Master's thesis

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

Simen Bergset
Andreas Johan Nyland

Ensuring Safe and Secure Operations in the Norwegian Petroleum Industry: A Study on Assessing Trends in Cyber Risk Levels

Master's thesis in Communication technology and digital security
Supervisor: Maria Bartnes
Co-supervisor: Thor Aleksander Buan, Roy Thomas Selbæk Myhre
June 2023

NTNU
Norwegian University of
Science and Technology

Simen Bergset
Andreas Johan Nyland

Ensuring Safe and Secure Operations in the Norwegian Petroleum Industry: A Study on Assessing Trends in Cyber Risk Levels

Master's thesis in Communication technology and digital security
Supervisor: Maria Bartnes
Co-supervisor: Thor Aleksander Buan, Roy Thomas Selbæk Myhre
June 2023

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

NTNU

Norwegian University of
Science and Technology

Ensuring Safe and Secure Operations in the Norwegian Petroleum Industry: A Study on Assessing Trends in Cyber Risk Levels

Simen Bergset
Andreas Johan Nyland

Submission date:	June 2023
Main supervisor:	Maria Bartnes, SINTEF
Co-supervisor:	Thor Aleksander Buan, Ren Røros Roy Thomas Selbæk Myhre, Sopra Steria

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Title:	Ensuring Safe and Secure Operations in the Norwegian Petroleum Industry: A Study on Assessing Trends in Cyber Risk Levels
Student:	Simen Bergset Andreas Johan Nyland

Problem description:

The petroleum sector has since the late 60s been an essential part of the Norwegian infrastructure, and it is well known that the industry contains risks – both for the workers and the environment. These risks have been addressed through the annual report «Trends in risk levels in petroleum activity» (RNNP). However, this risk assessment only addresses safety concerns and overlooks the growing threat of cyber attacks. With the increasing digitalization and an extensive supply chain that keeps growing, the sector is being more exposed to cyber threats. Operational Technology and Information Technology were previously separated but are now being more integrated. This increases the attack surface and damage potential. As threats increase, security and safety measures have yet to follow up on all the new ways attackers are trying to exploit and attack this critical infrastructure. This highlights the need for a comprehensive assessment of cyber security in the petroleum sector, including identifying potential vulnerabilities, implementing security measures to mitigate these risks, and monitoring the systems. Through these actions, the oil and gas industry can better protect itself against cyber threats and attacks and ensure the continued safe and secure operation of this critical infrastructure.

In this project, we will explore how cyber security can be incorporated into the risk assessment framework of the Norwegian petroleum sector. We will seek to identify key indicators for cyber security by performing a combination of empirical studies in the industry and a literature review. By including cyber security trends in the RNNP assessment, the trends in risk level will give a more comprehensive and holistic understanding of the risks in the sector, which in turn could enable improved risk management and a more robust infrastructure.

Approved on:	2023-03-22
Main supervisor:	Maria Bartnes, SINTEF
Co-supervisor:	Thor Aleksander Buan, Ren Røros Roy Thomas Selbæk Myhre, Sopra Steria

Abstract

This master's thesis provides valuable insights into the current practices and challenges associated with addressing cyber security risks in the petroleum sector. It explores the existing risk assessment practices, incident reporting, and exercises employed by industry stakeholders. The audits conducted by the Petroleum Safety Authority Norway (PSA) are examined, and the concept of an «audit light» approach is suggested as a means to enhance cyber security evaluations. The study emphasizes the importance of information sharing within the sector and the impact of relevant laws and regulations. It also highlights the need for concise summaries or similar sources of information to address the extensive and unstructured nature of threat analysis.

This study employs the design science methodology and conducts a thorough literature review to gain insights into the present scenario. In addition, comprehensive interviews with key actors in the sector are executed to enhance our understanding and obtain new perspectives about the industry. The research acknowledges that smaller operators face limitations in conducting comprehensive threat analyses due to resource constraints. It proposes the utilization of external resources as a means to enhance their capabilities. Going forward, the study recommends establishing more formal and informal forums to foster knowledge exchange about incidents, vulnerabilities, threats, and assets among specialist groups, companies, sectors, and government authorities. It also proposes the establishment of a clearer and centralized mechanism for sharing information related to vulnerabilities.

Our research emphasizes the need for a coordinated approach to cyber security risks in the petroleum sector, calling for proactive, continuously updated risk assessments. It identifies significant challenges such as a lack of standardized approaches, the inadequacy of existing threat intelligence reports, limited information access, the overwhelming number of service providers, and resource disparities. Recommended strategies include external expertise, robust incident response plans, and a strong cyber security culture. However, further improvements are necessary in the tools, practices, and sharing of best practices across the industry. Audits, «audits light», and information sharing are identified as critical components of managing cyber security risks in the petroleum sector. Overall, this study provides valuable insights and recommendations for effectively addressing cyber security risks in the petroleum sector and ensuring the protection of critical infrastructure.

Sammendrag

Denne masteroppgaven gir verdifull innsikt i dagens praksis og utfordringer knyttet til håndtering av cybersikkerhetsrisiko i petroleumssektoren. Den utforsker eksisterende risikovurderingspraksis, rapportering av hendelser og øvelser som brukes av aktørene i bransjen. Det gjennomgås tilsyn gjennomført av Petroleumstilsynet (PTIL), og konseptet med en «tilsyn light»-tilnærming blir foreslått som en måte å forbedre evalueringen av cybersikkerhet. Oppgaven legger vekt på betydningen av informasjonsdeling innen sektoren og virkningen av relevante lover og forskrifter. Den fremhever også behovet for konsise sammendrag eller lignende informasjonskilder for å håndtere den omfattende og ustrukturerte naturen av trusselanalyser.

Dette arbeidet benytter designvitenskapelig metodikk og utfører en grundig litteraturgjennomgang for å få innsikt i dagens scenario. I tillegg blir omfattende intervjuer med nøkkelpersoner i sektoren gjennomført for å forbedre vår forståelse og få nye perspektiver om industrien. Oppgaven erkjenner ressursbegrensningene mindre operatører står overfor i å utføre grundige trusselanalyser og foreslår å dra nytte av eksterne ressurser for å styrke deres evner. Videre anbefaler oppgaven etablering av mer formelle og uformelle forum for å fremme kunnskapsutveksling om hendelser, sårbarheter, trusler og verdier blant spesialistgrupper, selskaper, sektorer og myndigheter. Den foreslår også etablering av en tydeligere og mer sentralisert mekanisme for deling av informasjon knyttet til sårbarheter.

Oppgaven understreker behovet for en koordinert tilnærming til cybersikkerhetsrisikoer i petroleumssektoren og oppfordrer til proaktive, kontinuerlig oppdaterte risikovurderinger. Den identifiserer betydelige utfordringer som mangel på standardiserte tilnærminger, utilstrekkelighet av eksisterende trusselintelligensrapporter, begrenset tilgang til informasjon, det overveldende antallet tjenesteleverandører og ressursforskjeller. Anbefalte strategier inkluderer ekstern ekspertise, robuste tiltaksplaner for hendelser og en sterk kultur for cybersikkerhet. Imidlertid er ytterligere forbedringer nødvendige når det gjelder verktøy, praksis og deling av beste praksis på tvers av bransjen. Tilsyn, «tilsyn light» og informasjonsdeling blir identifisert som avgjørende komponenter for å håndtere cybersikkerhetsrisiko i petroleumssektoren. Alt i alt gir denne oppgaven verdifull innsikt og anbefalinger for å effektivt håndtere cybersikkerhetsrisiko i petroleumssektoren og sikre beskyttelsen av kritisk infrastruktur.

Preface

This master's thesis is submitted to the Norwegian University of Science and Technology (NTNU) as the final part of our Master of Science (MSc) in the Communication Technology and Digital Security degree. The research has been conducted from January to June 2023, and it is a continuation of the pre-project from the autumn of 2022.

We want to express our gratitude to all interviewees for sharing your knowledge, thoughts, and insight through fruitful conversations. You helped us get invaluable insight into the industry and gave valuable input to the project. We anticipate that our project will aid in providing the industry with an improved understanding of cybersecurity risks in the future.

We want to thank Maria Bartnes, Thor Aleksander Buan, and Roy Thomas Selbæk Myhre for their great support and guidance during these two semesters. You gave valuable feedback and kept us motivated during the project.

Finally, we would like to thank family and friends for their support during this last year.

Simen Bergset and Andreas Johan Nyland

Trondheim, 2023

Contents

Appendices

List of Figures

List of Tables

List of Acronyms

APT Advanced Persistent Threat.

CBM Cybersecurity Barrier Management.

CDS-forum Industry Forum for Cybersecurity of Industrial Automation and Control Systems.

CERT Computer Emergency Response Team.

CSF Cybersecurity Framework.

DMZ Demilitarized Zone.

HMI Human Machine Interface.

HSE Health, Safety and Environment.

IaaS Infrastructure-as-a-Service.

IACS Industrial Automation & Control Systems.

ICS Industrial Control Systems.

ICT Information and Communication Technology.

IEC The International Electrotechnical Commission.

IIoT Industrial Internet of Things.

IOA Information Object Addresses.

ISBR Information Security Baseline Requirement.

IT Information Technology.

MSc Master of Science.

NCS Norwegian Continental Shelf.

NIS Norwegian Intelligence Service.

NIST National Institute of Standards and Technology.

NOG Norwegian Oil and Gas Association.

NSD Norsk senter for forskningsdata.

NSM Norwegian National Security Authority.

NTNU Norwegian University of Science and Technology.

OT Operational Technology.

PaaS Platform-as-a-Service.

PCSS Process Control, Safety, and Support.

PSA Petroleum Safety Authority Norway.

PST The Norwegian Police Security Service.

RNNP Trends in risk levels in petroleum activity.

ROS Risk and Vulnerability Analysis.

RQ Research question.

SaaS Software-as-a-Service.

SCADA Supervisory Control and Data Acquisition.

SIS Safety Instrumented System.

SOC Security Operations Center.

