Master's thesis

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

Sara Waaler Eriksen
Sarmilan Gunabala

Cybersecurity Incident Management In The Electrical Energy Sector: Involvement Of Suppliers

Master's thesis in Communication Technology
Supervisor: Maria Bartnes, Roy Myhre
June 2020

NTNU
Kunnskap for en bedre verden

Sara Waaler Eriksen
Sarmilan Gunabala

Cybersecurity Incident Management In The Electrical Energy Sector: Involvement Of Suppliers

Master's thesis in Communication Technology
Supervisor: Maria Bartnes, Roy Myhre
June 2020

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

NTNU
Norwegian University of
Science and Technology

Title:	Cybersecurity Incident Management In The Electrical Energy Sector: Involvement Of Suppliers
Students:	Sara Waaler Eriksen and Sarmilan Gunabala

Problem description:

Electrical energy is crucial in today's society. It is considered one of the most integral infrastructures as it fuels several other industries. In the last few years, emerging technologies and new systems have been introduced into the energy sector. Process control systems, which previously existed in closed networks, are now connected to the Internet. By enabling for more connectivity and data utilization across systems, the digitization has resulted in higher availability, functionality and efficiency. Unfortunately, it has also resulted in an increased vulnerability with a broader attack surface.

In recent years, there has been an increase in cyber attacks on both the energy sector and on process control systems. Attacks like Stuxnet in Iran and the cyber attacks on the Ukrainian power grid in 2015 are proof of the existing threats. As more cyber attacks become successful, the need for incident management and well-prepared contingency plans arise. The energy sector has also experienced an increase in the number of suppliers that provide services and systems, even for process control systems. The complexity of incident management grows with the number of parties involved, and can, therefore, be challenging for the energy sector. The size of the suppliers varies, and the growing number of supply-chain attacks has unfortunately shown that security is not always their top priority.

Both cybersecurity and incident management in the energy sector have been widely researched, but there is a lack of research regarding the involvement of suppliers. In this project, we will investigate how Norwegian Distribution System Operators (DSOs) collaborate with suppliers in the management of potential cybersecurity incidents in their process control systems. The goal is to find possible areas of improvement and recommendations for how DSOs can collaborate with suppliers in a way that satisfies the requirements in today's threat landscape.

Responsible professor:	Maria Bartnes, IIK
Supervisor:	Roy Thomas Selbæk Myhre, TietoEVRY

Abstract

The electrical energy sector has become a cornerstone in today's society, and the dependence upon electrical energy continues to increase. Disruptions in this critical infrastructure will have severe consequences and can lead to loss of life. In recent years, there has been an increasing occurrence of cyberattacks aimed at the energy sector. Attacks against vital Process Control Systems (PCS) that were previously considered difficult are now feasible as a result of the digitalization process the sector has undergone. Many vulnerabilities have emerged explicitly from the introduction of Information Technology (IT) into the old Operational Technology (OT) systems that were created to exist in closed environments. The threat landscape has changed, and successful attacks are now inevitable, thus creating the need for well-prepared cybersecurity incident management processes.

The technological evolution has enabled Norwegian Distribution System Operators (DSOs) to make greater use of products and services from external suppliers. Although outsourcing provides resources, expertise and cost-effectiveness, it also introduces new dependencies and gates for potential attacks. As the dependence upon suppliers and the system complexity increase, the use of suppliers has to be taken into account in the cybersecurity incident management for the DSOs. Accordingly, this thesis has investigated current practices for the involvement of suppliers in incident management related to PCS. A qualitative approach with interviews and document reviews as data collection methods was used, and the results were categorized using the phases of the ISO/IEC 27035 standard. The research was conducted as case studies of four Norwegian DSOs, two small and two large, one supplier of PCS, in addition to an interview with a representative from the Norwegian Water Resources and Energy Directorate (NVE).

The findings of this study show distinct differences between small and large DSOs, and there are indications of some small DSOs not being prepared to handle cybersecurity incidents in their PCS. In general, based on the participating organizations, there is little involvement of suppliers in plans, exercises and the evaluation of incidents, and there was no interest from the interviewed supplier to participate in cybersecurity preparedness exercises. The combination of high supplier dependence and the small number of suppliers creates a vulnerability for the sector towards multiple, simultaneous attacks on several DSOs.

These findings, combined with accepted quality standards and good practice guidelines, resulted in a set of recommendations for improving the involvement of suppliers in incident management. The authors recommend that DSOs utilize the sector's unique possibility for collaboration to enhance their resources and thus reduce their dependence upon suppliers. Furthermore, they would benefit from more involvement of suppliers in preparatory incident management activities. Lastly, changes to the entire sector could be beneficial, such as further development of current legislation regarding supplier involvement and merging of smaller organizations. These suggestions are addressed to the authorities and other aspects than cybersecurity must be taken into account.

Sammendrag

Den elektriske energisektoren har blitt en hjørnestein i dagens samfunn, og avhengigheten til elektrisk energi fortsetter å øke. Forstyrrelser i denne kritiske infrastrukturen vil få alvorlige konsekvenser og vil i verste fall kunne føre til tap av liv. Det har i de siste årene vært en økning i forekomsten av cyberangrep rettet mot energisektoren. Som et resultat av den omfattende digitaliseringsprosessen sektoren har gjennomgått, er det nå mulig å gjennomføre angrep mot de viktige prosesskontrollsystemene som tidligere var ansett som vanskelige å angripe. Mange nye sårbarheter har oppstått eksplisitt fra introduksjonen av informasjonsteknologi (IT) inn i de gamle operasjonellteknologi-systemene (OT) som ble designet for å kun eksistere i lukkede miljøer. Trussellandskapet har dermed endret seg, og vellykkede angrep på energisektoren er nå uunngåelige. Dette skaper behovet for godt forberedte prosedyrer for håndtering av cybersikkerhetshendelser.

Et resultat av den teknologiske utviklingen er at norske nettselskaper i større grad benytter produkter og tjenester fra eksterne leverandører. Selv om tjenesteutsetting tilfører ressurser, kompetanse og kostnadseffektivitet, introduseres også nye avhengigheter og sårbarheter for cyberangrep. Ettersom avhengigheten til leverandører og kompleksiteten til systemene øker, bør leverandørene i større grad involveres i nettselskapenes håndtering av cybersikkerhetshendelser. På bakgrunn av dette har denne studien undersøkt gjeldende praksis for involvering av leverandører i håndteringen av cybersikkerhetshendelser relatert til prosesskontrollsystemer. Studien ble gjennomført med en kvalitativ tilnærming med intervjuer og dokumentstudier som datainnsamlingsmetoder, og fasene til ISO/IEC 27035-standarden ble brukt til å kategorisere resultatene. Forskningen ble utført som case-studier av fire norske nettselskaper, hvorav to små og to store, en leverandør av prosesskontrollsystemer, i tillegg til et intervju med en representant fra Norges vassdrags- og energidirektorat (NVE).

Funnene viser tydelige forskjeller mellom små og store nettselskaper, og de indikerer at noen små nettselskaper ikke er godt nok forberedt til å håndtere cybersikkerhetshendelser i prosesskontrollsystemene sine. Basert på de deltakende selskapene, er det lite involvering av leverandører i planer, øvelser og evalueringer av hendelser, i tillegg til en manglende interesse fra den intervjuede leverandøren til å delta i beredskapsøvelser. Kombinasjonen av høy leverandøravhengighet og det lave antallet leverandører gjør sektoren sårbar for angrep rettet mot flere nettselskaper samtidig.

Funnene, kombinert med anerkjente standarder og retningslinjer for god praksis, resulterte i et sett med anbefalinger for å forbedre involveringen av leverandører i hendelseshåndteringen. Forfatterne bak denne rapporten anbefaler at nettselskapene bruker den unike muligheten de har for sektorsamarbeid til å øke ressursene sine og dermed redusere avhengigheten til leverandører. Videre vil det være fordelaktig å øke involveringen av leverandører i de forberedende aktivitetene for hendelseshåndtering. Til slutt anbefales mulige endringer rundt videreutvikling av gjeldende lovverk om leverandørinvolvering og sammenslåing av mindre organisasjoner. Disse forslagene er adressert til myndigheten og betraktninger rundt andre aspekter enn cybersikkerhet vil være nødvendige.

Preface

This master's thesis is submitted to the Norwegian University of Science and Technology (NTNU) as the final part of the five-year Master of Science (MSc) in Communication Technology program at the Department of Information Security and Communication Technology (IIK).

We want to express our gratitude to the organizations that contributed to interviews or conversations for this master's thesis. You welcomed our questions with openness, thus giving us a unique insight into an exceptional and vital sector. We hope that our study and recommendations will contribute to organizations improving their involvement of suppliers in incident management and becoming better prepared for handling cybersecurity incidents in the future. Ultimately, improving the security and robustness of this critical energy infrastructure.

Maria Bartnes and Roy Myhre, we are grateful for your guidance and support throughout this project. With your dedication and good advice, we have been able to keep up the courage and deliver this thesis with pride.

Lastly, we want to thank family and friends for the support and the good memories we have gained during these past five years.

Sara Waaler Eriksen & Sarmilan Gunabala
Trondheim, 2020

Contents

List of Figures xi

List of Tables xiii

List of Acronyms xv

1 Introduction 1
- 1.1 Research Questions . . . 2
- 1.2 Scope and Limitations . . . 2
- 1.3 Outline . . . 3

2 Background 5
- 2.1 Norway's Electrical Energy Sector . . . 5
  - 2.1.1 Characteristics . . . 6
  - 2.1.2 Digitalization of the Energy Sector . . . 8
- 2.2 Outsourcing . . . 9
- 2.3 Vulnerabilities . . . 11
  - 2.3.1 Linked to IT/OT Convergence . . . 11
  - 2.3.2 By Outsourcing . . . 13
  - 2.3.3 Regarding Privacy and Confidentiality . . . 14
- 2.4 Current Threat Landscape . . . 15
- 2.5 Cybersecurity Incident Management . . . 16
  - 2.5.1 Why Incident Management is Needed . . . 17
  - 2.5.2 Cybersecurity Preparedness Exercises . . . 19
- 2.6 Standards, Guidelines and Legislation . . . 20
  - 2.6.1 Kraftberedskapsforskriften . . . 20
  - 2.6.2 The ISO/IEC 27035 Standard . . . 21
  - 2.6.3 NSM's Fundamental Principles for ICT Security . . . 23
  - 2.6.4 CFCS: Cybersecurity in Supplier Relationship . . . 24

3 Method 27
- 3.1 Qualitative Research . . . 27
  - 3.1.1 Background study . . . 28

3.1.2 Case Study . . . 28
3.1.3 Qualitative Interview . . . 30
3.1.4 Qualitative Data Analysis . . . 31
3.2 Participants . . . 32
3.3 Data Quality . . . 33
3.3.1 Validity . . . 33
3.3.2 Reliability . . . 34
3.4 Ethical Considerations . . . 35

4 Results **37**
Case Introduction: DSOs . . . 37
4.1 Phase 1: Plan and Prepare . . . 37
4.1.1 Attacks and Threat Landscape . . . 38
4.1.2 Organizational Structure and Roles . . . 39
4.1.3 Suppliers . . . 40
4.1.4 Involvement of Suppliers in Incident Management Plans . . . 42
4.1.5 Cybersecurity Preparedness Exercises . . . 42
4.1.6 Sector Collaboration . . . 44
4.2 Phase 2: Detection and Reporting . . . 44
4.3 Phase 3: Assessment and Decision . . . 45
4.4 Phase 4: Responses . . . 45
4.5 Phase 5: Lessons Learnt . . . 46
Case Introduction: Supplier . . . 47
4.6 About the Industry . . . 47
4.6.1 Lack of Security Knowledge . . . 47
4.6.2 Threats . . . 48
4.7 Contract Management . . . 48
4.8 Providing Sufficient Resources . . . 49
4.9 Power Balance . . . 49
4.10 Involvement in Incident Management . . . 50
4.11 Strengths and Improvements . . . 51
Interview with the NVE . . . 52
4.12 Cybersecurity . . . 52
4.13 Differences Between Small and Large DSOs . . . 52
4.14 Involvement of Suppliers in Incident Management . . . 52

5 Discussion **53**
RQ1: How are suppliers involved in Norwegian DSOs' cybersecurity incident management regarding process control systems? . . . 53
5.1 Resources . . . 53
5.1.1 Expertise . . . 53
5.1.2 Good Procurement Skills . . . 55

5.1.3 Security Audits . . . 57
5.2 Dependence upon Suppliers . . . 58
5.2.1 Vulnerability Towards Simultaneous Attacks on Multiple DSOs 58
5.2.2 Protection of System Information . . . 60
5.2.3 Continuous Preparedness . . . 60
5.2.4 Power Imbalance . . . 61
5.2.5 Trust . . . 62
5.3 Incident Management Plans . . . 62
5.4 During Incidents . . . 64
5.4.1 Responsibility when Outsourcing . . . 64
5.4.2 Communication . . . 65
5.4.3 Involving Several Suppliers . . . 66
5.5 Continuous Evaluation and Improvement . . . 67
5.5.1 Cybersecurity Preparedness Exercises . . . 67
5.5.2 Learning from Exercises and Incidents . . . 69
RQ1.1: What are possible improvements to the collaboration with suppliers on cybersecurity incident management? . . . 72
5.6 More Involvement In Preparatory Activities . . . 72
5.7 Enhancing Resources by Utilizing Sector Collaboration . . . 73
Recommendations . . . 76
5.8 For DSOs . . . 76
5.9 For Sectoral Changes . . . 78

6 Conclusion and Future Work **81**

References **83**

Appendices

A Letter of Consent (in Norwegian) **91**

B Interview Guide DSO **95**

C Interview Guide Supplier **101**

D Interview Guide NVE **107**

List of Figures

2.1 Separation of PCS and Administrative IT Network Using DMZ 8
2.2 Overview of the Bidirectional Power Grid 10
2.3 Relationship Between Cybersecurity and Other Security Domains 17
2.4 Incident Management Life Cycle 18
2.5 Customer/Supplier Relationship Phases 25

List of Tables

3.1 Choice of Research Method 29

5.1 [Phase 1] Recommended measures structured by the ISO/IEC 27035 standard. 77
5.2 [Phase 2 to Phase 5] Recommended measures structured by the ISO/IEC 27035 standard. 78

List of Acronyms

CFCS Centre for Cybersecurity.

CPS Cyber-Physical System.

DMZ Demilitarized Zone.

DSO Distribution System Operator.

ENISA European Network and Information Security Agency.

ICS Industrial Control Systems.

ICT Information and Communications Technology.

IEC International Electrotechnical Commission.

IRT Incident Response Team.

ISA International Society of Automation.

ISO International Organization for Standardization.

IT Information Technology.

NIST National Institute of Standards and Technology.

NOU Norwegian Official Report.

NSM Norwegian National Security Authority.

NTNU Norwegian University of Science and Technology.

NVE Norwegian Water Resources and Energy Directorate.

OT Operational Technology.

PCS Process Control Systems.

PST Norwegian Police Security Service.

SCADA Supervisory Control and Data Acquisition.

SLA Service Level Agreement.

SMB Small and Medium-sized Business.

TSO Transmission System Operator.

VPN Virtual Private Network.

Chapter 1
Introduction

Modern society has become increasingly dependent upon electrical energy, and a loss of electricity will profoundly impact all parts of society. As in other industries, digitalization has introduced Information Technology (IT) into substantial parts of the energy sector, creating a smart power grid. The aim of a smart power grid is to use information flow to create an automated advanced delivery network [FMXY11]. As a result, power delivery becomes more efficient and robust due to the power grid's ability to handle events such as component failure by redirecting the power flow. New equipment, systems and numerous suppliers also follow the introduction of IT into these systems. When these products and services connect to daily operations and core activities, such as Process Control Systems (PCS), the risk surface increases. Suppliers come in all shapes and sizes with different degrees of security, which can extend the attack surface of a distribution entity, also known as a Distribution System Operator (DSO). The DSOs' current reliance on suppliers can also become a problem due to the vulnerabilities caused by the increased complexity of the systems. Accordingly, there is a need for close collaboration between all parties involved during cybersecurity incidents.

The digitalization of the energy sector has also introduced many new threats. Although the smart grid improves safety and efficiency, systems not created to exist outside of a closed network are now connected to the Internet and exposed to a variety of threats. Norway's political system, valuable natural resources and commerce, defense and preparedness, as well as research and development are considered potential targets for espionage or damage by state actors or terrorist organizations. According to the Norwegian Police Security Service (PST)'s *Annual Threat Assessment* both for 2019 and 2020 [65, 66], the energy infrastructure is at risk of being a target for advanced network operations, digital mapping and sabotage. The attacks can also cause more severe consequences than before, such as long-lasting power outages or physical harm on the grid's surroundings, due to the integration of physical processes with networking and computation [oSN19]. The power grid has become a so-called Cyber-Physical System (CPS), which means that cyberattacks on the energy sector

can impact the physical systems and their environment, and physical attacks can impact the cyber component of the systems.

As successful attacks on the energy sector are becoming common and inevitable, it is no longer sufficient to only focus on prevention techniques. There is a need for well-prepared cybersecurity incident management schemes to handle incidents effectively and limit their impacts. Cybersecurity incident management has thus become a well-known term in the energy sector, and has been the subject of several studies [Lin15, HT13]. Smart grid security has also been studied thoroughly [LTJ11, KHLF10, WS19], but few studies have been conducted on how suppliers should be involved in incident management regarding PCS, which is the motivation for this project. The increasing amount of suppliers and the DSOs' dependence upon them affect incident management, involving several actors who must coordinate for emergency preparedness and responses. A report by the Norwegian Water Resources and Energy Directorate (NVE) investigated the relationship between customer and supplier, focusing on security challenges [KL18]. The report concluded that emergency preparedness in the energy sector needs to be studied in practice, with special emphasis on the interactions between the different actors in stressful situations.

1.1 Research Questions

This research project will investigate the involvement of suppliers in incident management in practice and the goal is to find possible improvements. Through literature reviews and a qualitative research approach with interviews of DSOs, a supplier and the NVE, the following research question and associated sub-question will be answered in this thesis.

RQ1: How are suppliers involved in Norwegian Distribution System Operator's (DSO's) cybersecurity incident management regarding Process Control Systems (PCS)?

> **RQ1.1:** What are possible improvements to the collaboration with suppliers on cybersecurity incident management?

1.2 Scope and Limitations

This study focuses on Norwegian DSOs and the involvement of suppliers in incident management regarding process control systems, thus excluding other parts of the incident management process. The study is restricted to a small number of DSOs to do in-depth studies and retrieve valuable information on all stages of the incident management process within the project's time restrictions. Although the small

number of DSOs makes it harder to generalize the findings, it also provides valuable insights. The study mainly focuses on PCS since it is an essential part of the systems, although it can be challenging due to confidential and energy-sensitive information. Furthermore, there is a lack of research and public information regarding supplier involvement in PCS, which may be a limiting factor for this project. The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27035 standard will be used in the data analysis, and, therefore, its limitations can also be applied to this project.

1.3 Outline

Chapter 2 provides necessary background information that is relevant for the project. It gives an introduction to the energy sector, what incident management is, how suppliers are related to this topic, and lastly presents relevant standards, guidelines and legislation.

Chapter 3 presents the organizations that participated in this study and discusses the qualitative approach used in this study.

Chapter 4 presents findings from the participating organizations in this case study.

Chapter 5 discusses and compares the findings from the interviews with existing literature and best practice. Finally, recommendations for improvement are given.

Chapter 6 draws a conclusion, points to improvements and how the authors envision this work to evolve in the future.

Appendix A provides the information sheet and letter of consent, originally written in Norwegian, sent to the participants.

Appendix B includes the interview guide with questions for the interviews with the DSOs, translated from Norwegian.

Appendix C provides the interview guide with the questions for the supplier, translated from Norwegian.

Appendix D includes the interview guide with questions for the NVE, translated from Norwegian.

Chapter 2
Background

This chapter will provide an introduction to the electrical energy sector, as well as insight into existing threats and incident management. Related work within this field will also be presented.

2.1 Norway's Electrical Energy Sector

The electrical energy sector is one of Norway's critical infrastructures, which are physical or technical infrastructures upon which society is highly dependent. Due to the importance of electrical energy, severe consequences are expected in case of failure, as it would not be possible to uphold the societal functions that the population needs [Min12]. The consequences of attacks span from a breach of privacy and information gathering to power outages. A long-term power outage can have fatal impacts on societal functions. Functions like transport infrastructure, hospitals and communication systems will be affected, hence causing harm to humans and ultimately leading to a loss of life [Gra19]. Inter-dependencies between infrastructures makes the network of critical infrastructures interconnected and complex, and electrical energy may be the most important part of it. As a result of globalization, energy is the subject of international trade and can, in many ways, be considered a commodity [Nor19]. Hence, an event of failure may affect other infrastructures as well as other countries.

In the electrical energy sector, produced power traverses through different entities and equipment before being consumed. Along the way, two main entities will process it; Transmission System Operators (TSOs) and Distribution System Operators (DSOs). TSOs are responsible for transporting the power from the producers to different geographical locations. This transmission infrastructure handles international connections as well as major consumers. DSOs, on the other hand, are responsible for the distribution to the end consumers. There is only one TSO in Norway, named Statnett, while the DSOs operate in regions around the country. The number of

DSOs in Norway has steadily been decreasing from, for instance, 157 in 2008 [Bre19]. In Norway, a Small and Medium-sized Business (SMB) is an organization with up to 100 employees [oNEN20]. As of 2020, there are 103 DSOs in Norway [Ene20], where the majority are considered to be SMBs [Bre18].

When the Norwegian Energy Act passed in 1990, Norway was ahead internationally in the context of liberalizing the energy market by dividing it into a competitive section and a monopolistic section [voeN16]. This led to organizational changes for the DSOs, while they retained their position of natural monopoly. The changes created the opportunity for an outsourcing of services to suppliers, which led to staff reductions in the following period.

The NVE[1] is responsible for managing the water and energy resources in Norway as well as leading the national preparedness of the energy supply. It is the NVE that has the authoritative responsibility for the legislation imposed on the organizations in the sector. KraftCERT[2] is the sector's advisory service. Three large entities in the sector founded it on an initiative by the NVE to support the energy sector both in preparatory work and the handling of cyber incidents. KraftCERT aims at better securing PCS by advising and informing organizations about relevant threats and vulnerabilities.

2.1.1 Characteristics

Several components and requirements make the energy sector different from other sectors, spanning from components to requirements. This subsection will present the ones most relevant for this study.

Operational Technology (OT) is primarily used to monitor, manage and control equipment functioning within the field of industrial operations, where the electrical energy sector is no exception. The technology interacts with automation and mechanical equipment both locally in a factory and between installations throughout regions, and is therefore essential to the sector. IT systems, on the other hand, usually focus more on business and enterprise services where information is processed, stored and distributed [iS20b]. Information and Communications Technology (ICT) is an extended acronym for IT and will, at times, be used in this thesis. Unlike IT systems that have life spans of years, the industrial systems in OT are designed to last for decades at a time, usually operating both day and night. Although both systems are designed for reliability and large-scale complex systems, they have different baseline requirements and concerns. Availability is a priority for both, but in different forms. Downtime is not acceptable in OT systems since an outage can be fatal for

[1] https://www.nve.no/english/
[2] https://www.kraftcert.no/english/index.html

some applications. Updates and patching must then be well-planned and executed in a manner that does not affect the production or cause frequent interruptions. Computational and communication systems utilize these processes with a focus on safety and security, by being tightly wound with precise time dependency, whereas IT systems can at points accept time delays. In IT, software is therefore frequently updated and since the availability requirement is not as strict as in OT, restarts and patching are often used to fix problems and vulnerabilities [LTJ11].

Process control systems (PCS), sometimes called Industrial Control Systems (ICS) or Industrial Automation and Control Systems (IACS), are systems that, in many ways, are the core of OT. These include support, control and monitoring of production, transmission, storage and distribution of electrical energy in combination with the control of support processes [HHT+17]. In the electrical energy sector, they function in equipment all the way from the production line to the distribution line by testing the processes in a variety of ways and returning data for monitoring and troubleshooting. PCS allow DSOs to keep their operations running within specified limits, thereby ensuring safety and reliability. The PCS' provision of automation functionality makes them vital to the sector due to the sector's geographical expansion and challenging terrain. It is also necessary for the preservation of safety for personnel and surrounding areas, due to the high voltage power lines. PCS are often highly restricted and complicated, consisting of several subsystems and components, which makes the implementation of an antivirus almost impossible. These systems are usually controlled through an operations center, which is protected through strict access control.

