitale Infrastructuur*) tests the selected case study organisation against European legislation and regulations, such as the European Network and Information Security (NIS2) directive. But also organisations such as DCMR, which performs audits surrounding environmental services, or the Dutch Ministry of Infrastructure and Water Management, which performs audits surrounding major accident risk accidents (Dutch: *Besluit risico's zware ongevallen*). Eventually, company inspections are organised where security components are included more often. However, no frequent quality checks are performed by the selected case study organisation itself towards the OT supplier based on the OT Security documents. Therefore, it is also challenging to assess if the OT supplier is in control of the stated agreements.

6.3.4 Contradicting governance

As stated by Internal Expert 1, the reason why only components 2-1 and 3-3 of the ISA/IEC62443 are included within the OT Security documents is that *"that is very basic because in those components the relevant information is included. The framework consists of more components, but they are not all relevant to the selected case study organisation's actual information security policy. Within the referenced components, that is where the technical measures are described and those end up in the policy"*. An answer was lacking when it was asked why component 2-3 is not included (patch management in the IACS environment) in the selected case study organisation's OT Security documents. Internal Expert 2 does not know this answer either since the answer to the same question was as follows: *"No, I have no idea because those are IT standards. So, I have no idea, and I have not been involved."*. In that case, it is extraordinary that the OT Security Policy, Requirements and Standards are based on an IT rather than an OT standard. Internal Expert 3 replies to the very same question: *"because the selected case study organisation does not perform security patching itself in the OT environment; this is done by the OT suppliers"* and *"it is the OT suppliers' responsibility and the OT suppliers' product. Whatever patch needs to be updated, the OT supplier will come and patch it; that's why it's the OT suppliers' responsibility"*.

Next to this, Internal Expert 3 of the selected case study organisation states that other frameworks are included next to the ISA/IEC62443, namely the NIST800-82 (a guide to improve OT security (Stouffer et al., 2022)), which is dedicated to OT and NIST800-53 (relating to security and privacy controls for information systems and organisations (NIST, 2020)), which is dedicated to IT. However, these frameworks cannot be found within the selected case study organisation's OT Security documents. Internal Expert 3 also says that ISA/IEC62443 component 3-2 is already incorporated into the selected case study organisation's current practices; this cannot be seen within the current OT Security Policy and Requirement documents. Cosman (2020) describes that component 3-2 *"addresses security risk assessment and system design for IACS"*, primarily directed at asset owners or end users. The substantiation of Internal Expert 3, for already incorporating this component into the current practices, is that the selected case study organisation organises external audits; next to this, the selected case study organisation has an internal risk assessment team, which is called 'internal audit team', the selected case study organisation has an OT regularly assessment for checking if there are any gaps, the selected case study organisation has the internal system *Service Now*, as logging system for maintenance of all assets, including documentation of end-of-life and end-of-service. Lastly, the selected case study organisation regularly performs business impact assessments (BIA) to assess these impacts, determine their size, and how to improve them.

Moreover, Internal Expert 1 of the selected case study organisation is responsible for reviewing the two documents, OT Security Policy and Requirements, as stated in the policy itself, yearly. However, Internal Expert 1 said during the interview that policies within the selected case study organisation are reviewed once every five years and standards are reviewed once every three years, based on the selected case study organisation's document management cycle. This contradicts the review frequency cycle given in those two documents. Next to this, as a result of the interview with Internal Expert 2, it emerged that this review cycle does not include Internal Expert 2. At the same time, it is remarkable that the person with subject-specific knowledge of implementing and maintaining the OT systems at the locations is not involved in this review cycle of these documents.

Besides that, the Internal Expert 1 said during the interview that security patching is already included in the onboarding process of new suppliers. It is omitted whether this concerns IT or OT suppliers since, according to Internal Expert 1: *"within the policy is already in place to keep the systems up-to-date and life-cycle-maintenance, so I don't understand why security patching has to be added?"*. When looking at the onboarding process of new suppliers, it is assessed if the new supplier can fulfil the given requirements of the selected case study organisation. During the interview, Internal Expert 2 explained that no specific cybersecurity aspect is applicable within the procurement process (performed by the selected case study organisation's procurement department).

Moreover, during the interviews with the selected case study organisation's experts, it became clear that the Global IT/OT team of the selected case study organisation is improving the onboarding process of new suppliers, where they are mainly focussing on IT governance and IT suppliers but is leaving the complexity behind for the application of this onboarding process towards OT suppliers. Internal Expert 1 said during the interview that the locations have to decide how to contract a new OT supplier and that they only have to adhere to the selected case study organisation's global standards, including security standards, which are not specific or measurable and guidance for implementation is missing. In addition, Internal Expert 2 confirms that there is less focus on OT suppliers, where it has been said that: *"it is not very often that new OT suppliers are contracted, especially for the process control systems of a location"*. It also appeared that two preferred OT suppliers were selected around six to seven years ago, resulting in less need to develop this. However, Internal Expert 2 thinks *"it would be a good thing, also with the changing law and regulations due to the NIS2 directive"*. The capability of the OT suppliers might be a limiting factor within this onboarding process within OT, according to Internal Expert 2: *"if the selected case study organisation is going to set more specific OT security requirements for OT suppliers, it might be that a lot of OT suppliers are not going to qualify, since cybersecurity is not always very high on their priority list, since within OT, cybersecurity is still far underdeveloped in some areas"*.

Internal Expert 3 describes only the local procurement process of a new OT system, where the first step is to order the OT system from the specific OT supplier, while mentioning that the OT system has to be compliant with ISA/IEC62443, if not compliant, the OT supplier has to give instructions how to be compliant in a later stadium. Beforehand, the specific OT supplier has to be approved based on certain OT supplier requirements and security levels. Within this particular phase, no format is available for the assessment; the local procurement employees of the selected case study organisation will assess the new OT system of the OT supplier themselves during multiple conversations and meetings about the possibilities, risks and vulnerabilities of the integration of the new OT system with the already existing OT systems within the location network. The second step in the local procurement process is to check and test the OT system, where technical requirements, functionalities, cybersecurity requirements and financial aspects are assessed in the third phase. When the OT system and OT supplier complete all stages of the local procurement process, an SLA will be concluded for the specific OT system and OT supplier. It can be seen that local procurement processes are available for OT systems and OT suppliers from a decentralised perspective, whereas a division can be seen in the governance of IT deployed from a centralised perspective.

6.4 Conclusion sub-research question 2

The insights from the internal document analysis are combined with the four themes: 1) outsourced responsibilities, 2) lacking communication at the selected case study organisation, 3) no regular quality checks on OT suppliers by the selected case study organisation, and 4) contradicting governance, resulting from the thematic analysis of the three semi-structured interviews with Selected case study organisation's experts. Many contradicting points were found, concluding that Selected case study organisation's security patching processes are not governed effectively, where the coordination among stakeholders is lacking.

The most important derived theme from the semi-structured interviews with the selected case study organisation's Expert is *contradicting governance*, it can be seen that the Global IT/OT team of the selected case study organisation is improving the onboarding process of new suppliers, where they are mainly focussing on IT governance and IT suppliers, but is leaving the complexity behind for the application of this onboarding process towards OT suppliers. Based on the selected case study organisation's governance, it can be concluded that local procurement processes are available for OT systems and OT suppliers from a decentralised perspective, where a division can be seen in the governance of IT deployed from a centralised perspective.

Internal Expert 3 substantiates this, indicating the difference between IT and OT assessment, where IT can be verified beforehand (by Microsoft), and the assessment is already mature. In contrast, OT is at least ten years behind and needs to be more mature, making it more challenging to govern OT processes, such as security patching. This is mostly due to the critical nature of these OT systems, including the compatibility of the ‘old’ hardware of the OT systems with ‘new’ software of these systems and the potential risks involved. However, verifying OT systems is very difficult since these systems interact with other OT systems at each location. Integration, security, and data management play a significant role in OT assessment, in contrast to IT. This results in a difference in risk and challenges between the two landscapes. Where in an OT environment, the operations are ongoing, and it is not possible to suddenly stop working to perform security patching, whereas in IT, this is more common, and security patching can be performed more frequently.

When looking at the policy foundation of the selected case study organisation’s OT Security documents, it can be concluded that the selected case study organisation’s experts can give no direct answers as to why only components 2-1 (security program requirements for asset owners) and 3-3 (security requirements and levels) of ISA/IEC62443 are included as policy foundation. In addition, the person responsible for maintaining these documents is not certified by this framework, making it even more challenging to implement it as a policy foundation of OT security at the selected case study organisation. It has been said that the selected case study organisation’s OT Security Policy and Requirements are IT documents and, therefore, not applicable within the scope of Internal Expert 2. At the same time, the OT Security Standard and SLA addendum are also based on the earlier mentioned documents, which are included within the scope of this expert. According to Internal Expert 3, component 3-2 (regarding risk assessment) is also included in practice but cannot be retrieved within these documents and component 2-3 (regarding patch management) is left out of these documents since the responsibility for security patching is completely deployed by the OT suppliers.

When zooming in on these outsourced responsibilities to the OT suppliers, it can be concluded that the selected case study organisation is not in control, the governance is not effective, and neither is the coordination between the stakeholders. The comparison of the OT Security documents results in much practical information being missing and unclear how the ‘how’ is met. The person responsible for these OT Security documents is too far away from the operations to incorporate the complexity. Resulting in the fact that the composed OT Security Policy and Requirement documents are not applicable in a practical way. Moreover, the OT Security Standard and the SLA addendum are too general and not measurable, which cannot be used to assess the OT suppliers.

OT suppliers must act according to the OT Security Standard and SLA addendum, where many *‘shall provide’* or *‘shall be’* statements are framed towards the OT suppliers, making it more difficult actually to assess the performance of each OT supplier. Quality checks are carried out and are solely based on internal audits, internal (risk or impact) assessments and external audits by various organisations such as independent bodies or government agencies (DCMR, National Digital Infrastructure Service, Dutch Ministry of Infrastructure and Water Management).

Lastly, there is lacking communication at the selected case study organisation between different departments (Global IT, Operations, and Procurement), where multiple contradictions can be seen. Most important of all, when questions were asked regarding monitoring vulnerabilities, which are published via CVE, all three experts responded in different ways. Where Internal Expert 1 said that the selected case study organisation does not check these, Internal Expert 2 said that the Global IT/OT team is checking CVE, and Internal Expert 3 said that monitoring CVE is part of the SLA with the OT suppliers, as one of many contradictions.

Chapter 7: Which factors give insight into the complexity of the security patching processes in an industrial, operational environment?

Semi-structured interviews were organised to enable an understanding of the complexity of the security patching processes at the selected case study organisation. The transcript of each semi-structured interview with the OT suppliers was analysed using a thematic analysis within the program Atlas.ti. Based on the derived codebook, which can be seen in Appendix 6, five interesting themes emerged from the data. These five themes are described below, each having its own sub-paragraph (Chapter 7.1 towards 7.5). Within Chapter 7.6, the conclusion of sub-research question three can be found.

7.1 Theme 1: Supplier dependence

The first emerging theme from the thematic analysis of the OT supplier interviews is the supplier dependence amongst the selected case study organisation's OT suppliers. Amongst the participating OT suppliers, 50 percent of the OT suppliers (six out of twelve OT suppliers) depend on their suppliers of the delivered OT systems at one of the selected case study organisation's locations. Within Table 7.1 below, it can be seen which OT suppliers perform security patching themselves or which OT suppliers are dependent on their supplier of the OT systems. The OT suppliers who outsource security patching towards their suppliers are not responsible for developing the software on the OT systems either. The organisation *OT supplier 12* is responsible for the software and security patching of OT supplier 1, whereas *OT supplier 12* does not have a direct SLA for supplying a Business Service with the selected case study organisation. However, *OT supplier 12* was asked if they were willing to participate in the research; with their approval, it became clear that two other OT suppliers of the selected case study organisation could be included in the research since they were also supplying OT systems of OT supplier 12 at one of the selected case study organisation's locations. Firstly, the organisation *OT supplier 15* is supplying a boiler of OT supplier 12 at one of the selected case study organisation's locations; this also applies to *OT supplier 13*, which is providing a PLC of OT supplier 12 at the selected case study organisation. The organisation *Fourth party 1* is responsible security patching and developing software for OT supplier 5 and OT supplier 6 distributed security patching and the software to the organisation *Fourth party 2*. Moreover, the organisation *OT supplier 14* is supplying a Tank Gauging system (OT supplier 3 Tankmaster) via OT supplier 3, which is also interviewed for this research and can be included in this research as well.

A more complex cooperation can be seen where the organisation OT supplier 7 is deploying security patching and the development of the software of their PLCs to their suppliers, where their most important supplier for the PLCs is OT supplier 4. This is particular since OT supplier 4 is also a direct OT supplier of the selected case study organisation for the SCADA system, located at one of the selected case study organisation's locations. Lastly, the two OT suppliers, OT supplier 10 and OT supplier 11 deployed the security patching and software development for another type of complexity. OT supplier 10 has outsourced the management software of their fire alarm control panels at the selected case study organisation's locations to *Fourth party 3*, where their software is used as management software. In the case of OT supplier 11, they have outsourced the performance of security patching and software development to *Fourth party 4* for using their software at their CCTV monitoring systems.

Table 7.1: Distinction between OT suppliers when looking at the performance of security patching

OT supplier	Performing security patching themselves vs. outsourced
OT supplier 1	Outsourced towards OT supplier 12
OT supplier 2	Themselves
OT supplier 3	Themselves

OT supplier 4	Themselves
OT supplier 5	Outsourced towards Fourth party 1
OT supplier 6	Outsourced towards Fourth party 2
OT supplier 7	Outsourced towards OT supplier 4
OT supplier 8	Themselves
OT supplier 9	Themselves
OT supplier 10	Outsourced towards Fourth party 3 (for their software)
OT supplier 11	Outsourced towards Fourth party 4 (for their software)
OT supplier 12 (does not supply directly to the selected case study organisation)	Themselves

7.2 Theme 2: Ignorance of the OT environment

Since 50 percent of the interviewed OT suppliers differ in performing security patching and developing the software used on these OT systems, or outsourcing towards their OT suppliers. Interest was aroused in investigating the OT systems of each interviewed OT supplier to dive deeper into the knowledge of the environment of these OT suppliers' systems. Some predefined questions, which can be seen in Appendix 4 (Informed consent form OT suppliers), were asked to compare the OT suppliers' knowledge of the environment where their OT systems are active. The comparison is made when looking at the following concepts:

- Checking CVE for vulnerabilities
- Performing scans on OT systems for proactive scanning on vulnerabilities, risks, defects or other threats or viruses
- Controlling the OT system based on KPIs
- Test environment to test or prepare the to-be-installed update or patch
- Generating backups of their OT system

These differences are shown among the OT suppliers in Table 7.2 below. Conclusions can be drawn to assess how ‘in control’ these OT suppliers are within the industrial, operational environment when comparing the findings in Table 7.2 with the selected case study organisation’s SLA Addendum of OT Security Requirements (Appendix 2), resulting in the second theme: ignorance of the OT environment.