VTS Asset (Verdi), Threat (Trussel) and Vulnerability (Sårbarhet).

Chapter 1 Introduction

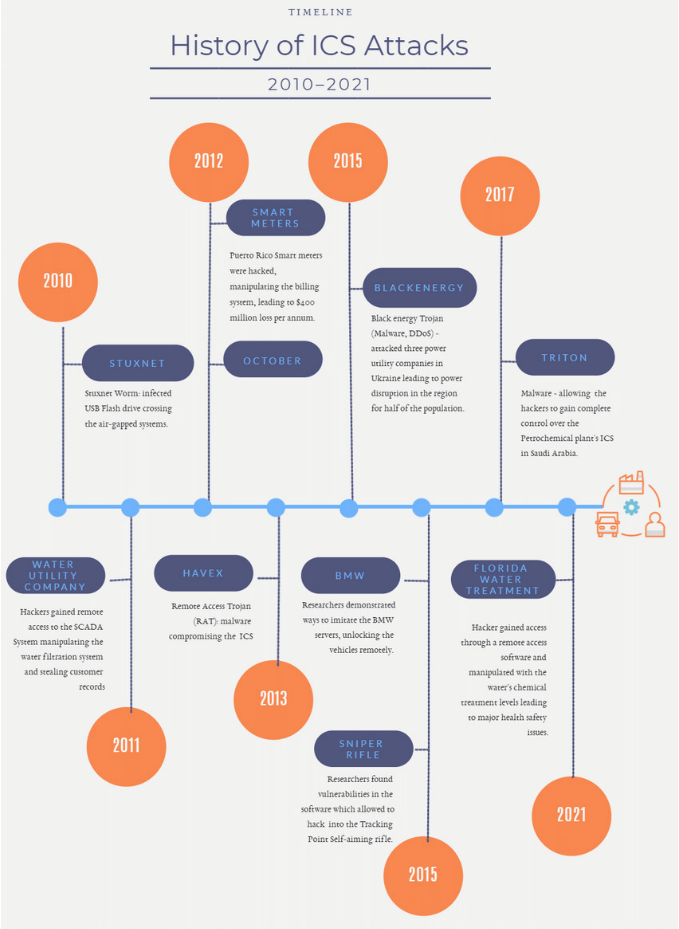
1.1 Motivation

The Norwegian petroleum sector has played a vital role in the country's infrastructure since the late 1960s, but it is also well-recognized that this industry carries inherent risks to both personnel and the environment. To address these risks, the industry has established the Trends in risk levels in petroleum activity (RNNP) framework, consisting of annual reports produced since 1999/2000 [PSAa]. However, these reports primarily focus on safety concerns and have not adequately considered the emerging threat of cyber attacks. As the sector experiences vast digitalization and integrates OT and IT, the potential for cyber threats has significantly grown. The increased attack surface and heightened vulnerability demand a thorough approach to addressing cyber security in the petroleum sector.

The ongoing digitalization of the sector has exposed it to a greater risk of cyber threats, highlighting the urgent need for a more comprehensive and robust evaluation of cyber security measures. Moreover, the threat landscape is continuously evolving, as evidenced by recent incidents such as drone activity near platforms [Eur22a] and ongoing conflicts worldwide. Another example of the changing threat landscape is the emergence of sophisticated modular malware named "Pipedream", capable of targeting tens of thousands of industrial devices in critical infrastructure [Inc23]. Additionally, significant attacks on Industrial Control Systems (ICS) have been observed since 2010. Figure 1.1 presents a timeline illustrating notable ICS attacks between 2010 and 2021. Some of these are further described in Section 2.6.

These events have underscored the importance of having a well-structured and thorough evaluation process in place to mitigate potential cyber security risks. It also means that the process of addressing cyber risks must be able to keep up with these rapid changes in order to remain effective and relevant. The increasing complexity of systems in the petroleum sector, combined with the ever-evolving threat environment, means that the challenge of addressing cyber risks is not only relevant now but will also be relevant in the future.

Therefore, there is an urgent need for a comprehensive and up-to-date approach to addressing risks concerned with cyber security in the oil and gas industry. This will require a combination of technical expertise, industry knowledge, and a thorough understanding of the evolving threat landscape and vulnerabilities in order to effectively mitigate potential cyber security risks. By taking a proactive and dynamic approach to address risks, the petroleum sector can ensure that it remains protected against potential cyber security threats in the present and the future. In this thesis, the term «petroleum» may be used synonymously with «oil and gas», reflecting common usage in the industry.



Stuxnet Worm: infected USB Flash drive crossing the air-gapped systems.

Puerto Rico Smart meters were hacked, manipulating the billing system, leading to $400 million loss per annum.

Black energy Trojan (Malware, DDoS) - attacked three power utility companies in Ukraine leading to power disruption in the region for half of the population.

Malware - allowing the hackers to gain complete control over the Petrochemical plant's ICS in Saudi Arabia.

Hackers gained remote access to the SCADA System manipulating the water filtration system and stealing customer records

Remote Access Trojan (RAT): malware compromising the ICS

Researchers demonstrated ways to imitate the BMW servers, unlocking the vehicles remotely.

Researchers found vulnerabilities in the software which allowed to hack into the Tracking Point Self-aiming rifle.

Hacker gained access through a remote access software and manipulated with the water's chemical treatment levels leading to major health safety issues.

Figure 1.1: Timeline and history of ICS cyber security attacks [DAN21].

1.2 Changes Regarding Problem Description

Initially, our problem description primarily emphasized the *assessment* of cyber risks and the existing frameworks for conducting risk assessments. However, as we progressed with our project, we came to realize that there is a broader requirement for a comprehensive approach to *address* cyber risks at a sector-wide level. We discovered that various standards and frameworks already exist for risk assessment, but there is a greater need to adopt a holistic perspective in effectively managing and mitigating cyber risks. Consequently, our project will focus on exploring how key cyber security indicators can be utilized to address and mitigate cyber security risks across the entire sector.

1.3 Objectives

The overall goal of this thesis is to suggest a method for how the petroleum sector can address risks associated with cyber security to enable improved cyber security risk management on a sector-level. The following Research questions (RQs) have been prepared to achieve this goal.

RQ1: How is risk associated with cyber security in the petroleum sector addressed today?

RQ2: How can risk associated with cyber security across the petroleum sector be effectively addressed going forward?

Because we do not know the petroleum sector very well from before, we must first understand the sector and how the risk associated with cyber security is addressed today. Through the specialization project, we discovered that there are many laws and regulations that apply to the sector and that these are mostly functional requirements that describe what is to be achieved and not how to achieve them. The Petroleum Safety Authority Norway (PSA) describes itself as «a government supervisory and administrative agency with regulatory responsibility for safety, the working environment, emergency preparedness, and security in the petroleum sector» [PSA19]. The first RQ aims to further investigate how laws, regulations, standards, best practices, and the interplay with the PSA works in practice.

To be able to answer the latter of the research questions, a profound understanding of the petroleum sector and how the risk associated with cyber security is addressed today is needed.

This will facilitate a more holistic overview of the risks in the sector and can help to mitigate these risks more effectively. Key indicators for cyber security, threat assessment, and trends will be addressed through a literature review and an empirical study of the sector.

1.4 Scope

Our starting point with this thesis was the title «Industrial Cyber Safety - Securing Critical Infrastructure». This is very broad and we needed to narrow it down quite a lot during our specialization project. With the help of our supervisors, we ended up deep diving into Information and Communication Technology (ICT) and OT and specifically within the petroleum sector. As the petroleum sector includes many different actors, narrowing down the scope further was necessary. The focus of this thesis is confined to the operators of the petroleum sector, that being the companies operating the platforms where oil and gas are extracted. In this way, it is possible to create a more specific and suitable method that is relevant to important actors in the sector. The results might still be applied to other parts of the sector with adjustments.

1.5 Limitations

Considering the sensitive nature of cyber security information, there may be limitations on the amount of information that operators are willing to share. However, sharing such information can effectively mitigate cyber security risks, given the similarity of threats and the potential for shared mitigation strategies.

Moreover, it is important to account for the varying sizes of operators within the sector. While larger companies may have their own cyber security divisions, smaller ones may rely on external and sector input. This creates a trade-off whereby larger companies may feel that sharing information is less beneficial, as they may already be familiar with the cyber risks and mitigation methods presented by smaller companies. As a result, obtaining information within the sector can prove challenging.

1.6 Outline

The master thesis has the following structure:

Chapter 2 gives a clear overview of how the Norwegian petroleum sector is structured today, as well as presenting relevant previous work, standards and guidelines, and basics of risk assessment and the threat landscape.

Chapter 3 explains how the chosen research methods are conducted along with the challenges and limitations of this methodology.

Chapter 4 presents the results from the interviews with the industry together with the results from the conducted literature review. The results are analyzed to identify recommended methods to improve how risks concerning cyber security can be addressed going forward.

Chapter 5 analyzes and discusses the findings from the previous chapter related to the research questions. The chapter concludes with a discussion of the validity of the research.

Chapter 6 presents a conclusion based on the findings, along with reflections on future work in the field of addressing risks concerning cyber security in the petroleum sector.

Chapter 2 Background

The upcoming chapter serves as a solid foundation for understanding the theoretical aspects central to cyber security risk assessment within the petroleum sector. Building upon the literature review outlined in Section 3.3, this chapter establishes the groundwork by presenting essential background information relevant to our study.

In this chapter, we will first present an overview of the Norwegian petroleum sector in section 2.1 with some of the industry's key actors and stakeholders especially important for our master's thesis in Section 2.2. A look at how IT has been introduced in OT is presented in Section 2.3. Section 2.4 will introduce relevant standards and guidelines when it comes to risk assessment (Sec. 2.5). Additionally, the chapter explains the current threat landscape in Section 2.6 and concludes with presenting work relating to our study in Section 2.7.