Supervisory Control and Data Acquisition (SCADA) manages PCS and their networks and operates as a communication link between components in the industrial network for production and operation. It can be seen as a display unit that combines several PCS on a supervisory level. System status, anomalies and operations are easily manageable by the user interface provided by the SCADA system [DS99, Wil15].

Demilitarized Zones (DMZs) are implemented in a system to create secure separations between the administrative network and PCS. As a result, it functions as an intermediary zone shielding the OT systems. When IT was introduced into the power grid, the time of the air gap was over, but several firewalls are often implemented to provide a logical separation [Rot18]. By avoiding a direct connection between the two networks, DMZs protect PCS against regular network traffic and the threats that follow. An example of a network architecture with a DMZ separation is illustrated in Figure 2.1.

Safety versus security is a challenge that has been introduced by the change

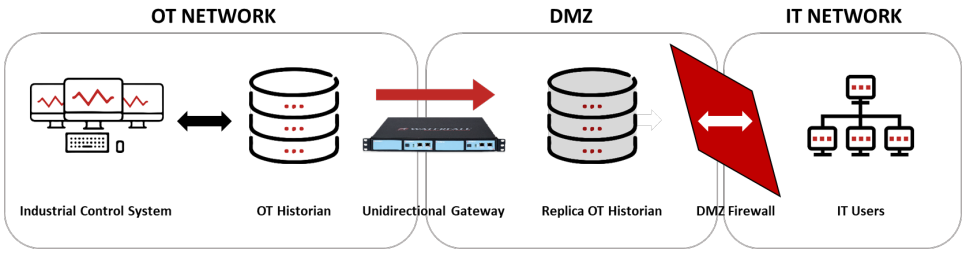

Figure 2.1: Separation of PCS and administrative IT network using a DMZ [Sch19].

of the power grid to a CPS, by merging physical and cyber environments. In the context of CPS', safety is defined as a system's inability to affect its surroundings in an undesirable way, while security is the inability of the surroundings to affect the system in an undesirable way. As the energy sector traditionally consisted of physical systems, it has generally been preoccupied with safety, while cyber systems have focused on security. In a CPS, the two concepts are interconnected as security failures can lead to threats to safety and vice versa. Therefore, both need to be taken into account when designing such systems.

The security requirements for the energy sector are stringent due to the importance of continuous energy delivery. Thus, the focus has mainly been on availability and reliability. Availability is the guarantee of an accessible and usable system when needed by an authorized entity, while reliability is the assurance that the system consistently behaves in the intended way. Also, system-level requirements in the energy sector usually concern safety and performance. In cybersecurity, on the other hand, the main requirements are confidentiality, integrity and availability, also referred to as the CIA triad [fSI12]. Confidentiality is protecting information against unauthorized access, and integrity is protecting information against unauthorized modification. With the introduction of IT into the critical infrastructure, these concerns also apply to the energy sector [MKB+11]. Information collected from process control systems and smart meters has to be confidential, and its integrity must be ensured to avoid attacks that exploit this kind of information. Thus, the energy sector is now facing more requirements than before, which can lead to conflicts in priority.

2.1.2 Digitalization of the Energy Sector

Industry 4.0, also known as the fourth industrial revolution, is the digital transformation that has been embraced by many industries. With it, industrial processes are facing changes within organization and control. The introduction of new technologies is the core of the evolution. Previously standalone equipment is now interconnected

via the Internet, making way for innovative methods for production and optimization [iS20a].

Convergence of IT and OT is the main factor that enables the industrial revolution. IT is being increasingly integrated so that systems like SCADA can function. From being two separate teams, with little collaboration, OT and IT personnel are starting to work in the same domain. The sudden cooperation can lead to challenges due to a lack of understanding of each other's domains and differences in priorities [LTJ11]. New and complex IT systems are enabling OT systems to function in new ways and adds factors like network security, becoming both more resource and cost-effective [Bab18]. Although there are many benefits, the power sector as a whole becomes more vulnerable when these components connect to the Internet. The convergence of IT and OT, therefore, introduces new challenges and vulnerabilities that will be discussed later in this chapter.

Smart grid has become a commonly used name for the digitized power grid, where IT and OT systems co-function. The digitalization process has transformed the entire sector, from sensors in the grid to smart meters in consumers' homes. The change from the old power grid to the smart grid leads to a change from a relatively small number of carefully controlled devices to a distributed environment that includes a huge number of devices. It also means introducing IT into all the phases from the energy production to the consumption; generation, transmission, distribution and utilization. The previously unidirectional chain of phases has now transformed into a bidirectional chain as consumers can be producers when excess electricity becomes available to other end consumers [MKB+11], as Figure 2.2 illustrates. The use of smart meters is an example of the digitalized energy sector and smart grid. Hourly automatic readings sent from the meters provide exact invoices for the consumers and assist DSOs in better planning and adjustments of power flow following the consumption level.

2.2 Outsourcing

Suppliers are external organizations that through an agreement provide products or services to entities. According to a report by the NVE, 8 out of 10 Norwegian organizations in the energy sector are dependent upon suppliers to handle incidents in their IT and operational control systems[3], and to restore the systems if they fail [inf17]. Thus, it is safe to say that the majority of today's DSOs utilize suppliers to some degree in their systems, which has both advantages and disadvantages.

[3]Operational control systems is a broader term than PCS, that includes support systems such as ventilation and cooling

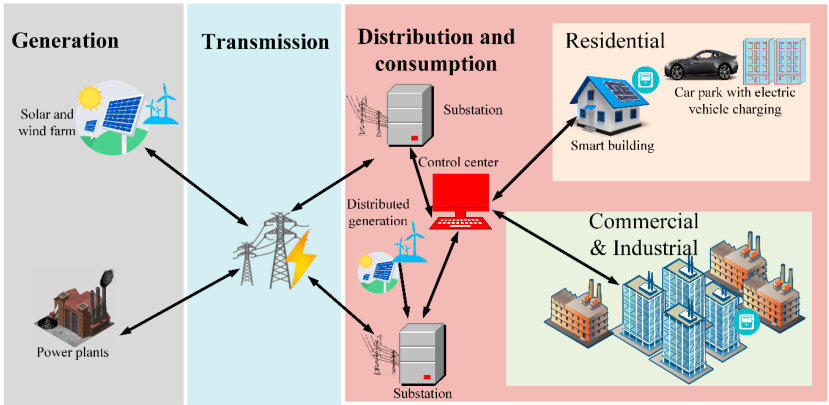

Figure 2.2: Overview of the bidirectional power grid [ABAH+20].

A report investigating the restructuring of Norwegian DSOs and the consequences it had on social security after the Norwegian Energy Act's passing, explains the impacts it had on the participating DSOs [AAF+08]. The main motive for outsourcing is better cost regulation and a higher quality of products and services. It brings components, systems and expertise which the DSOs may not possess. Also, it is expensive and almost impossible for small organizations to meet today's threat level with sufficient cybersecurity measures by themselves. Thus the rationale is often economically motivated. Outsourcing lets DSOs cultivate and focus on their core business areas [AAF+08].

With the restructuring of the energy sector, integrated organizational structures became disintegrated and regulated interfaces were introduced. As a consequence, DSOs have increased control of work progress and management as operational tasks are outsourced to suppliers. The restructuring has led to a centralization of operations centers consisting of PCS and suppliers. Therefore, interfaces have been established for external connection by suppliers into the closed network loop. Consequently, creating a need for connection establishment processes and protection of interfaces. In addition to the organizational changes outsourcing carries, it is important to note the less visible changes in competence and culture. Environments built on expertise were broken up and as such, resources and competence must be acquired through suppliers [AAF+08].

As many organizations are dependent upon their suppliers, the NVE investigated possible security challenges in the relationship between customer and supplier. The resulting report discloses that both energy companies and suppliers have control up to a maximum of two links in the supply chain [KL18]. The report also shows that it is hard to verify the security requirements stated in the contracts, and that

the DSOs do not use their right to audit them. Due to outsourcing, the DSOs remain as intermediary businesses, meaning that the authorities rely on them to conduct necessary controls towards the suppliers [AAF+08]. The report by the NVE concludes that it is necessary to investigate the emergency preparedness in practice, specifically the interactions between the different actors in stressful situations [KL18], an aspect this thesis investigates.

The increasing outsourcing and complexity of the systems in the energy sector have led to a supplier concentration, which creates a sectoral concentration risk, according to a report on the regulation of cybersecurity in the energy sector [HHT+17]. This type of risk is particularly evident when the products are essential, and there are few actors in the market. A desire for increased efficiency and technological innovation can introduce numerous new actors and more complexity, which in turn, can unintentionally enhance the risk for incidents with serious consequences. The high system complexity will also, most likely, restrict the number of actors in the market, creating dependencies that may pose risks. The report highlights five such risks:

- Resource shortage during extensive incidents
- Supplier-specific errors that can affect big parts of the sector
- Dependencies to key personnel can have consequences
- The complexity can lead to vendor locks
- The supplier can be acquired by an untrustworthy party

2.3 Vulnerabilities

The digitalization of the energy sector has challenged the way the sector operates, and as a result, new cybersecurity challenges and vulnerabilities have emerged. Cybersecurity can be defined as the art of protecting networks, devices, and data from unauthorized access or unlawful use while also ensuring confidentiality, integrity, and availability of information[4]. This section will introduce some vulnerabilities that are relevant to this thesis.

2.3.1 Linked to IT/OT Convergence

Due to the convergence of IT and OT, physical systems created to exist in a trustworthy and closed environment are exposed to the threats of the cyber world. Their protective cybersecurity measures originated in the telecommunications environment

[4]https://www.us-cert.gov/ncas/tips/ST04-001

where the requirements are different, which has created some vulnerabilities. The following top five vulnerabilities for OT systems illustrate this [top16] as they all stem from the lack of basic security mechanisms:

1. Legacy software where data is neither authenticated nor integrity checked
2. Configurations and modifications to default values on components from the manufacturer are often not conducted
3. Since availability is a strict requirement, encryption and its time-consuming processes are omitted. Username and password are, at times, transmitted with no encryption mechanisms
4. Backdoor access due to weak remote access policies as from administration IT systems
5. Different approaches to security by IT and OT personnel creates a gap and puts both systems at risk

The power grid is now a lot more susceptible to attacks than before due to the extensive amount of exposed legacy systems and components. PCS that were previously physically separated from administrative IT systems, through so-called air gaps, are now only logically separated from other systems through firewalls and traffic filtering. Even though the communication across the process control environment only happens through protocols with strict security requirements, such as DMZs, logical separation will never be 100% secure, but it reduces the risk. Physical separation will neither be 100% secure in today's networks. Legacy SCADA systems have, for instance, been exploited in many of the successful attacks on PCS and the energy sector. The increased use of general-purpose components and commodity software also opens up the possibility for infection by general-purpose malware whose only intent is to spread as much as possible [LTJ11].

Cyberattacks in today's sector can have physical consequences and vice versa. This extends the damage potential for manipulation of PCS as it can have direct consequences on life. Thus, attacks on PCS are much more dangerous than manipulations of other systems in the sector, such as administrative IT systems. Upgrading and patching is not done as frequently in PCS, which increases the lifetimes of vulnerabilities [HHT+17]. These vulnerabilities can become dangerous if an attacker obtains access to the PCS, utilizing such a hole in cybersecurity. It is therefore alarming that the security firm Kaspersky Lab found that a substantial number of ICS components are online and contain some kind of vulnerability [AGG+16]. By using Shodan[5] and other similar tools, they globally discovered more than 220

[5] A search engine for Internet-connected devices.

000 components online, and that insecure protocols were used in over 90% of the components. They also found many industries represented due to the same suppliers delivering to several industries.

The contrasting ways of handling attacks and issues in IT and OT systems can cause problems for the combined system. During an attack on an IT system, a shut down is often the initial suggestion to protect the data [Mul19]. Contrary to IT, such an approach can lead to catastrophic consequences in OT systems. The combination of controlling physical processes capable of causing significant harm to the surrounding environment and the need for continuous availability prevents this security measure in OT systems. These characteristics also complicate system updates and modifications, which makes it challenging to follow principles for good cybersecurity in PCS. The prevention of automatic updates and the need for thorough testing can lead to vulnerabilities with long lifespans [HHT+17].

Combining fundamentally different technologies, such as IT and OT, does not only create challenges from a technological perspective, but also for culture and management. The number of devices connected to the grid has drastically increased and will continue to multiply, which poses challenges for management and the monitoring of cyberintrusions. The fact that multiple distinct parties often manage the subsystems also makes security management more complicated for the DSOs [WS19]. Furthermore, human factors are equally as important as the technical ones in security management. The technical security measures are worthless if the cultural differences and lack of understanding between IT and OT personnel are too significant. Process control operators are not used to dealing with threats from the cyberworld, and their highest priority is to keep the system functional. IT workers are used to computer failures, so integrity and confidentiality are often prioritized over availability. Both parties are good at detecting incidents in their systems, but in order to detect security incidents in the integrated system, they need to understand the weaknesses for both systems. Combined management and governance is only possible if the needs and requirements for both systems are understood [LTJ11].

2.3.2 By Outsourcing

By the year 2006, 15 years after the Norwegian Energy Act came into effect, Norwegian Official Report (NOU) published findings that reported vulnerabilities and security challenges in the electrical energy sector [ea06]. The report highlights challenges associated with understanding and maintaining critical operating businesses. It states that ambiguous responsibilities and relocation of PCS may weaken the overall critical infrastructure.

Utilizing suppliers carries several risks and dependencies [Nas20]. They complicate the incident management process and open up for supply chain attacks. These types

of attacks are characterized by attackers using the supply chain and exploiting weaker subsystems to get access to the desired target. With Internet-connected systems and many different suppliers, a DSO can become the victim of an accidental attack that contaminates an element in the supply chain and corrupts the system until it causes system failure. A DSO can also become the victim of a targeted supply chain attack.

Another challenge that arises from outsourcing to several suppliers is coordination, since clarifications regarding who is in charge, who should do what and allocation of resources must be worked out upfront. If such assessments are delayed until after a critical cybersecurity incident has occurred in the PCS, it can have fatal impacts on the power distribution. Working in PCS requires specialized competence, strict access control, and all tasks must be conducted with caution due to the criticality and sensitivity of the systems. The relatively small size of the Norwegian electrical energy market, in the global context, imposes constraints on the number of competitors in the market due to the limited amount of possible customers. Thus, it is fair to assume that the number of PCS suppliers is small. This concentration of suppliers enables attackers to disrupt power distribution across the country by only targeting a small amount of suppliers [fsobM12].

A result of using several outsourcing services is that faults that could previously be fixed instantly, now have to traverse through several entities before they are rectified. When a cybersecurity incident occurs, the supplier monitoring the system might become the first to be alerted. The supplier will then notify the DSO, which has to decide whether to use internal resources or seek assistance from other suppliers. If assistance is needed, the DSO must establish contact and forward relevant information to all relevant parties. A weakness mentioned in the report on the restructuring of Norwegian DSOs [AAF+08] is that formal channels replace the previously informal contact and financial costs are incurred when using suppliers. This can result in weakened collaboration and information dissemination routines. Ultimately, the outsourcing model jeopardizes a DSO's ability to maintain a complete level of system knowledge.

2.3.3 Regarding Privacy and Confidentiality

Consumer privacy and data confidentiality are new topics to the energy sector that have emerged from the digitalization. Privacy is the right to control personal information and the use of it. Personal customer data is now sent from the smart meters over radio or mobile network to the Elhub, which is a national datahub. Thus, making it vulnerable to cyberattacks. Every smart meter also carries functionality that is exploitable through application programming interfaces. It is, for instance, possible to remotely turn off electricity to a building or an area. Readings from smart meters can also be abused to deduce when houses are vacant or what appliances are

used. Such readings can maliciously be read directly from the smart meter through physical access [SJ12]. Elhub also represents a single point of failure for sensitive information regarding all Norwegian electricity customers. However, it is required to have a high security standard with limited access to encrypted data [oe19a].

2.4 Current Threat Landscape

The motivation for this project comes from the continuously evolving threat landscape and the amount of both successful and unsuccessful attacks on the energy sector. Close to 70% of the organizations in the Norwegian energy sector experienced unwanted cybersecurity incidents from 2016 to 2017 [inf17].

Today's threat landscape is a lot different than it was in the past, which has attracted a lot of new adversaries with new motivations. The enhanced consequences of cyberattacks engage state actors and larger organized crime organizations. According to PSTs *Threat Assessment Reports* for 2019 and 2020, state actors are the biggest threat to Norway's national security [65, 66]. They pose a threat against Norway's energy supply, as well as other critical infrastructures. Nation-states are believed to be behind some of the most well-known attacks on the energy sector [NWM+20]. Vulnerabilities in critical infrastructures can become valuable in a politically unstable environment. These states will try to gather sensitive information about the Norwegian energy infrastructure through methods like espionage. The PST believes that the espionage will be aimed both at suppliers and subcontractors. Furthermore, they state that smaller organizations are particularly exposed due to their limited amount of resources for security.

The connection of legacy systems to the Internet makes remote attacks on the energy sector possible, and the increased connectivity in and between systems boosts the spreading of attacks. Multiple components can be affected by a single attack as failures propagate through systems. In such a highly interconnected sector, the system is not more secure than its weakest link. The amount of connected components and suppliers increases the risk surface, and the more complex supply chain has significantly impacted the threat landscape. Now, both accidental and targeted attacks on the supply chain are a threat, and the amount of targeted attacks has risen the past few years [Wue14]. The widespread use of general-purpose components with known IT vulnerabilities attracts new types of attackers. Also, the usability of IT knowledge in attacks on the energy sector extends the amount of possible perpetrators. The motivation to identify vulnerabilities increases when they are reusable on other systems with the same components [LTJ11].

The amount of software supply chain attacks increased by 200% from 2017 to 2018 [Sym18]. The following attacks demonstrate the importance of involving suppliers in

preparation for incidents. They also show that both PCS and the energy sector are attractive targets.

Stuxnet: In July 2010, a new and advanced malware that targeted industrial control systems appeared in Iran. By targeting vulnerable SCADA systems, the worm caused damage to Iran's nuclear program and infected around 100 000 hosts. It is the first known cyberattack against critical infrastructure and demonstrated that such attacks were possible [FMC10].

Ukranian power grid attack: In December 2015, the first targeted supply chain attack against the energy sector happened in Ukraine. The country's largest energy supplier was attacked and forced into manual operations, which caused a power outage that affected approximately 225 000 people. Phishing e-mails, hijacking of control systems, attack of critical components, and a distributed denial-of-service attack against the customer call-center were some of the methods used in the attack [CS17] [Zet16].

NotPetya: In June 2017, the malware named NotPetya caused a devastating attack on the global transport and logistics giant Maersk. The attackers used an infected upgrade of Ukraine's widely used tax software to spread the malware to more than 60 countries. Maersk's lack of a specific strategy for dealing with large-scale cyberattacks enhanced the damages, which illustrates the importance of well-prepared incident management processes [Rit19].

2.5 Cybersecurity Incident Management

This section will provide an overview of incident management and why it is needed, but some concepts first need to be clearly defined as there exist several different definitions.

In the ISO/IEC 27035 standard, an information security incident is defined as one or more deliberate or accidental information security occurrences indicating a failure of controls or a possible breach of confidentiality, integrity or availability of information. The occurrence(s) must have a significant probability of compromising business operations or harming business assets [fSI16]. The term cybersecurity incident is used in the *Framework for Improving Critical Infrastructure Cybersecurity* by National Institute of Standards and Technology (NIST). It is defined as a cybersecurity change that has been determined to have an impact on organizational operations, prompting the need for response and recovery [Tea18]. The ISO/IEC 27032 standard uses the term cybersecurity, or cyberspace security, and defines it as the "preservation of confidentiality, integrity and availability of information in the cyberspace". Cyberspace is here defined as the "complex environment resulting

from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" [fSI12]. Cybersecurity relies on information security, application security, network security and Internet security as fundamental building blocks, and Figure 2.3 illustrates its relation to the other terms. The term cybersecurity will be used in this thesis regarding cybersecurity incident management with incidents in PCS.

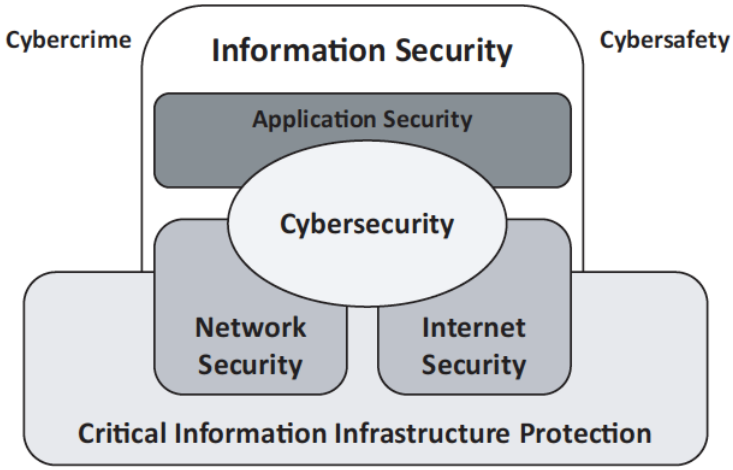

Figure 2.3: The relationship between cybersecurity and other security domains [fSI12].

Incident management is defined by ISO as the exercise of a consistent and effective approach to the handling of incidents [fSI16]. Incident management is a collective term that comprises all activities associated with managing an incident. It is not restricted to handling the incident, but includes additional work such as planning, learning from incidents, using lessons learnt as input in risk assessments, and identifying improvements to the implemented incident management scheme. Preparatory activities such as establishing an Incident Response Team (IRT), documenting procedures and training are also included in the incident management process. Incident management is a cycle that should be under continuous evaluation and improvement, as Figure 2.4 illustrates.

2.5.1 Why Incident Management is Needed

All organizations will, at some point, experience cybersecurity-related incidents. Different kinds of cybersecurity mechanisms are of crucial importance to prevent a great variety of incidents. However, it is still impossible, and economically infeasible, to prevent all incidents. Besides, some threats will always be impossible to foresee.

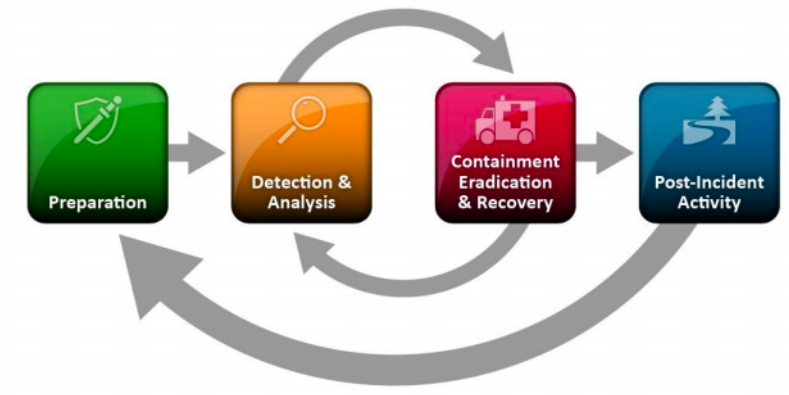

Figure 2.4: The incident management life cycle [CMGS12].

Consequently, there is a need for a well-established capacity for responding to unwanted incidents, which is where incident management comes in. Investment in establishing effective incident management processes will potentially reduce the impact of incidents and help improve resilience. Resilience refers to a system's or an organization's ability to continuously deliver the intended outcome, despite adverse cyberevents[6] [Kin20].