Table 7.2: Differences between OT suppliers

OT supplier	Check CVE?	Scans on OT systems?	KPI for control OT systems?	Test environment?	Backups?
OT supplier 1	No	No	No	No	Yes
OT supplier 2	No	Yes	Yes	Yes	No
OT supplier 3	Yes	Yes	Yes	Yes	Yes
OT supplier 4	Yes	Yes	No	Yes	Yes
OT supplier 5	No	No	No	Yes	No
OT supplier 6	No	No	No	No	Yes
OT supplier 7	No	No	Yes	Yes	Yes

OT supplier 8	Yes	Yes	Yes	Yes	Yes
OT supplier 9	Yes	No	No	Yes	Yes
OT supplier 10	No	No	No	Yes	Yes
OT supplier 11	No	No	No	Yes	Yes
OT supplier 12 (does not supply directly to the selected case study organisation)	Yes	Yes	Yes	Yes	Outside SLA

It can be concluded that only two OT suppliers check all boxes with 'Yes', OT supplier 3 and OT supplier 8, showing that they are in control of their OT system and have the expected knowledge. Since OT supplier 12 is not directly supplying OT systems at the selected case study organisation, no Service Level Agreement (SLA) is active between the selected case study organisation and OT supplier 12. For that reason, one concept does not apply to OT supplier 12: *Backups*. Therefore, OT supplier 12 also fulfils all appropriate boxes with 'Yes'. For the other interviewed OT suppliers, these concepts are compared with Selected case study organisation's SLA Addendum of OT Security Requirements (Appendix 2), resulting in the following insights:

1) Common Vulnerabilities and Exposures (CVE) is a publicly accessible database that identifies and catalogues known security vulnerabilities in software and hardware (Goodman, 2024a). Each vulnerability is assigned a unique ID, making it easier for organisations to share information, prioritise fixes, and protect their systems (Goodman, 2024a). The Common Vulnerability Scoring System (CVSS) is a standardised framework for measuring the severity of security flaws in information systems (Goodman, 2024b). It assigns each vulnerability a score between zero and ten, where higher scores meaning more severe issues. CVSS helps organisations decide which security threats need attention first based on their potential impact (Goodman, 2024b). When looking at the SLA Addendum, the requirement *"Shall provide vulnerability information about their installed system"* can be assessed if OT suppliers check CVE for vulnerability information. However, seven out of twelve OT suppliers are not checking the publicised vulnerabilities by CVE, which makes it very difficult to meet this requirement for the OT suppliers: OT supplier 1, OT supplier 2, OT supplier 5, OT supplier 6, OT supplier 7, OT supplier 10 and OT supplier 11.

2) Within the SLA addendum, a requirement is stated regarding anti-virus, where OT suppliers *"shall perform a full system scan at least each 6 months"*, this is assessed during the OT supplier interviews, where it appeared that seven out of twelve OT supplies are not scanning their OT systems at the selected case study organisation's locations. Since they are not performing proactive scans on OT systems for vulnerabilities, risks, defects or other threats or viruses, these OT suppliers cannot fulfil this requirement either.

3) The SLA addendum states one requirement regarding patch management, which the selected case study organisation described as: *"Supplier shall ensure that the patch levels of the operating systems shall be kept current to within at least 12 months of the security patch being available."*, besides the fact that the terminology of *patch levels* is not have been made measurable, this requirement is assessed in the OT supplier interviews when asking towards Key Performance Indicators (KPIs) for their security or patch levels. According to Böhme (2010), the security level is *"the variable in the model that summarises the quality of protection"*, where deterministic indicators can include patch level, existence

and configuration of intrusion detection systems and installed virus scanners. Moreover, to control the cybersecurity of the OT suppliers' OT systems, the OT suppliers have to use the security levels to indicate the actual security level of the OT systems, which contributes to the evaluation of security in the OT suppliers quantitatively (Böhme, 2010). This can be done by incorporating KPIs specified for cybersecurity since KPIs can be used to measure and monitor operational performance and progress across an organisation toward specific, measurable goals (Twin, 2024). As a result of the interviews, seven out of twelve OT suppliers are not using KPIs to indicate the security level of their OT systems. They cannot evaluate how in control their patch levels are.

4) The fourth interesting insight into the OT supplier's self-knowledge relates to the OT suppliers' test environments to test or prepare the to-be-installed update or patch on the OT systems at the selected case study organisation's locations. The SLA addendum states that: *"Supplier shall review whether updates for installed software are available at least annually"*, in the scenario that an update for installed software is available, these updates must first be tested before the actual installation of the update on the OT systems. Several consequences are at risk when the update is not tested within the operational environment. The most important consequence is the occurrence of errors after deploying a new patch or update of an OT system, resulting in *location downtime*. In this scenario, potential business disruptions could affect the ongoing operations of the location. These errors, bugs or other problems could be avoided when the patch or update is tested within a test environment before installation. During the OT supplier interviews, this requirement is assessed if OT suppliers test their updates or patches before installing these at the OT systems at the locations. Two out of twelve OT suppliers (OT supplier 1 and OT supplier 6) cannot test their updates in a test environment before installing them.

5) Another critical requirement of the SLA addendum relates to backups, where the *"Supplier shall make backups to ensure that the entire system/PLC can be recovered"* when looking at Table 7.2, two out of twelve OT suppliers cannot provide a backup of the OT system to ensure that it can be recovered in total, referring towards OT supplier 2 and OT supplier 5.

7.3 Theme 3: Certification is missing within the OT landscape

As described in Chapter 6.2, the policy foundation of the selected case study organisation's OT Security documents is based on the framework of ISA/IEC62443, components 2-1 and 3-3. During the OT supplier interviews, it was assessed which certification was incorporated into the cybersecurity of the participating OT suppliers, compared with the selected case study organisation's policy foundation. Various answers were given during the interviews, shown in Table 7.3 below, resulting in the third theme, where certification is missing within the OT landscape. The OT suppliers OT supplier 6, OT supplier 4, OT supplier 8 and OT supplier 11 did not even mention any certification during the interview for cybersecurity or other related aspects.

Table 7.3: Differences of certification between OT suppliers

Certifications	OT suppliers
ISA/IEC62443	OT supplier 1, OT supplier 5, OT supplier 12 (OT), OT supplier 3
ISO/IEC27001	OT supplier 1
NEN2535	OT supplier 10
DCMR regulations	OT supplier 10
NEN1010	OT supplier 7
NEN3140	OT supplier 7, OT supplier 3
ATEX directive	OT supplier 7

NAMUR recommendations (based on German legislation)	OT supplier 2
ISO/IEC27000 series	OT supplier 12 (IT)
NMi regulations	OT supplier 9

According to ISA Global Cybersecurity Alliance (ISAGCA) (2024), the ISA/IEC62443 Series of International Standards *"define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS)"*. These standards set best practices for security and provide a way to assess security performance (ISA Global Cybersecurity Alliance (ISAGCA), 2024). It can be seen that four out of twelve OT suppliers incorporated this certification within their business, which aligns with the policy foundation of the selected case study organisation's OT Security documents. Moreover, as stated by Edwards (2024), ISO/IEC27001 is *"an information security management standard that provides organisations with a structural framework to safeguard their information assets and information security management systems (ISMS), covering risk assessment, risk management, and continuous improvement"*. Only one out of twelve OT suppliers is certified by ISO/IEC27001 (OT supplier 1). ISO/IEC27001 belongs to the ISO/IEC27000 series, where more than a dozen standards cover additional best practices in data protection and cyber resilience (International Organization for Standardization, 2022). During the interview, OT supplier 12 stated that they had incorporated these standard series within their environment regarding IT, where OT supplier 12 indicated the adaption of ISA/IEC62443 for their OT environment.

Thirdly, NEN2535 provides rules for the design, realisation, compatibility, and quality of the installed fire detection systems, which are appliable to autonomous fire detection systems in buildings that are not integrated with other systems in terms of equipment and cabling (NEN, 2017). Since OT supplier 10 is the preferred OT supplier for fire alarm control panels at the selected case study organisation's location, this OT supplier is the only one out of twelve OT suppliers who can meet this standard. However, this standard does not include aspects surrounding cyber security. Next to this, OT supplier 10 has to comply with the environmental regulations provided by DCMR Environmental Protection Agency, since DMCR performs audits surrounding the selected case study organisation's environmental services. DCMR is the joint environment agency of the Province of South Holland and Thirteen municipalities in the Rijnmond region (DMCR Environmental Protection Agency, n.d.). Due to the large number of companies and heavy industry within the Rijnmond region, pressure is created on the regional environment, where the province of South Holland wants *"quality of life and safety to go hand in hand with the economic development of the Rijnmond area"* (DCMR Environmental Protection Agency, n.d.). To achieve these ambitions, they grant permits to organisations, monitor compliance with environmental regulations and take measures in case of violations, where special attention is devoted to the highest-risk companies with more stringent regulations.

Fourthly, the NEN1010 standard applies to the power supply and distribution of low-voltage electrical installations. This standard can also be used for checks and inspections upon delivery of projects (NEN, n.d.-a). NEN3140 is a standard that contains all relevant requirements for low-voltage installations within The Netherlands, where it applies to the operation of electrical installations and equipment up to a nominal voltage of 1000 Volt alternating current and 1500 Volt direct current (NEN, n.d.-b). OT supplier OT supplier 7 is NEN1010 and NEN3140 certified, whereas OT supplier 3 is also NEN3140 certified. During the interview, it appeared that OT supplier 7 also incorporated the ATEX directive within their operations; this relates to equipment and protective systems intended for use in potentially explosive atmospheres (European Commission, n.d.), where cybersecurity is not included in this certification on all three certifications.

Fifthly, NAMUR recommendations are industrial standards from Germany, primarily concerning process instrumentation and control, as a standardisation association for measurement and control in chemical industries (NAMUR, 2024). The NAMUR recommendations are incorporated as the policy foundation of one out of twelve OT suppliers (OT supplier 2).

Lastly, one of the OT suppliers (OT supplier 9) indicated that they have incorporated the NMI regulations into their policies. The Netherlands Measuring Institute (Dutch: *Nederlands Meet Instituut*) (NMi) measure OT supplier 9's instruments, which will be installed in the field, as referred to in the Dutch Metrology Act, where after the approval of the management system, the certificate holder may carry out activities as an accredited (accepted) verifier. The system's quality must be verified and re-verified that measuring instruments comply with Dutch regulations (NMi, n.d.).

Out of the given certifications and regulations, only three certifications include cybersecurity or security patching aspects: ISA/IEC62443, ISO/IEC27001, and ISO/IEC27000 series, with the result that five out of twelve OT suppliers, include cybersecurity or security patching aspects within their policies. Zooming in on these different certifications, only 33 percent (four out of twelve) of the OT suppliers incorporate the ISA/IEC62443 within their cybersecurity environment. It can be concluded that not all OT practitioners are certified and, therefore, not trained to perform security patching at the OT systems of their organisations; due to this, they have too little knowledge about security patching. Since the selected case study organisation is not checking the performance of the OT suppliers, based on the policy foundation of the OT Security Policy (ISA/IEC62443) as described in the OT Security documents, it can be seen that the OT suppliers are not focused on the requirements of this certification as well. Some OT suppliers only focus on environmental certifications, whereas a third of the participating OT suppliers (four out of twelve) did not mention any certification during the interview at all.

7.4 Theme 4: Human knowledge remains necessary

During the semi-structured interviews with the OT suppliers, another theme, human knowledge remains necessary, emerged from the data, resulting from the reflexive thematic analysis based on the transcripts of the semi-structured interviews with OT suppliers. Within this theme, three key areas show how human knowledge remains necessary with the OT systems overall due to 1) human knowledge or experience in diagnoses, testing and operating the OT systems (Chapter 7.4.1.), 2) preparation and compatibility of security patching within the OT systems (Chapter 7.4.2) and 3) specialised local OT knowledge and system customisation for the OT systems (Chapter 7.4.3). Each key area is further explained below, with substantiations from the OT supplier interviews.

7.4.1 Human knowledge or experience in diagnoses, testing and operating the OT systems

This key area emerged from in total five OT suppliers, as a result of reflexive thematic analysis of the transcript of the OT suppliers. The first OT supplier who contributed towards this key area was OT supplier 9. Within the interview, the expert stated, *"It is already difficult enough to train a person, let alone a computer"*, where the most challenging part in diagnoses, testing and operating the OT system is finding the cause of a problem. However, this becomes easier for an expert when the expert gains more knowledge or experience with the OT system or within the OT system's environment, according to OT supplier 9's expert. The second OT supplier who contributed to this key area was OT supplier 6, where the participating expert explains that *"human knowledge is most needed at control stations itself, this is not a Windows environment, the person is interacting with the software environment where all kind of coding and barcodes have to be known for handling the product and using the OT system"*. OT supplier 2 was the third OT supplier to contribute to this key area. It appeared in the interview that knowledge about the processes of the OT systems at the location is crucial, including testing the functionality of the OT systems, in other words, if the OT system does what it says it has to do. Human expertise is needed because: *"Testing cannot be performed automatically. That will always be the most prominent human interaction within the OT systems"*. Moreover, in the interview with OT supplier 3's expert, it came forward that human knowledge about the environment of OT systems, nodes, factors, and functions, including the knowledge within the preparation for security patching, is most important. OT supplier 3's expert had another addition to this, where knowledge of the overview of the OT system at a location remains necessary, including insights and understanding of possible risks based on the performed or to-be-performed actions in security patching by the local expert of that specific OT supplier. Lastly, the expert of OT supplier 8 discussed during the interview that human interactions are inevitable when managing the OT system. Due to understanding how the OT system communicates with other components within the OT network at the location, the mitigation of problems when corrective maintenance is performed at the OT system, solving defects, and issues of other type of errors.

7.4.2 Human interactions in preparation and compatibility of security patching

The second key area is substantiated by two OT suppliers, OT supplier 1 and OT supplier 4. OT supplier 1's expert discussed during the interview that human interactions are most needed when installing new updates of OT systems, including mapping the current state of each OT system and assessing which OT system has to be updated. Powerpex's expert added that compatibility is most difficult, where it has to be assessed by these experts if new software updates are compatible with older OT systems and stated: *"This is more well known in IT, but not in OT, so there is often no capacity in terms of labour for this"*. During the interview with OT supplier 4, the expert described the process of installing a software update: preparation for software update – production system offline – test system online – backups and restorations on test systems – install the update – eliminating possible bottlenecks while installing updates – test system offline – backup database of the test system – production system online, which is very time-consuming. Next to this, the expert cannot perform other tasks and must focus on each step's actions within the process. The knowledge of which buttons have which impact, in terms of violation of safety and physical and environmental impacts, is most important, according to OT supplier 4's expert.