2.1 The Norwegian Petroleum Sector

The petroleum industry is crucial for Norway's economy, providing a buffer during crises like the COVID-19 pandemic [oFin20]. Digitization in this sector will create new opportunities and enhance competitiveness, which is essential to address the anticipated lower oil prices and increased competition from emerging energy forms [Dig18]. However, the industry faces challenges from these emerging energy sources and increased environmental focus. As the petroleum industry embraces digitalization, it becomes increasingly exposed to cyber risks, which must be addressed to ensure operational continuity and resilience [Con16].

In the Norwegian petroleum industry, there were 39 exploration and production companies as of the end of 2022, with 18 of these being operators [Peta], operating both onshore and offshore. These companies manage daily operations from central control rooms located on platforms or other facilities. Each of the companies is self-responsible for their own safety and also security.

In Norway, there are various entities that hold responsibilities when it comes to safety and security in the oil and gas industry. These organizations not only enforce industry-specific guidelines and assure compliance with governmental regulations but also facilitate information sharing and incident reporting. They play a critical role in encouraging transparency, fostering open communication, and promoting a culture of safety within the industry. By facilitating the exchange of vital information and reporting of incidents, these organizations help to identify potential risks, improve practices, and enhance overall operational efficiency and safety in the industry. Some of these actors are PSA, Norwegian National Security Authority (NSM), and KraftCERT.

2.2 Actors and Stakeholders in The Petroleum Sector

This section introduces the three different official organizations PSA, NSM, and KraftCERT, which all are especially important for our master's thesis. They are, among many other actors and companies, vital in maintaining the safety, security, and resilience of Norway's petroleum sector. Chapter 4 presents results from interviews with key persons within each of these organizations.

2.2.1 PSA

The Ministry of Labor and Social Inclusion (Arbeids- og inkluderingsdepartementet) holds the primary authority over matters regarding the work environment, safety regulations, and emergency readiness within the petroleum sector in Norway [Petb].

Under the jurisdiction of the Ministry of Labour and Social Inclusion, the PSA operates as a subsidiary agency, as can be viewed in figure 2.1. It assumes the responsibility for ensuring technical and operational safety, emergency preparedness for handling accidents and intentional acts like sabotage, as well as maintaining a safe working environment across the entire petroleum industry. As a guide and watchdog, the PSA ensures prudent operations, continuous improvement, and effective risk management, emphasizing supervision, expertise, knowledge sharing, transparency, and trust [PSA19].

The PSA's expertise stems from its specialists' experience and supervisory activity findings. Knowledge sharing is facilitated through methods such as the annual RNNP report, technical meetings, and the publication of investigation and audit reports on their website [PSAb].

Transparency and trust are crucial for the PSA's supervisory authority, with high expectations from operators and other actors in the sector. The PSA fosters openness by publishing various documents, promoting knowledge propagation and experience sharing, and granting public access to case documents under strict confidentiality limitations.

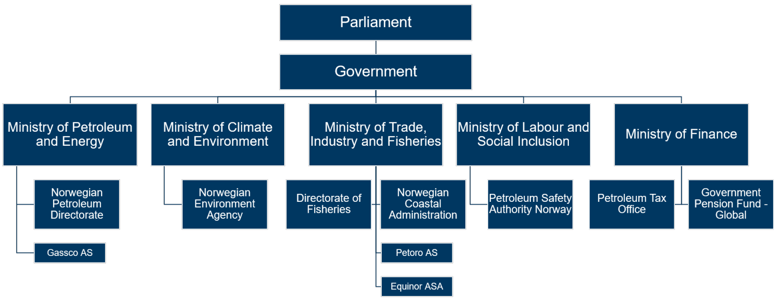

Parliament
Government
Ministry of Petroleum and Energy
Ministry of Climate and Environment
Ministry of Trade, Industry and Fisheries
Ministry of Labour and Social Inclusion
Ministry of Finance
Norwegian Petroleum Directorate
Gassco AS
Norwegian Environment Agency
Directorate of Fisheries
Norwegian Coastal Administration
Petoro AS
Equinor ASA
Petroleum Safety Authority Norway
Petroleum Tax Office
Government Pension Fund - Global

Figure 2.1: Overview of who has the jurisdiction and legislative oversight of the PSA. The figure is taken from [Petb].

Audits

An audit involves a systematic review of an organization's operations, processes, financials, and compliance with regulatory standards [Ben08]. For the petroleum sector, audits can be done by external or internal auditors who are independent when it comes to the department or process being audited. Audits are different depending on which area is being audited but contain some key steps in planning, fieldwork, analysis, reporting, and follow-ups. The external audits done in the Norwegian petroleum industry are mainly conducted by the PSA and published on their website [PSAb]. In this thesis, we primarily use the term «audit». However, it is important to note that many papers and reports use the term «supervision» interchangeably with «audit». Therefore, both terms will occur interchangeably throughout this work.

RNNP

The RNNP project was initiated in 1999/2000 to measure and monitor the risk level in the Norwegian petroleum industry, including onshore and offshore activities [PSAa]. Serving as an annual report, it aims to assess the effectiveness of Health, Safety and Environment (HSE) efforts, identify critical areas for improvement, and enhance understanding of accident causes and their impact on risk [PSAa]. RNNP utilizes various indicators, both reactive and proactive, to provide insights into the industry's safety performance. The annual report promotes collaboration among companies, authorities, industry associations, and research institutions. The trends highlighted in the reports are crucial, such as the direction of major accident risk. Its findings contribute to decision-making for preventive safety measures, emergency planning, regulatory changes, and research and development. However, it is important to acknowledge that the indicators used in RNNP provide a simplified view of the complex reality of safety and work environment in the petroleum sector [PSAa].

2.2.2 NSM

NSM, a cross-sectoral professional and supervisory authority for protective security services in Norway, plays a crucial role in maintaining the safety and security of the petroleum sector in Norway. By gathering and analyzing information relevant to protective security services, the NSM identifies potential threats and vulnerabilities within the industry [NSMb]. Through oversight and inspections, it ensures compliance with security regulations and upholds required safety standards. Information assurance is an essential aspect, as the petroleum sector relies on various information systems for its operations.

The NSM also provides valuable information, advice, and guidance, helping the sector develop and implement appropriate security measures [NSMb]. National and international cooperation allows for sharing of best practices and expertise, contributing to the overall security posture of the petroleum sector. Furthermore, the NSM's coordinating role in preventative work and responses against IT security breaches (through KraftCERT) is critical in protecting the petroleum sector's key infrastructure from cyber threats and facilitating effective responses to potential incidents.

2.2.3 KraftCERT

In Norway, sector-specific Computer Emergency Response Teams (CERTs) have been established for healthcare, finance, justice, energy, and universities/colleges, along with other sectors [Nor15]. These CERTs handle cyber threats and collaborate with relevant stakeholders to protect the sectors and strengthen Norway's defense against attacks [Nor15]. One of these CERTs is KraftCERT, a specialized CERT for the energy sector.

Traditionally, the oil and gas sector's primary focus has been on safety and addressing physical events related to operations. However, with the increasing digitalization of the industry, the need to address cyber security threats has become increasingly important. Recognizing this, the PSA has recently delegated the responsibility of collecting reports on cyber incidents within the petroleum industry to KraftCERT.

KraftCERT's deep understanding of the power sector provides a significant advantage when managing cyber incident reporting for the petroleum industry. Much like the power sector, the petroleum industry relies heavily on ICS and OT for their operations. These systems, while crucial for operations, are potential targets for cyber threats. KraftCERT's experience with similar systems in the power sector allows it to understand the vulnerabilities, potential threats, and implications of cyber incidents in the petroleum sector.

This initiative indicates a significant step forward in integrating cyber security into the broader safety framework of the oil and gas sector, reflecting the critical role of digital security in protecting modern energy infrastructure. Through this approach, KraftCERT's role in incident reporting is crucial for strengthening the cyber resilience of Norway's petroleum industry.

2.2.4 Other Actors

This subsection includes other actors relevant to the study. However, we have not interviewed any of the mentioned actors below.

Offshore Norway

Offshore Norway, formerly known as Norwegian Oil and Gas Association (NOG) from 2012 to 2022 [Kje22], is an industry association representing oil companies and supplier companies associated with oil operations on the Norwegian Continental Shelf (NCS). The organization plays a vital role in representing the interests of its member companies, fostering industry collaboration, and supporting a sustainable and competitive oil and gas sector in Norway.

In addition to its advocacy role, Offshore Norway also plays a crucial role in developing various guidelines to ensure industry standards and best practices are followed. One such guideline is NOG104 [Nor16], which is widely utilized and referred to in the Norwegian oil and gas sector [HOJ+21]. These guidelines offer valuable recommendations and guidance on various aspects of oil and gas operations, resulting in enhanced safety and increased efficiency across the industry.

NIST

National Institute of Standards and Technology (NIST) is a leading US government agency focused on advancing measurement science, standards, and technology [NIS09]. With a mission to enhance economic security and improve quality of life, NIST promotes US innovation and industrial competitiveness. The agency's core competencies include measurement science, rigorous traceability, and the development and use of standards. NIST is responsible for developing the NIST Cybersecurity Framework (CSF), a widely recognized set of guidelines and best practices for managing and improving cyber security posture in organizations [Nat18].

2.3 Introduction of IT in OT

Operational Technology (OT) systems, encompassing a broad spectrum of technologies such as ICS and Industrial Automation & Control Systems (IACS), were originally designed to operate in isolated environments with no connection to other networks [SFS11]. This design approach is commonly referred to as an air gap and was especially used within industries where the physical stakes are high, such as the petroleum industry. In such contexts, OT systems are critical to controlling and overseeing fundamental processes, and the importance of their availability and real-time operational capacity cannot be overstated (Figure 2.2). Any interruption or delay in the functioning of these systems can potentially result in significant operational and safety consequences [ØBJ+21].

In the current landscape, OT systems are increasingly integrated with IT systems to leverage the advantages of connectivity, automation, and real-time data [HOJ+21]. While this integration presents considerable benefits, it also exposes OT systems to cyber threats previously faced only in IT. As such, the original design principle of OT systems, focused on isolation and operational availability, is being challenged. This paradigm shift necessitates new strategies to ensure not only the operational integrity of these systems but also their resilience against an evolving threat landscape [Con16].