The technological changes in the energy sector have introduced new threats and vulnerabilities that make the systems more susceptible to both accidental and deliberate cybersecurity incidents [LTJ11]. As PCS are used to control crucial parts of society's critical infrastructure, incidents may have catastrophic consequences for the physical environment in addition to major costs for the attacked organizations [ABB+12]. The attacks presented in Subsection 2.4, as well as statistics presented by NVE [inf17], demonstrate that organizations in the energy sector are attractive targets for perpetrators. When incidents occur, it is vital to have a plan in place for incident handling, since planning increases efficiency, facilitates coordination and gives direction [mne20]. As author Alan Lakein famously said:

> *"Failing to plan is planning to fail."*
>
> — *Alan Lakein*

There is a need for an increased knowledge and understanding of cybersecurity and incident management in the setting of co-functioning IT and PCS. There exists various frameworks, guidelines and best practices for incident management such as the ISO/IEC 27035 standard [fSI16], NIST's *Computer Security Incident Handling*

[6] https://ieeexplore.ieee.org/document/8327227

Guide [CMGS12] and the *Good Practice Guide for Incident Management* by European Network and Information Security Agency (ENISA) [NE10]. There are, however, fewer standards and recommendations for incident management in settings where IT systems and PCS are intertwined and where incidents may cascade through systems. There is a need for universal and consistent security measures, detection and response to incidents, and understanding of threats and consequences of incidents. There is also a need for knowledge exchange and cooperation between OT and IT personnel in the Norwegian energy sector [BMH16].

2.5.2 Cybersecurity Preparedness Exercises

Cybersecurity preparedness exercises are vital in strengthening the response capabilities of an organization. Well-documented procedures and clear definitions of roles and responsibilities need to be in place prior to incidents. However, during an incident, there is a need for a more dynamic process that requires coordination and improvisation. Exceptions and violations must be managed, and cybersecurity preparedness exercises train personnel in responding to situations that deviate from normal operations. Furthermore, exercises provide a means for personnel to train for making the right decisions under pressure, which can either cause the incident to escalate or diminish [BM16]. As it is human nature to misjudge and overestimate own ability to improvise in stressful situations, it is crucial to simulate scenarios and develop improvisation techniques. Even though all organizations are different and require individual planning, exercising is a common key factor in improving resilience. The more experienced the personnel are in anticipating and responding to incidents, the better prepared they will be for recognizing and responding to unexpected events [HPWW11].

There are several types of exercises that, in different ways, prepare personnel for responding to incidents [GNB+06]. Tabletop exercises are a reasonably cost-efficient way of reviewing and learning documented plans and procedures. Different scenarios are presented and discussed in a room without the use of any specific equipment. Tabletop exercises allow for discussions of roles, responsibilities, procedures, coordination and decision-making. Functional exercises, on the other hand, are practical simulations of incidents with the use of physical equipment and the execution of several procedures. The two types of exercises supplement each other. Where tabletop exercises do not provide any practical demonstrations of the effects of an incident or the organization's true response capabilities, this is exactly what functional exercises provide [BM16]. Frequent exercising, including both tabletop exercises and functional exercises, makes the organization better prepared for unexpected incidents, as it is impossible to plan for all eventualities [HT13].

All who are intended to contribute in a cybersecurity incident should participate

in cybersecurity preparedness exercises. Suppliers that deliver the PCS will likely be involved in incidents concerning those systems. DSOs will, therefore, benefit from the conduction of exercises together with their suppliers [KL18]. According to Floodeen et al. [FHT13], exercising is essential in the development of mutual understanding and a shared mental model. Having these properties will increase performance during an incident management processes as the team will be better prepared for cooperation with concise communication.

2.6 Standards, Guidelines and Legislation

This section introduces relevant standards, legislation and guidelines on the topic of incident management and involvement of suppliers. Existing standards and recommendations in the area of incident management provide a useful baseline for organizations looking to implement or improve their scheme.

2.6.1 Kraftberedskapsforskriften

The organizations in the energy sector must adhere to the *Regulations on safety and emergency preparedness in the power sector for energy contingency* [oe19b], named *Kraftberedskapsforskriften* in Norwegian. It ensures contingency in the energy supply during and after extraordinary situations with the goal of reducing the societal consequences. *Kraftberedskapsforskriften* was updated on the 1st of January 2019 to include new requirements for cybersecurity and follows the Norwegian Energy Act. It is imposed on all DSOs and states that they are required to have a contingency plan to deal with and limit the effect of extraordinary situations. Furthermore, all DSOs are each required to have an "ICT security coordinator" that must retain an overview of the cybersecurity work in the organization. Digital information systems must be secured to uphold confidentiality, integrity and availability. DSOs must conduct exercises at least once a year to uphold and develop their abilities to handle all relevant incidents. Furthermore, they shall conduct post-evaluations of both incidents and exercises to improve the incident management.

The legislation also specifies requirements for the use of suppliers. DSOs must ensure that the suppliers they cooperate with are obligated to comply with the requirements stated in *Kraftberedskapsforskriften* regarding cybersecurity and sensitive information. The DSOs must implement systems and routines for checking the compliance, and if necessary, verify that the requirements are upheld. They need to control external connections to the PCS and have a predefined protocol for external connection. Furthermore, foreign suppliers used in operational control systems must originate from countries within the European Union (EU), North Atlantic Treaty Organization (NATO) or European Free Trade Association (EFTA) [oe19b].

There is a classification of DSOs based on performance and the number of customers of which their facilities are responsible. Based on the classification, different requirements are imposed on the facilities. These differences lead to larger facilities having stricter requirements concerning, for instance, security and system redundancy, than smaller facilities. This, in turn, leads to higher requirements for larger DSOs than smaller ones. "Energy sensitive data" applies to every organization, regardless of size, and is specific and in-depth information about the energy supply that can be used to damage power plants or systems, or affect functions that are significant to the supply [oe19b].

2.6.2 The ISO/IEC 27035 Standard

This section gives an introduction to the ISO/IEC 27035 standard, and the content is, unless specified otherwise, derived from [fSI16]. Content explicitly referencing suppliers or other external parties is highlighted in italic. Although the term cybersecurity is used in this thesis, information security will be used in this section due to the standard's use of it.

The ISO/IEC 27035 standard provides guidance on information security incident management, and implementing it will help organizations deal with information security incidents properly. The standard is recognized as the most comprehensive and best-fit guidance to establish a good baseline for incident management. One of its objectives is to provide guidelines that will help organizations in meeting the requirements specified by the ISO/IEC 27001 standard. The principles given in the standard apply to all organizations, regardless of size or type. This standard provides a structured approach to incident management by splitting it into five phases; plan and prepare, detection and reporting, assessment and decision, responses, and lessons learnt. Using a structured approach to information security incident management can yield benefits such as an overall improvement of information security, reduced impact of incidents, improved focus and better prioritization of security activities, and augmented information security risk assessment efforts.

Plan and prepare: The first phase is the most extensive one, and unlike the other phases, it runs continuously. Effective information security incident management requires appropriate planning and preparation, which should frequently be evaluated. Each organization needs to have a detailed incident management scheme that is documented and tested. The plan must gain commitment from top management to ensure commitment and resources, but the organization has to ensure that their use of resources is proportional to their needs. Furthermore, security and risk management policies should regularly be reviewed and updated.

The standard states the necessity of establishment and preservation of connections with external organizations directly involved in security events and incident manage-

ment. Examples of such are vendors of vulnerable software, other IRTs or contracted external support personnel. An IRT should be established and appropriately trained. Also, the use of the information security incident management plan should be tested, as well as its procedures and processes. *The testing does not only need to involve the IRT, but can involve all internal and external organizations involved in incident management.* Every exercise needs to go through the following phases; planning and preparation, execution and debrief and post-incident analysis. The results of the analysis are thus used as input to improve incident response plans.

Detection and reporting: In the first operational phase of incident management, the organization should ensure the detection and reporting of information security events and vulnerabilities. All information associated with the incident should be logged for later analysis, and stored in an information security database managed by the IRT. Situational awareness information should also be collected from both internal and external data sources. The reporting of security events should be in line with the organization's reporting policies, and the information reported should be as complete as possible to support assessments, decisions and actions to be taken in the next phase of incident management.

As it is the person first notified of an event that is responsible for starting the activities in this phase, all employees should be aware of and have access to the guidelines for reporting. The procedures should also be clear to follow for all people involved in incident handling. All relevant information about the incident should be passed to the point of contact and responsible IRT members. The standard recommends that one member of the IRT is appointed responsibility for incoming reports and for making assessments about further actions.

Assessment and decision: An assessment of information should be conducted in this phase, which decides whether an event should be classified as an information security incident. Once an event has been detected and reported, decisions on what actions to take, by whom and in what priority should be made. The IRT makes these decisions, and they involve both security and non-security personnel. To efficiently respond to the incident, a prioritization process should be conducted based on the level of business impact and the efforts required to respond.

Responses: Organizations should respond to an incident following the actions determined in this phase. Once an information security incident has been confirmed and the responses determined, the responsibility for different activities should be distributed among both security and non-security personnel as necessary. *External resources must be identified in order to respond to the incident. The organization should also communicate the existence of the incident and share relevant details with external organizations following organizational communication plans and information*

disclosure policies. It can be particularly important to notify other IRTs or other organizations that can assist with the management and resolution of the incident.

Lessons learnt: After incidents have been resolved, lessons can be learned from how incidents and vulnerabilities have been handled. The organization should identify the lessons learned from the incident, and review, identify and make improvements to the information security incident management policy as well as the existing information security risk assessment. The effectiveness of the process, procedures and reporting formats should be reviewed, and improvements to the information security incident management plan should be made accordingly. An evaluation of IRT performance and effectiveness should periodically be conducted. The results of the reviews can be communicated and shared within a trusted community. It should be determined whether information regarding incidents may be shared with partnering organizations to prevent similar incidents from occurring.

The standard emphasizes that information security incident management activities are iterative. Therefore, an organization should regularly make improvements to several elements over time based on reviews of data regarding incidents and responses.

Limitations: The standard's main limitation is its shortcoming in dealing with technical and strategic matters. It neglects them, and the focus is mostly on high priority incidents. The disadvantage of this is that incidents where the learning outcome is high, but the probability is low, might be neglected. Another limitation is that the ISO 27000-series requires hundreds of pages of written material, which can be too extensive to read through during an incident. Lastly, ISO/IEC 27035 addresses corporate systems in general and does not take any considerations related specifically to PCS.

2.6.3 NSM's Fundamental Principles for ICT Security

The Norwegian National Security Authority (NSM) has published the *Fundamental Principles for ICT Security*, a set of principles and measures for protecting systems against unauthorized access or abuse [Nas20]. They are aimed at all Norwegian businesses and describe best practices and purposes of securing ICT systems. The principles are split into four categories; identify and map, protect and maintain, detect, and manage and restore. They cover a wide area, so only the parts concerning suppliers and incident management are included in this section.

Identify and map: This category is focused on mapping deliveries and the value chain, including services from suppliers on which they are dependent. It is then used to protect and maintain high security.

Protect and maintain: Organizations are advised to establish a process for

procurement where new systems and components can be trusted and do not contain known vulnerabilities. Otherwise, the probability of supply chain attacks increases. It addresses how the system should be configured and maintained until the desired security is achieved.

Detect: Threats and vulnerabilities should be detected and removed through cybersecurity monitoring. Organizations should also discover deviations from desired safe states through data analysis.

Manage and restore: This category emphasizes that organizations must be protected by effective incident management processes to detect and control incidents quickly. The processes include plans, exercises and communication. When the incident occurs, it is too late to develop procedures, so they need to be developed and practiced frequently. After an incident is handled and closed, it is vital to quickly identify and learn from it. This allows for the improvement of security measures and incident management to avoid making the same mistakes again.

The principles highlight the outsourcing of ICT as a common process. Before an organization can decide if they want to outsource services or not, it is essential that they assess whether they can maintain cybersecurity throughout the whole outsourcing process. The organization needs to possess adequate procurement competence and set the appropriate requirements to the supplier. According to the NSM, suppliers should meet some minimum requirements such as transparency regarding security, access control, monitoring to discover security incidents, routines for incident management and reporting, and emergency plans that harmonize with the customer organization's plans. Services and ICT products from suppliers that are certified and evaluated by a trusted third-party should be preferred. Organizations should also request discretion regarding the customer relationship and product details to reduce the risk of outsiders acquiring system knowledge.

The principles provide guidance on how to implement effective cybersecurity incident management, to instantly be able to control any situation. The roles and responsibilities of relevant personnel should be mapped, plans updated regularly and system testing should be demanded. Agreements with suppliers that can provide support during an event should be established. Finally, preparedness exercises with relevant suppliers should be conducted, along with verification of the routines for detection and preparedness.

2.6.4 CFCS: Cybersecurity in Supplier Relationship

In 2019, the Danish national IT security authority, also called Centre for Cybersecurity (CFCS), published a paper addressing cybersecurity in supplier relationships [fC19]. CFCS aims to advise organizations working on critical societal functions

with prevention, detection and protection regarding cybersecurity. The paper is an assessment of cybersecurity threats against suppliers, including a guide on cybersecurity in the phases of a customer/supplier relationship. Figure 2.5 illustrates the phases. There are especially two factors that are emphasized as contributions to better cybersecurity; having both internal and external resources, and having thorough guidance on how to obtain suppliers safely.

Figure 2.5: Phases of a customer/supplier relationship translated and modified from [fC19].

The organizations in the energy sector should carefully consider what to outsource due to their vital systems and sensitive information. They should conduct risk assessments where the main focus areas are what needs to be outsourced and the customer's responsibility. Outsourcing makes it harder to keep track of where and who the data is seen and processed by, but the customer is ultimately responsible for its data and security. They need to recognize that although they have outsourced some parts, they still have to ensure proper cybersecurity. Thus, they need to ensure that they have competent personnel to manage and cope with the responsibilities related to outsourcing.

When choosing a supplier, the requirement specification for security should be clear and communicated regularly. Sadly, security is often one of the first requirements that are neglected if costs need to be lowered. CFCS recommends that organizations pose security requirements to the supplier that provide an economic incentive. The agreement should be customized, and both parties should be familiar with the responsibilities and tasks at hand. Since suppliers might enter similar agreements with several entities, it is vital to formalize communication details in case of an incident.

After the agreement is settled, the customer should be able to monitor and verify that the supplier is delivering products and results as promised. Both the customer and the supplier should preferably enforce the cybersecurity deliverance.

Chapter 3
Method

This project was conducted as an empirical study as it fit the following characteristics: it requires well-defined research questions, new data gathered through social research, a replicable methodology, and a conclusion that is drawn based on findings [Uni20]. Furthermore, a qualitative research approach with the case study method was chosen, where interviews were the primary data source. This chapter will present the chosen research method and justification of choices made during the project. It will also discuss limitations to the method and ethical considerations.

3.1 Qualitative Research

A qualitative research method based on relatively few informants was used in this study. The method was chosen as in-depth information from a few organizations was desirable to perform a rich and detailed analysis of the chosen research area. A qualitative research method tends to focus more on social research than a quantitative approach. Whereas the quantitative approach is theory-driven with quantifiable data, the qualitative approach is a flexible design strategy [Rob11, p. 131] that requires the discovery of patterns based on observations. The flexible design challenges and sets requirements for the researchers. The limitations on instruments and universal methodologies requires robust preparations by the researchers and creates the need for knowledge and analytical abilities. *Real World Research* [Rob11, p. 133-134] recommends personal skill sets containing sensitivity, responsiveness to conflicting evidence, openness and interest to qualify as a capable researcher. Personal abilities are essential and have a significant impact on the quality of the research. This became a challenge that could negatively impact the results as the researchers had little experience with this research method. Because of relatively few quantitative data to base the findings on, it was also important to be reflective and unbiased.

In this study, the observations were obtained through case studies, interviews, document analysis and literature review. Qualitative studies requires that the

researchers are adaptable during the process, due to the nature of the observations and the direction defined by intermediate results [Rob11]. This kind of research facilitates exploration for nuanced contexts. In-depth exploration of a few organizations is required to achieve it [Jac00, p. 46], as has been done in this project.

3.1.1 Background study

The first step was a background study of the energy sector and cybersecurity incident management, which had already begun in the pre-project for this thesis. Relevant literature was acquired and studied, such as standards and best practice guidelines, to gain sufficient knowledge within the field. The focus was mainly on some well-established and internationally accepted ISO/IEC standards and Norwegian legislation for the sector. Additionally, documentation and guidelines from NIST, ENISA and Norwegian Center for Information Security (NorSIS) to name a few was reviewed, as well as other related work. Furthermore, other sectors that could face similar issues were studied to see how they coped with it. In this literature study, published articles, theses and reports, both Norwegian and international, private and official, were analyzed.

To conduct a study that would be useful for the industry, introductory conversations with different actors in the energy sector were organized. They provided additional knowledge and a realistic perspective on incident management and the timeliness of the theme. These entities were a supplier that provides monitoring and IRT to DSOs, and several representatives from a cooperation company owned by numerous small and medium-sized DSOs. The knowledge gained from these conversations and the literature review helped the researchers formulate valuable research questions to guide the data collection. This extensive process became beneficial in the data analysis phase in comparing standards and best practices for incident management with the findings of this study. This approach is consistent with the definition of a case study, which recommends a background study to get a thorough understanding of the study's issues.

3.1.2 Case Study

The case study method was chosen due to the research questions seeking explanatory answers, hence using the query word *how*. According to *Case Study Research* by Robert K. Yin [Yin09, p. 8], research questions focusing on *how* questions by finding links over time, correlating events and behavior, calls for case study as a method. It is also well suited for studies focusing on contemporary events and real-world organizations as they have different experiences, history, documents and evidence, which makes each of them a unique case. These characteristics fit well with this

METHOD	Form of Research Question	Requires Control of Behavioural Events?	Focuses on Contemporary Events?
Experiment	how, why?	yes	yes
Survey	who, what, where, how many, how much?	no	yes
Archival Analysis	who, what, where, how many, how much?	no	yes/no
History	how, why?	no	no
Case Study	how, why?	no	yes

Table 3.1: Choice of research method, modified from [Yin09, p. 8].

study since the purpose was to find current practice, which removes the need for control over behavioral events. Table 3.1 illustrates the choice of method.

Variations within the case study method include both single and multiple-case designs, where the latter alternative was chosen due to several participating DSOs, a supplier and the NVE. An advantage of using multiple-case design, sometimes referred to as a comparative study, is that findings across cases are considered more robust and compelling [Yin09, p. 53]. This factor was preferable as the goal was to find current practice and possible improvements that could apply to a substantial portion of the sector. As organizations vary deeply, it was necessary to study several organizations. Thus, an essential factor worth focusing on was how to replicate the studies on several entities, to make the results comparable. All participating entities did therefore undergo a similar process when being researched.

This multiple-case study was of a holistic design, which focused on each DSO as one case. Focusing on each case as one entity, while only taking one level into account, is a disadvantage with the holistic approach. In this study, only the management level was in focus, without taking specific details on the operational level into account, which might have led to the loss of some perspectives. Because the cases were analyzed on an abstract level, deducting and examining single circumstances in operational detail was harder [Yin09, p. 50]. Another disadvantage of holism is that it is harder to test scientifically, which stems from its structure. The holistic structure

makes it harder to divide and isolate the cause of a problem since there are many interacting forces that cannot be separated.

3.1.3 Qualitative Interview

Interview is one of the most prevalent forms of data collection within social research studies. It can be categorized into structured, semi-structured or unstructured interviews. The difference between these types is how flexible the interviewer can be with the interview structure and further in-depth questions during the interview. Unstructured interviews tend to be more conversational in nature, rather than a strict set of questions and answers. An approach similar to semi-structured interview was chosen, to create an open atmosphere around the interview. Hence, the conversational flow of the interview did significantly affect the order of questions as well as unplanned follow-up questions when needed [Rob11, p. 278-282]. Still, it was challenging to balance the planned line of inquiry while preserving a conversational flow. The interviewees were handed an interview guide beforehand, containing information on topics that would be discussed to help them prepare for the interview. Some questions could also be sensitive, and the researchers were clear that not all questions were mandatory to answer. Furthermore, the goal was to ask neutral questions to avoid the interviewees giving answers they believed were desired. As interviews were the main data collection method, the quality of the interview questions had an impact on the result. The interviews were planned to last around an hour, a time limit that was held throughout most of the interviews.

In addition, unstructured interviews were conducted in the form of conversations with several entities throughout the research period to obtain data for this report. These were mostly used in the preparation for the interviews and during the background study as information was needed to both understand the topic and to ask valuable questions.

The aim was to conduct the interviews face-to-face, which is the preferred approach [Jac00, p. 131] as it benefits understanding and clear responses. It also aids building trust between the interviewer and the participants, which can contribute to more sincere answers. Personal contact can be achieved through physical presence, thus enabling a trust that is hard to achieve over any online medium, where people tend to have a lower threshold for dishonesty. Providing an open environment was crucial for this study, since it encouraged participants to give truthful responses about their current practices. This aided in painting a more accurate representation of the organizations. In addition, the participants' knowledge regarding the topics discussed could directly influence their answers, resulting in ambiguous responses, which negatively impacts the conclusions drawn. It was therefore preferred to conduct the interviews face-to-face, since it allows the interviewer to observe body language;

an essential part of any conversation. Body language helps the interviewer see if the subject is unsure, defensive, or wants to explain more. In terms of location, the interviews were conducted where the interviewees felt at home, usually at their offices. The context can have a psychological impact on the answers as false impressions can give artificial answers [Jac00, p. 134], and was therefore tried to be avoided.

The fact that there were two interviewers allowed for one main interviewer, while the other had an observatory role that made it easier to ask follow-up questions. The interviews were also recorded, providing more accurate material to analyze, rather than written notes taken during the interviews. If one were to transcribe during the interviews, it would lead to a significant amount of work and probably loss of information, so an audio recorder was beneficial. There are both advantages and disadvantages to using an audio recorder. It gives interviewers the ability to conduct more conversational interviews as well as the ability to obtain direct citations. It also provides the ability to take notes that indicate interesting statements or reflections, such as body language, that can be useful in the analyses. This possibility was therefore taken advantage of. On the other hand, the presence of a recorder might distract or frighten interviewees, but the authors found that the benefits outweigh the disadvantages.

3.1.4 Qualitative Data Analysis

As Robson states in *Real World Research* [Rob11, p. 466], there is no universally accepted analysis method for analyzing qualitative data. To deal with the data from the interviews, summaries were produced. Producing summaries enables understanding of the context and significance of the data source, thereby reducing the amount of data [Rob11, p. 474]. Although it would have been possible to transcribe all conducted interviews, it would have led to a significant amount of work. By making post-interview summaries with impressions and initial findings, it was possible to extract the main ideas and results for further analysis. In addition, it was vital to read between the lines of the interviews to find aspects that might have been communicated indirectly [Jac00, p. 173]. The same summary approach was also used in the analysis of other relevant documents.

To analyze the data, the qualitative data analysis software *NVivo 12* was acquired. A constant comparison analysis was applied [Rob11, p. 474-483] due to this study's comparison of different organizations. The material was classified using thematic codes, where the same thematic information from all interviews were assigned the same codes. Codes can be seen as keywords, such as the different phases of incident management, deviations from mentioned plans or aspects concerning suppliers. The codes were then compared and systematically categorized, and the categories were compared and abstracted into concepts. The main idea behind this method is

to continuously compare information to find connections. A strong side of the qualitative approach is the flexibility around planning, implementation and analysis. The opportunity to scale the project by including new interviews or scope according to findings becomes intuitive, enabling the researchers to include more participants if necessary.

Written documentation was gathered from other sources to limit the interviewees' impact on the study. Document analysis is important to substantiate and reinforce evidence from other sources, since documents have the advantage of being stable. They can thus be reviewed repeatedly and studied at any time, independently of other data collection activities. Documents also have extended time and events coverage, enabling them to provide insight into different events and settings [Yin09, p.101-105]. Hence, it was desirable to analyze different types of incident management related documents from the participating organizations. Access to some documents were gained, but due to the high sensitivity of the information, most participants kept them confidential. The documents allowed the researchers to corroborate statements from the interviews while shedding an objective light on current practices. However, it is essential to take into account that written material is biased by its authors and has been produced for purposes other than this study, when considering its relevance.

3.2 Participants

The focus of this project was on one particular part of the electrical energy sector; the DSOs. They were interesting to study as they operate the infrastructure and are geographically determined. This property means that they can be the subject of cyberattacks that can affect the physical infrastructure of the power grid and cause power outages.

There were a total of four DSOs, one supplier of PCS and the NVE participating as main data contributors in this empirical study, where all were studied as separate cases. The DSOs varied both in the number of employees and the number of energy subscribers. The Norwegian categorization of organizations is that it is a SMB if the number of employees is less than 100, and large if the number of employees exceeds that [oNEN20]. On the amount of energy subscribers, small DSOs each serve around 10.000 customers or less, and large ones serve close to 100.000 or more. Thus, two of the participating DSOs are in the category SMBs, and the other two are large businesses, both in the number of employees and customers. In each of the interviewed organizations, it was of interest to interview persons with positions such as ICT security coordinator since all DSOs are required to have that position. Also, the description of their responsibilities, as explained in section 2.6.1, fit well with the research area of this study.