7.4.3 Specialised local OT knowledge and system customisation

The third key area emerged from discussions with five of the twelve OT suppliers. Both participating experts of OT supplier 10 pointed out in the interview that specialised local OT knowledge is needed by the operating experts in terms of expanding new OT systems at locations and implementing new requirements, customer wishes, functionalities and replacements into the current OT system. The most important of all these aspects of local OT knowledge is implementing customer wishes and functionalities into the current OT system. As for the expert of OT supplier 5, specialised OT knowledge lies mainly in the control or instrumentation of the OT system itself. That is also the reason why OT supplier 5 outsourced their data registration systems to their supplier, Fourth party 1, so that they solely focus on the control or instrumentation of their OT systems. During the interview with OT supplier 7's expert, it appeared that specialised knowledge of the process at the locations is crucial. Experts providing that knowledge should be involved in the decision-making process of operations or maintenance since they can deliver the asset-specific knowledge and perform the actual maintenance on those specific assets. In addition, OT supplier 7's expert discussed that specialised local OT knowledge is required to set-up a new OT system at a location, including software programming, testing, and transforming the wishes of OT supplier 7's customers towards actual operating systems within the OT environment. This is also indicated by OT supplier 11's experts, who said that specialised OT knowledge is most needed at the set-up of the OT system, including generating the layout of the OT system during the preparation phase of a new project. However, OT supplier 7's expert adds to this substantiation out-of-the-box thinking when the operators of the customer's organisations are testing the newly developed OT system delivered by OT supplier 7. Based on the interview with OT supplier 12, it became visible that local OT knowledge at locations is most important, including the system integration of other components within the OT system's network. OT supplier 12's expert described that IT and OT knowledge are brought together at OT supplier 12 within their Security Operations Centre (SOC). But, it is very hard to find people who know both sides (IT and OT) of the operations.

It can be seen that resistance towards security patching has a significant impact on this key area. Only one out of twelve OT suppliers has no resistance towards security patching, as indicated in the interview with the experts of OT supplier 10. Nevertheless, they are not performing any security patching since they outsourced that to their supplier. Overarching reasons why this resistance towards security patching exists is due to:

1) Three of twelve OT suppliers said cybersecurity is not their core focus. For OT supplier 1, cybersecurity and security patching do not belong to their core business, system automation. For OT supplier 9, their core business is focused on the instrumentation of their OT systems, not cybersecurity. As for OT supplier 6, security patching of the Windows environment is outsourced to their supplier since their scope is solely on the hardware and software within their own environment.

2) Three of twelve OT suppliers indicated cultural or structural resistance that impacts location operations as the underlying reason for resistance towards security patching. Beginning with OT supplier 7, where the expert said during the interview that the weakest link within the OT environment is people: *"Everything is programmable, but people do something which results in changes within the OT systems when people not adhering to the procedures"*. OT supplier 7's expert added that, since people make mistakes, the goal should be to *"learn from the past mistakes and try to avoid these mistakes in the future"*. The explanation provided by OT supplier 12's expert for this resistance is that it comes from resistance to change within the higher, broader landscape: *"it is most likely that some people within those companies want to change but cannot overcome this cultural barrier"* or due to the expectations of the companies: *"the decisions that organisations make are financially feasible in the short term, but are dangerous in the long term, where decisions regarding NIS2 directive or Governance, Risk and Compliance (GRC) come afterwards"*. OT supplier 5s indicates that the government is *"demanding a lot"*, but assistance or guidance is missing towards the organisations: *"you have to hope that your suppliers are also on that level of knowledge or implementation"*. Especially with the upcoming NIS2 directive, guidance of the government is lacking, for the implementation of the NIS2 directive.

3) Three of twelve OT suppliers suggested that balancing automation with human knowledge and control can be a reason for the resistance towards security patching. OT supplier 3's expert stated: *"the more you automate, the fewer human interactions are required, resulting in more efficiency (less human errors), but more risk can arise since you have no feeling or insights into what is happening within the OT systems or automated processes at the locations"*. As for OT supplier 4's expert, it was suggested that all OT suppliers have their own software, which is used differently, resulting in the fact that it demands specific knowledge of the practitioners of all these types of software at all those types of OT systems, supplied by each OT supplier at a location. The amount of differentiation between the same type of OT systems could be reduced by selecting preferred OT suppliers for the same type category of OT systems within a Business Unit. The expert of OT supplier 8 stated that human interactions should be avoided within security patching processes or OT systems. However, security patching cannot be performed

within the current state fully autonomous within the OT environment, due to validation and confirmation within these processes.

4) Two out of twelve OT suppliers described IT and OT as separate worlds. OT supplier 2's expert stated that OT and IT are *"two separate deployments where changes are not desired within the industry environment"*. OT supplier 11's experts discussed the contradiction between IT and OT at, for example, the set-up phase of a new project, where customers have to be more specific and more aware of the scope and requirements within OT: *"sometimes customers don't know what they want at all"* and *"OT systems are so-called 'air-gapped-systems', but customers are less aware of the risks in terms of safety at the OT domain"*.

7.5 Theme 5: Complexity within the OT domain causing delays for security patching

A last identified theme, resulting from the reflexive thematic analysis of the transcript of the semi-structured interviews, relates to delays in security patching due to complexity within the OT domain, divided into three key areas: 1) ignorance of OT suppliers about terminology (Chapter 7.5.1), 2) different patch log processes without uniformity amongst OT suppliers (Chapter 7.5.2), and 3) no central point for documentation of the reported problems (Chapter 7.5.3). Each key area is further explained below, with substantiations from the OT supplier interviews.

7.5.1 Ignorance of OT suppliers about terminology

Ignorance of the OT suppliers can be seen in the terminology of security patching as the first key area. Several definitions of security patching were heard during the interviews: 'mitigation of unplanned vulnerability' (OT supplier 1), 'preventive updating and installing software on its assets' (OT supplier 3), 'preventive maintenance' (OT supplier 7), 'error or bug fixing' (OT supplier 10 and OT supplier 5) and where other OT suppliers within the industry use security patching as 'installing updates'. The selected case study organisation uses security patching as 'installing and updating the digital assets within the IT or OT domain'. Academics use security patching as "*Additional pieces of code developed to address problems in software. Patches are also known as bugs, whereby they enable additional functionality or address security flaws within a program"* (Mell et al., 2005) and Dissanayake et al. (2022a). A contradiction can be seen between the definition of security patching used by OT suppliers within the industry and the definition of security patching used by academics.

7.5.2 No uniformity in patch (log) processes of OT suppliers

During the interviews with the OT suppliers, it was revealed that eight out of twelve OT suppliers (OT supplier 9, OT supplier 1, OT supplier 12, OT supplier 6, OT supplier 3, OT supplier 10, OT supplier 2, and OT supplier 8) have a patch log process within their organisation, with some ticketing or patch log process, and priority of these patch logs. However, many differences can be seen among the OT suppliers in initiating a patch log, prioritising patch logs, following up times and actions, and documenting these patch logs, contributing to delays in security patching.

If new software must be installed on OT supplier 9's OT systems, the NMi has to approve the instrumentation and its software since it is used for measuring and weighing calibrated instruments. Because of this, the actual implementation times can vary a lot amongst each other since OT supplier 9 is dependent on the certification provided by the NMi. This applies for the same reason when performing security patching, where the NMi has to approve the instrumentation, and delays in follow-up actions with their follow-up times may vary a lot before implementation. In the meantime, OT supplier 9 has to devise temporary mitigating measures to prevent further risks.

When looking at OT supplier 1's security patching process, in case of a vulnerability in their OT systems, a support log (also known as a patch log) is created by OT supplier 1 towards their supplier OT supplier

12. Based on the patch log, the follow-up times differ quite a bit, where ‘quick fixes’ are resolved within a couple of days, but significant problems or difficulties are resolved when several weeks, months or even years have passed. During the interview with OT supplier 12, it was asked how they have designed their security patching processes. OT supplier 12’s expert described two types of patch logs that can be created: reactive patch logs and patch logs within a specific Service Level Agreement (SLA) between the OT supplier and OT supplier 12. Diving into the first type of patch log as reactive; this type is free of charge for the OT supplier, where the addressed problem can be seen as a ‘patch trigger’. This will be examined within office work hours, resulting in follow-up actions taking multiple days, based on the availability of OT supplier 12’s employees. When a patch log is created via a ticketing system from the OT suppliers’ customers (e.g. the selected case study organisation) towards the OT supplier (e.g. OT supplier 1), the OT supplier has to redirect this ticket towards OT supplier 12. OT supplier 12 will examine the patch log via a diagnosis tooling (log collection tool). After this, the stated diagnosis will be sent to the OT supplier with an update or further instructions. As a final step, the OT supplier will visit the customer’s location (e.g. the selected case study organisation’s location) to install the newly provided update. The second type of patch log can be created via a Service Level Agreement between the OT supplier and OT supplier 12; this type is a paid version, where prioritising of the created patch logs is possible. In cases where the priority of patch logs is labelled as ‘high’, within thirty minutes after the initiation, the patch log or problem will be investigated, and further instructions or other types of follow-up will be given to the OT supplier. This support is not limited to office work hours and can be assessed directly (24/7 support). OT supplier 12 indicates that the most chosen form of creating patch logs is the first type (reactive), where this type of patch logs is “*mostly abused since it is free of charge”*, as stated by OT supplier 12’s expert. Examples were given where, via the reactive type of patch logs, pressure was provided by multiple OT suppliers towards OT supplier 12 for receiving further instructions or updates via this type of patch logs, even in scenarios where the reported problems or patch logs cause production disruptions at the locations of the OT suppliers (or customers of these OT suppliers). However, this is not where reactive patch logs are intended for. Follow-up times can add up to waiting times of a week for the results. A more specific example of the reactive patch log is where tickets are created for design topics of software or tickets for preparation for security patching, where it is mostly not critical for production. On the other side, examples for patch logs within the Service Level Agreements with OT suppliers are more focused on security or technical problems, such as tickets regarding the hard disks of PCs, which are mostly critical for the production of the OT supplier’s customer. It can be seen that this type of patch log is less chosen by OT supplier 12’s customers (e.g. OT supplier 1).

In the case of OT supplier 6, patch logs can be generated for two types of problems: for Windows problems or defects in their own software or hardware packages. If a defect is reported as patch logs regarding their software or hardware, OT supplier 6 will solve this immediately by themselves. But for patch logs regarding Windows, their supplier *Fourth party 4* has to resolve this. The follow-up time for receiving feedback from *Fourth party 4* towards OT supplier 6 is an average of one day.

If the selected case study organisation addresses a vulnerability to OT supplier 3, a call (issue) is logged. OT supplier 3 will first check if the vulnerability applies to OT supplier 3’s systems at the locations of their customers, including the performance of a risk assessment and mitigating measures for the vulnerability if needed. OT supplier 3’s expert explained that one vulnerability has been reported towards the selected case study organisation in the past ten years. However, when a patch log is logged at OT supplier 3, OT supplier 3’s Global Support Centre (GSC), the internal organisation behind Guardian, will investigate the created patch log; questions were asked regarding the initiated patch logs, and based on the criticality of the OT system, the patch log is prioritised. A distinction can be seen within the priority, where problem fixing within a critical system will be labelled as ‘high priority’ and problem fixing within an offline system, or when new software is tested will be labelled as ‘low priority’. This department of OT supplier 3 will look for solutions globally, where their database will be updated with possible new insights or lessons learned from the patch log. The result will be that the patch or hotfix is being sent to the local OT supplier 3 Expert to install this at OT supplier 3’s customer locations. It is also possible to initiate a patch log via another route; when a vulnerability has been published, the helpdesk is called, and the GSC will resolve the reported problem at the patch log.

If an error, problem, or bug has to be mitigated at the OT system of OT supplier 10, this will be reported towards their supplier *Fourth party 3*, whereby OT supplier 10 receives an update from *Fourth party 3* with the to-be-installed software update, which OT supplier 10’s experts will install at their customers. The follow-up actions and time depend on the cause of the error, problem or bug, which can take weeks before receiving the update. Within the interview, the most common problems can be seen when drivers of the OT systems are not working. Labelling priority on the patch logs is possible, but *Fourth party 3* is responsible for managing the patch logs. OT supplier 10’s experts indicate that they receive every six months an update of *Fourth party 3* for their OT suppliers where: *“it is most likely that these updates includes security components”*.

When security breaches in firmware are signalled, a log file (patch log) will be generated towards OT supplier 2’s headquarters, located in Germany. An investigation will be deployed, in which firmware version the security breach is signalled, for those specific firmware versions, updates will be created and those have to be installed at OT supplier 2’s customers, to mitigate the security breach.

If problems arise that the OT systems of OT supplier 8, the local OT supplier 8 expert at one of their customers’ locations, will inform OT supplier 8’s security patching department in Germany. This department will investigate and assess the priority of the reported problem and based on the business impact, solutions will be generated. A distinction can be seen in prioritisation, where problems that cause fewer business disruptions are labelled as ‘low-priority’, such as problems within operational or workstations; multiple workstations at a location cause fewer business disruptions, and problem-solving is less urgent since the ongoing operations can be managed via another workstation. Based on availability within office hours, support will be provided for follow-up actions and mitigating measures. If the priority is labelled as ‘high’, the business disruptions significantly impact the ongoing production, where the problem will be resolved within one hour (on average). Allocation of priority to the problem is based on the assessment of the local expert of OT supplier 8 on their customers’ location (based on that person’s knowledge and experience), where the tickets (patch logs) have to be initiated by OT supplier 8’s customers, and the solutions will be provided reactive to these customers.

7.5.3 No central point for documentation of the reported problems

As for the other participated OT suppliers, four OT suppliers (OT supplier 5, OT supplier 11, OT supplier 7, OT supplier 4) have no central point for documentation of the reported problems, which can trigger a patch, making it more difficult to manage the reported problems, have an overview of the to-be-resolved issues or derive lessons learned from it, to apply the gathered knowledge to other locations or their customers, especially over a long time line of several years and multiple employees at both sides (the selected case study organisation and the OT supplier itself).

This can be seen at OT supplier 5, where errors and other defects are reported via email exchange from the selected case study organisation to OT supplier 5, where OT supplier 5 is responsible for the investigation of the cause of the reported problem. OT supplier 5 outsourced the development of new software and security patching towards their supplier, Fourth party 1, but that their supplier “has nothing to do with this” when discussing patch logs with OT supplier 5’s expert in the interview. However, when discussing follow-up actions, based on data breaches (problems which could trigger a patch), OT supplier 5 describes that *Fourth party 1*, is responsible for any documentation with its follow-up actions regarding error or bug fixing. Due to misalignment with the terminology of security patching or patch logs, it appeared that OT supplier 5 uses email exchange as patch logs. Still, no central documentation place can be seen for these reported problems.