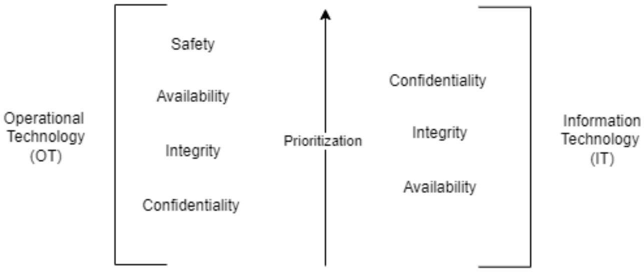


Figure 2.2: General priorities for the security objectives when concerning typical IT systems vs. OT systems. The figure is adopted from [GTA+22].

Priority in IT vs. OT

IT and OT systems have traditionally prioritized different security attributes. IT systems, driven by data management needs, focus on confidentiality, ensuring only authorized individuals have access to data, and integrity, maintaining and assuring the accuracy and consistency of data [GTA+22].

On the other hand, OT systems, fundamental to critical infrastructure, prioritize availability highest, as shown in Figure 2.2. The key objective for OT systems is to maintain continuous, efficient operations, considering that downtime could lead to significant consequences for the operating company. This focus results in different responses to cyber threats where an IT system might completely shut down the affected part, whereas an OT system typically tries to isolate the threat while maintaining ongoing operations [HOJ+21].

However, the merging of IT into OT systems for increased efficiency and cost savings demands a greater emphasis on confidentiality and integrity, characteristics traditionally associated with IT, in OT settings. This incorporation has unintentionally increased the vulnerability of OT systems to cyber threats, as they are now more exposed to internet-based attacks usually targeted at IT systems. The task of harmonizing these differing security priorities in a connected environment is significant, necessitating a comprehensive cyber security strategy that respects the unique requirements of both IT and OT systems.

Network Topology of OT

A network topology in the petroleum industry would demonstrate a clear division between IT and OT with the use of a Demilitarized Zone (DMZ) [OBH+22]. In Figure 2.3, the IT network, represented by the pink zone, Level 4/5: Enterprise, connects to the Internet via a DMZ. A DMZ is a subnetwork that separates an internal network from an untrusted external one, usually the Internet, providing an additional layer of security [JWBK21]. The OT network, represented by the yellow, beige, blue, and purple zones (Level 0, 1, 2, and 3) connects to IT via another DMZ, depicted by the green zone, Level 3.5: DMZ. Although a DMZ separates IT and OT, the two systems remain interconnected, allowing for potential maneuvering between them.

Historically, attacks on IT systems did not affect OT systems due to the air gap between the two. However, with the current interconnection, IT systems could serve as a gateway to OT systems, thereby increasing the attack surface for OT systems and paving the way for new types of attacks on the petroleum industry. The integration of IT into OT systems not only allows for the exploitation of other vulnerabilities but also means that attacks primarily targeting IT systems could indirectly impact production by affecting OT systems [HOJ+21].

2.4 Standards and Guidelines

This section provides an overview of relevant standards and guidelines utilized in the industry. Table 2.1 presents the most applicable ones for our master's thesis. It is worth noting that while there are other frameworks and guidelines available for risk assessment and cyber security, the ones included in the table are the ones we have familiarized ourselves with through our research.

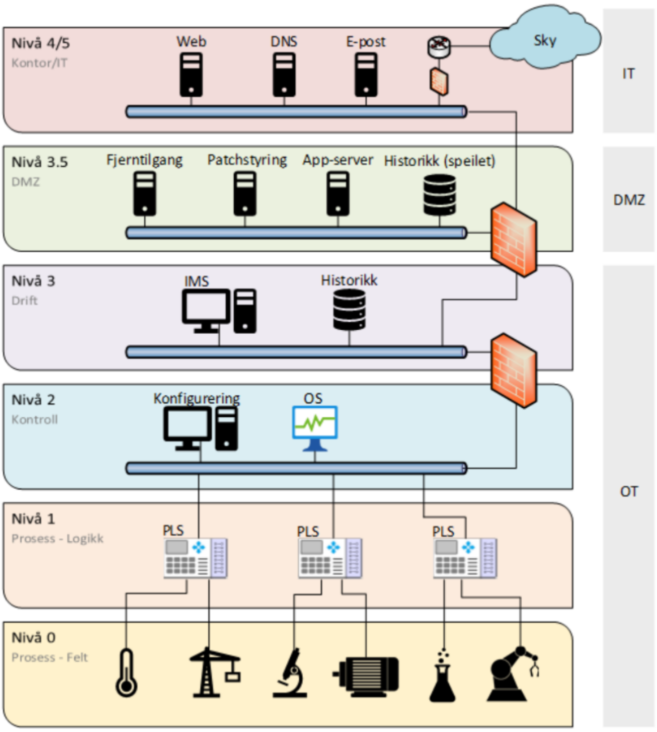


Figure 2.3: Illustration of how IT and OT are separated in a network topology. The figure is taken from [JWBK21].

2.4.1 IEC 62443

The The International Electrotechnical Commission (IEC) 62443 series of standards and technical reports are dedicated to enhancing the security of IACS, providing a standardized framework that enables shared understanding and more robust security across all parties involved in the supply chain. This is particularly beneficial to industries like the Norwegian petroleum sector, which recognizes IEC 62443 as a fundamental part of its cyber security strategy and implementation [HOJ+21].

Given its universal applicability, IEC 62443 plays a vital role in the petroleum industry. Key aspects such as establishing an IACS security program (IEC 62443-2-1) [Int10], conducting security risk assessments and system design (IEC 62443-3-2) [Int20], and defining security requirements and levels (IEC 62443-3-3) [Int19], all come together to fortify the cyber security posture in the context of critical infrastructure such as pipelines, drilling platforms, and refineries.

Despite the numerous benefits offered by the IEC 62443 standards, stakeholders often find understanding and implementing these standards challenging due to their complexity and extensiveness, spanning over 900 pages. Certain parts may also be incomplete, outdated, or yet to be created, adding to the challenge. Furthermore, while IEC 62443 provides a comprehensive framework outlining cyber security requirements that should be included by industries, it does not specify the methods for incorporating these, thus leaving organizations with substantial work needed for practical implementation. However, with the right approach, commitment, and resources, the petroleum industry can significantly enhance its cyber security measures, mitigating risks and threats inherent to this sector.

2.4.2 NOG104

In collaboration with the industry, the NOG (now Offshore Norway) formulated a set of guidelines, known as NOG104. This guideline aims to address the critical aspect of information security in the domain of Process Control, Safety, and Support (PCSS)) within the ICT systems. Regarded as a «good practice», this guideline is designed to complement an organization's existing information security policies effectively [Nor16].

NOG104 provides guidance on how to implement the Information Security Baseline Requirements (ISBRs), which is a set of standards that detail minimum acceptable practices for information security. The ISBRs cover a range of areas, including risk management, user access management, incident management, and more [Nor16]. They help organizations maintain a robust security posture and manage their information security risks effectively.

To facilitate this, NOG104 structures the guidelines according to the five security functions defined in the NIST CSF. These functions are *Identify*, *Protect*, *Detect*, *Respond*, and *Recover* [Nat18]. By using this structure, organizations can address the ISBRs in a bow-tie manner. Subsection 2.5.4 provides more info on the bow-tie model. The first three functions, *Identify*, *Protect*, and *Detect*, form the right side of the bow-tie and focus on proactive measures before a security incident occurs. The remaining two functions, *Respond* and *Recover*, form the left side of the bow-tie and focus on reactive measures after a security incident has occurred.

Despite the industry's acknowledgment that NOG104 is outdated [HOJ+21], it is still the only cyber security guideline noted in the PSA regulations. Consequently, the industry continues to reference it in its efforts to mitigate security challenges.

2.4.3 DNVGL-RP-G108

DNVGL-RP-G108 is a recommended practice that provides guidelines for implementing the IEC 62443 series of standards specifically in the oil and gas industry

[DNV17]. The guidelines focus on practical implementation details, addressing the unique cyber security needs of the sector. The practice covers aspects such as risk assessment, security management systems, and supplier requirements. By following these guidelines, organizations can enhance their cyber security measures in industrial automation and control systems [DNV17].

Table 2.1: Table of relevant standards and guidelines

Institution	Short Title	Last Revision	Title and Description
IEC	62443-1-1	2009	Industrial communication networks - Network and system security - Part 1-1: Terminology. Defines key terms and concepts for secure industrial communication networks in accordance to the IEC 62443 series [Int09]
IEC	62443-2-1	2010	Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program. Provides guidance for establishing security programs in industrial automation and control systems [Int10]
IEC	62443-3-2	2020	Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design. Addresses security risk assessment for system design in industrial automation and control systems [Int20]
IEC	62443-3-3	2019	Industrial communication networks Network and system security Part 3-3: System security requirements and security levels. Defines system security requirements and security levels for industrial communication networks [Int19]
Offshore Norway	NOG 104	2016	104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety, and support of ICT systems. Provides recommended practices for oil and gas companies [Nor16]
DNV	RP-G108	2017	Cyber security in the oil&gas industry based on IEC 62443. Provides recommended practices for IEC 62443 in the Oil&Gas Sector [DNV17].

2.5 Risk Assessment

Risk management is defined as «Coordinated activities to direct and control an organization with regard to risk» by the PSA [Nor17]. Risk assessment is a crucial process in the broader field of risk management, providing the necessary foundation for understanding the potential risks faced by an organization. There are three primary approaches used to estimate risk levels in risk assessments: qualitative, semi-quantitative, and quantitative.

Qualitative risk assessment relies on expert judgment and descriptive scales to assign subjective risk levels. Semi-quantitative risk assessment combines qualitative scales with numerical values to provide a more structured evaluation of risk. On the other hand, quantitative risk assessment involves statistical methods or other quantitative techniques to assign numerical values, offering a precise and quantitative measure of risk [MBFA06].