A selection of both large and SMBs was chosen for participation. Small organizations have fewer resources than large organizations and thus struggle more with managing the cybersecurity risks they face [BCGL17]. According to the introductory conversations with entities in the sector, there is a need for an enhancement of the SMBs' security competence as the threats continue to advance. Also, a study from Gjøvik University College [SWF10] found large organizations to be better at establishing cybersecurity policies, defining cybersecurity incidents and conducting rehearsals based on their incident management plans, indicating that they are better at incident management. Thus, it was interesting to examine the assumptions that experienced organizations perform incident management better than smaller organizations. Furthermore, SMBs constitute a considerable portion of Norwegian DSOs. It was therefore preferable to include both SMBs and large businesses to see if there were any areas where they could learn from each other. It was also beneficial as the goal was to propose recommendations for organizations of all sizes.

When determining the number of participating organizations, it was important to find a balance as having too much or too little information to process could harm the results. The researchers believed that by increasing the number of participants above a certain level, they would gradually provide less new information, leading to the selected amount of participants. In addition, contact with KraftCERT was established to get their perspective on aspects like the threats against Norwegian DSOs and their contributions to the sector with regards to the topic. Unfortunately, they did not have the time to participate in this study.

3.3 Data Quality

This section will discuss the generalizability of this study for the whole sector and the degree of reliability and validity of the obtained data. These two factors affect the quality of qualitative data [Rob11, p. 486].

3.3.1 Validity

Validity is a tool for measuring the quality of the data that forms the basis of this thesis. By examining the extent of what a thesis says it will analyze with what it analyzes, one will get an idea of the validity. It looks at whether the obtained data is what the researchers aimed to obtain and if it can be generalized to other contexts [Jac00, p. 205].

The validity of this thesis and its research questions is built up through a comprehensive background study of relevant topics. It showed correlations between the liberalization in the electrical energy sector resulting in the entry of suppliers and the threat landscape utilizing the vulnerabilities that came with it. Also, the

participating organizations were questioned whether the chosen topic was only a hypothetical problem or a real one, in order to test the validity. They believed it to be a valuable study and an important area of research that both they and the electrical energy sector would benefit from. As they expected there to be possibilities for improvement, they looked forward to seeing the results. Before the interviews, the participants were informed that the researchers wanted honest and reflected answers. Chapter 4 was then sent to all participating organizations, to allow them to validate their answers and correct any misunderstandings. All, except one participating organization, replied and approved of the content. The last one did not answer the request. This process is known as member checking, and it limits researcher bias and shows the participants appreciation of their contribution [Rob11, p. 158]. A control mechanism used for validity is to involve parties with different interests and perspectives. This was done by obtaining the NVE's authority perspective, DSOs own experiences, and a supplier's perspective and insight into the market. Another way to further enhance the validity would be to interview sources not in management to get more detailed, first-hand knowledge regarding the processes. This was omitted due to the time constraints of the study.

External validity is a sub-form of validity that focuses on how generalizable a study is, based on its findings. Although similarities and possible improvement areas recurred in the selected organizations, the findings do not necessarily apply to the whole sector. Time and space also delineate generalization as one cannot generalize for others than the participating organizations and the time when the data is obtained [Jac00, p. 363]. Some tendencies and connections might be of relevance for the selected participants and sometimes for the sector as a whole, but will not have the statistical foundation to apply to all. Therefore, to achieve generalization, a much more extensive and broader sample range than in this study is needed. However, by interviewing a supplier of many DSOs, the findings of this thesis still provide an overall perspective. Thus, the resulting recommendations from the project are identifiable and implementable for a bigger sample than were involved in obtaining the data.

3.3.2 Reliability

Another quality assessment tool is the trustworthiness and reliability of the data foundation. The overall goal is to keep error at a minimum with a low degree of bias [Yin09, p. 45]. Measures were taken to cope with this and mitigate unreliable answers, as explained in Subsection 3.1.3. The interviewees received the same topics beforehand and all interviews followed the same recipe.

Data triangulation is a methodology to increase the reliability of the data and conclusions. Incident management documentation was therefore obtained to verify

the interviews and get other perspectives. Data triangulation makes it easier for other researchers to replicate this study. Being two researchers mitigates bias and enhances the objectivity of this thesis. On the other hand, there exists some skepticism on whether complete impartiality is possible in a qualitative study, particularly with interviews as they are impacted by both the interviewer, interviewee and context [Jac00, p. 221].

3.4 Ethical Considerations

The critical nature of the energy infrastructure and the current threats against it, induced some ethical considerations to this study. The primary concern was the potential disclosure of confidential information. Details regarding security practices and emergency preparedness can be misused in the hands of an adversary and thus had to be kept confidential. Hence, participating organizations and individuals had to be kept anonymous, by removing identifying information so that neither the source nor the organization could be recognized. Questions that breached the NVE's confidentiality requirements on "energy sensitive data", explained in Subsection 2.6.1, were also avoided during the interviews.

The privacy of the participants was also a concern as the interviews were audio-recorded. If the participants were worried about being identified it could enable an unwillingness to participate or provide truthful information [Rob11, p. 208]. They therefore received an information sheet about the project and the handling of collected data. They signed a statement of consent and had the right to withdraw from the study at any time. The project was reported to and approved by the Norwegian Centre for Research Data[1] to protect the privacy of the interviewees. After the project's end, recordings were deleted, and all sensitive information was removed. The information sheet, including the statement of consent, can be found in Appendix A. Moreover, during the research and discussion of the participating organization, code words were used to further anonymize them. Each organization was assigned a code word that was consistent in all of the researchers' notes to avoid using the real name of the organization.

[1] https://nsd.no/nsd/english/index.html

Chapter 4
Results

This chapter will introduce results from the studies of the four DSOs, the supplier and the NVE participating in this project. The results from the DSOs will be presented first, and each DSO will then be referred to as Organization A to D. The findings will be categorized by the five incident management phases of the ISO/IEC 27035 standard, as presented in Chapter 2. Written material from the DSOs will supplement the findings from the interviews. Lastly, the results from the interview with the supplier and the NVE will be presented.

Case Introduction: DSOs

Findings from the four DSO interviews will be grouped by topic and presented together in this section. Organizations A and B were large DSOs, while organizations C and D were small, according to the categorization in Section 3.2. The small DSOs were both members of the cooperation company owned by several SMBs in the sector. In all of the conducted interviews, the ICT security coordinator participated. In addition, the head of ICT participated from Organization B, and the head of operations from Organization C.

As a result of matters regarding energy sensitive data, some participating organizations chose not to share documents related to incident management. However, Organization B provided a non-sensitive version of the report used for monthly reporting, and Organization C shared several documents regarding their incident management plans. It is important to note that these received documents are just a selection and not the comprehensive planning for this DSO.

4.1 Phase 1: Plan and Prepare

The large DSOs, A and B, had both used ISO/IEC 27001 [fSI18], NSM's principles [Nas20] and good practice guides as the basis for their contingency plans. However,

none of them strived to become ISO certified. Organization D, on the other hand, had mainly used the NVE's propositions and regulations in addition to NSM's principles and guidelines from the cooperation company to which they belong. All DSOs also got alerts from KraftCERT regarding current threats and incidents.

The large organizations had developed definitions of cybersecurity incidents. Organization B had an overall guideline describing how cybersecurity incidents should be handled and reported. Incidents spanned from malware to leaked sensitive information, with this list not being absolute. At Organization A, on the other hand, any unwanted ICT activity was categorized as a cybersecurity incident. Yet, not all incidents triggered their plans for incident handling. A phishing e-mail would not trigger emergency contingency plans, but all incidents had predefined routines that should be followed.

4.1.1 Attacks and Threat Landscape

To precisely plan and prepare for incidents, organizations have to analyze the threat landscape and perform risk assessments of their systems. None of the participating organizations had experienced any cybersecurity incidents in their PCS. Still, both large organizations frequently experienced minor incidents in other parts of their systems. Organization A had a noticeable amount of "background noise", such as phishing e-mails, and had once detected a security breach where sensitive information was available to unauthorized personnel. The breach resulted in a backtracking of several years of traffic to ensure that there had not been any exploitation. Both small organizations, C and D, had been victims of ransomware attacks on their administrative IT systems. Other than that, Organization D occasionally experienced phishing e-mails.

Both large organizations acknowledged that they were more attractive targets for cyber threats than small ones. Organization A believed malicious actors use times of peace to gather information about the organization and the energy infrastructure to enable future attacks. Hence, they strived to uphold an emergency preparedness level where they could handle cybersecurity incidents in-house, without being dependent on external resources. Organization B claimed to, at all times, act as if they were at risk as they viewed themselves as an attractive target for adversaries. Organization D also believed that even though the organization was small, it was a possible target for some actors. In contrast, Organization C did not consider itself an attractive target for targeted attacks against PCS. Instead, they viewed insiders as the biggest threat, in addition to incidents caused by weather or component failure. The insiders were not necessarily malicious, but could be employees that were tricked by attackers into providing access to unauthorized personnel. Therefore, their focus was on the security awareness of their employees. Nevertheless, their written contingency plans

contained essential assets to which they delivered energy.

Accessing Process Control Systems The DSOs' networks were usually split into different zones. Everything connected to PCS were in a closed and secure network, separated from administrative IT systems and other Internet services. Both small organizations claimed the PCS were well secured and difficult to access. The only access point was through a dedicated computer without any Internet connection. However, they could enable remote connection via a home office. The computer rotated within the group of people that had access to the PCS. If the DSOs were to lose this computer, they admitted that a security breach would be possible. Organization C mentioned that this designated computer had not been updated in many years, but that accessing it required a physical security key stored in a separate place from the computer. Moreover, the interviewee from Organization D pointed out the risk of penetration through the substations distributed all over the country, but that it was not a plausible threat.

According to the acquired contingency plans of Organization C, the home office computer would connect to the PCS via a broadband connection or wireless network, through a secure Virtual Private Network (VPN) connection. This computer, which was provided by the PCS supplier, would be checked once a year according to the Service Level Agreement (SLA). A SLA is a contract between a service provider and its customer that defines the service standards the provider is obligated to meet and help them manage customer expectations [Cas20]. To connect, the supplier needed a password from the DSO. This supplier was also in possession of backups regarding the organization's systems.

4.1.2 Organizational Structure and Roles

The organizational structure and dedicated cybersecurity personnel of the participating DSOs varied. How they organized and divided the network as well as tackled cybersecurity matters, will be presented in this section.

ICT Security Coordinator: In the large DSOs the ICT security coordinators dedicated 100% of their time to cybersecurity, while in the small DSOs it was only a small part of the role. Organization C's coordinator spent approximately 10% of the time on cybersecurity. At the same time, cybersecurity was only paid attention to "sometimes" in Organization D. The ICT security coordinators in the small organizations also had other roles, such as head of administration and operations engineer. They did not believe the ICT security coordinator role would ever become a 100% position, unless it could be shared between several small DSOs.

The ICT security coordinator role was the same in all the participating DSOs. This role had the overall responsibility for cybersecurity, including the main responsibility

for cybersecurity incidents. Whether it concerned the administrative network or the PCS, the coordinator would have primary responsibility and coordinate actions toward suppliers and authorities.

All reported incidents were initially appointed to the ICT security coordinator in all of the organizations. In Organization B, incidents were then delegated based on type; the ICT security coordinator handled incidents regarding integrity and confidentiality, while incidents concerning availability were transferred to the head of operations. In Organization C, on the other hand, incidents regarding PCS would be coordinated by the head of operations. In their contingency plans, the ICT security coordinator role was not mentioned further than as part of the crisis staff.

Cybersecurity Resources: In Organization A, the ICT security coordinator was the only role fully dedicated to cybersecurity. Also, one person would always lead the operative matters and be responsible for emergency preparedness 24 hours a day. In the other large organization, other people were working on cybersecurity in addition to the ICT security coordinator. Contrary to the large organizations there were fewer resources dedicated to cybersecurity in the small ones.

Incident Response Team: Organizations A, B and D all had internal IRTs, while Organization C got its IRT from a supplier. All that had internal IRTs could also get help from suppliers if necessary, but both large organizations claimed to be able to handle most incidents themselves.

4.1.3 Suppliers

The DSOs each had one supplier of PCS in addition to other suppliers of hardware and software connected to the PCS. Other sub-contractors provided services such as network, cabling and setup. The large DSOs also had suppliers that used intrusion detection and sensors to monitor the process control network at all times. The small organizations both had the same supplier of PCS, while the large organizations both had the same supplier of the monitoring service. According to the interviewee from Organization A, the use of suppliers was desirable from an economic perspective. This was because DSOs might possess fewer resources than they need and then have to use external resources to compensate when needed. Conversely, the interviewee also stated:

> *"If you outsource everything to the suppliers, you have also outsourced the knowledge and ability to handle an event."*
>
> — *ICT security coordinator of a large DSO*

The involvement of suppliers in incident management differed between the participating DSOs. The small organizations were more likely to seek aid from their suppliers than the large ones. As Organization C's IRT was external, it was natural that they were dependent upon the supplier. Organization D would contact the supplier relatively quickly after the detection of an incident, in case the supplier had any helpful knowledge or were aware of something the DSO was unaware of. Both Organizations B and C mentioned that if the supplier of PCS needed to do maintenance work, upgrades or patching on the systems, they had to be physically present in the DSO's facilities. Alternatively, the DSO could give them access remotely. The same applied when the supplier assisted the DSOs in handling cybersecurity incidents.

Contract Management: The large DSOs had extensive procurement processes. Organization A first presented some requirements that had to be met by the supplier and claimed that by being a large organization, they were good at both establishing and terminating contracts. Organization B always conducted a risk and vulnerability analysis before entering new agreements. Except for Organization A, which had conducted security audits twice in the last two years, the DSOs had little insight into the security of the suppliers. Organization B trusted its monitoring service supplier as they believed they were the best in the business. Hence, their security must be good. Organization C had requested information regarding the security of their PCS supplier, but had not received it. Still, they fully trusted the supplier. The interviewee from Organization D admitted to having no knowledge of the suppliers' economy, employees or security. They acknowledged that they should check these factors, but they have chosen to trust the supplier instead. In contrast to the others, Organization D had no long-term contract with the PCS supplier. They only had a loose agreement regarding contact if its internal IRT was not sufficient to handle the incident. However, during the year 2020, they want to agree on a long-term partnership that will benefit both parties.

Get Sufficient Resources: If several organizations simultaneously would require help from the same supplier, the supplier would be pushed to the limits of its capacity. Thus, all the participating organizations agreed that they did not believe that they would receive the promised resources in such a scenario. Although the DSOs were promised aid within a certain amount of time after the occurrence of an incident, this could be hard to uphold if several DSOs experienced simultaneous failures or attacks. None of the DSOs were aware of any possibility to buy priority from suppliers in the event of an extraordinary situation. The small DSOs even believed they would be in the rearmost end of the queue in that scenario. According to them, suppliers prioritized those who pay the most, and the small organizations pay less for their services than larger ones do. For Organization D, this could lead to significant problems as they were not in possession of any spare components to the PCS. The spare parts they had access to were shared with other organizations. Thus, their

systems could be paralyzed for months as the result of an incident. Organization B believed they had a great support system that could provide assistance in case of an incident. However, getting a formal SLA that included 24-hour preparedness by a supplier could be problematic, according to Organization A. This was believed to be a problem for the whole industry, and that such an agreement was necessary to maintain high availability.

4.1.4 Involvement of Suppliers in Incident Management Plans

Organization A's attitude towards plans was to focus more on the mapping of available resources, rather than preparing detailed and extensive plans. Therefore, the DSO kept an overview of available resources and their expertise, both internal and external, regardless of their current job position. As a result, they would know who to contact and assign various tasks in a critical situation. However, for some specific incidents, like if all smart meters in the region got hacked, Organization A had more detailed plans. Similarly to Organization A, Organization D's plans mentioned which suppliers should be contacted during an incident, but there was not much mention of how suppliers should otherwise be involved in incident management.

Organization B's policy was to use external services instead of having all the necessary expertise in-house. The reasoning was that maintaining good cybersecurity required huge expertise. Their plans for incident management therefore contained an agreement with an external IRT they could contact if necessary. The interviewees believed their plans for incident management were good and well-tested, but they were prepared for deviations from the plans if an incident occurred in their PCS. On paper in Organization C, it was the ICT security coordinator's responsibility to have contact with suppliers and coordinate actions. However, in reality, they delegated incidents based on system type. So, if the incident involved PCS, the head of operations would coordinate actions and communicate with suppliers. Their plans for contingency were comprehensive, but lacked aspects where a cyberattack was the main problem. The focus was on situations like fire, physical attacks or component failures due to weather conditions. The plans obtained by the authors also lacked mention of when and how suppliers should be involved. They only contained contact information and information that the PCS supplier could assist during incidents. The authors tried to get a confirmation regarding this point from Organization C, but without success.

4.1.5 Cybersecurity Preparedness Exercises

There were variations between the DSOs in how they involved suppliers in cybersecurity preparedness exercises. However, all the participating DSOs had conducted cybersecurity preparedness exercises without suppliers to some extent in recent years.

Yet, these had not been specifically directed at PCS. According to Organization C, the NVE requires them to test their incident management plans at least once a year, and the exercise must be practical every third year.

The only conducted exercises that were aimed at the PCS had been tabletop exercises. However, Organization C had not conducted any exercises in their PCS at all. This was mainly due to the continuous availability requirement of PCS. Organizations C and D had both participated in exercises arranged by the cooperation company they were members of, but those were not aimed at the PCS. Organization C had also conducted three exercises in 2019, and the security of their PCS was once tested by the NVE. The result was then negative for intrusion both from the outside and the inside of their network. Organization D's strategy regarding exercises had been to identify possible threats and whom to contact during an incident. Additionally, they had discussed how to manually control the PCS if necessary. Similarly, Organization B had only conducted tabletop exercises for the PCS. However, they regularly tested other parts of the system through practical exercises where communication and cooperation were in focus. Organization B's routines during an incident were also tested regularly, sometimes daily, through outages caused by weather or defect components.

There had not been any involvement of suppliers in the exercises conducted by the small organizations. Organization D excused it with a lack of resources. During the interview with Organization C, it dawned on the interviewees that the phone number they had been given to contact the external IRT in case of an incident had never been tested. This lack of testing was due to the absence of suppliers in exercises. They agreed that the contact should have been tested, but usually, if any questions or concerns appeared during the day, they would contact the supplier through acquainted personnel. Organization C's contingency plans showed that their overall objective was to prepare involved personnel for potential, real life situations. Still, external suppliers were not included and no exercises directly tested the involvement of suppliers. During Organization B's tabletop exercise regarding PCS, neither the external IRT nor the PCS supplier were involved. The external IRT was available on the phone if needed, but was not utilized. They had, however, involved a supplier in exercises in the administrative IT systems. When it comes to Organization A's involvement of suppliers, it happened more occasionally in an ad hoc manner. Suppliers were involved when needed in tabletop exercises, and to a greater extent if specific scenarios were planned upfront. Suppliers had exercised together at one point, but this was organized by the PCS supplier.

Although there was barely any involvement of suppliers in exercises, a common factor among the participating DSOs was that they saw the advantages of it. Organization D found it especially advantageous regarding testing of the acquisition

of spare parts for the PCS. Organization A mentioned that more involvement of suppliers in exercises would be advantageous to test whether the suppliers would provide the resources they claimed they were able to provide during an incident. The main reasons for limited exercises with suppliers were time and resource limitations. The organizations acknowledged that it should be prioritized in the future as it is beneficial, but it needs to be prepared well in advance. When asked if they found it advantageous to involve several suppliers in the same exercise, both organizations A and C said it would be beneficial if the systems from the different suppliers were interconnected. In the current situation, however, they believed the systems in the PCS to be separate, and it was therefore not relevant to involve several suppliers in the same exercise.

4.1.6 Sector Collaboration

There were plenty of collaborations within the sector regarding cybersecurity, according to Organization B. KraftCERT assisted its members in handling cybersecurity incidents mainly through advice and relevant information. The DSOs did, for instance, receive alerts regarding new vulnerabilities. The sector also arranged sector meetings to share information and strengthen the collaboration. Through their memberships in the cooperation company, the small DSOs were part of a joint procurement of computer equipment, as well as an academic community regarding cybersecurity. The collaboration enhanced their competence and helped them improve their procurement skills and routines regarding cybersecurity and incident management. The contingency plans of the small organization revealed that companies in the same area had established an emergency preparedness cooperation. Agreement on the exchange of personnel and other resources during incidents was enabled through the cooperation company.

4.2 Phase 2: Detection and Reporting

Both large organizations used a monitoring service, and as such, together with the supplier, they were responsible for detecting security incidents in their PCS. In Organization C's case, both the DSO and the PCS supplier detected incidents. The interviewee from Organization D, on the other hand, did not mention any organizations other than themselves that were responsible for detection. Organizations A, B and C all said they would be contacted immediately if the supplier detected the incident, either to handle the incident or to provide necessary access to the PCS.

If the incident was detected by the DSO the approaches for contacting the suppliers differed. The large organizations would not contact the supplier unless they needed help in handling the incident, excluding contact after they had handled the incident. According to Organization A, reporting and communication towards suppliers was

crucial in the occurrence of an incident, but not always the top priority. First, they needed to establish an overview of the situation and then, only the necessary resources would be contacted. If they gathered unnecessary resources, too much effort would be required to coordinate all parties. Organization D had a different approach than the large organizations. If an incident was detected, they would contact the supplier as soon as possible in case they had any helpful knowledge or to raise awareness regarding aspects on which the DSO might be unaware. Organization C would naturally also contact the supplier quickly as they did not have an internal IRT. All organizations, except Organization C, had tested the reporting channels towards suppliers and were satisfied with the communication. Organization B also mentioned that it got up to daily reports from the supplier, in addition to regular meetings.

4.3 Phase 3: Assessment and Decision

The main responsibility for handling cybersecurity incidents were at the ICT security coordinators, regardless of whether they had outsourced incident handling. The large participating organizations had sufficient knowledge to handle some incidents regarding the PCS internally, but the supplier possessed the expertise in the systems. They had some influence on the suppliers, and could force them to fix discovered vulnerabilities. Each supplier of hardware and software were responsible for fixing their vulnerabilities. Organization C pointed out that they were merely a user of the systems and did, therefore, not understand how the PCS function. Decisions regarding incident handling would thus be taken by the supplier, even though the responsibility for assessment and decision was at the DSO.

Although the DSO was responsible for assessments and decisions, the interviewee from Organization D was not satisfied with the power balance in the relationship with the supplier of PCS. The supplier had too much influence as it controlled the systems and specified how communication to and from the systems would be carried out. Thus, the supplier decided how the DSOs related to them. The large organizations expressed more influence over the suppliers than the smaller organizations did.

4.4 Phase 4: Responses

None of the organizations had experienced any cybersecurity incidents in their PCS, but they had tested responses during exercises and incidents in other parts of the system. They all agreed that if the situation required it, suppliers would be involved in responses. Organization D had not involved any suppliers in responses to neither incidents nor during exercises. However, they found it beneficial to include suppliers to improve communication and handle incidents more efficiently. Suppliers had not cooperated when responding to a threat or an incident, something Organization D

believed could be beneficial. If so, the communication would go through the DSO. Both organizations A and C did not view cooperation between suppliers as very relevant, as they pointed out that the PCS were isolated with only a few suppliers in the systems. However, they said it might be beneficial in the administrative IT network, which had more suppliers or if there were any shared interfaces in the PCS.

4.5 Phase 5: Lessons Learnt

One large and one small organization, Organizations A and D, believed it was valuable and natural to include all parties that were involved in the incident management process in post-evaluations. According to them, it was essential to communicate well with the supplier and listen to their input regarding improvements to the handling of incidents. Both organizations had routines for collaboration with suppliers in the evaluations of incidents, but only the DSOs used the information collected during incidents. When Organization D implemented significant changes after lessons learnt, all relevant suppliers were notified via e-mail regardless of their participation in this phase.