At OT supplier 11, the situation is comparable, where problems can be reported from the selected case study organisation towards OT supplier 11 (without the usage of ticketing), and OT supplier 11 calls their supplier *Fourth party 4*. After this, a ticket is generated by *Fourth party 4* in their internal portal, and related data can be uploaded by OT supplier 11, where priority to the ticket can also be added. *Fourth party 4* will prioritise the reported problem based on the information uploaded to the ticket. The type of priority results in the response time of the follow-up actions of the reported problem. A diversion is made between 'high' and 'low' priority tickets at *Fourth party 4*. An example of a high-priority ticket is when the newly installed server has hardware problems, causing server failures. An example of a low-priority ticket is when cameras move a bit twitchy or other minor issues. When the follow-up actions are published, OT supplier 11 has to perform these at their customers' locations (e.g. the selected case study organisation's locations). Between OT supplier 11 and the selected case study organisation, there is also a lack of a central place for documentation of the reported problems. Only tickets as patch logs can be seen between OT supplier 11 and their supplier *Fourth party 4*.

The selected case study organisation notifies OT supplier 7 via email exchange as a form of patch logs when problems or other types of security breaches, issues, or bugs have to be resolved. After this, OT supplier 7 notifies OT supplier 4 (their most important supplier) via ticketing. OT supplier 4 guides OT supplier 7 in problem-solving, and they will investigate the ticket's reported error, problem or issue. OT supplier 4 will provide the follow-up actions with mostly a hotfix or update towards OT supplier 7, where OT supplier 7 will install this at their customers' locations (e.g. the selected case study organisation). Further causes of the reported issue won't be provided for OT supplier 7 or the selected case study organisation, but they state that a programming defect is the most common cause of a defect or error. When questions were asked about the security patching or patch log process towards the expert of OT supplier 4, different types of patches can be seen: patches for Microsoft software, OT supplier 4 software, Status software (as redundant partner), Dell (for desktops) and Wyse Management suite (for Thin Clients). The patch log process at OT supplier 4 will be that the OT supplier (e.g. OT supplier 7 or even the selected case study organisation, since the selected case study organisation also has a direct SLA with OT supplier 4) directly calls OT supplier 4 and describes the occurred problem, remote support is provided based on the available employee at one of the three help desks, giving support 24/7, where a case (patch log) is created on an SLA-basis. Based on the information within the created patch log, the problem will be investigated and resolved. The OT supplier 4 support help desks can provide global information about the OT systems, and the local OT supplier 4 expert will provide OT-specific knowledge. For both the OT systems of OT supplier 7 and OT supplier 4, the documentation regarding the reported issues is not stored in a central place. the selected case study organisation emails OT supplier 7 with the occurred problem, breach, issue or bug, and OT supplier 7 notifies OT supplier 4, whereas OT supplier 4 may also be called directly by the selected case study organisation.

7.6 Conclusion sub-research question 3

The first derived factor is *supplier dependency*, where 50 percent (six out of twelve) OT suppliers are dependent on their supplier of the OT systems for security patching and developing the used software. The OT suppliers who are not performing security patching or developing the software, state: that cybersecurity is not their core business, so little attention is given to this and preferably outsourced towards their supplier.

The second derived factor is *ignorance of the OT environment*. When looking at the comparison of the OT suppliers and the SLA Addendum of OT Security Requirements (Appendix 2), it can be seen that the majority of the interviewed suppliers, 75 percent (nine out of twelve OT suppliers) are not in control and are ignorant about the environment of their OT system. This is concluded due to the fact that not all OT suppliers are checking publicised CVE, are neglecting proactive scans of their OT systems, are not using KPIs to indicate or evaluate the security levels of their OT systems, cannot test their patches or updates in a test environment before installing them at the OT systems at a location, provide backups of the OT system to ensure that it can be recovered in total.

The third derived factor is that *certification is missing within the OT landscape*. The selected case study organisation is not checking the performance of the OT suppliers, based on the policy foundation of the OT Security Policy (ISA/IEC62443) as described in the OT Security documents, but it can be seen that the OT suppliers are not focussing on the requirements of this certification as well. Only 33 percent (four out of twelve) of the OT suppliers incorporate the ISA/IEC62443 within their cybersecurity environment. Other OT suppliers are only focussing on environmental certifications, whereas four of twelve participating OT suppliers did not mention any certification during the interview at all. It can be concluded that not all OT practitioners are certified and, therefore, not trained to perform security patching at the OT systems of their organisations; due to this, they have too little knowledge about security patching.

The fourth derived factor is that *human knowledge remains necessary*. Three key areas were identified based on the interviews with the OT suppliers where human interactions with the OT systems are most needed:

- Diagnoses, testing and operating the OT systems (five out of twelve OT suppliers).
- Preparation and compatibility of security patching (two out of twelve OT suppliers).
- Specialised local OT knowledge and system customisation (five out of twelve OT suppliers).

Where resistance towards security patching has a significant impact on this key area. Only one OT supplier out of twelve had no resistance towards security patching. Overarching reasons why this resistance exists is due to: 1) non-cybersecurity core focus (three out of twelve OT suppliers), 2) cultural or structural resistance that impacts location operations (three out of twelve OT suppliers), 3) balancing automation with human knowledge and control (three out of twelve OT suppliers), and 4) IT and OT are two worlds (two out of twelve OT suppliers).

The last derived factor is *complexity within the OT domain causing delays for security patching*. This is based on the findings where several OT suppliers differ in the follow-up times on generated patch logs. Reason for this is that 50 percent of the participated OT suppliers are supplier-dependent since they have outsourced the development of software and, therefore, security patching towards their suppliers. For the other 50 percent of the participated OT suppliers, the following reasons cause the delay in security patching:

1) Ignorance of OT suppliers about the terminology of security patching. Several definitions of security patching were heard during the interviews: ‘mitigation of unplanned vulnerability’ (OT supplier 1),

‘preventive updating and installing software on its assets’ (OT supplier 3), ‘preventive maintenance’ (OT supplier 7), ‘error or bug fixing’ (OT supplier 10 and OT supplier 5) and where other OT suppliers within the industry use security patching as ‘installing updates’. The selected case study organisation uses security patching as ‘installing and updating the digital assets within the IT or OT domain’. Academics use security patching as “*Additional pieces of code developed to address problems in software. Patches are also known as bugs, whereby they enable additional functionality or address security flaws within a program”* (Mell et al., 2005) and Dissanayake et al. (2022a).

2) Each OT supplier has a different patch log process, whereby most OT suppliers focus on mitigating the unplanned vulnerability, occurred problem, defect, or risk. There is no uniformity in how OT suppliers create a patch log, how to prioritise the patch logs, follow-up times, and how to document these patch logs.

3) There is no central point for documentation of the reported problems, which can trigger a patch from the selected case study organisation towards the OT suppliers, which are mostly sent via emails to the OT suppliers. The information can be lost in email traffic between several employees of the selected case study organisation towards the OT suppliers, even when the OT suppliers depend on their suppliers for security patching. It is impossible to have an overview of all documented patch logs from the selected case study organisation to the multiple OT suppliers based on several emails between employees of the selected case study organisation, the selected case study organisation’s OT suppliers and their suppliers. Making it even more challenging to control the follow-up actions over several years.

Chapter 8: Conclusion

Using an embedded single-case study, applied with the socio-technical systems theory of Mumford (2000), security patching processes were researched within an industrial, operational environment, where the selected case study organisation was selected as the single-case study. The main research question for this research was as follows:

What lessons can be learned from the current practices, governance and complexity factors within security patching processes in an industrial, operational environment?

Since the socio-technical systems theory of Mumford (2000) described three stages in problem-solving within socio-technical approaches, including social and technical components, three sub-research questions were generated to answer this main research question. The first sub-research question investigated the current state of the security patching processes at the selected case study organisation, by identifying interactions between social elements as human actors and technical elements as security patching, where these interactions were framed as strengths, weaknesses, opportunities and threats via multiple observation rounds. These framed strengths, weaknesses, opportunities and threats are transformed into the following lessons learned:

1. Incorporate OT security assessments to define the criticality of OT systems at a location.
2. Incorporate OT systems as standalone systems at a location, without a connection towards the internet, preventing the risk of unwanted malware.
3. Perform Last Minute Risk Assessment before issuing work permits to OT suppliers who perform security patching at the location.
4. Incorporate earlier gained knowledge of cyber incidents towards an organisation's business contingency plan.
5. Generate overviews of updated or security patching statuses of OT systems at locations or, when this is not possible, control the responsible OT supplier on this.
6. Implementing preferred OT suppliers and defining solutions for equal OT systems at locations within an organisation's Business Units, resulting in fewer differences in OT suppliers and, therefore, fewer differences in frequency cycles of performed security patching by OT suppliers.
7. Install security patches more frequently on OT systems. This may result in fewer technical malfunctions, which can cause *location downtime*, where much production time might be lost to find the cause.
8. Incorporate more recommendations via audits (internal or external) into the current state of security patching processes at the selected case study organisation.
9. Avoid OT suppliers bringing USB sticks to locations for transferring data and software towards OT systems, letting them use safe data transfer systems.
10. Deploy earlier gained knowledge of more mature stakeholders within the industry to SLAs with other OT suppliers regarding insights into general processes or operations of security patching or cybersecurity.
11. Develop strategies to make current security patches more efficient when operations are paused (planned *location downtime*).
12. Create safer strategies for password management and rotation of the OT systems at locations.
13. Arrange security patching in time to avoid unplanned *location downtime*.
14. Invest in the in-house knowledge levels of location employees regarding security patching, risk management and problem-solving within this environment to avoid supplier dependency.

The second sub-research question focused on how these security patching processes were governed within the operational domain. The assessment of internal OT security documents, based on policies, requirements, standards and service level agreements, and comparing three OT expert interviews reveals a lack of effective governance and coordination among stakeholders. The following key issues can be seen as lessons learned from the current security patching governance at the selected case study organisation; this includes mainly focussing on IT governance and IT suppliers and leaving the complexity behind for the application of this onboarding process towards OT suppliers. Unlike IT systems, OT systems cannot easily be paused for security patching due to ongoing location operations and due to the critical nature of these OT systems, including the compatibility of the 'old' OT systems with 'new' software, and the potential risks involved. In this case study, the OT Security Policy relies on ISA/IEC62443 components, while uncertified employees by ISA/IEC62443 are responsible for maintaining these documents. Next, answers cannot be given as to why certain components are left out or have been applied in practice but are not retrievable from these documents. Within this case study, it can be seen that the selected case study organisation's governance lacks control over its OT suppliers. It is challenging to verify the performance of these OT suppliers since the OT security standard and SLA addendum are too general and lack measurable metrics (or key performance indicators). In addition, communication gaps between departments (Global IT, Operations and Procurement) further magnify the contradictions, such as inconsistent responses on vulnerability monitoring (e.g. CVE checks). Overall, decentralised oversights in OT, the lack of performance checks, and policy misalignment hinder effective OT security governance, which can be seen as lessons learned.

Where the last sub-research question elaborated on which factors gave insights into the complexity of these security patching processes in an industrial, operational environment. Within the social-technical approach of Mumford (2000), the third phase is designed to enable an understanding of the complexity of extracted factors and how these factors emerged from the interactions within the OT landscape. Via the thematic analysis of twelve semi-structured interviews with OT suppliers, five key factors were highlighted, which can be seen as lessons learned in understanding the complexity of these security patching processes in an industrial, operational environment. First, *supplier dependency* shows that 50 percent of participated OT suppliers rely on their own suppliers for security patching and software development, often due to a limited cybersecurity focus. Secondly, *ignorance of the OT environment* indicates that 75 percent of OT suppliers neglect cybersecurity measures like CVE checks, proactive scanning of OT systems, usage of KPIs, testing security patches or updates in a test environment and providing backups for ensuring recovery of the OT systems. Thirdly, *certification is missing within the OT landscape*; it has been seen that certification (e.g. ISA/IEC62443) is used for only 33 percent (4 of twelve) of the participated OT suppliers, adhering to this relevant standard. Fourth, *human knowledge remains necessary* for diagnoses, testing and operating OT systems, preparation and compatibility checks, and specialised local OT knowledge and system customisation. However, resistance to security patching continues due to non-cybersecurity core focus, cultural or structural resistance that impacts location operations, balancing automation with human knowledge and control and the perspective towards IT and OT as separate worlds. Lastly, *complexity within the OT domain causes delays in security patching*, partly due to varied terminology of security patching, no uniformity in patch (log) processes of OT suppliers, and no central point for documentation, where most reported problems, which can trigger a patch in a later stadium, are lost in email traffic between the many stakeholders within the industrial operational environment at locations, before being officially logged as 'patch log'.

Chapter 9: Discussion

Within this Chapter, the findings of the research will be further interpreted. At first, the reflection on the OT-specific considerations is elaborated in Chapter 9.1, as the industry perspective. Furthermore, the reflection towards the organisation will be addressed from the selected case study organisation's perspective (Chapter 9.2). Where lastly, Chapter 9.3 indicates the limitations of the research.

9.1 Reflection on OT-specific considerations (industry perspective)

The reflection of OT-specific considerations is divided into three sub-categories. Firstly, it is indicated that little information about security patching in OT is given in Chapter 9.1.1. Secondly, Chapter 9.1.2 reflects on the enormous impact of patching behaviour, and thirdly, the reflection of the missed governance guidance in Chapter 9.1.3.

9.1.1 Little information available about security patching in OT

As stated at the beginning of this research, a distinction is made between information technology and operation technology, where OT systems are autonomous, isolated and run on proprietary software. Conversely, IT systems are connected to the internet, lack autonomy and run on operating systems such Windows (Fortinet, 2024). In the literature review of this research, the literature was found regarding security patching within an IT environment, where little information is available about security patching within an OT environment. Due to the fact that the nature of IT and OT systems are different, differences can be seen within cyber security and security patching as well.

Evripidou and Watson (2024) also indicate this in their recently published paper about understanding OT personnel's mindset and their effect on cybersecurity. Evripidou and Watson (2024) described that due to the technical differences between IT and OT, OT security measures must be tailored to fit operational environments. For example, installing updates in OT requires longer timeframes than in IT, and OT systems cannot be shut down as easily. Therefore, already existing security patching strategies, based on earlier lessons learned or gained knowledge about security patching, cannot easily be 'copied' from IT perspectives into the OT landscape. This has to be taken into account, when implementing the identified lessons learned (from Chapter 8) or recommendations (Chapter 10).