In this study, our primary focus is on qualitative risk assessment. Because, as noted by Sopra Steria, «Regular, qualitative assessments of risk contribute to providing an overview of possible incidents and consequences, an updated understanding of risk, and increased knowledge of the risk picture» [GTA+22]. This underscores the importance of qualitative risk assessment as a method for gaining a comprehensive understanding of the various risks an organization might face.

A primary goal of our research is to gain insight into how the PSA and other actors view the assessment of cyber security risk and to understand their considerations on this topic for the future. NSM recommended using a triangle consisting of asset, threat, and vulnerability already in 2016 [Nat16]. This is an approach that not explicitly addresses likelihood commonly known in more numerical forms of risk assessments, but is often used in the fields of cyber security and IT [NSMa]. The Asset (Verdi), Threat (Trussel) and Vulnerability (Sårbarhet) (VTS) model, depicted in Figure 2.4, shows the interrelationship between an asset attracting a threat, which in turn exploits a vulnerability, thereby exposing the asset(s). This conceptual model underscores the interconnected nature of these components in shaping the cyber security risk landscape.

The IEC 62443 part 2-1 standard, «Establishing an industrial automation and control system security program», specifies the importance of selecting an appropriate risk assessment methodology. It highlights that the organization should choose a specific approach and methodology that effectively identifies and prioritizes risks based on the security threats, vulnerabilities, and consequences associated with their IACS assets [Int10]. Furthermore, it recognizes that the triangle of threat, vulnerability, and consequence can serve as a valuable framework. A consequence is closely linked to an asset, as any consequences will directly impact the asset. Therefore, the two

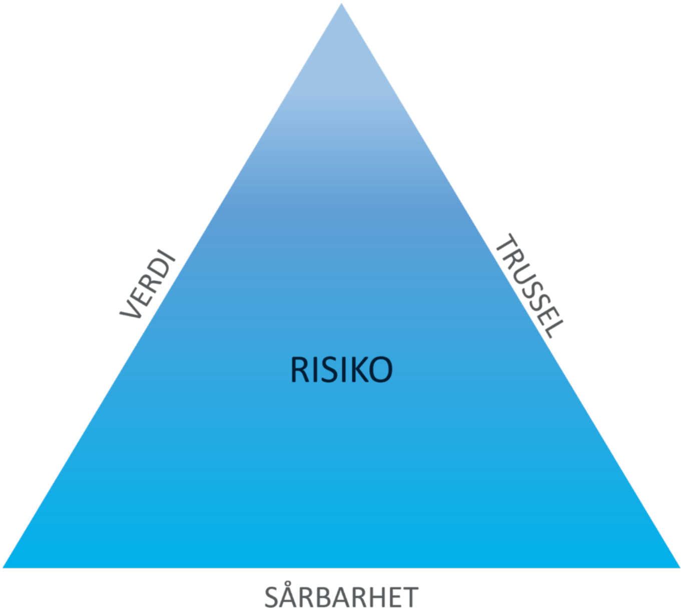


Figure 2.4: The VTS model. Figure collected from [Jan21].

triangles share similarities and reinforce the adoption of a risk assessment method that incorporates the triangle of threat, vulnerability, and consequence.

2.5.1 Assets

Businesses in all sectors rely heavily on various types of information for their operations, making it a valuable asset that needs to be protected [GTA+22]. The potential damage resulting from information being inaccessible, inaccurate, or exposed to unauthorized entities underscores the importance of implementing appropriate security measures. Identifying and valuing this information is crucial for optimal resource utilization, informing the type and extent of the required security measures.

In the petroleum industry, the availability of OT systems stands as one of the most valuable assets. The convergence of IT and OT within critical infrastructure, however, introduces an increased level of complexity. This escalates the challenge of accurately identifying all assets which together form a value chain [NSMa]. Complexity and interdependencies in value chains directly amplify a company's vulnerabilities. As dependencies increase, so does the risk of chain reactions from a single incident. The intricate nature of these value chains can make it difficult to identify responsible actors and system ownership, potentially leading to uncontrolled incidents that can halt critical processes.

In order to mitigate risks, a company must establish effective processes for recognizing valuable assets and their roles within the organization. This is a complex, time-consuming task, with varying practices across companies and sectors. In many cases, security measures may not be adequately tailored due to this complexity [GTA+22]. Hence, the focus should not be exclusively on the assets of a company, but also on the vulnerabilities within these assets that could be potentially exploited by threat actors, causing significant exposure of these valuable assets.

2.5.2 Threats

When talking about threats in this study, we talk about cyber threats which are «a circumstance or event that has or indicates, the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society» [DNV17].

Determining the threat landscape in cyber security is a complex task that extends beyond just the numerical quantification of risk. The petroleum sector, specifically, faces significant challenges in identifying weaknesses, dependencies, and potential damage. This means there are many qualitative aspects that cannot be accurately quantified or effectively communicated [GTA+22].

A more detailed analysis of the threat landscape is explained in Section 2.6, providing insights into historical attacks against ICS. Furthermore, the same section discusses threat assessments, offering an overview of different threat actors and their capabilities.

2.5.3 Vulnerabilities

DNV-RP-G108 defines a vulnerability as a «flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy» [DNV17].

The dark figures survey (Mørketallsundersøkelsen) 2022 reveals that 40% of those impacted by cyber incidents stumble upon them coincidentally [Nær22]. This is due to the increasing interconnectivity between systems, closer ties between IT and OT, augmented automation, and a general rise in digitization. The complexity and interconnectedness of these value chains may elevate vulnerability levels, as highlighted in [DNV22] and [Zio16].

Vulnerabilities Potential Leading to ICS Attacks

ICS are vital to the operation of critical infrastructure, such as power plants, water treatment facilities, and oil and gas fields. Because they control physical processes and operations, attacks on these systems can have real-world consequences, making them an attractive target for adversaries looking to cause disruption, damage, or gain control of significant systems [JWBK21]. Later Section 2.6.1 will present attacks on ICS that are possible to perform due to different aspects. Common for all of them is that they have exploited vulnerabilities within their targets. Some of the most typical vulnerabilities are «related to remote access, incorrectly installed/configured software, use of standard passwords, open protocols, incorrectly installed equipment such as firewalls, ports, and services open to the outside, operating systems that do not have the most recent updates, etc.» [GTA+22].

The three broad categories of vulnerabilities that these systems may face include human, technological, and organizational vulnerabilities [GTA+22]. The vulnerabilities to ICS can often be described by factors such as the complexity and diversity of systems, the use of legacy systems, increasing network connectivity, the motivation of attackers, and a lack of awareness and training among workers.

Human Vulnerabilities

Human vulnerabilities often come from the complexity and diversity of systems and a lack of awareness and training among employees [DMT+19]. These systems are often complex, each with unique vulnerabilities that can be difficult for untrained workers to navigate. Employees may have an inadequate understanding of facilities, processes, threat landscapes, attack vectors, and cyber security concepts. This lack of knowledge can lead to human errors that expose the system to significant security risks. Additionally, a poor grasp of work requirements, guidelines, and secure work practices can further compound the risk.

Technological Vulnerabilities

Technological vulnerabilities are influenced by the complexity of ICS, the use of legacy systems, and the increased network connectivity as part of the Industrial Internet of Things (IIoT). Many ICS in the petroleum industry are built on older technologies that were not designed with modern cyber security threats in mind [OBH+21]. This could lead to an increased number of vulnerabilities due to outdated software, old operating systems, and proprietary protocols, all of which could be exploited by attackers [GTA+22]. Furthermore, the increased connectivity exposes ICS to the same types of threats faced by traditional IT systems, including cyber intrusions and malware.

Organizational Vulnerabilities

Organizational vulnerabilities can be increased due to the high motivation of attackers and a lack of awareness and training among workers [DMT+19]. Given the high potential impact of a successful attack on ICS, these systems are attractive targets for attackers, including state-sponsored actors engaging in cyber warfare or espionage. A successful attack could cause significant real-world damage or disruption. At the organizational level, a lack of proper training and awareness among employees can make it easier for these attacks to be successful. Inadequate information security requirements, a lack of clearly defined responsibilities within cyber security, and a poor security culture can all contribute to an insecure environment and result in security lapses [GTA+22].

Given the critical nature of the petroleum industry, these vulnerabilities can have significant implications. A successful cyber-attack could cause disruption, damage, or even gain control of critical systems, leading to significant economic loss and potential safety hazards [GTA+22]. Therefore, a clear understanding of these vulnerabilities is essential for comprehensive risk assessment and the development of robust security strategies.

2.5.4 Barrier Management

In the petroleum industry, often when doing a risk assessment a common theme is to talk about barrier management. Barrier management is «Coordinated activities for establishing and maintaining barriers so that they fulfill their functions at all times» according to the PSA [Nor17], Further, they define a barrier as «A measure intended to identify conditions that may lead to failure, hazard and accident situations, prevent an actual sequence of events occurring or developing, influence a sequence of events in a deliberate way, or limit damage and/or loss».

Barrier elements can be technical, organizational, or operational according to the PSA [Nor17]:

- Technical barrier element: Equipment and systems involved in the realization of a barrier function.

- Organizational barrier element: Personnel with defined roles or functions and specific competence involved in the realization of a barrier function.

- Operational barrier element: The actions or activities that personnel must perform in order to realize a barrier function.

Sopra Steria argues that «...that without a good overview of threats, vulnerabilities, and assets, it will be a very challenging task to identify appropriate measures and barriers» [GTA+22]. So, a comprehensive risk assessment is necessary to identify the different types of barriers. Measures and barriers are often talked about interchangeably in this thesis. One of the tools used to get an overview of barriers and to analyze and visualize risk scenarios is the bow-tie model [Nor17].

Bow-Tie Model

One useful strategy in barrier management is placing barriers in a bow-tie diagram. This diagram, fittingly named for its shape, uses the central «knot» to depict a possible incident or unwanted event. Threats leading to the undesired event are positioned on the extreme left of the bow tie, depicted as a phishing mail in Figure 2.5. In the same figure, the possible consequences of the event are situated on the extreme right.