Organization B did not include suppliers in the process of learning from incidents. Still, they had routines for learning from incidents, and their plans for incident management were reviewed and improved regularly. The changes based on lessons learnt had been internal, resulting in it not being natural to communicate them to suppliers. However, they notified the monitoring supplier when significant changes to the PCS were made. Organization C's contingency plans were insufficient regarding external suppliers. Other than that all parties should have a quick and factual orientation and assessment for future conditions, they mentioned little about the involvement of suppliers.

Organization C did not have any routines for involvement of suppliers in lessons learnt. However, they did not have much routines for learning from incidents in general. The interviewees admitted that after an incident, the personnel were happy with it being over and did not pay much attention to the performance or if there were any areas to improve. They might have made some changes to the incident management plans and were more security conscious, but said they should be better at using the incident to improve incident management. Nevertheless, they did conduct a review of the ransomware attack, with a supplier that assists them during incidents. However, this collaborative review was arranged by the cooperation company Organization C was part of and not by the DSO itself.

Case Introduction: Supplier

This section will present results obtained through the interview with a supplier delivering PCS to several Norwegian DSOs. To differentiate from suppliers mentioned by the interviewed DSOs, this supplier will be referred to as Supplier S.

This international supplier had several offices in Europe, among them Norway. Up to 99% of their international customers were DSOs, power producers or suppliers to those entities. In Norway, their customer base included dozens of DSOs of all sizes. Their PCS ran on closed network loops without Internet connection and were usually accessed through DMZs, due to regulations by the NVE. There were few Norwegian DSOs without SCADA systems. The fact that the supplier had customers of all sizes gave the interviewee the ability to reflect on observed patterns between organizations.

4.6 About the Industry

There were only a small handful of PCS suppliers in Norway, most of which were international. Supplier S had an agreement with KraftCERT for joint reporting of unwanted incidents, and they also had contracts with equipment manufacturers for the same reason. Most of their DSO customers conducted risk analyses and handled security incidents with internal or external IRTs from other organizations. The amount of possessed expertise at the DSOs varied, and was usually parallel with the size of the DSO. The more they had outsourced, the more they relied on suppliers. Although Supplier S did not offer IRT services to DSOs, they were contacted in case of incidents on their systems, such as faulty components. Because of regulations, they were not allowed to do continuous monitoring of PCS, but had logging systems that they could periodically retrieve. According to the interviewee, the tendency among DSOs were an increased interest in patching of systems and SLAs containing software maintenance. This interest could be a consequence of the NVE's increased focus in this area. As the PCS were not connected to the Internet, it was not necessary to have an updated version of the access computers at all times.

4.6.1 Lack of Security Knowledge

The knowledge regarding cybersecurity was varying among the supplier's DSO customers. Many DSOs did not possess sufficient knowledge about the PCS and legislation concerning them. As an example, the interviewee described a situation where a DSO wanted to have the PCS in the cloud and control the switches using mobile phones. It was technically possible, but the customer lacked the knowledge about it contradicting the legislation and why it is strongly advised against from a cybersecurity perspective. The interviewee stated that this problem dates back to

the late 1990s, where the Norwegian energy sector was put through major changes. The sudden increase in outsourcing forced many to leave their jobs, as resources were to be bought and not owned. This change resulted in lost expertise, giving ripple effects to this day with too few employees throughout the sector.

4.6.2 Threats

Supplier S acknowledged that they could be an interesting organization for attackers to penetrate. Although there were dedicated system monitoring personnel, no one could be completely safe from an attack. Neither their systems, nor the PCS they have delivered to customers, have experienced any successful attacks. It was the interviewee's opinion that the lack of breaches was the result of the strict regulations the energy sector was facing. The interviewee was also confident that it would be hard for attackers to exploit Supplier S to enter the networks of Norwegian DSOs. Perpetrators attacking Supplier S could, if successful, obtained information about their network and technological systems and solutions. However, they would not be able to access their customers' PCS. As the PCS were separated from other networks, there were no backdoors into those systems from this supplier's network. As no continuous connections to the PCS existed, Supplier S had to request access whenever needed.

4.7 Contract Management

Supplier S usually operated with standard contracts that offered DSOs the services they believed were important to both themselves and the DSO. According to the interviewee, the procurement skills differed with the size of the organization. Smaller DSOs relied more on and trusted suppliers to a higher degree, while large organizations were more in control and customized every detail. The medium-sized organizations varied somewhere in the middle. In general, the agreements were similar, but details on hardware updates, response times and 24/7 readiness differed. Although Supplier S had the opportunity to offer 24/7 SLAs, they tried to avoid it due to the enormous amount of resources it required. The interviewee could not see any direct differences or patterns between what kind of agreements DSOs of different sizes chose.

The DSOs had conducted few to none security audits of Supplier S' network or systems. Usually, the contracts did not contain details regarding the supplier's infrastructure or security. The DSOs were not focused on auditing the supplier's compliance with the security requirements stated in the contracts, although they had the authority to do so. Supplier S had experienced one DSO that set a formal requirement for Supplier S' office network infrastructure, as well as a requirement of ISO 27001 compliance. The requirements were so the DSO could send sensitive data to the supplier. However, the DSO could not meet a similar requirement from the

supplier. Thus, the DSO could not ensure that sensitive data from the supplier was secure. This data contained sensitive information about the PCS, and the interviewee stated that this example explains why DSOs also need to have secure infrastructures.

4.8 Providing Sufficient Resources

In a situation where a few DSOs would require assistance simultaneously, the interviewee believed Supplier S could handle it by acquiring resources from their offices in other countries. As of now, this has not been a problem, since there were few system failures. They could probably handle events increasing from once a month to 2-3 times a week. If a massive cyberattack against several Norwegian DSOs or several of their Nordic customers were to happen, the supplier admitted to having trouble offering necessary assistance to all. This was due to a lack of extra capacity and that not every employee possessed the necessary knowledge or was allowed to access the customers' networks.

In a scenario where several of their customers would be attacked simultaneously, the supplier would have to prioritize whom to help. By buying a specific response time, a customer was practically buying a priority. However, smaller DSOs would never buy a SLA with a response time of, for instance, 2 hours as it is quite costly. Larger DSOs, on the other hand, may have required it and bought it accordingly. After response time had set priority, an assessment of criticality and the least negative impact on society would be used. Therefore, they would probably help the largest organizations first since they have the most extensive customer base.

4.9 Power Balance

Although the systems they provided were expensive, Supplier S did not feel that the power balance between them and the DSOs was uneven. Their financial results reflected marginal profits, since the tendering procedures by the DSOs could emphasize the price to count up to 70% of the tender. Supplier S was committed to having a good relationship with the smaller DSOs. Small DSOs tended to be more loyal, and the supplier focused on not breaking the trust. In terms of price, the smaller ones got a component for the same price as the larger ones. The difference came when the large organizations ordered a larger quanta. There was also not much room for losing customers, as there were a limited amount of them in the Norwegian market.

Only being a few actors that provided PCS to Norwegian DSOs was an advantage, according to Supplier S. The DSOs knew the suppliers and were confident the suppliers knew the peculiarities of the sector and legislation. It also lessened the price pressure on the suppliers, which allowed them to compete on quality instead of only price.

4.10 Involvement in Incident Management

The interviewed supplier was usually not involved in the incident management processes of DSOs. Some customers had wanted to test the systems against Man-in-the-middle attacks, but no invitations to cybersecurity preparedness exercises had been received.

> *"It is not really important that we participate in exercises [arranged by the DSOs], but it is very important that we become involved in the phase afterward [Phase 5 in ISO/IEC 27035] where we go through things."*
>
> — *A supplier of PCS*

The supplier did, according to the mentioned quote, not have any intention of initiating exercises with DSOs. Supplier S did, however, see an advantage of external parties testing the systems since their mindset is different, which enabled them to find new loopholes. It could also be beneficial to test the DSOs knowledge of, for instance, backups and whether the DSO was successfully able to reinstall a backup. However, the supplier did not see the need to be involved in such testing. According to the interviewee, these skills were also related to the size of the organization. Supplier S would participate in exercises if the customer preferred it, but saw no reason for it while pointing out the cost and amount of resources it required.

The interviewed supplier wished to be more like a competent advisor to the DSOs, rather than a sales organization. Incidents in the DSOs' PCS that were not communicated to the supplier were, therefore, considered problematic. Thus, Supplier S strived to have a good and open dialogue with the DSOs and claimed that this was working well. The DSOs had access to most of the information the supplier stored regarding their systems, so that the supplier could be an advisor and provide as much helpful information as possible. These were, for instance, various logging features such as login attempts, IP traffic and ports. All in all, the interviewee admitted that there were no routines for learning from incidents with DSOs.

The incidents where the supplier was usually involved were often caused by faulty components. Then, several other suppliers may be involved too. The interviewee admitted that it was desirable to unite all involved parties in case of a cyberattack. If several suppliers were involved in an attack, they would probably point at each other, and everybody would be reluctant to take the blame. A large-scale attack, where several DSOs or suppliers would have to work together, would be coordinated by the NVE.

4.11 Strengths and Improvements

Even though there was little involvement of the supplier in the DSOs' incident management processes, the supplier was overall satisfied with the involvement. Considering enough information about potential risks and incidents were well communicated. By being an international organization, Supplier S had insight into the energy sector in other countries. Their impression was that the large Norwegian DSOs were a step ahead of their colleagues, especially when it came to testing and implementation of new technologies. The small and medium-sized DSOs, on the other hand, had the potential to improve. Lastly, Supplier S hoped for a boost in knowledge about PCS and the legislation, since they experienced a slight lack of knowledge in this area.

Interview with the NVE

This section will present matters obtained through an unstructured interview with a representative from the NVE.

4.12 Cybersecurity

According to the representative, cybersecurity has gotten more attention in the energy sector in recent years due to the increased focus on it in general, such as the update of the Security Act[1]. The threat actors were, however, more evolved than the organizations in the energy sector. Consequently, there had been a successful attack on the PCS of a small Norwegian DSO. The representative believed the financial sector to be better at cybersecurity management.

4.13 Differences Between Small and Large DSOs

Even though all Norwegian DSOs were small on the global scale, there were differences between the small and large DSOs when it came to cybersecurity. The small organizations typically lacked security competence, while large organizations were better purchasers and better at attracting competence. However, the NVE did not have enough observations of the DSOs' security to statistically and officially conclude on any differences between small and large organizations.

4.14 Involvement of Suppliers in Incident Management

Procurement affects security even though it may not be the intention. As such, it was beneficial to include suppliers in the cybersecurity preparedness exercises of DSOs. Still, the NVE was not planning to include how suppliers should be involved in incident management in the legislation (Kraftberedskapsforskriften). In the case of extensive incidents in the energy sector, the NVE would coordinate actions. Yet, it was the representative's view that Norway did not have sufficient capacity to handle security incidents that compromised multiple organizations. In such a scenario, the suppliers would not be able to help all affected organizations due to the existing supplier concentration in the sector.

[1] https://lovdata.no/dokument/NL/lov/2018-06-01-24

Chapter 5
Discussion

In this chapter, the findings from Chapter 4 will be discussed and linked to the research questions presented in Chapter 1. The chapter is divided into the two parts of the research question, and lastly, the authors' recommendations for improving the involvement of suppliers in incident management will be presented.

RQ1: How are suppliers involved in Norwegian DSOs' cybersecurity incident management regarding process control systems?

5.1 Resources

The results show that there is a big difference between small and large DSOs when it comes to the amount of resources they have. According to the interviewed supplier, it is proportional to the size of the organization. The use of internal or external IRT could also be a measure of the resources and expertise an organization has, and it confirms the findings. The trend has been to outsource as much as possible, which has led the DSOs to limit the internal resources to what is strictly necessary [AAF+08]. This tendency is probably present in all sectors, but is problematic when it concerns a critical infrastructure. Large organizations are, however, required by law to be able to maintain the energy supply by themselves [oe19b] and will therefore have more resources than smaller organizations and be less dependent upon external IRTs.

5.1.1 Expertise

Limited resources in total lead to less focus and dedication to cybersecurity, procurement of services and incident management. This is confirmed by viewing the amount of time the ICT security coordinators in the different organizations were able to dedicate to cybersecurity. Organizational size is a fundamental factor in

building sufficiently robust academic communities [Gro19]. The representative from the NVE confirmed that small organizations typically lack security competence and claimed that large organizations attract competence better than small ones. The large organizations will therefore continue to strengthen security and incident management. The *Future Competence Needs II* report by NOU, specifies that the Norwegian market is in short supply of ICT specialists [Hea19]. These specialists can manage networks, develop and operate software, and have expertise in cybersecurity. A shortcoming of such personnel will have repercussions for obtaining a qualified workforce for the energy sector. A report published by the NVE in 2017 revealed that human errors and a lack of knowledge is stated as the number one reason for cybersecurity incidents in the energy sector [inf17].

Line et al. [LTJ11] stated that there is a shortage of personnel with expertise in IT and OT within the sector. This was confirmed in the information obtained from the supplier. According to the interviewee, many individuals in DSOs do not understand that PCS have to be in a separate network from other systems. It is alarming if people responsible for the systems that previously have been exploited in most of the successful cyberattacks on the energy sector [CS17], do not understand why they can not put the system online and control it from their phones. This inadequacy of proper knowledge was also apparent in the DSO interviews where some, both large and small organizations, were insisting that air gaps provide adequate security to protect their PCS. Considering the elimination of air gaps as a consequence of the digitization [Rot18], this is a problematic statement. The fact that the interviewees continued by stating the possibility for remote connection to their PCS via VPN, shows a lack of understanding of cybersecurity. Such a misunderstanding can allow for adverse cyber-related events that could have been avoided with proper knowledge. Another example appeared from one of the small DSOs, where all incidents regarding PCS are handled by the head of operations. This person's OT training means that the possible lack of IT knowledge can lead to problems when handling cybersecurity incidents.

The lack of cybersecurity expertise can, to some extent, be explained by the IT and OT convergence the sector has gone through. The energy sector is characterized by long-term employees and a few key personnel with vast knowledge of the overall system. This sort of resource is hard to uphold in the long run [AAF+08], and dependence on key personnel creates risks [HHT+17]. The digitalization requires adjustment and knowledge update of long-term employees. While they were likely excellent at protecting the old sector, the new threats have different characteristics. Cybersecurity incidents are characterized by their short or no warning, high speed and that they are geographically unbound [fSI12]. Although there has been a lot of changes, the transition to the digitalized sector started years ago, so sufficient knowledge regarding cybersecurity is fair to expect at this point in time.

To enhance their expertise, organizations acquire different systems and services from suppliers [AAF+08]. Hence, small DSOs outsource more services than large DSOs, which leads to the expertise necessary to handle cybersecurity incidents being at the supplier and not the DSO. This was confirmed by one of the small DSOs when asked how they will handle a cybersecurity incident in the PCS:

> *"We will have to get help from the supplier, there is no doubt about that. They will have to investigate it because we are only a user of the system and do not understand the underlying functions."*
>
> — *Head of Operations at a small DSO*

The systems that the head of operations referred to in the quote above are vital in the delivery of energy to essential societal functions such as hospitals as well as numerous households. For such a lack of expertise to be acceptable, the DSO has to be entirely sure that it will get immediate help from the supplier in case of an incident. However, that is hard to guarantee for suppliers [HHT+17]. Furthermore, organizations that outsource services will have difficulties gaining back the knowledge. An effect that increases even more when the DSOs' internal, experienced workers get replaced as years go by, and new technical staff become dependent on recorded information [ERL06]. This effect makes it hard for small organizations to fill the knowledge gap they currently have. The current lack of system knowledge shows that there is a need for suppliers with this expertise. If the sector is to be less dependent upon suppliers, many DSOs need to increase their knowledge in cybersecurity and IT and OT convergence. One of the small organizations described itself as forward-leaning and progressive, and claimed there is a lot of openness towards learning new things and a willingness to change. These are important qualities when it comes to improving IT security.

5.1.2 Good Procurement Skills

As a thorough preparation is the cornerstone of the final delivery, it is important to be a good procurer when outsourcing systems or services. To be a good procurer and recognize what resource is needed, it is essential to possess the right expertise. Several private and official resources, among them CFCS [fC19], introduced in Subsection 2.6.4, have published guidance documents with good practices for the procurement process. Before initiating an outsourcing process, DSOs should consider their fitness to handle all the phases of the procurement process [Nas20]. They need to map existing internal knowledge, why outsourcing is desirable and what systems will be affected. A well-outsourced service is recognized by having good measures regarding the implementation and management of the outsourced service. Clarifications on access control and established routines for notification, reporting

and evaluation should be in place to optimize the relationship. Agreements should emphasize key points like responsibility and reliability, and legislative changes from authorities towards DSOs during the contract period must be communicated and rectified in collaboration with the supplier [KL18]. It is necessary to ensure that cybersecurity can be maintained throughout the entire life cycle of the outsourcing service. Cybersecurity matters during the involvement of suppliers are also explained in the checklist made by the NVE called *ICT security with procurement and service delivery in the energy industry* [MKG20].

To ensure cybersecurity, it should already be in focus in the early stage of designing and implementing a product. Hence, DSOs should focus on cybersecurity from the beginning of the involvement of suppliers in PCS. The International Society of Automation (ISA), has with IEC published the ISA/IEC 62443 standard. It consists of several standards and technical reports that define procedures for implementing PCS with secure practices and performance [All20]. While the ISO 27000-series with the ISO/IEC 27035 standard focuses on business and IT systems, this standard addresses PCS' physical processes and systems, thus being applicable to PCS. Key mechanisms like zones and DMZs are, for instance, highly emphasized. As stated in NSM's *Fundamental Principles for ICT Security* [Nas20], products should be tested and certified by a trusted third-party, for instance with the ISA/IEC 62443 standard as a basis. Considering the lifespan of PCS in decades, there are no doubt that the cybersecurity threats will evolve throughout their lifetime. Suppliers that run maintenance on PCS are therefore expected to be involved in risk assessments, either conducted by the asset owner or by conducting an independent analysis themselves. Documents that verify and prove the security of the components must be provided by the supplier, along with recommended analytical tools to cope with the stated level of cybersecurity.

New solutions around an outsourcing of the entire procurement process have arisen in the last few years [oPS20]. Such services can partially or fully take over the procurement processes in organizations, hence freeing capacities to focus on strategic matters. One of the concerns with this solution is whether the procurement supplier will be fully capable of correctly understanding the needs and requirements of PCS and DSOs. To do so, they will have to specialize in the energy sector, which is yet to be seen. Another concern is the financial resources of the DSOs and whether it is a good investment. Although it might be financially beneficial for SMBs, critical internal knowledge will be outsourced and lost.

The procurement skills of the participating DSOs differed with the size of the organization. Both large organizations seemed to possess some of the qualities that characterize good procurers. They go through an extensive process with risk and vulnerability analyses and lists of requirements before procuring new systems and

services from suppliers. This shows that they are making an effort to maintain cybersecurity. Maintaining the necessary competence is demanding if one is not part of an academic community, but being a large organization provides this community. The small DSOs' more limited procurement skills are probably due to their smaller academic communities and lesser resources. Scarce total resources result in less resources granted to the process of finding the appropriate supplier. Similar findings have also been revealed by the NVE [KL18]. The members of the cooperation company that both participating DSOs take part in collaborate to some degree regarding the procurement of new systems and establishing appropriate requirements to suppliers. Although it increases their skills, the interviewed supplier differentiated the DSOs' procurement abilities based on size, which indicates that there is still room for improvement. However, since the supplier was not asked specifically about the interviewed DSOs, this may concern other organizations.

A direct result of enhancing their procurement skills is that smaller DSOs will improve cybersecurity and incident management as they are able to set better requirements and acquire better outsourcing services. It is the contract that regulates the relationship between the contracting parties, so it is essential to impose the correct requirements on the suppliers through contract terms.

5.1.3 Security Audits

Performing security audits and checking the supplier's compliance with the requirements set in the contract is a right the DSOs have, but seldom utilize. Only one of the large organizations had conducted security audits and the participating supplier had not experienced any audits of its contracts or systems. This shows that it concerns many DSOs. The lack of security audits was confirmed by all participating parties, even though the DSOs are recommended to do so by the NVE's checklist and legislation [MKG20, oe19b], by the NSM [Nas20] and CFCS [fC19]. By not auditing suppliers, there is a possibility that the security requirements in the contract are not fulfilled. The Norwegian oil and gas industry learned this the hard way when an employee from an Indian IT company remotely stopped the production on one of Statoil's refineries through a typing error [RT16b]. The incident led to the discovery that over 100 employees from this Indian IT company had access to all of Statoil's computer systems. If Statoil had checked the supplier's access through a security audit as they should, this incident could have been avoided [RT16a].

Security audits have not been prioritized by the DSOs so far. The lack of performed audits may either be due to a lack of resources or because it is not viewed as important. Cybersecurity is unfortunately often given low priority due to cost and the lack of observable results in the absence of incidents. Following up on agreements is resource consuming, but the consequences of not taking cybersecurity seriously

could be severe. The DSOs should therefore perform security audits and check compliance, both internally in the organization and externally towards suppliers. One of the large organizations acknowledged this as an area of improvement, as their biggest concern is not getting the expected resources from suppliers in case of an incident.

5.2 Dependence upon Suppliers

A DSO's dependency upon suppliers is mainly impacted by the amount of resources and expertise it possesses, which inversely correlates with organizational size. As outsourcing is done to acquire expertise, smaller organizations are often more dependent upon suppliers than large organizations. It is, however, worrying that 8 out of 10 organizations in the energy sector admit to being dependent upon suppliers to handle incidents [inf17], and study by the NVE states that the small DSOs are too dependent upon their suppliers [KL18]. This correlates with the findings of this study, which indicate that some small DSOs are not equipped to handle cybersecurity incidents in their PCS by themselves. As the majority of Norwegian DSOs are SMBs, this implies that many DSOs are highly dependent upon suppliers in the handling of incidents. There are a number of reasons why this is problematic, one of them being that it increases the necessity of proper involvement of suppliers in incident management. This issue will be discussed in the next section.

5.2.1 Vulnerability Towards Simultaneous Attacks on Multiple DSOs

The dependence upon suppliers is problematic as there are few suppliers in the Norwegian energy sector. This finding was clearly illustrated by both small organizations having the same PCS supplier, and both large organizations having the same monitoring supplier. Having so few suppliers can have a positive impact on the market as these suppliers will probably have extensive knowledge of the sector and legislation due to their deep involvement and large amount of DSO customers. The scarce number of suppliers does however create a sectoral concentration risk. A concentration of suppliers can lead to a resource shortage during extensive incidents. It also means that supplier-specific errors can affect substantial parts of the sector [HHT+17]. Consequently, the Norwegian energy sector may be highly vulnerable to simultaneous successful attacks on multiple DSOs. This vulnerability is to some extent independent of organizational size as they use PCS from the same suppliers. Large organizations may have better defense against attacks, and their 24/7 system monitoring may help them detect attacks quicker, but a vulnerability in the PCS can be exploited nevertheless.

An incident at the large supplier of IT services, Tieto, in 2011 showed the vulnerability a supplier concentration creates in a market [fsobM12]. A technical error at Tieto's systems affected approximately 50 of their customers, and some of them were unable to use their IT systems for several weeks. The incident illustrated that a supplier concentration may lead to a greater number of affected organizations by the same attack, and that the consequences for society can be severe. A supplier concentration thus increases the need for better coordination and collaboration during incidents. The incident also showed that the supplier did not have sufficient resources to help all of its customers, which worsened the consequences for some organizations. A similar situation could occur in the Norwegian energy sector if one of the suppliers were to be attacked. The PCS they deliver could either be attacked through the supplier or directly at the DSOs. Then, the supplier would be incapacitated and the dependent DSOs would struggle without assistance. It is conceivable that if several DSO customers of the same supplier are attacked simultaneously, the attacks will be of the same nature. If so, a solution to the attack at one suffered entity can be migrated to solve the problems at the other DSOs. However, DSOs whose dependence on the supplier is high will likely be impaired until the supplier is able to assist.

With today's amount of attacks on PCS, the suppliers in the energy sector have sufficient capacity to assist their DSO customers. Nonetheless, if several DSOs simultaneously need help from the same suppliers there may not be enough resources to help everyone. When addressed with this issue, none of the participants believed the suppliers would be able to provide sufficient assistance in that scenario. As many of the suppliers are large international companies, they have the ability to allocate resources from other parts of the organization. They may therefore have more resources than it seems. Nevertheless, the interviewed supplier agreed and admitted to not being prepared to handle simultaneous cyberattacks. Based on this, the energy sector is vulnerable to targeted attacks on multiple DSOs at the same time, and will struggle if they are successful.