Zanutto et al. (2017) showed in their study that a varying demand for multiple stakeholders in industrial control systems represents many organisational challenges. These challenges were reviewed during the interviews with the OT suppliers for sub-research question three, where it was discussed that complexity arises due to these many assets or components of the OT systems at a location. Another argument for these complexities is based on the fact that these OT systems are intertwined with other OT systems, often from other OT suppliers, including the fact that these OT systems are the 'beating heart' of each location when looking at the performance of operations. Another implication can be drawn from this because the possibility exists that inventories of used equipment within OT might be incomplete. This could be possible when OT suppliers or even location employees are unaware of some used equipment when access to that specific part of a location is denied.

Another difference between IT and OT was discussed by McBride et al. (2020), who compared OT and IT cyber security practices to develop an OT cybersecurity workforce development framework. McBride et al. (2020) declare a difference between prioritisation in both IT and OT. IT prioritisation is based on data confidentiality, integrity, and availability (CIA), and OT prioritisation is based on processes' safety, reliability, and availability (SRA). During the interviews with the OT suppliers, it appeared that 50 percent of the participating OT suppliers indicated that security patching or cybersecurity is not their core business. Combined with the fact that less information about *security patching* in OT is available, misalignment of the terminology of security patching is caused. Within the industry, it can be seen that *security patching* is interpreted as ‘installing updates’, whereas some OT suppliers referred to security patching during the interviews as ‘mitigation of unplanned vulnerabilities’, ‘preventive updating and installing software on assets’, ‘preventive maintenance’, and ‘error or bug fixing’. The selected case study organisation uses *security patching as* ‘installing and updating the digital assets within the IT or OT domain’, where academics refer to *security patching* as *“Additional pieces of code developed to address problems in software. Patches are also known as bugs, whereby they enable additional functionality or address security flaws within a program”*, as indicated by Mell et al. (2005) and Dissanayake et al. (2022a).

9.1.2 Patching behaviour has an enormous impact

As said before, security patching in OT differs greatly from security patching in IT. Fortinet (2024) describes that security patching is rarely performed in OT, as doing so may require the entire production process to be halted. By comparison, many IT suppliers have designated ‘patch days’ where the IT systems are rapidly evolving (Fortinet, 2024). McBride et al. (2020) state that *“the plant is a profit centre, if it stops, the money stops flowing in. Consistency is expected. Where emergency fixes and even ‘patch Tuesdays’ fall outside this operational reality”*, indicating that *location downtime* due to security patching will not be approved by location management. Even the risk of more disrupted operations, where not performing security patching results in malfunctions of the OT system since the hardware, firmware, or software is outdated (McBride et al., 2020).

Moreover, Mell et al. (2005) underscore the critical importance of timely patching. According to a report of the Centre for Information Security and Privacy Protection (Dutch: *Centrum informatiebeveiliging en privacybescherming*) (2022), it is most important to perform security patching on time, where timely is stated as adapt to the seriousness of the threat or vulnerability and combine with the advice of the specific OT supplier. One of the most important causes of cyber breaches is generating a backlog in performing security patching, which may increase the risk of hacking and data leaks or breaches (Centre for Information Security and Privacy Protection, 2022). When reflecting on practice, based on the semi-structured interviews with the OT suppliers, security patching is not always performed. Some OT systems are not patched at all since the employees of the OT suppliers do not have the knowledge to do this. They are not certified with a required standard (e.g. ISA/IEC62443). It can also be seen that human knowledge or expertise plays a big part in validating security patching at OT systems, which is very time-consuming. This is due to the required capability or knowledge of the OT supplier’s experts to create mitigating measures or problem-solving in case of an unplanned vulnerability, cyber incidents, or other types of disruptions to resolve these disruptions at the locations. It was indicated that only one out of twelve OT suppliers had no resistance to security patching, whereas, for the other eleven participating OT suppliers, resistance was given by statements that cybersecurity and security patching are not their core business or due to different cultural or structural effects.

Next to this, one OT supplier gave another reason why security patching is not performed within the industrial, operational environment, with the following quote: *“The reason why we patch very little within the industry is that other vulnerabilities are much bigger, such as password management. If I am continuously logged into the system with an ‘admin-admin’ role, the front door to the system is wide open and screaming: “Get in here!”. So actually, security patching of this kind of environments only makes sense if the other vulnerabilities have been fixed.”*, where password rotation and password management were already indicated as a threat in sub-research question one of this research, and safer strategies for password management and rotation of the OT systems at locations, can be seen as a lesson learned.

Dissanayake et al.'s (2022b) research about the consequences of delayed patch applications emphasised the need for a more comprehensive understanding of the practical reasons behind delays. When reflecting on this, it can be concluded that this knowledge gap has been made smaller. The factors indicated in sub-research question three provide insights into the complexity of the security patching processes in an industrial, operational environment, including some reasons behind the delays in security patching: 1) ignorance of OT suppliers about the terminology of security patching, 2) no uniformity in patch (log) processes of OT suppliers, whereby most participating OT suppliers focus on mitigating the unplanned vulnerability, occurred problem, defect, or risk. More in detail, these differences can be seen regarding the steps in creating a patch log, prioritising patch logs, follow-up times and documentation, and 3) reported problems, which can trigger a patch, are mostly sent via email exchange between the OT supplier and their customers, and information can be lost in traffic between the several employees of the different parties, and even over several years. For these reasons, security patching in terms of OT deserves more attention in academic literature and within the practical landscape of an industrial operational environment.

9.1.3 Governmental guidance is missing

It has been said that the European Union has been working on the Network and Information Security (NIS2) directive since 2020 (National Cyber Security Centre, 2024a). This directive is focused on improving the digital and economic resilience of European member states and will be implemented in The Netherlands as the Cyber Security Act (CBW: *Cyberbeveiligingswet*). European member states must comply with the new NIS2 directive before 1 July 2025, which has been set as the implementation date. This means that some organisations within the Netherlands have to improve their current digital environment to comply with this directive.

According to the National Cyber Security Centre (2024a), European member states must support critical, essential and important entities (such as the selected case study organisation) in improving their resilience to digital threats by giving them advice and assistance. Government support can also consist of information exchange, guidelines, and resilience-enhancing instruments, such as the performance of risk assessment towards these critical, essential and important entities (such as the selected case study organisation). However, in terms of the *duty of care*, which obliges organisations to carry out a risk analysis themselves as the basis on which they take appropriate measures for securing the network and information systems they use to provide their business services (National Cyber Security Centre, 2024b), making it unclear for OT supplier within the industrial, operational environment, which are not listed as critical, essential and important entities, how these parties have to be compliant with this NIS2 directive. Governmental guidance is missing towards these OT suppliers of the critical, essential entities (such as the selected case study organisation). This governmental guidance is even more necessary when many responsibilities, such as the performance of security patching, are outsourced to these OT suppliers. For them, applying the NIS2 directive is more complex and challenging without Governmental guidance, even when the level of knowledge regarding cybersecurity at those OT suppliers is less available.

As stated by Cosman (2020), the ISA Global Cybersecurity Alliance (ISAGCA) was formed to part in help increase awareness and adoption of the ISA/IEC62443 standards, as *“the world’s only consensus-based series of automation cybersecurity standards”*. Although these standards have existed for a long period of time, Cosman (2020) states that acceptance and adoption of these standards *“is still not where it should be”*. It can be seen that only 25 percent (three out of twelve) of the participated OT suppliers within this research incorporate the ISA/IEC62443 within their cybersecurity environment. According to Cosman (2020), the reasons may be as follows:

1) The amount of information included in the standards and their perceived complexity.

2) Asset owners find it frightening to understand the standards fully.
3) Asset owners are faced with very real challenges of deciding how to begin to address the ISA/IEC62443, which can be seen as a complex and challenging topic.
4) Awareness of what is available is the start of acceptance and adoption of the ISA/IEC62443.

When reflecting on this last point together with the complex, industrial and operational environment, it can be seen that supplier dependency plays a big role in this. Due to the high level of complexity within the industrial and operational environment, and where managing the OT systems is outsourced to OT suppliers, and sometimes these OT suppliers outsource the software, hardware, and firmware also to other suppliers. Due to this, vulnerabilities may arise when OT suppliers are narrowed down into 'blind corners', where OT suppliers depend on the knowledge of most other market players, stakeholders and other parties. Suppose most market players do not have specific knowledge of security patching within an OT environment. How can the critical, essential, and important entities (such as the selected case study organisation) be compliant with the NIS2 directive if they are dependent on OT suppliers without this knowledge?

9.2 Reflection on the selected case study organisation's perspective

Bhatti et al. (2013) state that Key Performance Indicators (KPIs) can be used to manage the performance of organisations. Even within an industrial, operational environment, KPIs can be used to determine the performance of the OT suppliers for security patching, as stated by the Centre for Information Security and Privacy Protection (2022). They described how several examples of KPIs can be incorporated within the SLA addendum of the selected case study organisation's OT Security Requirement, combined with suggestions for KPIs for security patching by Unterfingher (2023):

1) Security patching performed on time [% installed patches]
2) Amount of resolved vulnerabilities [%average open vs. closed vulnerabilities, based on severity rate]
3) Patching rate [# of patches/year]
4) Scan rate [amount of scans on assets for vulnerabilities/year]
5) Time to detect [time to discover a vulnerability]
6) Time to resolve [time gap between vulnerability detection and resolution]
7) Risk score [determination of overall risk score of the vulnerability]
8) Vulnerability maturity [passed time since the disclosure of vulnerability]
9) Average audit score [determination of average results of audit]
10) Patch prioritization based on vulnerability rating [determination of security score, based on nature of patch]

When reflecting towards the current SLA addendum of the selected case study organisation's OT Security Requirements, none of these types of measurable KPIs can be seen, especially not regarding cybersecurity. This could result in hidden costs due to the following reasons: 1) additional labour costs, since employees need time to recover the OT systems from a data breach, 2) lost revenue due to production standstill as a result of cyber breaches, 3) OT system failures cause business disruptions since the software is not patched or due to missed patches, resulting in loss of turnover, 4) lost time since employees have to be trained to mitigate cyber breaches or other types of malfunctions.

9.3 Limitations of the research

The first limitation of the research can be seen in that the embedded single-case study is organised from the perspective of the selected case study organisation. Moreover, within the selection for including OT suppliers for deriving factors into the complexity of the security patching processes in an industrial, operational domain (sub-research question three), the scope is based on OT suppliers from the Business Unit The Netherlands. Since this is also the scope of the selected case study organisation Expert 2, which was interviews for the second sub-research question. A filter is added to this selection, where only OT suppliers from Business Unit The Netherlands were selected with business services (OT systems) with the criticality of the OT systems labelled as ‘gold’ and ‘monitoring is required’. Moreover, there is a possibility that some OT suppliers of OT systems forgot to invite for the participation in this research, when the selected case study organisation employees are not aware of the existing OT systems on the locations within Business Unit The Netherlands, with the earlier mentioned labels. It could be possible since some operator stations have limited access and all OT systems are manually entered within the selected case study organisation’s asset maintenance program *Service Now*.

Another limitation of the research is that not all OT suppliers who were invited to participate in this research participated in the research. This was due to two reasons: the invited OT suppliers did not want to participate in the research, or the OT supplier did not respond to the invitation for the semi-structured interview for the research. Eventually twelve out of thirty-one OT suppliers with the earlier mentioned labels within Business Unit The Netherlands were included into the research.

A final limitation of the research is that the semi-structured interviews with the OT suppliers were conducted directly with OT practitioners, not with software engineers/employees of the research and development departments of these OT suppliers. Where one participating OT supplier did not have a direct service level agreement with the selected case study organisation for a delivered OT system at the selected case study organisation’s locations, but their OT system was delivered through an intermediary at the selected case study organisation’s locations, which was also interviewed within the research.

Chapter 10: Recommendation for future research or practice

Within this Chapter, recommendations for future research or practice are given. Within Chapter 10.1 recommendations for the industry related to OT suppliers are shown. Whereas recommendations for the selected case study organisation within this research can be seen within Chapter 10.2.

10.1 Recommendation for the industry within the operational domain

The recommendation for the industry within the operation domain is to close the knowledge gap within the cybersecurity environment in OT. There is much ignorance about cybersecurity and security patching for OT applications, where it can be seen that not all OT suppliers are in control and most are missing knowledge in OT cybersecurity since they: 1) are not checking CVE, 2) are neglecting proactive scans of their OT systems, 3) are not using KPIs to indicate or evaluate security levels of their OT systems, 4) cannot test their updates or patches within a test environment, before installing them at the OT systems at locations, 5) cannot provide backups of OT systems to ensure restoring of the entire OT system, and finally 6) are not certified for implementing cybersecurity standards. Within the operational landscape, it can be seen that there are many stakeholders and many OT suppliers, and knowledge is left behind, resulting in *supplier dependence*: dependence on suppliers who actually can perform security patching or develop software.

10.2 Recommendations for the selected case study organisation

On the other side, the three recommendations for the selected case study organisation within this research are as follows:

1) Implementing patch management into the selected case study organisation’s OT security documents (policy, requirements, standards and SLAs). When this is incorporated within these documents, the new suppliers' onboarding process must also be adjusted, resulting in the inclusion of patch management. Within the current state of these documents, very little information is available about the deployment of security patching processes and patch logs.

2) Set up more preferred OT suppliers and define solutions for other locations. When implementing this recommendation, not every location has to reinvent the wheel; consensus is equalised so that fewer OT suppliers are contracted to locations within the same Business Unit (for example, not four OT suppliers of CCTV monitoring systems within the Business Unit The Netherlands) and lessons learned are incorporated into the business services at other locations or service level agreements with other OT suppliers. Where the amount of differentiation between same type of OT systems is reduced within the Business Unit.

3) The current SLA addendum for OT Security Requirements has to be revised so that the OT suppliers can be assessed based on their performance and their quality. The selected case study organisation cannot indicate if the OT suppliers are in control based on the requirements given in the current SLA addendum for OT Security. When Key Performance Indicators (KPIs) are included within the revision of the SLA addendum, the performance, including the quality of the OT supplier, can be measured.

4) Local certification of the ISA/IEC62443 has to be achieved. These standards are the fundamental policy of the selected case study organisation’s OT Security documents. However, no local knowledge is available regarding this certification with standards, making implementing and assessing these standards within the internal OT Security documents challenging.