A bow-tie diagram serves as a visual representation of how barriers can be integrated into a system. Depending on whether they are introduced before or after the occurrence of an undesired event, a barrier can be either proactive or reactive. A proactive barrier aims to prevent an event from happening, while a reactive barrier aims to mitigate the consequences if the event has already occurred. It is important to note that barriers can be proactive or reactive irrespective of whether the barrier element is technical, operational, or organizational.

The bow-tie model, seen in Figure 2.5, shows how a risk assessment of security measures can be implemented in a barrier diagram. The reason behind risk assessment is to identify conditions that can lead to failure, hazard, and accident situations [Nor17]. In the model, the barriers are visually represented as red columns. The preventive measures depicted can be utilized to shape companies' security plans, whereas the reactive measures can aid in formulating emergency plans. One of the preventive barriers can be translated to risk assessment, which plays a crucial role in identifying potential threats and determining appropriate preventive actions to mitigate them.

2.6 The Threat Landscape

The number of cyber attacks against Industrial Control Systems (ICS) is on the rise, and adversaries target oil and gas companies more frequently than ever before [PST20]. It is crucial for the industry to stay updated on the current threat landscape to effectively prepare for potential attacks. By examining past incidents and attacks, the sector can gain insights into the relevant threats. This knowledge enables companies

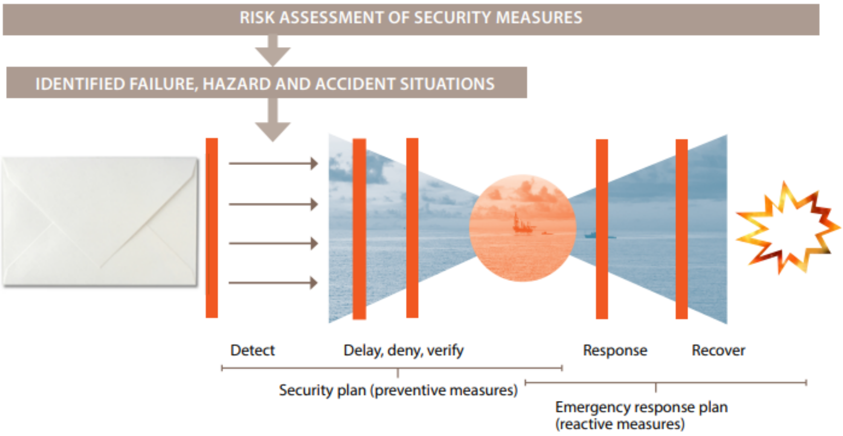

RISK ASSESSMENT OF SECURITY MEASURES
IDENTIFIED FAILURE, HAZARD AND ACCIDENT SITUATIONS
Detect
Delay, deny, verify
Response
Recover
Security plan (preventive measures)
Emergency response plan
(reactive measures)

Figure 2.5: Principles for barriers used for security. Adopted from [Nor17].

to develop scenarios and conduct exercises to better prepare themselves against such attacks.

To gain insight into the current threat landscape, we conducted a comprehensive analysis of previous incidents. These findings are presented in Subsection 2.6.1 before a detailed threat assessment is presented in Subsection 2.6.2.

2.6.1 Examples of Cyber Attacks Against ICS

The targeting of ICS by cyber attacks is not a new phenomenon, as threat actors continuously seek new methods to exploit industries and critical infrastructures [Inc23]. In this section, we will highlight some of the most notable and severe cyber attacks that have specifically targeted ICS systems regardless of their sector. Table 2.2 provides an overview of past attacks, including those mentioned in [DAN21], as well as relevant additional cases such as CrashOverride, Solarwinds, Colonial Pipeline, Industroyer 2, and Pipedream, which are of particular relevance to this thesis. The table includes information on the year, name, type of attack, and the affected target(s). The most relevant attacks are highlighted in yellow in Table 2.2.

Stuxnet

Stuxnet, cited as «the first confirmed example of ICS tailored malware leveraged against a target» [Inc17], utilized a highly sophisticated computer worm to specifically

Table 2.2: Table of Attacks based on [DAN21] with relevant additions

Year	**Name**	**Type of Attack**	**Target**
2010	**Stuxnet**	Malware	Iranian Nuclear Facilities
2011	Water Utility Company	Cyber Intrusion [Kre11]	US Water Facility
2012	Smart Meters	False Data Injection [Int12]	Puerto Rican Electric Power Authority (PREPA)
2013	Havex	Malware	IACS in the U.S
2015	Blackenergy	Malware	Human Machine Interfaces (HMIs) in IACS
2015	BMW	Cyber Intrusion [Wil15]	BMWs equipped with Connected Drive
2015	Sniper Rifle	Cyber Intrusion [Gre15]	TrackingPoint self-aiming rifles
2016	**CrashOverride**	Malware	Electric Power Grid Systems
2017	**Trisis/Triton**	Malware	Safety Instrumented System (SIS) in the oil and gas sector in the Middle East
2020	**Sunburst(Solarwinds)**	Supply Chain Attack	The software company SolarWinds. US agencies
2021	Florida Water Treatment	Cyber Intrusion [Kar21]	Florida Water Treatment Facility
2021	**Colonial Pipeline**	Ransomware	American Oil Pipelines Company
2022	**Industroyer2**	Malware	Electric Utility Provider in Ukraine
2022	**Pipedream**	Malware	Not yet deployed

target Iran's uranium enrichment operations. By exploiting zero-day vulnerabilities, the attack successfully caused operational degradation to the centrifuges. This incident exemplifies the potential impact of malware on the interconnection between IT and OT. It demonstrates how an adversary can sabotage a company's OT system through their IT system, resulting in damage to both domains.

CrashOverride

«CRASHOVERRIDE is the fourth ever piece of ICS-tailored malware (STUXNET, BLACKENERGY 2, and HAVEX were the first three) used against targets and the second ever to be designed and deployed for disrupting physical industrial processes (STUXNET was the first)» [Inc17].

CrashOverride, also known as Industroyer, was a highly sophisticated malware framework developed by the threat group Electrum [Inc23] and used in the 2016 Ukraine power event [Slo19]. It targeted electric transmission operations, encoding process manipulation to create hazardous conditions. By disabling control and Supervisory Control and Data Acquisition (SCADA) systems, removing visibility, and exploiting vulnerabilities in protective relays, it aimed to cause physical equipment damage. While it did not fully succeed, CrashOverride displayed increased ambition and potential for extended disruption, emphasizing the need for process integrity and protection in critical infrastructure.

Trisis/Triton

Trisis, also known as Triton, emerged in 2017, targeting a Saudi Arabian oil and gas refinery. It aimed to gain undetected control over Schneider Electric Triconex Safety Instrumented System (SIS) and enabled arbitrary modifications to the SIS, potentially causing plant shutdowns or removing safety controls [Slo19]. The attack, although not highly scalable, serves as a blueprint for adversaries targeting SIS and represents an escalation in the type of attacks seen to date. It specifically focuses on compromising the safety function of the process, highlighting the increasing sophistication of industrial cyber attacks.

Solarwind

The SolarWinds attack, also referred to as the SUNBURST attack, was a highly sophisticated and significant cyber attack that came to light in December 2020. Although it did not specifically target ICS, its impact reached various sectors, including government agencies and private organizations. SolarWinds, an American software company, was utilized as the attack vector in this instance [Wil20].

The attack involved targeting users of SolarWinds Orion products, which are widely used by over 300,000 customers, including actors in critical infrastructures and the U.S. Government [Wil20]. By compromising SolarWinds' software update process, the threat actors were able to distribute a malicious software update to more than 18,000 private and government users. This breach granted them network access and allowed them to monitor internal emails at prominent US agencies [Pau20].

The SolarWinds attack, categorized as a supply-chain attack, did not have a direct focus on ICS. Nevertheless, it took advantage of SolarWinds' trusted role as a supplier to infiltrate and gain unauthorized access to its customers' networks. This type of attack brings forth notable concerns for industries, particularly those heavily reliant on vendors for various components of their ICSs, such as the petroleum sector. The incident highlights the potential risks associated with supply-chain vulnerabilities and emphasizes the need for heightened security measures in industries relying on external vendors for critical infrastructure components.

Colonial Pipeline

The Colonial Pipeline attack in May 2021 resulted in a significant disruption to the gas pipeline system along the East Coast of the United States [Ker22]. The attack, carried out by the DarkSide group, involved ransomware and led to the shutdown of the pipeline for several days. The incident impacted consumers, airlines, and fuel supplies [Ker22]. The root cause of the attack was traced back to an exposed password for a VPN account. Despite official guidance recommending against it, Colonial Pipeline made the controversial decision to pay the ransom [SW21]. The incident highlighted the importance of securing critical infrastructure and the need for robust cyber security measures.

Industroyer 2

In April 2022, an electric utility provider in Ukraine was targeted by Industroyer 2, a variant of the original Industroyer (CrashOverride) malware. Industroyer 2 is the sixth known ICS-specific malware and continues to focus on industrial control systems in the electric utility sector. This incident is significant because it involved the reconfiguration and redeployment of ICS-specific malware in an electric utility environment previously impacted by CrashOverride in 2016 [Inc23].

Electrum, the group behind the attack, had previously used malware in the 2016 Ukrainian ICS electric grid attack. Industroyer 2 is a newer variant with reduced capabilities, but it utilizes the IEC 104 protocol to manipulate Information Object Addresses (IOA). By changing the state of IOA, the malware can toggle physical breaker statuses between open and closed, resulting in disruptive effects on the targeted infrastructure [Inc23].

Pipedream

In 2022, a new modular malware called Pipedream emerged as a significant advancement in ICS attacks. Developed by the threat group Chernovite, Pipedream targets industrial control systems managing critical infrastructure, potentially impacting tens of thousands of devices across sectors such as electrical grids, oil and gas pipelines, water systems, and manufacturing plants [Inc23].