In case of an attack on multiple DSOs, the small ones will probably not be prioritized. None of the participating DSOs believed it was possible to buy priority, but the supplier contradicted this. Small organizations are not likely to pay for a 24/7 preparedness SLA due to its high cost. Hence, they will not be prioritized in case of an incident as organizations paying for certain response times will be favored by the supplier. The supplier will then prioritize the organizations with the most extensive customer base, with the reasoning of them being more important to society. However, the largest organizations are not necessarily the most important ones. Smaller organizations can deliver energy to vital societal functions, such as hospitals and military bases, even though they have fewer customers than large organizations. Will it therefore be appropriate to prioritize aid solely based on organizational size?

The PST views small organizations in the sector as especially susceptible to attacks due to the less amount of resources dedicated to security. Consequently, they may be easier to attack [66]. They may also be as interesting as large organizations for advanced threat actors who want to map the Norwegian energy infrastructure, since they constitute a significant portion of the sector.

5.2.2 Protection of System Information

The main threat against the energy sector is currently information gathering through espionage by advanced threat actors, according to the PST [65]. Information concerning PCS used by many DSOs can be particularly interesting for that purpose and must therefore be protected. A study conducted by the NVE found lots of energy sensitive information from Norwegian DSOs online [kra19]. Among it, PCS and information such as supplier and model, and pictures revealing security measures and personnel. These findings concerned DSOs of all sizes, which makes them alarming.

Information gathering correlates with one of the large organizations' views on possible threats and according to the PST, it is also aimed at suppliers [65]. SCADA has been proven to be vulnerable in many situations by previous successful attacks [CS17]. A supplier of PCS to many DSOs is, therefore, an attractive target. Still, due to the strict and limited access between the supplier and PCS, it is difficult to attack multiple DSOs through the supplier's systems. Sensitive system information, on the other hand, can be used to enable simultaneous attacks on multiple DSOs. Hence, DSOs and suppliers have a joint responsibility to protect system information as leakages do not only concern their systems, but can also jeopardize large parts of the energy infrastructure. One of the interviewed supplier's large customers had strict requirements for the supplier's network infrastructure. However, the DSO itself could not meet the same requirements within their systems, so the supplier could not verify that sensitive system information was protected throughout the cooperation. As the NSM addresses [Nas20], suppliers should be discreet regarding customer relationships, but this shows that discretion also should be practiced by the DSOs as customers. To protect sensitive information, all involved parties must participate and be accountable.

5.2.3 Continuous Preparedness

Kraftberedskapsforskriften requires DSOs to have a continuous focus on protecting their PCS [oe19b]. The legislation considers it more appropriate to analyze vulnerabilities and consequences, rather than focusing on the probability of the occurrence of an incident. Undetected vulnerabilities are difficult to account for, so risk analyses should map outcomes if systems fail. Any residual risk, risk that remains after

implemented measures, should be mentioned and practiced regularly to achieve continuous preparedness.

Continuous preparedness can be achieved through 24/7 preparedness SLAs with suppliers. The DSOs dependence upon suppliers can become challenging when suppliers are reluctant to provide such SLAs, which applied to the interviewed supplier. According to one of the large DSOs, it concerns the whole sector. The reluctance comes from the significant amount of resources and cost it requires. It is understandable as it may seem unnecessary to have such a high level of preparedness at all times, considering the small amount of cybersecurity incidents. However, when an incident occurs, the expense of a successful attack is high [ABB+12] and the SMBs will be heavily affected. Not to mention that a power outage will result in thousands of people losing many of their necessities in today's society.

5.2.4 Power Imbalance

The small organizations expressed an existing power imbalance between them and the suppliers. It is mainly caused by the high cost of the systems and the large size of the international suppliers. According to a paper published in the *International Journal of Supply and Operations Management*, a power imbalance is one of the factors that deeply influences the development of relationships between companies [EZZ16]. When there is an imbalance, the stronger company can impose unfavorable conditions on the weaker partner. To some degree, this was the case as one of the small DSOs felt that it had to agree to the supplier's requirements instead of it being the other way around. An existing power imbalance was specifically mentioned as a problem for the whole sector by one of the small DSOs. The same opinion was, however, not found in the large organizations, which is probably due to the larger amount of resources they possess.

PCS are expensive and complex systems, which can create a vendor lock for small organizations [HHT+17]. This was supported by the participating supplier saying that small organizations are more loyal customers than large organizations. Vendor locks may lead small DSOs to continue relationships with suppliers, even if they are unsatisfied with the service or the cooperation. This can become a problem if it impairs the management of cybersecurity incidents. As Organization C tended to be happy that an incident is over instead of evaluating it to improve, they may be more likely to stay with a supplier with whom they are not content.

The supplier did not see an uneven power balance between itself and the DSOs. The statement was countered with a suggestion that the power lies with the DSOs, since they pick suppliers based on cost. Also, the limited amount of possible customers for the suppliers means they have to compete for them, which may shift the power balance in favor of the DSOs. It is also possible that there will always be a power

imbalance between organizations of different sizes, so it is important to address this issue to keep it from obstructing good incident management.

Despite the mentioned power imbalance, one of the small and one of the large DSOs, B and D, specifically stated that they are pleased with the communication and cooperation with their suppliers. However, Organization D also said they are not pleased with the contract they have with the PCS supplier and that they want to renegotiate it. This may indicate that small DSOs DSOs may have problems with the power balance when establishing the contact in a vendor lock situation. Yet, when the cooperation starts, they are satisfied with the relationship.

5.2.5 Trust

Even though DSOs are required by law to ensure suppliers' compliance with security requirements [oe19b], it is difficult to ensure that these requirements are met. Expecting all suppliers to prove every detail is impossible and unreasonable. Hence, it may be easy to conclude that there needs to be some degree of trust between the vendor and buyer. It is, however, argued whether trust is an imperative property of a supplier relationship [mne20]. Best practice is to follow the Zero Trust Model, based on the idea of "never trust, always verify", but with scarce total resources this could be a challenge. This model should also be part of the acquisition process, where one conducts a risk analysis instead of trusting the supplier [mne20].

The participating DSOs currently operate on trust in the relationships with suppliers, and they do not verify their security or expertise. One of the small DSOs even trusted the supplier after their request for security documentation was ignored. Draining already scarce resources to verify every little detail of the contract might not be beneficial, but operating a critical infrastructure solely based on trust can also be dangerous. The Statoil incident is an excellent example of what happens if organizations do not keep tabs on suppliers and have too much trust in them [RT16b]. If Norwegian DSOs put too much trust in the suppliers, as some currently do, a similar scenario is unfortunately possible. Thus, a middle ground where the organizations have some trust in the suppliers, but do not trust them blindly, may be the best alternative. For instance trusting the suppliers on non-critical operations, but verify that the most vital operations, e.g. incident management, works as expected. If suppliers do not participate in cybersecurity preparedness exercises, the DSOs can not verify that they can handle incidents as expected.

5.3 Incident Management Plans

The ISO/IEC 27035 standard clearly states that to ensure quick and effective responses to cybersecurity incidents, all external parties for support should have access to

the documented procedures related to crisis management [fSI16]. If suppliers are not informed of the incident management plans, it is difficult to create procedures that conform to those of the DSOs. This will in turn make the collaboration during incidents less smooth. An important part of incident response is the coordination of work and making collaborative decisions. Cybersecurity incidents in PCS will likely imply collaboration between personnel from different parts of the organization, and as the DSOs are dependent upon suppliers, they will also be likely participants.

There are two types of coordination: predefined and situated [LT99]. Situated coordination occurs when a situation, like a cybersecurity incident, is unanticipated or unknown. Predefined coordination, on the other hand, takes place prior to the coordination situation. It is typically developed from the establishment of written or unwritten rules, procedures, routines and roles. Hence, it resembles the incident response scheme of the ISO/IEC 27035 standard [fSI16]. To achieve predefined coordination, it is necessary to involve and share incident management plans and procedures with suppliers. Contrary to this, the results of this study show that there is little sharing of plans and procedures with suppliers prior to incidents. Research conducted in the petroleum sector [JEAL09] got similar results; suppliers were not adequately involved in incident planning, even though the operators in many cases would depend on them during incident management.

For external connections to be useful during incident management, it is necessary to make sure these connections are established beforehand, according to ISO [fSI16]. Points of contact should be defined between the organizations, including how and when to communicate. The standard recommends detailed and extensive plans, but the large amount of written material this produces is also one of its limitations. The incident management plans of the participating DSOs mention less about supplier involvement than what can be expected considering their dependence upon them. The lack of correlation between organizational size and level of detail may indicate that this is a shortcoming for the whole sector. There was little information regarding when and how suppliers shall be involved and what they can contribute with, and some only had the contact information. One of the large organizations argued that a mapping of resources is the most valuable asset during an incident. It may however be inadequate information for inexperienced personnel, which can lead to uncertainty and confusion. As recommended by several standards and guidelines for incident management, all employees must know whom to contact for different expertise, with clear distributions of responsibility. If the plans are straightforward and easily understandable for all personnel, it will enhance the robustness of the incident management process against illness and changes in the workforce.

The ICT security coordinator is a natural point of contact for suppliers regarding incident management due to the main cybersecurity responsibility. This main point

of contact was, to some degree, followed by the DSOs, as all new incidents first were appointed to the coordinator. Then they were delegated to other employees based on type or systems, which must not obscure the point of contact for suppliers. In many ways, the coordinator is responsible for involving suppliers in the right manner and cooperate in such a way that all parties can work toward secure systems. The small DSOs and the cooperation company expressed a desire for a joint ICT security coordinator role for several DSOs. This is not allowed by the NVE, but it could free resources and increase the cybersecurity competence of the coordinator. On the other hand, it would remove the coordination role and point of contact and would mean that one person would be responsible for a lot of suppliers at many DSOs. This would in itself pose a risk against illness or other harm as there would only be one key personnel.

The lack of plans on supplier involvement can, to some degree, be explained by the lack of experienced attacks against PCS and the DSOs' views on their attractiveness as targets. Nevertheless, the current threat landscape shows that attacks on DSOs are likely. Given these threats, there is no doubt that perpetrators are progressing on complex and sophisticated attacks. The successful attack on a Norwegian DSO's PCS and the two ransomware attacks experienced first-hand by the participating DSOs, should also generate awareness.

5.4 During Incidents

When the competence for the vital PCS lies with suppliers, the involvement of suppliers during incidents becomes essential. There was a lack of conformity between the DSOs' plans and predicted actions. However, it is not surprising as there were few instructions regarding suppliers in the plans. The deviations were especially related to the small DSOs as they would be quicker than the large ones to contact suppliers in the event of an incident. Hence, they should include supplier involvement to a greater extent in their plans. Although it will never be possible to plan for all incidents, organizations should strive to act according to the incident management scheme as planning increases efficiency, facilitates coordination and gives direction [mne20].

5.4.1 Responsibility when Outsourcing

By outsourcing services to suppliers, DSOs may lose the sense of ownership and responsibility [fC19]. Still, outsourcing of either detection or assessment and response does not mean an outsourcing of responsibility for cybersecurity. Outsourcing of incident management means to trust the supplier's expertise and decisions, but not blindly. Both small DSOs said the suppliers make decisions regarding incident handling and that they trust the suppliers to make the right decisions. They have

been satisfied with the supplier's decisions so far, but they have not experienced any major incidents in their PCS. The DSO must also possess the knowledge of when and with what the supplier can assist, which creates the need for clear definitions of responsibility. The allocation of responsibility must regularly be followed up to ensure that both the DSO and supplier know what their duties are. This is necessary both to handle the incident in the best possible way and to guarantee that no tasks fall in between both parties. Another concern when the supplier handles incidents, is that the supplier only knows its own system, while it is the DSO's responsibility to have an overview of the whole system infrastructure. This increases the need for communication.

5.4.2 Communication

Regardless of existing written plans and procedures, there will be a need for coordination and improvisation during incidents [BM16]. Hence, good communication and collaboration with suppliers is crucial during incident management. According to a paper published in the journal *Information Management & Computer Security*, incident management is collaborative in nature [WMHB10]. Customers and suppliers often handle different parts of the incident [HT13], and it is therefore not without reason that communication is listed as one of the five key skills required for diagnostic work by Werlinger et al. [WMHB10]. Thus, the collaboration with suppliers must be sufficient to handle cybersecurity incidents quickly and satisfyingly, due to the usual time-sensitivity of cyberattacks.

Two of the DSOs and the supplier claimed to be very satisfied with the collaboration, but one can question whether they have enough experience with it to have grounds for such statements. Neither the supplier nor any of the DSOs had experienced any cybersecurity incidents in their PCS. Also, most of the organizations had not involved suppliers in their exercises. This means that they had not tested the collaboration at the adequate stress level needed with a mix of predefined and situated coordination efforts [LT99]. Stating that collaboration is good could then be an exaggeration. This is problematic as they are less likely to change and improve the collaboration when they believe it is well-functioning. Unfortunately, they will not discover the real quality of the collaboration until an incident occurs, with an outcome that could be profoundly affected by the collaboration.

There are likely cultural differences between the large international suppliers and the small and medium-sized DSOs, which can lead to challenges in communication and incident handling. When organizational cultures are similar, organizations are expected to interact more easily and with better results than if there are cultural differences, according to Knoben and Oerlemans [KO06]. This is due to the common interpretations and routines that allow the organizations to give meaning to actions

without further thought. There will be a smoother collaboration without having to make implicit knowledge and actions explicit. While small organizations may have fluid roles and are more likely to handle each incident differently, large organizations usually have more protocols and defined roles. Such differences can affect the collaboration negatively if they go undetected. This suggests that fundamentally different organizations have to practice communication more than similar organizations, to counteract their cultural differences. However, the participating supplier gave the impression of being very familiar with the sector and should therefore know the peculiarities of small Norwegian DSOs and their actions, which can help reduce the cultural gap between the organizations.

5.4.3 Involving Several Suppliers

The participating DSOs involve suppliers in the handling of incidents. Yet, some incidents may involve more than one supplier, which introduces new challenges. According to Werlinger et al. [WMHB10], it complicates the collaboration further, hence increasing the need for better communication. When several parties are involved, it is important to maintain a balance in reporting. All involved parties have to get the necessary information, but at the same time, unnecessary reporting will occupy resources. The DSOs must therefore have well-established routines for reporting of adequate information to relevant suppliers through proper channels.

Other challenges that emerge from involving several suppliers in incident handling are related to communication and coordination of their roles. What happens if one supplier monitors the system while another handles incidents? According to the participants, several suppliers have not cooperated when responding to threats or incidents. Also, if several suppliers are involved, the DSO will be the coordinator. This implies that the monitoring supplier will first have to contact the DSO, which will then contact the supplier that handles the incident. This situation requires precise coordination and correct transfer of information. A counterargument to this challenge is that of the interviewed DSOs, only the large ones use a monitoring service, and they are more capable of handling incidents internally. In some cases it will also be the monitoring supplier that will assist the DSO, which simplifies the situation. Lastly, for one of the small DSOs, it is the PCS supplier that, together with the DSO, is responsible for detecting and handling incidents. Thus, there is currently mainly collaboration between the DSO and one supplier during cybersecurity incidents.

The participating organizations were divided in whether it would be beneficial for suppliers to cooperate during incident response. Some of them claimed that the PCS are isolated with such few suppliers that it is not relevant. However, in today's complex systems, it is unlikely that PCS will be completely isolated. Hence, it will probably be necessary to contact other suppliers of interfacing components, such as

firewalls, during cybersecurity incidents.

5.5 Continuous Evaluation and Improvement

Incident management is a cyclic process that should be under continuous improvement through exercises and learning [fSI16]. The conduction of exercises and evaluation of exercises and incidents is an essential part of the improvement, as pointed out by several standards and guidelines in Section 2.6. The activities provide a retrospect of how processes have been conducted to further develop existing practises and it is beneficial if all relevant parties participate, both internal and external [KL18, FHT13, Nas20].

5.5.1 Cybersecurity Preparedness Exercises

The results from this study reveal that there are few exercises regarding PCS in general and almost no involvement of suppliers in them. Only one of the participating DSOs had involved suppliers and the interviewed supplier had not been invited to participate by any of its numerous DSO customers. This indicates that there are a lot of Norwegian DSOs that do not involve suppliers in exercises. Not involving them contradicts the recommendations by Floodeen et al. of participation by all parties who play a role during incidents [FHT13]. One of the DSOs had not even tested the communication channel to the supplier, which illustrates the importance of involving suppliers in exercises. In a worst case scenario, this could lead to them not getting help, or at least a delayed assistance, causing an unnecessary escalation of the incident. So why are not Norwegian DSOs involving suppliers in their exercises?

DSOs' Reasoning

The main reason for the lack of exercises in the PCS was resources, according to the participants. As explained in Section 2.1.1, PCS exist in areas with logical air gaps and strict requirements of availability and safety. This means that the conduction of exercises requires more planning and resources. It also makes it more difficult to conduct the exercises in an environment that is as close as possible to real-life, which was found to be important by Gåsland [Gå14]. Due to the criticality of the energy supply, it is also crucial to conduct frequent exercises without unnecessarily disturbing operations. Although tabletop exercises do not allow for practical demonstration [BM16], they may be a good alternative for PCS as they do not disturb system operations. Another option is to use joint test platforms that unite suppliers and DSOs, to limit the difficulties of conducting exercises in restricted systems. This is currently being studied at NTNU where a cyber range for the electrical energy sector is under development [Mik20]. Its goal is to facilitate training of incident routines and protocols for employees in the industry. If such platforms can imitate

PCS and involve suppliers, it will be a good way to perform exercises in PCS. The lack of experienced cybersecurity incidents may be another reason for the lack of focus and priority on PCS exercises [BMH16]. However, as explained in Section 5.3, they should be aware of the threats at this point in time.

The reason the DSOs gave for the lack of supplier involvement in exercises was the same as for the lack of exercises in PCS; resources. It requires more planning and resources to introduce other parties in the process. Nevertheless, this reasoning should be compared to the effect of the exercises without the participation of essential parties. Without suppliers, the scenarios will not be realistic and they will not be able to test the collaboration and develop a mutual understanding and a shared mental model [FHT13]. The large amount of trust that the DSOs have in the suppliers may also contribute to the little involvement in exercises as it leads them to believe that the suppliers can handle cybersecurity incidents. However, the lack of previously experienced incidents and involvement in exercises means that the DSOs base their belief solely on reputation and documentation.

There was a collective agreement among the participating DSOs that exercises would increase the collaboration and understanding between the involved parties. As a result, exercises will improve incident management overall. This shows an understanding of best practice, but a lack of execution abilities. Gåsland's study of preparedness exercises initiated by the NVE [Gå14] discovered similar findings. There was a positive attitude toward participating in exercises and an understanding of the importance of collaboration in problem-solving processes, such as cybersecurity incident handling. However, exercises must compete with daily tasks for prioritizing, which explains the lack of execution.

Supplier's Perspective

Contrary to all other opinions found during this study; from DSOs, the NVE and academia [Nas20, FHT13, KL18], the supplier did not see the point of participating in exercises, despite the DSOs' dependence upon them to handle cybersecurity incidents. The supplier's opinion is problematic, and it may also influence the opinions of the DSOs. Especially the DSOs that view them as experts and feel inferior to them. It should however be noted that this is the opinion of only one of the largest suppliers to the Norwegian energy market, and not necessarily all of them. Still, it shows that the DSOs can not rely on suppliers to improve incident management through exercises. They have to initiate participation in exercises themselves, and it should probably be stated in the contract. One of the small DSOs expressed a desire for including it when they renegotiate the contract with Supplier S.

In systems where several suppliers are present, it may also be relevant to include more than one supplier in the same exercise. In the case of a cybersecurity incident,

the interviewed supplier admitted that suppliers will likely be reluctant to take the blame and will probably point at each other. It requires more coordination, but if there are dependencies in the systems or incident handling, the same argument for involving one supplier in the exercise applies; there is no point in practicing unless all relevant parties are involved [KL18].

Do suppliers have anything to gain from participating in exercises? Is that why they are reluctant to participate? Exercises consume resources from other parts of their services and may at first sight not look beneficial. They may have less to gain from the participation than the DSOs, since it is the DSOs that are responsible for the outcome of incidents regardless of who handles them [fC19]. Nevertheless, suppliers will benefit from a well-functioning incident handling, since unsatisfied or disappointed customers will, likely, be more willing to terminate the collaboration. Satisfied customers are also desirable for suppliers as there are only a limited amount of possible customers in the Norwegian market. Effective incident handling will also improve their reputation, which has proven itself to be important in this sector. Therefore, the suppliers will gain from participating in exercises. Moreover, as conducted research show that their participation is necessary to improve incident management, they should participate regardless of own gain due to the criticality of the infrastructure. It will be most beneficial if suppliers see the advantages of involvement as they will likely be more devoted to the exercise. Yet, in the end, "the customer is always right" as the DSOs are ultimately responsible for the energy supply, and they should therefore set requirements to the suppliers regarding participation.

5.5.2 Learning from Exercises and Incidents

Scholl and Mangold [SM11] state that attending to small security events can prevent major security incidents. Applying the same routines for all incidents will allow for real life minor incidents to function as exercises for more severe incidents as they occur in the actual environment that operates the critical infrastructure, which is essential [Gå14]. Minor incidents will therefore be a good way to test and improve the collaboration with suppliers. This creates the need for defining cybersecurity incidents with suppliers, since some events are insignificant and should not enable the incident management process. Following the procedures for supplier involvement during minor incidents may not be a realistic option for some DSOs. Large DSOs will for instance not contact suppliers unless they have to, which will probably be the case for minor incidents. Contacting suppliers will test the involvement process, but may cause unnecessary fuzz. However, the same argument can be used regarding exercises, but exercises are still considered necessary.

The learning phase after exercises and incidents is essential to improve incident management [Nas20]. It is an obstacle to learning if exercises are not used as a means

of making improvements afterward [Gå14]. The learning phase can, for instance, provide increased interdisciplinary learning across departments within the same organization and improve collaboration with suppliers. PCS operators and managers are given the opportunity to exchange methods and experiences by looking at how the operators in the administrative network involve and cooperate with suppliers. Nevertheless, Bartnes et al. found a lack of prioritization among Norwegian DSOs for incident response training and post-incident evaluations [BMH16]. However, the findings of this study contradict the results of Bartnes et al. as it was found that all, except one small DSO, perform post-evaluations of incidents. Bartnes et al. stated that one explanation was a lower risk perception among the organizations than it should be from the level of current threats. On the other hand, among the participating DSOs of this study, the risk perception was found to have been improved overall, although the small DSOs still do not view themselves as attractive targets for targeted attacks. This correlates with the research of Rhee et al., who demonstrated that management often underestimate their organization's vulnerability and overestimate their ability to control security threats [RRK12].

Although there was a broad agreement between all participating parties regarding the importance of learning from exercises and incidents, there were differences in the extent of supplier involvement. They span from two DSOs viewing it as was both important and natural, to one doing it occasionally with significant changes, to the last one lacking routines. Similar results were found in the petroleum sector, where suppliers and service providers were not adequately involved in the learning after incidents [JEAL09]. If suppliers are not involved, the DSO will only be able to see one point of view, and necessary enhancements may be lost. The authors acknowledge that not every part of the reviewing process will be of interest to the suppliers. However, as incident management is a collaborative activity [WMHB10], involving suppliers enables sharing of understandings and expertise. In a sector where trained personnel is difficult to acquire [LTJ11], it is vital to collectively increase the knowledge within the community. Suppliers should review changes in incident management plans, and involvement will prove most beneficial if happening at a low threshold. Not only will it better prepare DSOs for future incidents, but it will give the supplier insight into their systems from another point of view, thereby indirectly increasing their ability to assist other DSO customers.