References

- Arora, A., Krishnan, R., Nandkumar, A., & Heinz, H. J. (2004). Impact of vulnerability disclosure and patch availability – An Empirical analysis. *ResearchGate*. https://www.researchgate.net/publication/228969534
- Ary, D., Jacobs, L. C., & Sorensen, C. (2006). *Introduction to research in Education.* Wadsworth Publishing Company.
- Automox. (2020a). *New cyber hygiene report uncovers a patching dilemma in America.* Retrieved 12 February 2024, of https://www.automox.com/resources/news/2020-cyber-hygiene-report-announcement
- Automox. (2020b). 2020 *Cyber Hygiene Report: What You Need to Know Now Webinar Recap.* Automox. https://www.automox.com/blog/2020-cyber-hygiene-report-webinar-recap
- Bauer, J. M., & Herder, P. M. (2009). Designing Socio-Technical systems. In *Elsevier eBooks* (pp. 601–630). https://doi.org/10.1016/b978-0-444-51667-1.50026-4
- Bhatti, M. I., Awan, H. M., & Razaq, Z. (2013). The key performance indicators (KPIs) and their impact on overall organizational performance. *Quality & Quantity, 48*(6), 3127–3143. https://doi.org/10.1007/s11135-013-9945-y
- Böhme, R. (2010). Security Metrics and Security Investment Models. In *Lecture notes in computer science* (pp. 10–24). https://doi.org/10.1007/978-3-642-16825-3_2
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/qrj0902027
- Braun, V., & Clarke, V. (2020). One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology, 18*(3), 328–352. https://doi.org/10.1080/14780887.2020.1769238
- Casula, M., Rangarajan, N. & Shields, P. (2020). The potential of working hypotheses for deductive exploratory research. *Qual Quant, 55*(5), 1703–1725. https://doi.org/10.1007/s11135-020-01072-9
- Centre for Information Security and Privacy Protection. (2022). Managing information security; tools for directors and CISOs. In *Bio-overheid*. https://bio-overheid.nl/media/wdxhzwsn/sturen-op-informatieveiligheid.pdf
- Cosman, E. (2020). *Structuring the ISA/IEC62443 Standards.* ISA Global Cybersecurity Alliance (ISAGCA). Retrieved on 24 October 2024, of https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Sage Publications, Inc.
- DCMR Environmental Protection Agency. (n.d.). *DCMR Environmental Protection Agency.* Retrieved 6 November 2024, of https://www.dcmr.nl/dcmr-environmental-protection-agency
- Deakin University. (2023, 17 July). *Primary versus secondary data.* Deakin University Library. Retrieved 15 January 2024, of https://www.deakin.edu.au/library/research/manage-data/plan/primary-versus-secondary-data#:~:text=Primary%20data%20are%20the%20original,both%20types%20of%20research%20data.
- Denzin, N. K. (1970). *The research act: A theoretical introduction to sociological methods.* New York: Aldine.
- de Smale, S., van Dijk, R., Bouwman, X. B., van der Ham, J., & van Eeten, M. J. G. (2023). *No One Drinks From the Firehose: How Organizations Filter and Prioritize Vulnerability Information*. 203-219. Paper presented at 2023 IEEE Symposium on Security and Privacy (SP), San Francisco,

California, United States. https://www.computer.org/csdl/proceedings-article/sp/2023/933600a203/1He7XVgB584

- Dissanayake, N., Zahedi, M., Jayatilaka, A., Babar, A. (2021). A grounded theory of the role of coordination in software security patch management. *Proceedings of the 29th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE '21), ACM, New York, NY, USA*. http://dx.doi.org/10.1145/3468264.3468595.
- Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, A. (2022a). Software Security Patch Management - A systematic literature review of challenges, approaches, tools and practices. *Information & Software Technology, 144*, 106771. https://doi.org/10.1016/j.infsof.2021.106771
- Dissanayake, N., Zahedi, M., Jayatilaka, A., & Babar, M. A. (2022b). Why, how and where of delays in software security patch management: An Empirical investigation in the healthcare sector. *Proceedings of the ACM on human-computer interaction, 6*(CSCW2), 1–29. https://doi.org/10.1145/3555087
- Edwards, M. (2024, 12 March). *The Ultimate Guide to ISO 27001.* ISMS.online. https://www.isms.online/iso-27001/
- Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532. https://doi.org/10.2307/258557
- Emerson. (2024). *Safety Instrumented Systems.* Retrieved 2 November 2024, of https://www.Emerson.com/nl-nl/automation/control-and-safety-systems/safety-instrumented-systems-sis
- European Commission. (n.d.). *Equipment for potentially explosive atmospheres (ATEX).* Internal Market, Industry, Entrepreneurship And SMEs. Retrieved 6 November 2024, of https://single-market-economy.ec.europa.eu/sectors/mechanical-engineering/equipment-potentially-explosive-atmospheres-atex_en
- Evripidou, S., & Watson, J. D. McK. (2024). Understanding Operational Technology Personnel's Mindsets and Their Effect on Cybersecurity Perceptions: A Qualitative Study With Operational Technology Cybersecurity Practitioners. *EuroUSEC 2024.* https://eurousec24.kau.se/pre-proceedings/63.pdf
- Feng, N., Zhang, H., Chen, D., Zhang, J., Li, M., & Xie, J. (2022). Optimal adoptions of freemium version and patching strategy: network and security externalities. *Journal of Management Science and Engineering, 7*(1), 107–132. https://doi.org/10.1016/j.jmse.2021.10.001
- Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal Of Qualitative Methods, 1–1.* http://www.ualberta.ca/~iiqm/backissues/5_1/pdf/fereday.pdf
- Fortinet. (2024). *Information Technology (IT) vs. Operational Technology (OT) Cybersecurity.* https://www.fortinet.com/resources/cyberglossary/it-vs-ot-cybersecurity#:~:text=There%20are%20significant%20OT%20and,systems%20like%20iOS%20and%20Windows.
- Gill, P., & Baillie, J. (2018). Interviews and focus groups in Qualitative Research: An Update for the Digital Age. *British Dental Journal, 225*(7), 668–672. https://doi.org/10.1038/sj.bdj.2018.815
- Gillis, A. S. (2023, 27 January). *Distributed control system (DCS).* TechTarget. https://www.techtarget.com/whatis/definition/distributed-control-system
- Goodman, C. (2024a, 21 October). *What are Common Vulnerabilities and Exposures (CVE)?* Balbix. https://www.balbix.com/insights/what-is-a-cve/

- Goodman, C. (2024b, 25 October). *What is the Common Vulnerability Scoring System (CVSS)?* Balbix. https://www.balbix.com/insights/understanding-cvss-scores/
- Greiner, L., Overby, S., & Gibbons, L. (2024, 21 June). *What is an SLA? Best practices for service-level agreements.* CIO. https://www.cio.com/article/274740/outsourcing-sla-definitions-and-solutions.html
- Gürel, E. (2017). SWOT analysis: a theoretical review. *Journal Of International Social Research, 10*(51), 994–1006. https://doi.org/10.17719/jisr.2017.1832
- Hecker, J., & Kalpokas, N. (2023, 17 September). *The Ultimate Guide to Qualitative Research - Part 2: Handling Qualitative Data.* ATLAS.ti. Retrieved 20 December 2023, of https://atlasti.com/guides/qualitative-research-guide-part-2/qualitative-data-analysis
- Inductive automation. (2018, 18 September). *SCADA: Supervisory Control and Data Acquisition.* Inductive Automation. Retrieved 3 November 2024, of https://inductiveautomation.com/resources/article/what-is-scada
- International Organization for Standardization. (2022, 25 October). *ISO/IEC 27000 family.* International Organization For Standardization. Retrieved 6 November 2024, of https://www.iso.org/standard/iso-iec-27000-family
- ISA Global Cybersecurity Alliance (ISAGCA). (2024). *The world's only Consensus-Based Automation and Control Systems cybersecurity standards.* Retrieved on 24 October 2024, of https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- Islam, C., Babar, M. A., & Nepal, S. (2019). A Multi-Vocal review of security orchestration. *ACM Computing Surveys, 52*(2), 1–45. https://doi.org/10.1145/3305268
- Kovacs, E. (2019, 8 April). *Most OT Organizations Hit by Damaging Cyberattacks: Survey.* Securityweek. https://www.securityweek.com/most-ot-organizations-hit-damaging-cyberattacks-survey/
- Marlow, C.R. (2005) *Research Methods for Generalist Social Work.* Thomson Brooks/Cole, New York.
- Maylor, H. (2001). Beyond the Gantt chart: *European Management Journal, 19*(1), 92–100. https://doi.org/10.1016/s0263-2373(00)00074-8
- McBride, S. M., Schou, C. D., & Slay, J. (2020). *A security workforce to bridge the IT/OT gap.* Industrial Cyber Force. Retrieved from https://industrialcyberforce.org/wp-content/uploads/2020/08/A-Security-Workforce-to-Bridge-the-IT-OT-Gap.pdf
- Mell, P., Bergeron, T., & Henning, D. (2005). Creating a Patch and Vulnerability Management Program. In *NIST* (Nr. 800-40 version 2.0).
- Ministry of Economic Affairs, Agriculture and Innovation. (2023, 3 January). *Information and communication technology (ICT).* Rijksoverheid. Retrieved 28 January 2024, of https://www.rijksoverheid.nl/onderwerpen/ict/veilige-infrastructuur
- Ministry of Justice and Security. (2021, 26 February). *IACS/OT.* Cyber Security Council. Retrieved 8 November 2024, of https://www.cybersecuritycouncil.nl/advisory-documents/iacs-ot#:~:text=Industrial%20Automation%20%26%20Control%20Systems%20(IACS,their%20destination%2C%20containers%20are%20being
- Mumford, E. (2000). A Socio-Technical Approach to Systems Design. *Requirements Engineering, 5*(2), 125–133. https://doi.org/10.1007/pl00010345
- NAMUR. (2024). NAMUR – *Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V.* Retrieved 6 November 2024, of https://www.namur.net/en/index.html

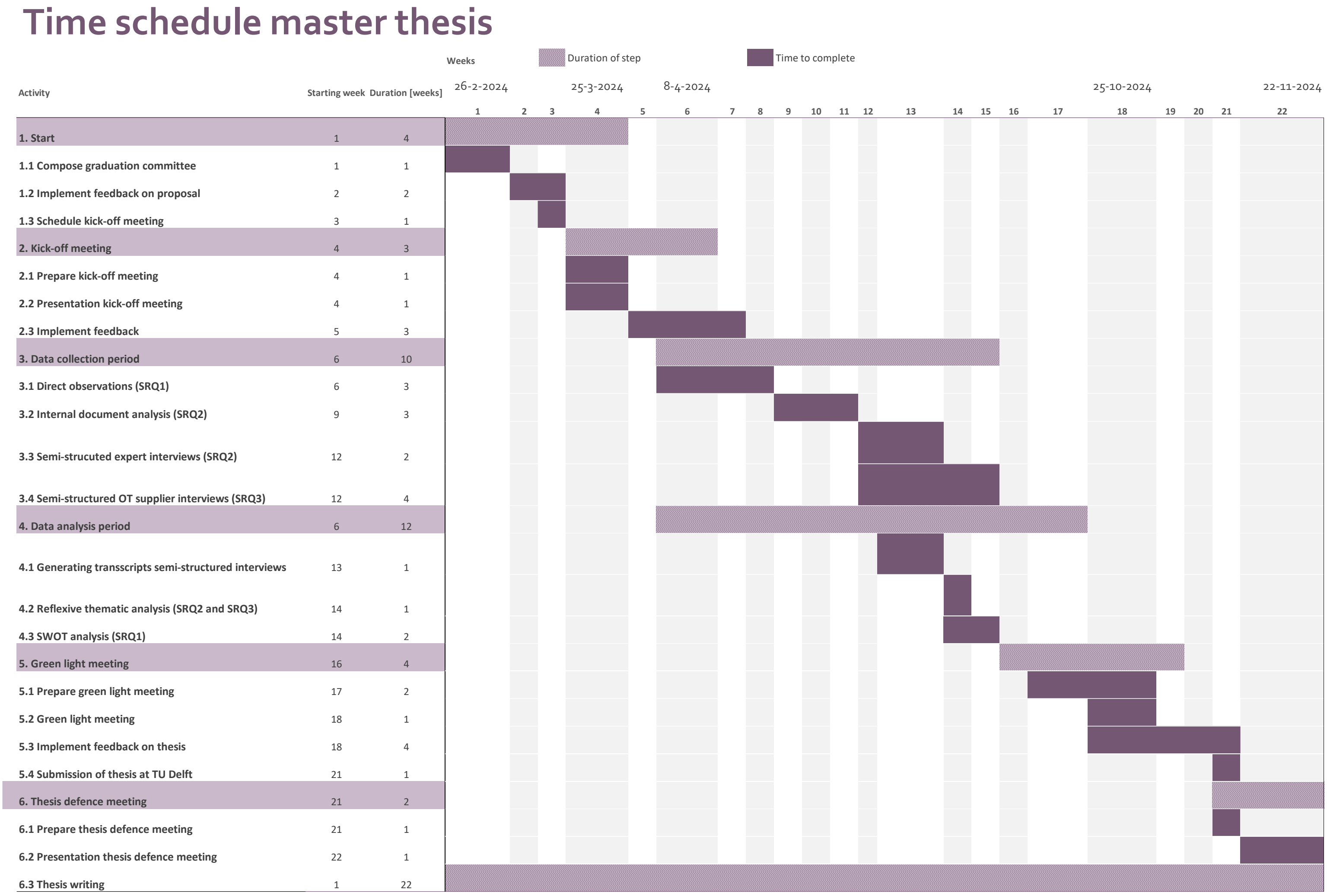
- National Cyber Security Centre. (2024a, 24 September). *Network and Information Security (NIS2) directive.* https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie
- National Cyber Security Centre. (2024b, October 10). *Rights and obligations.* https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/samenvatting-nis2-richtlijn
- NEN. (n.d.-a). *NEN 1010 Low-voltage installations.* Retrieved 6 November 2024, of https://www.nen.nl/elektrotechniek/installatievoorschriften/nen-1010-laagspanningsinstallaties
- NEN. (n.d.-b). *NEN 3140 Low-voltage installations*. Retrieved 6 November 2024, of https://www.nen.nl/elektrotechniek/werkvoorschriften/laagspanninginstallaties
- NEN. (2017, 1 December). *NEN 2535:2017 nl.* https://www.nen.nl/nen-2535-2017-nl-236752
- NIST. (2020). Security and Privacy Controls for Information Systems and Organizations. In *NIST | National Institute Of Standards And Technology* (Nr. 800-53 Revision 5). https://doi.org/10.6028/nist.sp.800-53r5
- NMi. (n.d.). Certification of quality systems. NMi | Certificates. Retrieved 3 November 2024, of https://nmi.nl/services/certificates/
- Norman, D. (2016, 9 September). *What are Socio-Technical Systems?* The Interaction Design Foundation. Retrieved 11 December 2023, of https://www.interaction-design.org/literature/topics/socio-technical-systems#:~:text=A%20socio%2Dtechnical%20system%20(STS)%20in%20software%20engineering%20is,of%20a%20system.
- Paessler. (n.d.). *What is CCTV?* Retrieved 5 November 2024, of https://www.paessler.com/it-explained/cctv
- Porcedda, M. G. (2018). Patching the patchwork: Appraising the EU regulatory framework on cyber security breaches. *Computer Law & Security Review, 34*(5), 1077–1098. https://doi.org/10.1016/j.clsr.2018.04.009
- Rebensky, S., Carroll, M., Nakushian, A., Chaparro, M., & Prior, T. (2021). Understanding the last line of defense: human response to cybersecurity events. In *Lecture Notes in Computer Science* (pp. 353–366). https://doi.org/10.1007/978-3-030-77392-2_23
- Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., & Lightman, S. (2022). Guide to Operational Technology (OT) security. In *NIST | National Institute Of Standards And Technology.* https://doi.org/10.6028/nist.sp.800-82r3
- Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *ACM*. https://doi.org/10.1145/2601248.2601268
- Trist, E. L., & Bamforth, K. W. (1951). Some Social and Psychological Consequences of the Longwall Method of Coal-Getting. *Human Relations, 4*(1), 3–38. https://doi.org/10.1177/001872675100400101
- Twin, A. (2024, 22 Augustus). *KPIs: What Are Key Performance Indicators? Types and Examples.* Investopedia. https://www.investopedia.com/terms/k/kpi.asp
- Unterfingher, V. (2023, 7 March). *KPI Examples for Patch and Vulnerability Management.* Heimdal Security Blog. https://heimdalsecurity.com/blog/kpi-examples-for-patch-and-vulnerability-management/
- Yin, R. K. (2011). *Applications of case study research.* SAGE Publications.
- Zanutto, A., Shreeve, B., Follis, K. S., Busby, J. S., & Rashid, A. (Reds.). (2017). *The Shadow Warriors: In the no man's land between industrial control systems and enterprise IT systems.* Symposium On Usable Privacy and Security.

https://www.researchgate.net/publication/317693873_The_Shadow_Warriors_In_the_no_man%27s_land_between_industrial_control_systems_and_enterprise_IT_systems

- Zola, A. (2024, 22 March). *Programmable logic controller (PLC).* TechTarget. https://www.techtarget.com/whatis/definition/programmed-logic-controller-PLC#:~:text=A%20programmable%20logic%20controller%20(PLC)%20is%20a%20small%2C%20modular,for%20performing%20a%20particular%20task.