Pipedream, the seventh and last ICS-impacting malware as of the time of writing, is the first cross-industry ICS malware with disruptive capabilities, posing a supply chain risk. It has the ability to execute 38 percent of known ICS attack techniques and 83 percent of known ICS attack tactics [Inc22a]. This demonstrates its wide-ranging impact and effectiveness in compromising ICSs.

Dragos and partners discovered and analyzed Pipedream before it was employed, offering an opportunity for proactive defense [Inc23]. While Pipedream represents a significant escalation, no known deployment has occurred, providing a chance for defenders to prepare and strengthen their defenses against this emerging threat.

2.6.2 Threat Assessment

The threat landscape is ever-evolving, but to get an overview of the current threat landscape the industry is facing today, different threat assessments have been evaluated. These assessments provide insight into the threat landscape trends based on past incidents and widespread risks across different sectors. We examined one evaluation specifically from the oil and gas industry, while the others offered a more universal perspective applicable to all industries. By studying these, we were able to compile a comprehensive overview of the present-day threats as identified by various actors. The following assessments were used:

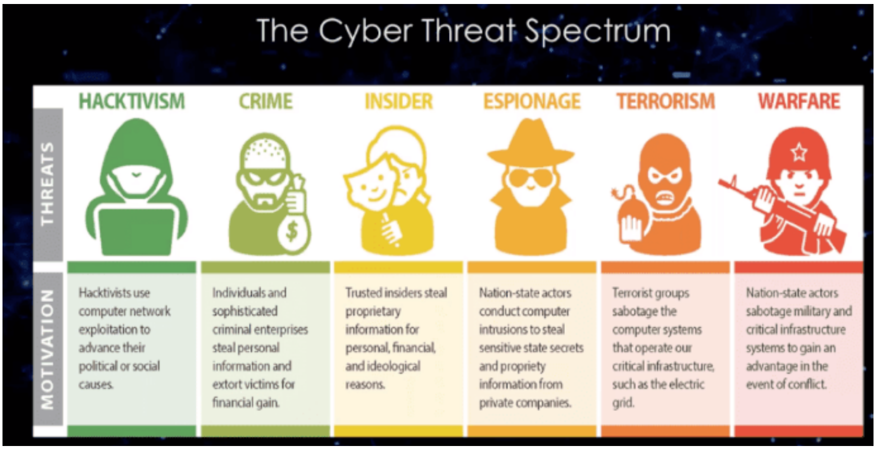
Title	Title in Norwegian	Publisher
ICS/OT CYBERSECURITY YEAR IN REVIEW 2022	-	Dragos [Inc23]
The Threat of Intelligence Against the Norwegian Petroleum Sector	Etteretningstrusselen mot norsk petroleumssektor	The Norwegian Police Security Service (PST) [PST20]
National Threat Assessment 2023	Nasjonal Trusselvurdering 2023	PST [PST23]
Risk 2023	Risko 2023	NSM [NSM23]
Focus 2023 - The Intelligence Service's assessment of current security challenges	Fokus 2023 - Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer	Norwegian Intelligence Service (NIS) [NIS23]

Table 2.3: Cyber Threat Reports (Rapporter om Cybertrusler)

This subsection will look at the different threat actors presented in the various assessments. In addition, it will emphasize and evaluate the highlighted threats within these documents to give a clear understanding of the current state of the threat landscape.

Threat Actors

Threat actors, in the context of cyber security and the assessment, refer to an individual, group, or entity with the intent of causing harm and presenting a risk against the security and stability of a system, network, or organization. Usually, they are grouped into categories based on their motivation and capabilities. In Figure 2.6, The Cyber Threat Spectrum, the threats the different actors present are organized in colors from left to right where the capability and potential harm increase along the way.



The Cyber Threat Spectrum

THREATS	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Figure 2.6: The Cyber Threat Spectrum. The figure is adopted from [Mor19].

The first group, hacktivism, has a broad range of actors, from script kiddies to cyber criminals, but common for all of them is that their capabilities are low and limited [BJD17]. Moving on, organized criminals have moderate capabilities [BJD17] and can be viewed as an overlap between crime and insider mentioned in Figure 2.6. Here the motivation is often driven by financial or personal gain.

At the far end of the spectrum, we encounter activities such as espionage, terrorism, and warfare, which can be classified as Advanced Persistent Threats (APTs). APTs are highly sophisticated and targeted cyber attacks typically carried out by state-sponsored actors or nations. Figure 2.6 provides insights into the motivations behind each APT. Common for all of these is that they possess significant capabilities and abundant resources to execute their operations.

The Dragos *ICS/OT CYBERSECURITY YEAR IN REVIEW 2022* report [Inc23] provides an extensive analysis of both established and emerging threat groups as of the end of 2022. Some of them are further examined in Subsection 2.6.1 along with the attack(s) they have carried out.

Beyond the entities referenced in [Inc23], PST, NSM, and NIS all underscore the significant influence of nations as key threat actors. Russia and China, in particular, are consistently brought up in these discussions, as noted in [PST23] and [NIS23].

Threat Intelligence

From their document on threat intelligence in November 2020, PST said that «In the next 18 months, it is expected that the intelligence activity against the Norwegian petroleum sector will persist» [PST20]. This has continued and the national threat assessment of 2023 states that Norway currently faces a multifaceted threat landscape from the intelligence agencies of various countries operating within its borders. The most significant concern is the Russian intelligence services, which are seen as the largest threat this year [PST23]. These agencies employ a wide array of methods including digital network operations, covert acquisition activities, and recruitment of local sources. Even though a Russian sabotage operation in 2023 is considered unlikely by PST, the risk could increase with escalating tensions between Russia, NATO, and the West.

Insider Risk

In their latest available security report [Mne21], Mnemonic emphasizes that industries, such as the petroleum sector, which possess critical assets, face significantly elevated risks when it comes to insider threats. It is important to distinguish between intentional and unintentional insiders. According to the report, intentional insiders are individuals within an organization who purposefully misuse their access to cause harm, driven by motives such as financial gain or revenge. On the other hand, unintentional insiders pose a threat due to negligence or lack of awareness, inadvertently causing harm, for instance, by falling for a phishing scam or accidentally sharing sensitive information.

NSM emphasizes the risk associated with an insider in their annual risk assessment report for 2023 [NSM23]. The focus of this assessment is primarily on intentional insider threats, and security authorities pay a lot of attention to insider risks. Insider threats can emerge at any stage during an individual's employment, making measures like background checks or security clearances insufficient as standalone strategies to mitigate this risk. Further insight on how to handle insider risk can be viewed in this report by the PSA [DNV19].

Humans as the Weakest Link

Phishing attacks will remain the most straightforward and frequently employed approach to acquire information about individuals or businesses [NSM23]. NSM continuously observes the exploitation of human, technological, and organizational vulnerabilities to facilitate malicious cyber operations against multiple Norwegian enterprises.

In order to execute attacks similar to those mentioned in subsection 2.6.1, threat actors attempt to exploit vulnerabilities such as weak passwords, outdated software, and the absence of two-factor authentication to gain unauthorized access to ICT systems.

Rather than directly targeting the networks of organizations, these threat actors exploit individuals and third-party services that businesses rely on, as they are considered easier targets compared to the primary objectives. The NSM report Risk 2023 [NSM23] emphasizes the need for the petroleum sector to mitigate vulnerabilities and make it more challenging for threat actors to carry out their activities. Therefore, it remains crucial to maintain awareness of these «simple» types of attacks that exploit the human factor and prioritize training and awareness programs for employees.

Malware and Ransomware

The discovery of Pipedream as the seventh ICS-impacting malware, as mentioned in Subsection 2.6.1, highlights an alarming trend. According to the Dragos report [Inc23], Chernovite's Pipedream toolkit possesses the capability to impact tens of thousands of critical infrastructure-controlling industrial devices. Table 2.2 clearly demonstrates a steady increase in ICS malware since the initial Stuxnet incident, indicating a growing reliance on malware-driven attacks. Notably, both Industroyer 2, which reconfigured and redeployed a previous ICS malware, and Pipedream represent the constant evolution of new malware and its ability to find innovative pathways to target ICSs.

Ransomware attacks, a type of malware, on industrial infrastructure organizations nearly doubled in 2022, with a staggering 87 percent increase, according to cyber security firm Dragos [Inc23]. Over 70 percent of these attacks specifically targeted manufacturing entities across various subsectors. The escalating ransomware activity heightens the risk for OT networks, particularly those lacking proper segmentation. Colonial Pipeline mentioned in Section 2.6.1 is just one of many examples of ransomware attacks against critical infrastructure. It is crucial to implement robust cyber security measures and network segmentation to counter the growing threat of ransomware attacks on industrial systems.

2.7 Related Work

The presented literature has played a significant role in developing the interview guide, alongside the material presented in Table 2.1, Table 2.3, and Table 2.5. It has also served as the foundation for acquiring knowledge to shape this chapter and adequately prepare for the semi-structured interviews (presented in Section 3.4). The objective here is to engage in a smooth and meaningful dialogue with the candidates, where the interviewer can ask relevant follow-up questions as necessary. Therefore, it is vital for us as interviewers to possess a sufficient understanding of the subject matter to ensure a productive conversation.

This section presents related work conducted on ICT security in the petroleum sector. Table 2.4 summarizes analyzed literature done to familiarize ourselves with the sector in regards to our problem description and RQs. All of the literature is described with title, author(s), type of publication, and focus area(s) relevant to our study.