The supplier also expressed a clear desire for involvement in the learning phase. One can question how they can contribute when they do not want to participate in exercises, but after incidents, they should participate. Nevertheless, this study found more willingness for involvement in lessons learnt than in exercises from both the DSOs and the supplier. It is also currently being done to a higher degree, despite the legislation's lack of mention of supplier involvement in post-evaluation [oe19b]. Suppliers are also informed of changes made to the incident management plans

that will affect them, regardless of their involvement in the learning phase, but that should be considered a minimum. Considering the absence of cybersecurity incidents in the PCS and the lack of supplier involvement in exercises, there have not been many possible improvements to the collaboration with suppliers. It might be tempting to neglect to conduct a thorough analysis retrospectively after an incident when everybody is happy that the incident was handled without a severe outcome, as one of the small DSOs admitted. However, such satisfaction in the absence of incidents is not recommended. Instead, the attitude should emphasize a constant room for improvement, even if things worked out in the end. By keeping in mind that professional perpetrators might be a few steps ahead, as the NVE stated in the interview, DSOs should strive to conduct thorough analyses of both exercises and incidents on a continuous basis. In order to complete the incident management process, it is essential to address the learning phase well by always striving for constant learning and improvement.

RQ1.1: What are possible improvements to the collaboration with suppliers on cybersecurity incident management?

Possible improvements to the involvement of suppliers have emerged from the findings of this study. They can be divided into two main categories; more involvement in preparatory activities and utilizing sector collaboration to enhance the DSOs' resources.

5.6 More Involvement In Preparatory Activities

A possible improvement is to increase the involvement of suppliers in the preparatory parts of the incident management process, which mainly includes plans, exercises and learning. More involvement in those areas will improve the preparedness for incidents and the collaboration with suppliers, which will in turn improve the incident management overall.

Plans: Considering the degree of supplier involvement during incidents, the focus on suppliers in DSOs' plans for incident management should increase. A middle ground between their currently limited plans and what ISO recommends may be the best solution as both people and situations differ. To further improve the collaboration, DSOs should give suppliers increased insight into the established plans to make it possible to create conforming procedures in accordance with the guidelines for best practice.

Exercises: Involvement of suppliers in cybersecurity preparedness exercises seems to be one of the biggest potential enhancements to current practice. To achieve increased involvement there is a need for a cultural change both from DSOs and suppliers towards prioritizing exercises. DSOs should demand participation in the contracts. The best alternative is, however, if there is an increased willingness from suppliers regarding participation. To cause less disruption from the supplier's daily tasks and preparedness, several small organizations that use the same supplier may conduct joint exercises. DSOs should also practice the same routines for all incidents.

Lessons Learnt: The DSOs that do not involve suppliers in lessons learnt will benefit from strengthening their involvement of suppliers as the impact it has on incident management and collaboration is widely acknowledged. The wide agreement among both DSOs and suppliers regarding the benefits of involving suppliers should make it easier to establish routines for lessons learnt.

5.7 Enhancing Resources by Utilizing Sector Collaboration

Many of the issues discussed in this chapter stem from the DSOs' lack of resources. Enhancing and optimizing the use of the resources the organizations already have and increasing their knowledge regarding the systems and cybersecurity incident management, will reduce the issues and contribute to better involvement of suppliers. Utilizing sector collaboration will increase the resources of the DSOs and thus possibly improve the collaboration with suppliers on incident management. An enhancement of resources will also improve the overall security of the sector.

The energy sector differs from many other sectors in that there is a natural monopoly among the DSOs. They are competitors in some ways, but not like in other sectors, due to their geographical distribution. This opens up for collaboration between the organizations in a way that would probably not have been possible if they were competing for the same customers. This opportunity for collaboration is taken advantage of to some degree by the sector, with cooperation between small DSOs, the sector's own emergency response team, KraftCERT, and sector meetings. There is a wide agreement that the collaboration improves the security in the sector, but the improvement may be biggest for smaller organizations as it gives them a wider academic community and operational security.

The energy sector can learn from the financial sector regarding both sector collaboration and how security incidents are handled. As the financial sector is highly dependent upon the trust of its customers, cybersecurity and privacy must be of top priority. A risk and vulnerability analysis conducted by The Financial Supervisory Authority of Norway (Finanstilsynet), contains some of the same challenges that are covered in this thesis [Fin20]. In particular, it highlights that internal auditing and ICT competence management should be included in the organization's overall management model. TIBER[1], a framework that focuses on and improves cybersecurity is also mentioned in the report. A similar solution for the energy sector where attacks are simulated and preparedness is tested for PCS would have a positive impact on the sector's security. The implementation of such a solution must be considered and decided by the sector itself in collaboration with the authorities.

Increased System Knowledge: Acquiring necessary IT and OT expertise is a problem, not only for this sector, but in Norway overall. There are few graduates with expertise in both IT and OT, and it is difficult to attract them towards work in rural areas where many of the small DSOs are. DSOs should therefore focus on building their in-house expertise through better facilitation for the collaboration between IT and OT personnel. One way to increase this expertise and system knowledge is through sector collaboration. Small organizations can exchange valuable knowledge

[1] https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

and share resources, and large organizations, with their larger academic communities, can help small ones enhance their expertise.

Reduced Vulnerability Towards Multiple Attacks: Increased expertise and system knowledge at the DSOs will reduce the sector's vulnerability towards simultaneous attacks on multiple DSOs as it will reduce the DSOs' dependence on suppliers. Improved collaboration with suppliers through more involvement in preparatory exercises will also reduce this vulnerability as suppliers can assist more efficiently.

Better Procurement Skills: Sector collaboration can help the DSOs become better procurers. Increased collaboration between SMBs will help them become more similar to large organizations when working with suppliers. Hence, they can get the price reduction due to quanta that large organizations get and better contracts due to shared requirements. Collaboration across organizational size is also a possibility. The NVE has found a desire for a national collaboration regarding outsourcing [KL18]. It will put less pressure on resource-scarce businesses if large DSOs can help small ones become better procurers by sharing their experience and expertise. With the large DSOs' lists of requirements, small organizations will be able to set correct requirements to suppliers.

Reduced Power Imbalance: It is conceivable that a power imbalance always will exist in a partnership between organizations of different sizes and that one has to find ways to reduce that imbalance. Increased system knowledge and better procurement skills at the DSOs through sector collaboration will contribute to evening out the imbalance. If the DSOs possess expertise and good procurement skills, the power imbalance may even be negligible due to the small organizations being the customers.

Enhanced Trust: The well-known proverb "Trust, but verify" clearly recommends that DSOs should conduct the security audits they have the right to, which will be easier to prioritize with more available resources and expertise. By performing security audits, the trust they have in suppliers will be strengthened, which will in turn improve the collaboration and incident management. Checking suppliers' compliance with contracts will also ensure that the DSOs get what they are promised and is thus important for the security of the whole critical infrastructure.

Improved Security: Sector collaboration can also contribute to better overall security in the sector. As ISA/IEC 62443 is perceived as too general and comprehensive for any sector, a suggestion is to advise the industry to unite and develop a recommended practice specifically for the electrical energy sector. DNV-GL RP-

G108[2] is an example of this, which is customized for the oil industry using ISA/IEC 62443. When the authors addressed the publisher of the report, a confirmation that they are preparing a guidance document on cybersecurity for the electrical energy sector together with the Nordic TSOs was received.

[2]http://rules.dnvgl.com/docs/pdf/DNVGL/RP/2017-09/DNVGL-RP-G108.pdf

Recommendations

This two-part section first presents the authors' recommendations for a more appropriate involvement of suppliers in incident management, and then presents some sectoral changes that should be evaluated by the authorities.

5.8 For DSOs

This chapter has discussed current practice for involvement of suppliers in incident management, focused on issues, and suggested possible improvements to the collaboration. However, it is important to note that some practices are already good and should be preserved while others should be strengthened. The organizations in the sector have a very valuable positive attitude toward collaboration and helping each other. They are also forward-leaning and interested in improving their practices. Currently, the sector collaboration is mainly utilized by SMBs, but should be further enhanced, also across organizational sizes. Furthermore, the large organizations are good procurers, have a competent academic community and are capable of handling many incidents themselves. These are qualities that should be preserved and increased to enhance cybersecurity and incident management.

Based on the findings of this study and the discussion of the research questions, the authors have developed the following measures and recommend that they should be evaluated by DSOs to improve the involvement of suppliers. Table 5.1 and Table 5.2 shows the connection between the recommendations and the phases of the ISO/IEC 27035 standard to make them easier to implement. The measures are presented in the left column, while their objectives are in the right column. However, the proposed measures will vary in relevance and difficulty of implementation for different DSOs as the DSOs are divergent in resources and expertise. Also, some of the measures are already being conducted by some organizations and will, therefore, be irrelevant or not possible to improve.

Measure	Objective
Phase 1: Plan and Prepare	
1.1 Clearly define cybersecurity incidents with supplier(s)	Ensure common understanding and initialization of incident handling
1.2 Acknowledge all DSOs' attractiveness toward attackers and map valuable consumer assets	Enhance cybersecurity awareness and incident management processes
1.3 Increase understanding of IT/OT and current legislation	Improve incident management and prevent avoidable incidents
1.4 Increase system knowledge regarding PCS and incident handling	Increase efficiency in understanding and reacting to incidents, and decrease dependence upon suppliers
1.5 Increase the importance and understanding of the responsibilities of the security coordinator role, and dedicate more resources to cybersecurity	Improve cybersecurity and incident management by having a stronger coordinator role
1.6 Improve procurement skills and procedures	Procure appropriate systems and services, set explicit requirements to suppliers and thus reduce power imbalance
1.7 Perform security audits and access control	Ensure compliance with cybersecurity requirements throughout the outsourcing process
1.8 Establish appropriate routines for the sharing of plans with suppliers	Provide ability for conformed plans and procedures with suppliers and possibility for feedback, and improve collaboration during incidents
1.9 Increase the detail of plans regarding the involvement of suppliers during incidents and their responsibilities	Ensure proper and efficient involvement of suppliers during incidents
1.10 Supplier participation in exercises concerning PCS	Test collaboration and incident handling
1.11 Involve several suppliers in the same exercises if applicable	Effectively coordinate and react to incidents
1.12 Increase sector collaboration	Utilize available knowledge and information in the sector and increase the sector's robustness

Table 5.1: [Phase 1] Recommended measures structured by the ISO/IEC 27035 standard.

Measure	Objective
Phase 2: Detection and Reporting	
2.1 Establish effective communication and reporting procedures between DSO and supplier(s)	Increase efficiency and accuracy in information flow between relevant parties
Phase 3: Assessment and Decision	
3.1 Establish clear responsibilities between DSO and supplier(s)	Increase efficiency in decision of responses and ensure coverage of all tasks
Phase 4: Responses	
4.1 Increase collaboration between internal IT and OT departments, and seek inspiration from other sectors	Utilize and improve internal resources and knowledge to more effectively respond to incidents
4.2 Standardize response procedures and lower the threshold for applicability	Use minor incidents to test incident management processes
Phase 5: Lessons Learnt	
5.1 Establish routines and procedures for the evaluation of exercises and incidents	Ensure improvement of the incident management process after exercises and incidents
5.2 Involve suppliers in the evaluation of exercises and incidents	Get supplier's input in the evaluation process to improve collaboration

Table 5.2: [Phase 2 to Phase 5] Recommended measures structured by the ISO/IEC 27035 standard.

5.9 For Sectoral Changes

The scope of this project was the involvement of suppliers and cybersecurity incident management within PCS. Despite this, the authors came across aspects that are unrelated to changes DSOs can apply and that need to be analyzed from other perspectives than cybersecurity, such as socio-economic aspects. They may also need an increased willingness from the authorities.

It should be discussed whether the criticality of the energy infrastructure calls for the requirement of all organizations being able to handle incidents without the help of suppliers. As large organizations are more capable of handling incidents themselves than SMBs, an option is to move towards fewer, but larger DSOs. This has also been

the trend in recent years [Bre18]. In 2019, the director of the NVE and the Minister of Petroleum and Energy stated that merging DSOs into larger organizations will reduce costs and improve the robustness for continuity of the energy supply [sam19]. Merging has, however, faced high resistance from the SMBs in the sector, so an alternative approach is increased collaboration between DSOs, which is currently being done to some degree.

Realistically, there will probably never be total independence from suppliers in the handling of incidents. From a societal perspective considering resources, expertise and cost, outsourcing to suppliers is beneficial both for DSOs and society. The main benefit of outsourcing is the pool of resources that suppliers bring. From specialized knowledge to the larger amount of available resources, suppliers provide elements that DSOs probably neither can afford nor obtain by themselves.

From a cybersecurity perspective, all Norwegian DSOs should have 24/7 system monitoring and preparedness agreements with suppliers, regardless of size. Even though small organizations are believed to be less attractive targets and will be given low priority in the case of limited supplier resources, they can still be of interest for advanced threat actors as previously discussed. Evaluations related to whether 24-hour SLAs should be required should therefore be made by the authorities in light of the likelihood of an attack and its subsequent consequences. The basis for this comes from attacks against other countries' energy supplies combined with the last threat intelligence from the PST. Continuous preparedness and system monitoring do, however, require a lot of resources from the supplier and high cost from the DSO, which also must be taken into account.

The security of the energy sector could benefit from a more explicit legislation [oe19b] regarding the involvement of suppliers in incident management. *Kraftberedskapsforskriften* only states that DSOs shall implement measures to handle incidents and protect the systems. It does not specify whether they should be able to do it themselves. Taken into account that the representative from the NVE does not believe DSOs will get sufficient help from suppliers in case of an extensive incident and this study's findings that DSOs are dependent upon suppliers to handle incidents, it may be necessary to specify the legislation further. Another alternative is to set explicit demands to the suppliers regarding, for instance, allocated resources, response time and exercises, to guarantee the necessary assistance during an incident. The authorities can also evaluate solutions that will increase the number of suppliers to reduce the supplier concentration in the market.

The legislation is also somewhat unclear regarding the verification of compliance. It is stated that DSOs must have the right to perform security audits and that they must implement routines for inspection, but they are only required to perform audits

”if necessary”. It is however hard to know the meaning of necessary unless an incident happens, like at Statoil, but then the damage will already be a fact. It will be easier for DSOs to prioritize security audits if it is required by the legislation.

Lastly, there is little mention of the involvement of suppliers in *Kraftberedskaps-forskriften* concerning exercises and the evaluation of incidents. The representative from the NVE found it beneficial for DSOs to involve suppliers in exercises, but said they are not planning on including requirements or recommendations regarding this topic in the legislation. If the NVE decided to include it, it would send a signal to the sector that this is necessary. Hence, it may enhance the involvement of suppliers in exercises. Also, there is no mention of external parties during the evaluation of incidents. The lack of specification puts more responsibility on the DSOs to understand how they can evaluate incidents in such a way that it improves incident management and whether or not they should include suppliers to achieve that. By specifying that relevant parties should be included, it will be easier for DSOs to prioritize it. As of now, DSOs are in many ways saving costs on not prioritizing involvement of suppliers and being poorly prepared. Unless an incident occurs as the cost of a cybersecurity incident probably will exceed the cost of proper preparation. By changing the legislation, all DSOs must prioritize involvement and are thereby obliged to increase preparedness, removing the cost-saving element of not involving suppliers. Thus, there are many changes that would improve security and the incident management of the DSOs that are beyond what DSOs can do, and should be evaluated by the authorities.

Chapter 6
Conclusion and Future Work

This project has studied the involvement of suppliers in Norwegian DSOs' cybersecurity incident management, with primary focus on their PCS. Conducted as a qualitative case study with interviews as the main source of information, the study has given insight into a unique sector characterized by a high degree of digitalization. Current practice for incident management was identified and analyzed using the phases of the ISO/IEC 27035 standard. Furthermore, a comparison of current practices and relevant standards and guidelines was conducted, which resulted in recommendations for potential improvements.

Considering the high dependence upon suppliers in PCS, a relatively low supplier involvement among the DSOs was found in preparatory activities, exercises and evaluation of incidents. Through an increasing involvement in the development of PCS as well as provision of assistance and IRT during cybersecurity incidents, suppliers have developed a more prominent position in the operations and distribution of electrical energy. However, there are noticeable resource-based differences between large and small DSOs regarding their expertise in systems and cybersecurity, procurement skills and procedures for incident management. Thus, smaller DSOs tend to be more dependent upon suppliers - even to the extent that could be characterized as unhealthy.

From a cybersecurity perspective, indications were found that some small DSOs are not prepared to handle cybersecurity incidents in PCS. Hence, they may not be properly equipped to handle the responsibility they have been given to uphold the Norwegian electrical energy supply. There may be several reasons for this, including financial limitations and limited understanding of responsibility and risk, and the study material is not sufficient to determine whether it is caused by inability or neglect. The large DSOs seem to be in better shape regarding cybersecurity and incident management. They possess good procurement skills and can handle a diversity of incidents in the PCS without the assistance from suppliers. Large Norwegian DSOs are even in the lead internationally by adopting new technologies and proactively

working towards new development, according to the interviewed supplier.

Based on the continuously evolving threat landscape and society's increasing dependence and demand for an uninterrupted supply of electrical energy, there is a need for an improvement in cybersecurity incident management. The high degree of supplier dependence combined with the low number of suppliers makes the Norwegian energy sector susceptible to simultaneous cyberattacks on multiple DSOs.

The authors have combined the already existing research within the field of cybersecurity incident management with good practice guidelines for the involvement of suppliers, to develop an approach that could be applicable to entities managing critical infrastructure using both IT and OT systems. Thus, the insight obtained through this study has resulted in a set of recommendations for potential improvements on how to involve suppliers, formulated as a guide following the five phases of incident management with different measures and their corresponding objectives. The overall recommendation is that the organizations in the energy sector could improve cybersecurity incident management by increasing the suppliers' involvement in preparatory exercises, and on a longer term reduce dependence upon suppliers by utilizing the sector's willingness and unique ability to collaborate and thus enhance the resources of small DSOs. The ultimate goal of this project would be to improve the cybersecurity and robustness of this critical energy infrastructure. Furthermore, the authors suggest further development of current legislation regarding supplier involvement and merging of smaller organizations. These suggestions of sectoral changes are addressed to the authorities and other aspects than cybersecurity must be taken into account.

As there has been little research on the involvement of suppliers in incident management and the inclusion of suppliers in standards and guidelines is incomplete, the authors are of the opinion that it would be valuable to continue the research on how suppliers should be involved in incident management in critical infrastructures. As this study was restricted to a small selection of participating organizations, the generalizability of the findings is limited. Thus, it would be interesting to supplement this study with a quantitative study to identify whether the issues discussed are evident in the majority of the Norwegian DSOs. Involving other personnel who work specifically with PCS and have first-hand experience with responses would also be interesting. A similar, but more extensive, qualitative study with a larger number of participating organizations can reveal new aspects of current practice, thus leading to improved recommendations.

References

[AAF+08] P. G. Almklov, S. Antonsen, J. Fenstad, E. Jacobsen, A. Nybø, and G. Kjølle. Fra forvaltning til forretning - restrukturering av norske nettselskaper og konsekvenser for samfunnssikkerhet. Technical report, Norsk Forskningsråd, 2008. (In Norwegian).

[ABAH+20] A. H. Al-Badi, R. Ahshan, N. Hosseinzadeh, R. Ghorbani, and E. Hossain. Survey of smart grid concepts and technological demonstrations worldwide emphasizing on the oman perspective. *Applied System Innovation*, 3(1), 2020.

[ABB+12] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. Eeten, M. Levi, T. Moore, and S. Savage. Measuring the cost of cybercrime. 11th Workshop on the Economics of Information Security, 2012.

[AGG+16] O. Andreeva, S. Gordeychik, G. Gritsai, O. Kochetova, E. Potseluevskaya, S. I. Sidorov, and A. A. Timorin. INDUSTRIAL CONTROL SYSTEMS AND THEIR ONLINE AVAILABILITY. Technical report, Kaspersky Lab, 2016.

[All20] ISA Global Cybersecurity Alliance. Quick start guide: An overview of isa/iec 62443 standards. Technical report, The International Society of Automation (ISA), 2020.

[Bab18] M. Babikir. Convergence of it and ot in energy and manufacturing. *Digitalist Magazine*, 11, 2018.

[BCGL17] N. Bartol, M. Coden, D. Gee, and C. Lawton. Ensuring cybersecurity in the electric utility industry. The Boston Consulting Group (BCG), 2017.

[BM16] M. Bartnes and N. B. Moe. Challenges in it security preparedness exercises: A case study. *Computers & Security*, 67:280–290, 2016.

[BMH16] M. Bartnes, N. B. Moe, and P. E. Heegaard. The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, 61:32–45, 2016.

[Bre18] A. Brenna. Hvor mange nettselskaper er det i norge? https://enerwe.no/hvor-mange-nettselskaper-er-det-i-norge/165909, 2018. Accessed: 2020-02-20 (In Norwegian).

[Bre19] A. Brenna. Norge importerte strøm i hver femte time i fjor. https://enerwe.no/norge-importerte-strom-i-hver-femte-time-i-fjor/152323, 2019. Accessed: 2020-01-20 (In Norwegian).

[Cas20] Cascadeo. What is SLA? https://www.cascadeo.com/cascadeo-services-level-agreement/, 2020. Accessed: 2020-05-26.

[CMGS12] P. Cichonski, T. Millar, T. Grance, and K. Scarfone. *Computer Security Incident Handling Guide*. The National Institute of Standards and Technology (NIST), 2 edition, 2012. Special Publication 800-61.

[CS17] J. Corell and T. J. Skucas. Supply chain risks of SCADA/industrial control systems in the electricity sector. In *Public-Private Analytic Exchange Program (AEP)*. Office of the Director of National Intelligence, 2017.

[DS99] A. Daneels and W. Salter. WHAT IS SCADA? In *International Conference on Accelerator and Large Experimental Physics Control Systems*, Trieste, Italy, 1999. CERN.

[ea06] S. Ullring et. al. Når sikkerheten er viktigst. Technical Report 6, Departementenes servicesenter Informasjonsforvaltning (DSS), 2006. (In Norwegian).

[Ene20] Gudbrandsdal Energi. Netteiere i norge. https://www.ge.no/netteiere, 2020. Accessed: 2020-05-05 (In Norwegian).

[ERL06] A. O. Eggen, L. Rolfseng, and B. I. Langdal. Storskala nettforvaltning. tilstandsindikatorer for nettstasjoner, høyspennings kraftledninger og kabler. Technical report, SINTEF Energi Forskning, 2006. (In Norwegian).

[EZZ16] D. Essabbar, M. Zrikem, and M. Zolghadri. Power imbalance in collaboration relationships. *International Journal of Supply and Operations Management*, 2(4):1021–1034, 2016.

[fC19] Center for Cybersikkerhed. *Informationssikkerhed i leverandørforhold*. Number 1. Digitaliseringsstyrelsen, 2019. (In Danish).

[FHT13] R. Floodeen, J. Haller, and B. Tjaden. Identifying a shared mental model among incident responders. In *7th International Conference on IT Security Incident Management and IT Forensics 2013*, page 15–25. IEEE Computer Society, 2013.

[Fin20] Finanstilsynet. Risiko- og sårbarhetsanalyse (ROS), 2020. (In Norwegian).

[FMC10] N. Falliere, L. O. Murchu, and E. Chien. W32.stuxnet dossier. *Symantec Security Response*, 1.3, 2010.

[FMXY11] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid - the new and improved power grid. *IEEE Communications Surveys & Tutorials*, 14(4):944–980, 2011.

[fSI12] International Organization for Standardization (ISO). Nek iso/iec 27032:2012. Technical report, Norsk Elektroteknisk Komité, 2012.

[fSI16] International Organization for Standardization (ISO). Nek iso/iec 27035-1:2016. Technical report, Norsk Elektroteknisk Komité, 2016.

[fSI18] International Organization for Standardization (ISO). Nek iso/iec 27000:2018. Technical report, Norsk Elektroteknisk Komité, 2018.

[fsobM12] Myndigheten för samhällsskydd och beredskap (MSB). Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter, 2012. (In Swedish).

[GNB+06] T. Grace, T. Nolan, K. Burke, R. Dudley, G. White, and T. Good. *NIST SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*. National Institute of Standards and Technology (NIST), 2006.

[Gra19] R. Gray. What would happen in an apocalyptic blackout? *BBC Future*, 2019.

[Gro19] Thema Consulting Group. Ekstern rapport: Hvilket potensial har teknologi og organisering til å redusere strømkundenes nettleie? Technical Report 4, Norges vassdrags- og energidirektorat (NVE), 2019. (In Norwegian).

[Gå14] S. Gåsland. Gjør øvelse mester? om læringsfaktorer i beredskapsøvelser initiert av nve. Master's thesis, Universitetet i Oslo (UiO), 2014. (In Norwegian).

[Hea19] S. Holden and et. al. Fremtidige kompetansebehov ii. Technical Report 2, Departementenes servicesenter Informasjonsforvaltning (DSS), 2019. (In Norwegian).