Appendices

Appendix 1: Time schedule research



Time schedule master thesis

▨ Duration of step

■ Time to complete

Activity	Starting week	Duration [weeks]
1. Start	1	4
1.1 Compose graduation committee	1	1
1.2 Implement feedback on proposal	2	2
1.3 Schedule kick-off meeting	3	1
2. Kick-off meeting	4	3
2.1 Prepare kick-off meeting	4	1
2.2 Presentation kick-off meeting	4	1
2.3 Implement feedback	5	3
3. Data collection period	6	10
3.1 Direct observations (SRQ1)	6	3
3.2 Internal document analysis (SRQ2)	9	3
3.3 Semi-strucuted expert interviews (SRQ2)	12	2
3.4 Semi-structured OT supplier interviews (SRQ3)	12	4
4. Data analysis period	6	12
4.1 Generating transscripts semi-structured interviews	13	1
4.2 Reflexive thematic analysis (SRQ2 and SRQ3)	14	1
4.3 SWOT analysis (SRQ1)	14	2
5. Green light meeting	16	4
5.1 Prepare green light meeting	17	2
5.2 Green light meeting	18	1
5.3 Implement feedback on thesis	18	4
5.4 Submission of thesis at TU Delft	21	1
6. Thesis defence meeting	21	2
6.1 Prepare thesis defence meeting	21	1
6.2 Presentation thesis defence meeting	22	1
6.3 Thesis writing	1	22

Figure 11.1: Gantt chart time schedule

Appendix 2: SLA Addendum regarding OT security requirements

This information has been removed within this published external version of the thesis due to sensitive information of the case study organisation.

Figure 11.2: SLA Addendum regarding OT security requirements

Appendix 3: Questionnaire for semi-structured interview with the selected case study organisation's expert employees

1. **Introduction of participant**
    a. What is your current role or job description at the selected case study organisation?
    b. What is the scope of your responsibilities (IT/OT/both)?
    c. What specific responsibilities do you have?
    d. How do you cooperate with the Global IT/OT team?

2. **Governance at Selected case study organisation**
    a. Who is responsible for the policy or governance of the following documents?
        i. Referring towards the selected case study organisation's internal documents: CIS-P-003, CIS-S-504
    b. Why are only two components of ISO/IEC-62443 implemented within these documents?
        i. Components 2-1 and 3-3?
    c. What are the responsibilities of the Global IT/OT team of the selected case study organisation?
    d. Who performs quality checks on OT suppliers?
    e. How is the onboarding process of new (OT) suppliers facilitated?
        i. Regulated via procurement? Or somewhere else?
        ii. Is there a difference between IT and OT?
    f. Why is there no overview of all the suppliers/vendors contracted with business services within the OT domain?

3. **Security patching processes/SLA at the selected case study organisation**
    a. How is the governance structured concerning responsibilities for detecting, registering and prioritising cybersecurity vulnerabilities?
        i. Who takes ownership/responsibility for patching (the OT supplier or the selected case study organisation)?
    b. Who drafted the current SLA addendum (see Appendix 1)?
        i. Why are these requirements not SMART formulated?
    c. What are the KPIs for security patching at the selected case study organisation within the OT domain?
    d. Who monitors the OT supplier to ensure they meet the required quality standards?
    e. How is the quality measured of the performed activities of the OT suppliers?
    f. Why are the security patching processes within OT outsourced to the OT suppliers?
        i. Via the SLA addendum?
    g. Why is the IT security patching managed by the selected case study organisation itself, but OT is not?
    h. Within the SLA is stated, that there are vendor-meetings, what is discussed during these vendor-meetings?
        i. Can you show me the agenda of this meeting?
        ii. What is discussed yearly/half yearly/monthly/weekly?
    i. What are the selected case study organisation's cybersecurity regulations?
        i. Regarding (periodic) patching, anti-malware updates, offsite backups, and restore tests

   - ii. The selected case study organisation uses patching *'to install updates at their assets'*, not necessarily to solve vulnerabilities within the cyber environment, as suggested by academic literature, why?
- j. Are scans performed on each (virtual) asset to assess vulnerabilities?
   - i. If yes, which scans are performed?
   - ii. If not, why aren't scans performed?
- k. How are high-impact disruptions reported, registered, communicated and escalated at the selected case study organisation?
   - i. How are lessons learned captured to prevent the reoccurrence of vulnerabilities or high-impact disruptions?
- l. Are cyber incidents included within the business contingency plan on the locations?
   - i. If yes, how?
   - ii. Is this implemented at each location, or are there some differentiations amongst the locations?
- m. Who decides which cybersecurity points which are included on the list in the annual internal audit? Is this yearly reviewed or updated?

4. Vulnerabilities and risks with cybersecurity

- a. Who is responsible for monitoring and alerting of new vulnerabilities?
- b. Is it controlled by the selected case study organisation or dependent on the OT supplier?
- c. How does the selected case study organisation identify its cybersecurity vulnerabilities?
- d. When is a (virtual) asset vulnerable?
- e. How are risks mitigated if an unplanned vulnerability has occurred at the (virtual) assets?
   - i. Are scans performed by Selected case study organisation on each (virtual asset) to examine this?
   - ii. If yes, which scans are performed? If not, why aren't scans performed?
- f. How does the selected case study organisation determine if a (virtual) asset needs an update or installation?
- g. How are vulnerabilities managed and monitored at the selected case study organisation?
- h. Does the selected case study organisation regularly check CVE for vulnerabilities?
   - i. If not, why not?

Appendix 4: Informed consent form interviews OT-suppliers

Dear participant,

You are invited to participate in a research study titled *The complexity of security patching processes within the OT landscape at a logistic service provider in the liquid bulk industry.* Rozemarijn Schraven is doing this study in the name of the TU Delft and the selected case study organisation.

The purpose of this research study is to analyse the security patching processes within the OT domain of the selected case study organisation with their performance, regarding the interactions of human behaviour. Based on this synthesis, possible improvements can be generated, leading towards valuable aspects for redesigning these processes. To analyse the security patching processes, your perspective, attitude, opinion and expertise are needed, via this open-ended interview. This will take you approximately 45 minutes to complete.

The gathered information will be used to gain insights into the security patching processes within the OT domain of the selected case study organisation and to visualize these processes in schematic overviews. For this purpose, the open-ended interview will be recorded, so the researcher can relisten the recording when transcribing the interview. After the transcript is completed, the participant receives the transcript, to check and give approval for usage as data within the Master thesis. If adjustments are necessary before the approval, this will be executed first. The open-ended interview will be started with the starting questions below, whereafter follow-up questions will be formulated based on the previous answers of the participant. The participants of this open-ended interview are employees or experts of various ICT suppliers. These ICT suppliers perform security patching as a result of their service-level agreements with the selected case study organisation. The starting questions are given below, whereby these questions are combined within five topics:

1. Introduction of the participant and organisation
    a. What is your role or job description nowadays at your organisation?
    b. In which domain are you active?
    c. How long have you been working at your organisation?
    d. How is your organisation related to the selected case study organisation?
    e. How does your organisation interact with the selected case study organisation? Or how is the cooperation between your organisation and the selected case study organisation?
        i. What are the advantages or disadvantages?
    f. Is this cooperation with the selected case study organisation equivalent to cooperations with other clients of your organisation?

2. Vulnerabilities and risks within the cyber security
    a. Who is responsible for monitoring and alerting of new vulnerabilities?
    b. How do you know as an organization that you are vulnerable within cyber security?
        i. Or when your (virtual) asset is vulnerable?
        ii. Are scans performed on each (virtual asset) to examine this?
        iii. If yes: which scans are performed? If not: why aren't scans performed?
    c. How do you identify if a (virtual) asset needs an update or installation?
    d. How are the vulnerabilities being managed at the selected case study organisation's locations within the OT domain?
    e. In what kind is OT included within the cyber security environment?
    f. Are there special considerations for vulnerabilities and risks within the OT environment?

   g. How are risks mitigated if an unplanned vulnerability has occurred at the (virtual) assets?

3. Knowledge about security patching
   a. How is your work related to security patching?
   b. How much time do you spend on security patching compared with a 40-hour work week?
   c. Are there KPIs drafted for security patching within this organization?
   d. How do you as a (smaller) ICT supplier know when to patch?
      i. Are you checking CVE regularly? Or another catalogue?
      ii. Do you include any risks? Example: risk of a shutdown of a location while installing?
   e. Is there a test environment at the organization, where the newly developed updates are being tested, before installing the updates at the selected case study organisation's location?
   f. Can you show me where to find information about how this organisation performs the security patching processes for the selected case study organisation?
      i. If not: Can you describe the current security patching process(es) with its sub-steps?
   g. Are human interactions needed to perform actions or process steps within these security patching processes? If yes: for which elements?
      i. Human interactions are described as actions employees have to carry out while performing the patchwork. It could also be the interaction between the employees and the security patch process itself.
      ii. If human interactions are involved, how much time do these take?
      iii. If no human interactions are involved, is there some other process step where expert knowledge is required?

4. Patch logs
   a. Some companies use patch logs, to indicate a weakness within the cyber environment (within IT or OT). Tickets are generated within the organization whereby the team (mostly ICT) of the organization will mitigate and solve the weakness within the cyber environment. Does this organization have a comparable patch log system nowadays?
   b. If this organization uses patch logs, how is this carried out? (If not: why is this not used?) Follow-up questions could be:
      i. How much time are you spending to register a patch log?
      ii. Why are you logging a patch in this way? Or why are you not logging a patch in this way?
      iii. What kind of expertise is needed to log a patch?
      iv. Can you describe for me what kind of (manual) actions you have to handle to register a patch log?
      v. Do you receive a follow-up on this patch log?
      vi. How much time is there between the initiation of the patch log and the follow-up of the patch log?
      vii. Are these patch logs archived in a place where the involved experts of the organization of others (employees of the selected case study organisation) can retrieve these?

5. Updating security patching processes
    a. How often are the security patching processes updated or adjusted (of the selected case study organisation or the ICT supplier)?
    b. If the process is updated regularly, are you being trained to know the new version of the security patching process?
    c. If not: do you have a wish for this?
    d. What else is related to the security patching processes at the selected case study organisation (based on your perspective)?
    e. What can be improved within the security patching processes at the selected case study organisation (based on your perspective)?
    f. How are the security patching processes formed in the ideal situation (based on your perspective)?

As with any online activity, the risk of a breach is always possible. To the best of our ability, your answers in this study will remain confidential. We will minimize any risks by making the transcript fully anonymous (by changing the name to the function of the participant within the transcript) and deleting the recording when the transcript is approved by the participant. The original recordings will be kept available for the researcher until 31 October 2024, whereby after this date, the recordings will be deleted. The recording of the open-ended interviews, as well as the signed consent form will be stored at Microsoft Teams on the server of the TU Delft. Access towards the signed consent forms and the anonymous transcripts will be the supervisors of the master thesis form the TU Delft and the selected case study organisation. The stored audio recordings will only be accessible to the researcher and the supervisor of the TU Delft. The findings or synthesis of the transcripts, which again will be fully anonymized, will be used within the Master Thesis and can be found within the Annex of the Master Thesis itself, which after submission can be found on the TU Delft Repository. The anonymous transcripts will be deleted after one month after the submission of the master Thesis itself.

Your participation in this study is entirely voluntary *and you can withdraw at any* time. You are free

Signatures

I, as participant, understand the expectations of this open-ended interview and approve the described procedures for contributing to this Master thesis by signing this consent form.

______________________________ ______________________________ _______________

Name of participant Signature Date

I, as researcher, have accurately read out the information sheet to the potential participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.