[HHT+17] J. Hagen, O. Hermansen, Ø. Toftegård, J.-M. Pettersen, R. Steen, and S. L. Paulen. Regulering av ikt-sikkerhet. Technical Report 26, Norges vassdrags- og energidirektorat (NVE), 2017. (In Norwegian).

[HPWW11] E. Hollnagel, J. Pariès, D. Woods, and J. Wreathall. *Resilience Engineering in Practice - a Guidebook*. Ashgate Publishing Ltd., 2011.

[HT13] C. Hove and M. Tårnes. Information security incident management: An empirical study of current practice. Master's thesis, The Norwegian University of Science and Technology, 2013.

[inf17] Informasjonssikkerhetstilstanden i energiforsyningen. Technical Report 90, Norges vassdrags- og energidirektorat (NVE), 2017. (In Norwegian).

[iS20a] i SCOOP. Industry 4.0: the fourth industrial revolution – guide to industrie 4.0. https://www.i-scoop.eu/industry-4-0/, 2020. Accessed: 2020-04-01.

[iS20b] i SCOOP. Operational technology (ot) – definitions and differences with it? https://www.i-scoop.eu/industry-4-0/operational-technology-ot/, 2020. Accessed: 2020-02-04.

[Jac00] D. I. Jacobsen. *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. HøyskoleForlaget, 1st edition, 2000.

[JEAL09] M. G. Jaatun, I. A. Tøndel E. Albrechtsen, M. B.Line, and O. H. Longva. A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, 2(1-2):26–37, 2009.

[KHLF10] H. Khurana, M. Hadley, N. Lu, and D. Frincke. Smart-grid security issues. *IEEE Security & Privacy*, 8(1):81–85, 2010.

[Kin20] National Cyber Security Centre United Kingdom. 10 steps to cyber security. https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/incident-management, 2020. Accessed: 2020-01-27.

[KL18] E. Kirkebø and M. Ljøsne. Ikt-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen. Technical Report 90, Norges vassdrags- og energidirektorat (NVE), 2018. (In Norwegian).

[KO06] J. Knoben and L.A.G. Oerlemans. Proximity and inter-organizational collaboration: A literature review. *International Journal of Management Reviews*, 8(2):71–89, 2006.

[kra19] Metode for å finne kraftsensitiv informasjon på internett. Technical Report 11, Norges vassdrags- og energidirektorat (NVE), 2019. (In Norwegian).

[Lin15] M. B. Line. *Understanding information security incident management practices*. PhD thesis, Norwegian University of Science and Technology (NTNU), 2015.

[LT99] N. Lundberg and H. Tellioğlu. Understanding complex coordination processes in health care. *Scandinavian Journal of Information Systems*, 11, 1999.

[LTJ11] M. Line, I. A. Tøndel, and M. Jaatun. Cyber security challenges in smart grids. *IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, 2, 2011.

[Mik20] S. Mikkelsen. Disse studentene gjør livet surt for hackerne. https://www.universitetsavisa.no/student/2020/02/05/Disse-studentene-gj%C3%B8r-livet-surt-for-hackerne-21002524.ece, 2020. Accessed: 2020-04-05 (In Norwegian).

[Min12] The Norwegian Ministries. *Cyber Security Strategy for Norway*. Ministry of Government Administration, Reform and Church Affairs, 2012.

[MKB+11] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2011.

[MKG20] M. Maal, K. Krogedal, and A. Gjengstø. Ikt-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen - sjekkliste. Technical Report 1, Norges vassdrags- og energidirektorat (NVE), 2020. (In Norwegian).

[mne20] mnemonic. 2020 security report. *Security Report*, 2020.

[Mul19] M. A. Mullane. Cyber security strategies for the energy sector: how to achieve resilience. *IEC e-tech*, (5), 2019.

[Nas20] Nasjonal Sikkerhetsmyndighet (NSM). *NSMs Grunnprinsipper for IKT-sikkerhet*, 2.0 edition, 2020. (In Norwegian).

[NE10] The European Network and Information Security Agency (ENISA). Good practice guide for incident management, 2010.

[Nor19] Energy Facts Norway. The electricity grid. https://energifaktanorge.no/en/norsk-energiforsyning/kraftnett/, 2019. Accessed: 2020-01-20.

[NWM+20] A. Narayanan, J. W. Welburn, B. M. Miller, S. T. Li, and A. Clark-Ginsberg. Deterring attacks against the power grid. Technical report, RAND Corporation, 2020.

[oe19a] Olje og energidepartementet. Forskrift om kraftomsetning og nettjenester, 2019. (In Norwegian).

[oe19b] Olje og energidepartementet. Kraftberedskapsforskriften, 2019. (In Norwegian).

[oNEN20] Confederation of Norwegian Enterprise (NHO). Fakta om små og mellomstore bedrifter (smb). https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/, 2020. Accessed: 2020-03-15 (In Norwegian).

[oPS20] Oxford College of Procurement and Supply. Do the benefits of outsourcing in procurement outweigh the risks? https://www.oxfordcollegeofprocurementandsupply.com/procurement-supply-outsourcing-risks-benefits/, 2020. Accessed: 2020-02-27.

[oSN19] The National Institute of Standards and Technology (NIST). CYBER-PHYSICAL SYSTEMS. https://www.nist.gov/el/cyber-physical-systems, 2019. Accessed: 2020-01-28.

[65] The Norwegian Police Security Service (PST). Annual threat assessment 2019, 2019. (In Norwegian).

[66] The Norwegian Police Security Service (PST). Annual threat assessment 2020, 2020. (In Norwegian).

[Rit19] R. Ritchie. Maersk: Springing back from a catastrophic cyber-attack. https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack, 2019. Accessed: 2020-01-23.

[Rob11] C. Robson. *Real World Research*. John Wiley & Sons, Inc., West Sussex, United Kingdom, 2011.

[Rot18] T. Roth. What's in a DMZ? https://www.automationworld.com/home/blog/13319420/whats-in-a-dmz, 2018. Accessed: 2020-03-03.

[RRK12] H.-S. Rhee, Y. U. Ryu, and C.-T. Ki. Unrealistic optimism on information security management. *Computers & Security*, 31:221–232, 2012.

[RT16a] A. C. Remen and L. Tomter. Indiske it-arbeidere mister tilganger på statoils anlegg. https://www.nrk.no/norge/indiske-it-arbeidere-mister-tilganger-pa-statoils-oljeplattformer-1.13282643, 2016. Accessed: 2020-05-07 (In Norwegian).

[RT16b] A. C. Remen and L. Tomter. Tastefeilen som stoppet statoil. https://www.nrk.no/norge/xl/tastefeilen-som-stoppet-statoil-1.13174013, 2016. Accessed: 2020-05-07 (In Norwegian).

[sam19] Nve og energiministeren: Færre nettselskaper kan gi billigere strøm. *Teknisk Ukeblad Energi*, 2, 2019. (In Norwegian).

[Sch19] C. Schneider. DMZ: THE INDUSTRIAL CONTEXT. https://waterfall-security.com/dmz-the-industrial-context/, 2019. Accessed: 2020-03-22.

[SJ12] F. Skapalen and B. Jonassen. Veileder til sikkerhet i avanserte måle- og styringssystem. Technical Report 7, Norges vassdrags- og energidirektorat (NVE), 2012. (In Norwegian).

[SM11] F. Scholl and M. Mangold. Proactove incident response. *The Information Systems Security Association Journal*, 9, 2011.

[SWF10] L. A. Sand, G. B. Wangen, and A. S. Frogner. Hendelseshåndtering i små og mellomstore bedrifter. Bachelor's thesis, Gjøvik University College, 2010. (In Norwegian).

[Sym18] Symantec. Executive summary 2018 ISRT. *Internet Security Threat Report*, 23, 2018.

[Tea18] The NIST Cybersecurity Framework Team. *Framework for Improving Critical Infrastructure Cybersecurity*. The National Institute of Standards and Technology (NIST), 1.1 edition, 2018.

[top16] Critical infrastructure and scada/ics cybersecurity vulnerabilities and threats. https://www.checkpoint.com/downloads/products/top-10-cybersecurity-vulnerabilities-threat-for-critical-infrastructure-scada-ics.pdf, 2016. Accessed: 2020-04-11.

[Uni20] The Pennsylvania State University. Empirical research in the social sciences and education. https://guides.libraries.psu.edu/emp, 2020. Accessed: 2020-02-03.

[voeN16] Norges vassdrags-og energidirektorat (NVE). 1991: Den nye energiloven - fra forvaltning til forretning. https://www.nve.no/om-nve/vassdrags-og-energihistorie/nves-historie/1991-den-nye-energiloven-fra-forvaltning-til-forretning/, 2016. Accessed: 2020-04-02 (In Norwegian).

[Wil15] G. Williamson. OT, ICS, SCADA - what's the difference? https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference, 2015. Accessed: 2020-01-21.

[WMHB10] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov. Preparation, detection, and analysis: the diagnostic work of it security incident response. *Information Management & Computer Security*, 18(1):26–42, 2010.

[WS19] S. Weerakkody and B. Sinopoli. *Challenges and Opportunities: Cyber-Physical Security in the Smart Grid*. Smart Grid Control. Power Electronics and Power Systems. Springer, Cham, 2019.

[Wue14] C. Wueest. *Targeted Attacks Against the Energy Sector (White paper)*. Security Response. Symantec, 1st edition, 2014.

[Yin09] R. K. Yin. *Case Study Research: Design and Methods*, volume 5 of *Applied Social Research Methods Series*. SAGE, 4th edition, 2009.

[Zet16] K. Zetter. Inside the cunning, unprecedented hack of ukraine's power grid. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 2016. Accessed: 2020-01-23.

Appendix A

Letter of Consent (in Norwegian)

Forespørsel om deltagelse i intervju i forbindelse med masteroppgave

Dette er en forespørsel til deg som ønsker å delta i et forskningsprosjekt for en masteroppgave ved NTNU. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Vi er to masterstudenter ved Kommunikasjonsteknologi på NTNU Gløshaugen i Trondheim som skriver masteroppgave i informasjonssikkerhet. Fokuset for masteroppgaven er på sikkerhet i kraftbransjen. Oppgaven vår går ut på å analysere hvordan norske nettselskaper involverer leverandører i håndteringen av IKT-sikkerhetshendelser i prosesskontrollsystemer. Vi vil se resultatene i sammenheng med dagens trusselbilde for å avgjøre om praksisen er tilstrekkelig og finne områder med forbedringspotensiale.

For å kunne svare på denne oppgaven ønsker vi å gjennomføre intervjuer (estimert til å vare i ca. en time) med en eller flere personer fra utvalgte nettselskaper. Spørsmålene vi ønsker å stille omhandler hendelseshåndtering og hvordan nettselskapets leverandører inkluderes i dette.

Intervjuene vil bli foretatt av oss og deler kan bli diskutert med ansvarlig professor Maria Bartnes, førsteamanuensis II ved NTNU og Forskningssjef i SINTEF Digital, og veileder Roy Thomas Selbæk Myhre, Avdelingsleder Network & Security i TietoEVRY.

Oppbevaring og behandling av data
Resultatene fra intervjuene vil bli en del av en rapport som leveres på NTNU. Alle opplysninger vil bli behandlet i fortrolighet og resultatene vil bli anonymisert i rapporten, slik at ingen enkeltpersoner eller virksomheter vil kunne identifiseres. Vi vil bruke lydopptaker under intervjuene og de vil bli gjennomført i full fortrolighet. Informasjonen og opplysningene som innhentes vil ikke brukes til noe annet formål enn dette prosjektet. Opptakene, notater og eventuelle andre dokumenter som inneholder sensitive opplysninger vil bli oppbevart og behandlet konfidensielt på NTNU. Ved prosjektets slutt, 10. juni 2020, vil alle lydopptak slettes og øvrig datamateriale anonymiseres.

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke ditt samtykke uten å begrunne det noe ytterligere. Alle opplysninger om deg og virksomheten vil da bli anonymisert og lydopptak slettes.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,

- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Vi behandler opplysninger om deg basert på ditt samtykke.

Studien er meldt inn til og godkjent av Norsk senter for forskningsdata (NSD).

Dersom du har noen spørsmål er det bare å kontakte oss.

Med vennlig hilsen
Sara Waaler Eriksen og Sarmilan Gunabala
sarae@stud.ntnu.no / sarmilag@stud.ntnu.no
466 88 888 / 994 44 017

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om masteroppgaven, og har fått anledning til å stille spørsmål.
Jeg samtykker til å delta i intervju der lydopptaker benyttes.
Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, 10. juni 2020.

Navn på deltaker Dato/Sted Signatur

Appendix B

Interview Guide DSO

Interview guide DSO

Note: This document was originally in Norwegian, but has been translated to English for this thesis.

The goal of our study is to analyze how Norwegian DSOs relate to and include suppliers in the management of cybersecurity incidents in process control systems. Process control systems are systems that support, control and monitor production, transmission, storage and distribution of electrical energy. Administrative IT systems are therefore out of scope for this study. Relevante suppliers for the interview are those involved in process control systems and that can be helpful or should be contacted during an incident in the process control systems. Incident management includes planning and practice, the management of the incident and learning from it afterwards.

Introduction

1. What is your role in the organization?
    - 1.1. How long have you had this role?
    - 1.2. What are your areas of responsibility?
    - 1.3. How are your areas of responsibility be related to management of cybersecurity incidents in process control systems?
    - 1.4. Approximately how much of your time is dedicated to cybersecurity?

General

2. How many energy subscribers do you have? How many employees do you have?
3. How do you define a cybersecurity incident?
    - 3.1. Do all types of incidents trigger your incident management plans?
4. Do you believe the organization is in danger of a cybersecurity breach?
5. Have you been the victim of a cybersecurity breach in your process control systems? Preferably involving a supplier.
6. How is the cybersecurity organized in the company?
    - 6.1. Do you handle cybersecurity incidents in your process control systems with an internal or external IRT?
7. Do you have any cooperation/agreement with companies like KraftCERT, NVE, Nettalliansen or others?

7.1. What is the collaboration about?

7.2. How does it improve your emergency preparedness?

Suppliers

Focus on one or two suppliers to make it easier to answer questions.

8. Can you tell us about the suppliers in your process control systems?
    8.1. Which supplier is the most critical?
    8.2. What do the suppliers in the process control systems do?
    8.3. Approximately how many suppliers are involved in the process control systems?
    8.4. How do you communicate with the suppliers?
    8.5. Who from both parties communicate?
9. What kind of insight do you have of the cybersecurity of the suppliers? Do you validate that the cybersecurity requirements in your contract are upheld?
10. Are you guaranteed to get the necessary resources from the suppliers when needed? If they have contracts with several companies and have promised the same aid to all, what happens if several companies need help at the same time?
11. Are the contracts you have with the suppliers general or custom made?

Incident management

Talk about cybersecurity exercises if they have not experienced any incidents.

Phase 1: Plan and prepare

12. We reckon you have plans for managing incidents in your process control systems. Have you used any standards to make them and define cybersecurity requirements (ISO/IEC, Kraftberedskapsforskriften)?
13. What do your plans say about the involvement of suppliers?
    13.1. Are they followed in reality?
14. Do you conduct any cybersecurity preparedness exercises or validation of the plans?
    14.1. Are the suppliers involved in those exercises? If so, what types of exercises?
        14.1.1. *If not:* why not?

14.1.2. *If yes:* do you conduct exercises with several suppliers at the same time, in order to be tested together?

14.1.3. *If some are included:* why and how often?

14.2. Do you find it advantageous to include suppliers in the exercises?

Phase 2: Detection and reporting

15. Who are responsible for the detection of incidents - the DSO, the supplier or both?

15.1. *If incident management is outsourced:* How is the process if you and not the supplier detect a cybersecurity breach in the process control systems?

16. Are there any plans for communication between you and the supplier at detection of an incident? *Person of contact or communication channels.*

16.1. *If the supplier conducts incident management:* Are you contacted before or after the incident is handled?

16.2. *If the DSO conducts incident management:* Do you contact the supplier before or after the incident is handled?

16.3. Do you experience any problems with the communication or cooperation?

Phase 3: Assessment and decision

17. Who is responsible for deciding what is to be done?

17.1. In case of detection of an incident at a supplier, are they authorized to handle it or does it have to go through the DSO?

17.2. Is it defined which suppliers take care of which cybersecurity breaches?

17.3. Does the distribution of responsibility work well?

17.3.1. *If not:* are you doing anything about it?

Phase 4: Response

18. Do the suppliers cooperate in the response?

18.1. *If yes:* do you or the suppliers coordinate it?

18.1.1. *If incident management is outsourced:* does the external IRT coordinate everything?

19. How was the involvement of suppliers carried out? Was it conducted according to plan?

19.1. Were there any problems with the communication or cooperation with the supplier?

20. What was the DSOs role during the response?

Phase 5: Lessons learnt

21. *If the incident the interviewee know of did not involve a supplier:* If the incident had involved a supplier, would your plans have been sufficient to manage the incident in a satisfying way?

22. Who uses the information stored after an incident? What is it used for?

23. Are there any routines for collaboration with suppliers during lessons learnt (or after exercises if they have not experienced any incidents)?

23.1. *If no:* is it because the DSO does not have any routines for lessons learnt in general?

23.2. Have you made any changes in plans or routines as a result of this?

23.3. How often are the plans reviewed or changed?

23.4. Are the suppliers involved in or informed about the changes?

24. Have you established any collaboration with other DSOs that is relevant to the topic incident management and suppliers? (work groups, forums, regular meetings, common ICT systems etc.)

24.1. What does the collaboration give you? Does it help improve your emergency preparedness or keep you updated on the threat landscape?

Closing questions

25. Do you see any improvements in how you involve suppliers in incident management?

26. Is there anything you do regarding the involvement of suppliers that you do well, and that you would recommend to other DSOs?

27. Did you find this study useful? Have you gotten anything out of this interview?

28. Is it possible for you to send us any contingency plans or other relevant documents?

Appendix C
Interview Guide Supplier

Interview Guide Supplier

Note: This document was originally in Norwegian, but has been translated to English for this thesis.

The goal of our study is to analyze how Norwegian DSOs relate to and include suppliers in the management of cybersecurity incidents in process control systems. Process control systems are systems that support, control and monitor production, transmission, storage and distribution of electrical energy. Administrative IT-systems are therefore out of scope for this study. It is interesting to interview a supplier like you since you are involved in the process control systems and can be of help or should be contacted during a cybersecurity incident in the process control systems. Incident management includes planning and practice, the management of the incident and learning from it afterwards.

General

1. What is your role in the organization?
2. How many Norwegian DSOs do you have among your customers?
    2.1. How is the ratio between the number of small and large DSOs in your portfolio?
3. Approximately how many suppliers of process control systems are there in the Norwegian market?
4. Do you believe that your organization is in danger of a cybersecurity breach?
    4.1. Do you believe anyone would be interested in targeting your organization as a step in a supply chain attack against Norwegian DSOs?
5. Do you know if any of your DSO customers have been the victim of a successful attack on the process control system?
6. Do you have any cooperation or agreement with companies like KraftCERT, NVE or others?
    6.1. What is the collaboration about?

Customers

Focus on one or two DSO customers to make it easier to answer questions

7. Can you tell us about this organization's role regarding the DSOs' incident management?
    7.1. Do most of the DSOs have internal incident response teams or external incident response teams delivered by your organization?
8. What insight do the DSOs have into your cybersecurity?
    8.1. Do they check if you comply with the cybersecurity requirements stated in the contract?
9. Are the agreements/contracts you have with the customers general or customized?
    9.1. Are there any differences in agreements between small and large DSOs?
10. What qualities do you consider a good procurer to have?
11. Are you certain you will be able to provide customers the guaranteed resources when needed? If you have contracts with several DSOs and have promised the same aid to all, what happens if several DSOs need help simultaneously?
    11.1. Do you have any routines for who to prioritize in that scenario?
12. Do you have any thoughts on the power balance between your organization (and other suppliers of process control systems) and the DSOs?

Incident Management

Talk about cybersecurity exercises if they have not experienced any incidents.

Phase 1: Plan and Prepare

13. How do your organization become involved in DSOs plans for incident management?
    13.1. Are you aware of the plans?
    13.2. Are there any differences in how large or small/medium DSOs involve your organization in the incident management process.
14. Are you involved in DSOs' cybersecurity preparedness exercises or validation of plans for incident management? If so, what types?
    14.1. *If yes:* By approximately how many DSOs? Large or small, or is it independent of size?
    14.2. *If yes:* Are other suppliers involved in the same exercises as you?
    14.3. Do you find it beneficial to participate in such exercises?

15. Do you initiate own exercises regarding incident management in process control systems?

Phase 2: Detection and reporting

16. Do you experience any problems with the communication or cooperation with DSOs in the detection and reporting of incidents?

Phase 3: Assessment and decision

17. Is it your organization or the DSO who is responsible for deciding what is to be done during a cybersecurity incident?
    17.1. Does the distribution of responsibility work well?

Phase 4: Response

18. Do you cooperate with other suppliers in the response?
    18.1. Who coordinates it? One of the suppliers or the DSO?
19. Was the involvement of you conducted according to the plans set for incident management?
    19.1. Were there any problems with the communication or cooperation with the DSO?
20. Are there any difference between small and large DSOs in how dependent they are upon you (or other suppliers) to handle cybersecurity incidents in process control systems?

Phase 5: Lessons learnt

21. Do you gather and store any information relating to incidents or do you have access to the DSOs' logs etc.?
22. Do the DSOs have any routines for collaboration with you during lessons learnt (or after exercises if they have not experienced any incidents)?
    22.1. Are there any differences between small and large organizations?
    22.2. Have you initiated any lessons learnt after incidents with the DSOs?
    22.3. If a DSO makes any changes to the incident management plans, will you be informed? Have you ever been informed about any changes in plans?

23. Have you established any collaboration with other suppliers that is relevant to the topic incident management?
    23.1. What do you hope that these collaborations give you??

Other Questions and Areas of Improvement

24. Are you satisfied with the way DSOs involve you in their incident management or do you see any areas of improvement?
25. Norwegian DSOs are quite small on the global scale. Are there any differences between Norway and other countries? What can Norway learn from other countries?
26. Is there anything the DSOs do regarding the involvement of suppliers that works well?
27. We understand there are relatively few suppliers in the Norwegian market, do you see any problems with this?

Closing Questions

28. Did you find this study useful? Have you gotten anything out of this interview?
29. Is it possible for you to send us any documents relevant to our study?

Appendix D
Interview Guide NVE

Interview Guide NVE

Note: This document was originally in Norwegian, but has been translated to English for this thesis.

General:

1. NVE audits all DSOs on information security. Do you perceive the cybersecurity in these organizations as adequate?
    1.1. Are there significant differences between large and small and medium-sized DSOs regarding cybersecurity?
    1.2. Why are so many of the Norwegian DSOs small?
    1.3. Our preparatory work indicates that the NVE desires fewer, but larger DSOs. Is that correct and is it connected to cybersecurity?
2. What kind of data / standards did you use for the "Regulations on safety and emergency preparedness in the power sector for energy contingency" (Kraftberedskapsforskriften)?
3. What are your thoughts on the increasing use of suppliers in the electrical energy sector? Does it enhance or reduce cybersecurity?
4. Your thoughts on the threat landscape of the electrical energy sector (nationally/internationally):
    4.1. Do you believe Norwegian DSOs to be attractive targets for cyberattacks?
5. Our preparatory work found that there is a supplier concentration in the Norwegian market. Is that a weakness for the entire sector?
    5.1. How robust are they against cyber attacks on a key supplier?
6. Do you see any possibilities for improvement to the way DSOs currently involve suppliers in cybersecurity incident management?
7. Some of the DSOs claim their systems have air gaps and that it is impossible to access their process control systems - are they too confident with their own security?

Cybersecurity Incident Management:

8. Do you believe the DSOs are sufficiently prepared for cybersecurity incidents in their process control systems where the incident management involves suppliers?

9. Are you aware of any DSOs involving suppliers in cybersecurity incident management or cybersecurity preparedness exercises?
10. Do you think that the DSOs should involve suppliers in cybersecurity incident management and cybersecurity preparedness exercises?

Sara Waaler Eriksen & Sarmilan Gunabala

Cybersecurity Incident Management In The Electrical Energy Sector: Involvement Of Suppliers

NTNU
Kunnskap for en bedre verden