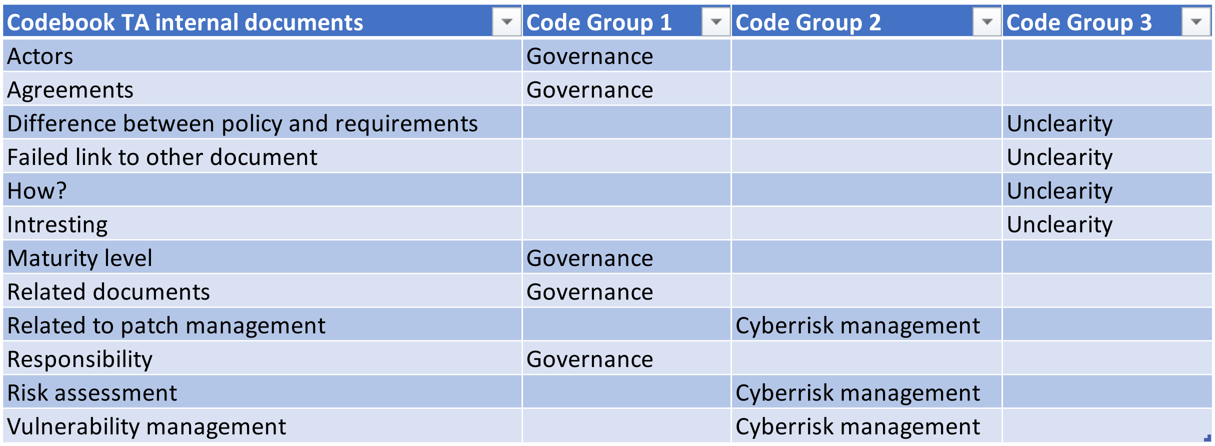
______________________________ ______________________________ _______________

Name of researcher Signature Date

Please tick the appropriate boxes.	**Yes**	**No**
A: GENERAL AGREEMENT – RESEARCH GOALS, PARTICIPANT TASKS AND VOLUNTARY PARTICIPATION		
1. I have read and understood the study information dated [DD/MM/YYYY], or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	☐	☐
2. I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.	☐	☐
3. I understand that taking part in the study involves: - Open-ended interviews with audio recordings - Anonymized transcripts of the interviews in text - The audio recording will be destroyed after 31 October 2024 - Data will be kept at Microsoft Teams on the server of TU Delft	☐	☐
4. I understand that the study will end around 31 October 2024.	☐	☐
B: POTENTIAL RISKS OF PARTICIPATING (INCLUDING DATA PROTECTION)		
5. I understand that taking part in the study involves the following risk as with any online activity, the risk of a breach is always possible. I understand that these will be mitigated by the ability to ask for the interview to stop at any point. Next to this, the answers to the questions in this study will remain confidential and the transcripts will be made fully anonymous. Lastly, the recording will be deleted after 31 October 2024.	☐	☐
6. I understand that personally identifiable research data (PIRD) is considered sensitive data within GDPR legislation.	☐	☐
7. I understand that the steps described in point B.5 will be taken to minimise the threat of a data breach and protect my identity in the event of such a breach.	☐	☐
8. I understand that personal information collected about me or provided within the interview that can identify me, such as [e.g. my name], will not be shared beyond the study team or included within the Master thesis.	☐	☐
C: RESEARCH PUBLICATION, DISSEMINATION AND APPLICATION		
9. I understand that after the research study, the de-identified information I provide will be used for providing conclusions of the gathered data within the master thesis report. This can be seen after finishing the master thesis on the TU Delft Repository and possibly as a publication of a research paper. Hereby all de-identified information will be generalized and anonymized.	☐	☐
10. I agree that my responses, views or other input can be quoted anonymously in research outputs.	☐	☐
Please tick the appropriate boxes.	**Yes**	**No**
D: (LONGTERM) DATA STORAGE, ACCESS AND REUSE		
11. I permit the de-identified open-ended interview anonymous transcript that I provide to be archived as an element of the master thesis on the TU Delft repository so it can be used for future research and learning.	☐	☐

Appendix 5: Codebook Thematic analysis internal document analysis

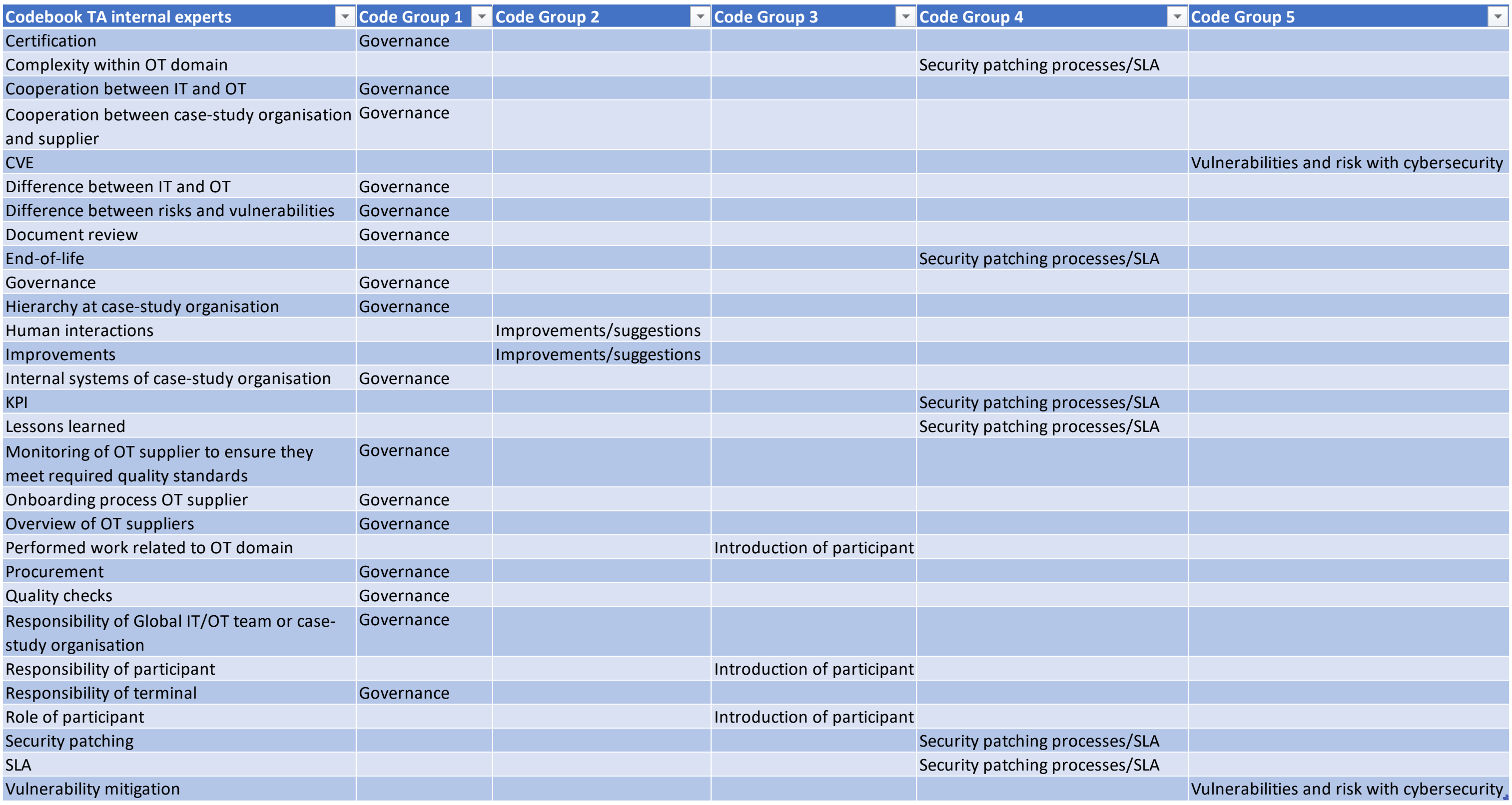
Table 11.1: Codebook Thematic analysis internal documents



Codebook TA internal documents	Code Group 1	Code Group 2	Code Group 3
Actors	Governance		
Agreements	Governance		
Difference between policy and requirements			Unclearity
Failed link to other document			Unclearity
How?			Unclearity
Intresting			Unclearity
Maturity level	Governance		
Related documents	Governance		
Related to patch management		Cyberrisk management	
Responsibility	Governance		
Risk assessment		Cyberrisk management	
Vulnerability management		Cyberrisk management	

Appendix 6: Codebook Thematic analysis transcript internal experts

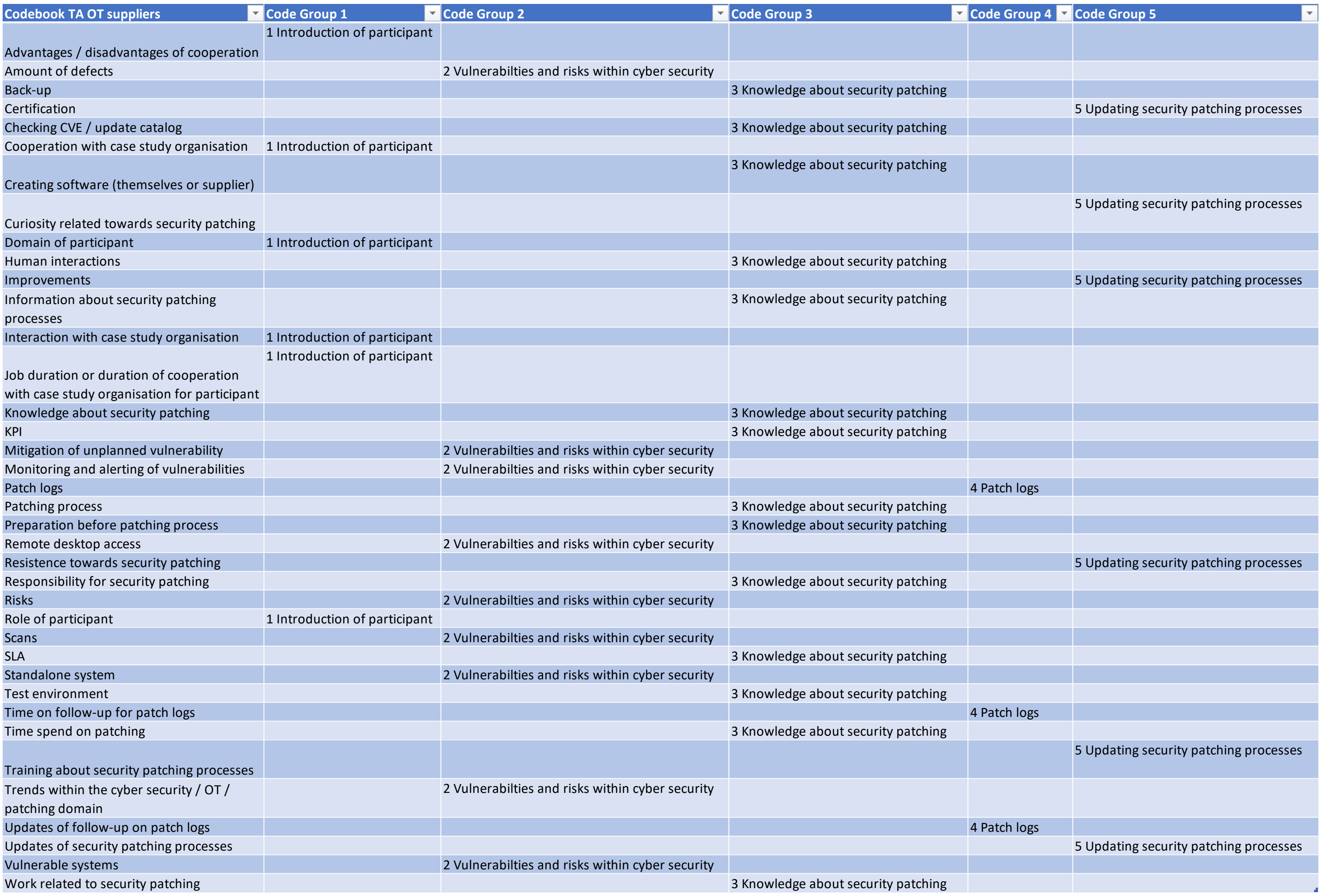
Table 11.2: Codebook Thematic analysis transcripts internal experts



Codebook TA internal experts	Code Group 1	Code Group 2	Code Group 3	Code Group 4	Code Group 5
Certification	Governance				
Complexity within OT domain				Security patching processes/SLA	
Cooperation between IT and OT	Governance				
Cooperation between case-study organisation and supplier	Governance				
CVE					Vulnerabilities and risk with cybersecurity
Difference between IT and OT	Governance				
Difference between risks and vulnerabilities	Governance				
Document review	Governance				
End-of-life				Security patching processes/SLA	
Governance	Governance				
Hierarchy at case-study organisation	Governance				
Human interactions		Improvements/suggestions			
Improvements		Improvements/suggestions			
Internal systems of case-study organisation	Governance				
KPI				Security patching processes/SLA	
Lessons learned				Security patching processes/SLA	
Monitoring of OT supplier to ensure they meet required quality standards	Governance				
Onboarding process OT supplier	Governance				
Overview of OT suppliers	Governance				
Performed work related to OT domain			Introduction of participant		
Procurement	Governance				
Quality checks	Governance				
Responsibility of Global IT/OT team or case-study organisation	Governance				
Responsibility of participant			Introduction of participant		
Responsibility of terminal	Governance				
Role of participant			Introduction of participant		
Security patching				Security patching processes/SLA	
SLA				Security patching processes/SLA	
Vulnerability mitigation					Vulnerabilities and risk with cybersecurity

Appendix 7: Codebook Thematic analysis transcripts OT-suppliers

Table 11.3: Codebook Thematic analysis transcripts OT-suppliers



Codebook TA OT suppliers	Code Group 1	Code Group 2	Code Group 3	Code Group 4	Code Group 5
Advantages / disadvantages of cooperation	1 Introduction of participant				
Amount of defects		2 Vulnerabilties and risks within cyber security			
Back-up			3 Knowledge about security patching		
Certification					5 Updating security patching processes
Checking CVE / update catalog			3 Knowledge about security patching		
Cooperation with case study organisation	1 Introduction of participant				
Creating software (themselves or supplier)			3 Knowledge about security patching		
Curiosity related towards security patching					5 Updating security patching processes
Domain of participant	1 Introduction of participant				
Human interactions			3 Knowledge about security patching		
Improvements					5 Updating security patching processes
Information about security patching processes			3 Knowledge about security patching		
Interaction with case study organisation	1 Introduction of participant				
Job duration or duration of cooperation with case study organisation for participant	1 Introduction of participant				
Knowledge about security patching			3 Knowledge about security patching		
KPI			3 Knowledge about security patching		
Mitigation of unplanned vulnerability		2 Vulnerabilties and risks within cyber security			
Monitoring and alerting of vulnerabilities		2 Vulnerabilties and risks within cyber security			
Patch logs				4 Patch logs	
Patching process			3 Knowledge about security patching		
Preparation before patching process			3 Knowledge about security patching		
Remote desktop access		2 Vulnerabilties and risks within cyber security			
Resistence towards security patching					5 Updating security patching processes
Responsibility for security patching			3 Knowledge about security patching		
Risks		2 Vulnerabilties and risks within cyber security			
Role of participant	1 Introduction of participant				
Scans		2 Vulnerabilties and risks within cyber security			
SLA			3 Knowledge about security patching		
Standalone system		2 Vulnerabilties and risks within cyber security			
Test environment			3 Knowledge about security patching		
Time on follow-up for patch logs				4 Patch logs	
Time spend on patching			3 Knowledge about security patching		
Training about security patching processes					5 Updating security patching processes
Trends within the cyber security / OT / patching domain		2 Vulnerabilties and risks within cyber security			
Updates of follow-up on patch logs				4 Patch logs	
Updates of security patching processes					5 Updating security patching processes
Vulnerable systems		2 Vulnerabilties and risks within cyber security			
Work related to security patching			3 Knowledge about security patching		