Table 2.4: Overview of relevant literature

Title	**Author(s)**	**Type**	**Focus area(s) relevant for our study**
A Systematic Mapping Study on Cyber Security Indicator Data [MTE+21]	Meland et al.	Article	Security indicators for estimating Cyber Risk
IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience [Con16]	Conklin	Document	IT/OT, Security/Safety, Resilience
Critical Infrastructures Vulnerability and Risk Analysis [Zio16]	Zio	Article	Risk, Critical Infrastructures
The Cyber Priority [DNV22]	DNV	Report	ICS, Cyber Security, Threats
Operational Technology and Information Technology in Industrial Control Systems [Hah16]	Hahn	Book	OT/IT, ICS
How to Improve the Security Awareness in Complex Organizations [DMT+19]	De Maggio et al.	Article	Security awareness, Critical infrastructure protection

Continued on next page

Table 2.4 – *Continued from previous page*

Title	**Author(s)**	**Type**	**Focus area(s) relevant for our study**
Oil and Gas 4.0 era: A systematic review and outlook [LGAH19]	Lu et al.	Article	Oil and Gas 4.0, IIoT, Digitization
Security and Independence of Process Safety and Control Systems in the Petroleum Industry [OBH+22]	Onshus et al.	Article	Independence, Security, Safety
Quantitative Risk Reduction Estimation Tool for Control Systems [MBFA06]	McQueen et al.	Preprint for Journal	Risk Estimation, Control System Security, Network Security
A systemic approach for preliminary risk analysis of cyber security of Industrial Control Systems [FG21]	Flaus, Georgakis	Document	cyber security, Systemic, Risk analysis
cyber security of Offshore Oil and Gas Production Assets Under Trending Asset Digitalization Contexts: A Specific Review of Issues and Challenges in Safety Instrumented [ZL21]	Zhu, Liyanage	Article	cyber security, IACS, SIS Systems

2.7.1 Knowledge Reports

This subsection presents an overview of relevant knowledge reports that align with the scope of our master's thesis.

In recent years, the PSA has ordered several knowledge reports on various aspects of ICT security prepared by Sintef [PSA21a], DNV [PSA20], and Sopra Steria [PSA21b]. These reports aim to enhance understanding of the petroleum sector, identify relevant issues, and address necessary defenses to ensure robustness against cyber threats. We have extensively utilized these resources to gain a comprehensive understanding of past and potential future efforts in addressing cyber security within the petroleum sector. The most relevant ones for our research questions are presented in Table 2.5.

A Sintef project for PSA involving six reports to research various aspects of the topic of ICT security – robustness in the petroleum sector [PSA21a] was conducted in 2020, where 4 of them are relevant and included in our research, number 1-4 in Table 2.5. Also, a newer report - ICT Security and Independence - have been included in the literature review, number 5 in table 2.5.

Table 2.5: Knowledge reports - title and brief description

No	Title and description	Ref.
1	**Regulation of ICT security in the petroleum sector (SINTEF, 2021)** The objective of this report is to provide clarity on the regulatory landscape governing ICT security in the petroleum industry, encompassing current regulations, recognized standards, norms, and guidelines. Additionally, the report aims to clarify the expectations of regulatory authorities, as well as provide an overview of the recent developments and status of initiatives concerning ICT security within the petroleum industry. By doing so, this report aims to assist petroleum companies in enhancing their own practices related to ICT security in industrial ICT systems, while adhering to existing regulations. Furthermore, it can serve as a foundation for a PSA memorandum on ICT security.	[ØBJ+21]
2	**Principles of digitalization and IT-OT integration (SINTEF, 2021)** The objective of this report was to illustrate and evaluate the impact of digitalization and the adoption of cloud services on industrial ICT systems, as well as the necessary security measures to ensure their safe utilization. The regulations implemented by the PSA are mainly focused on the principles of segregation and independence, which serve as fundamental strategies for ensuring safety and security. This report focuses on the ongoing digitalization of both existing and new facilities, drawing on information gathered from drilling companies and operators.	[HOJ+21]

No	Title and description	Ref.
3	**Data quality in digitalization processes in the petroleum sector (SINTEF, 2021)** The main aim of this report is to investigate the data sources and types utilized within industrial ICT systems, as well as the processes involved in handling and preparing the data before it is made accessible within an office network. The report explores the strengths and vulnerabilities associated with data quality and data security. Data quality revolves around ensuring timely access to relevant data. Numerous factors impact data quality in ICT systems, such as data integrity, accuracy in data acquisition, reliability in data transmission, and the surrounding environment.	[MOL+21] **NB:**Report only available in Norwegian
4	**Core principles of ICT security in industrial ICT systems (SINTEF, 2021)** The purpose of this report is to enhance the industry's understanding of how to implement NSM's core principles for ICT security (version 2.0) within industrial ICT systems in the petroleum sector. It also evaluates relevant aspects of the Norwegian Water Resources and Energy Directorate's Power Preparedness Regulations. The report identifies specific measures within the NIST cyber security Framework (CSF) that are applicable to OT systems, but not explicitly covered by the core principles.	[JWBK21] **NB:**Report only available in Norwegian
5	**ICT Security and Independence (SINTEF, 2021)** This report examines the regulations of the PSA in terms of system independence in the face of future technical solutions. It emphasizes the need for improved system independence and cyber security measures in the petroleum industry, particularly due to the increasing offshore-to-onshore information transfer. The report also advocates for the expansion of the definition of barriers in regulations to include information security, referencing the IEC 62443 series.	[OBH+21]

No	Title and description	Ref.
6	**Regulations and audit methodology (DNV GL, 2020)** The objective of this report was to evaluate the suitability of the PSA's existing regulatory framework concerning ICT security and the associated threat landscape. Another goal was to examine the suitability of the PSA's audit methodology for ICT security, considering the range of audit objects and the current threat scenario.	[GL20b] **NB:**Report only available in Norwegian
7	**Cyber security SIS and intrinsically secure components, communication protocols (DNV GL, 2020)** This report focused on the incorporation and maintenance of ICT security in Safety Instrumented Systems (SIS), from design to commissioning and operation. A crucial element of the project was to evaluate the application of security principles as outlined in IEC 61508/511 and IEC 62443. Additionally, the partial delivery discusses trends and advancements in industrial ICT systems, particularly concerning network-based components.	[GL20a] **NB:**Report only available in Norwegian
8	**Resilience to cyber incidents and can blockchain contribute? (DNV GL, 2020)** The report describes how resilience, along with related techniques, can be harnessed to increase the security and thus the robustness of industrial ICT systems. It further discusses the application of ICT security principles in the context of blockchain technology, exploring how the adoption of blockchains can safeguard and potentially enhance security. Additionally, the report assesses whether, based on the latest information and research, blockchain can positively impact resilience and pave the way for innovative strategies that boost cyber security within industrial ICT systems (OT) and at the intersection between IT and OT.	[GL20c] **NB:**Report only available in Norwegian

No	Title and description	Ref.
9	**Protection of data at rest and in transit (Sopra Steria, 2022)** This report summarizes the challenges and opportunities in data protection within the petroleum sector amid digital technology advancements. The focus is on safeguarding data at rest and in transit, acknowledging the complexities and vulnerabilities introduced by Industry 4.0, which tightly integrates Operational Technology with Information Technology and cloud services. The discussion emphasizes the sector's need for strengthened knowledge development, risk management, and security practices to navigate the shifting threat landscape and ensure robust information and IT safety.	[GTA+22]

Chapter 3 Methodology

In this master's thesis, two primary methods were employed. Firstly, a literature review was carried out to gain a comprehensive understanding of the topic, before semi-structured interviews were conducted to gather new insights into the industry. The goal is to contribute to the field by providing an updated perspective and suggesting future directions. By doing this we hope to be able to answer our RQ.

This chapter begins by presenting the preliminary work conducted in the thesis (Sec. 3.1). It then provides an overview of Design Science and how this research method is applied in our study (Sec. 3.2), followed by the Literature Review discussed in Section 3.3. Additionally, the Interview Process and its implementation are described in Section 3.4, while the data analysis method is presented in Section 3.5. The chapter concludes with Sections 3.6 and 3.7, which address the Challenges and Limitations, as well as the Ethics associated with this master's thesis.

3.1 Preliminary Work

Our preliminary work for this project has been rewarding, including attending the Industry Forum for Cybersecurity of Industrial Automation and Control Systems (CDS-forum) [SINa] and completing the specialization project TTM4502 beforehand [NTN]. Attending the CDS-forum provided us with the latest information and insights on different topics in the oil and gas field. The forum also allowed us to network with industry professionals and peers, which has proven to be invaluable for our project.

In addition to attending the conference, we also completed a specialization project. This project allowed us to gain a wider understanding of the unique cyber security challenges faced by companies in the petroleum industry, such as data breaches, industrial espionage, and cyber-attacks. This foundation of knowledge and experience has contributed to the related work presented in section 2.7, but also to the literature review.

Overall, our preliminary work has been essential in preparing us for conducting the master's thesis. It has allowed us to gain a better understanding of the subject matter, identify potential gaps in knowledge or areas that require further exploration, and develop both research and interview questions. We are confident that our preliminary work has helped us get a good foundation for further working on the thesis.

3.2 Design Science

Our thesis seeks to explore the current petroleum sector and how the risk associated with cyber security is assessed, but also how it can be assessed going forward. Therefore, we want to use existing knowledge, risk assessment, the threat landscape, and the current state of the sector, to be able to derive new methods and find areas of improvement for the petroleum industry. However, to be able to do this a research approach that is well-organized and rigorously examined is necessary. One such method is design science [JP14], which is about a special strand of design research which «In contrast to empirical research, ... is not content to just describe, explain, and predict. It also wants to change the world, to improve it, and to create new worlds». This method is a research approach commonly used in Information Systems and Software Engineering [Wie14] that involves the iterative creation, testing, evaluation, and refinement of an innovative artifact.

Artifacts are designed by humans to address specific issues and to solve a problem by interacting with their «context». These artifacts can manifest as hardware, software, organizational structures, or methodologies. Context refers to any entity that interacts with or influences an artifact, and can include individuals, values, concerns, or even other artifacts. The problem context, which is the specific environment where the artifact is expected to foster an improvement, typically contains a mixture of these elements. In this thesis, the artifact is seen as a new or improved way of doing the risk assessment in the petroleum sector, where the context is represented by the petroleum sector itself. The problem context is the combination of the context and the constant threat of ever-evolving cyber threats against ICS in the oil and gas industry. Despite being proficient at risk assessment concerning safety, the industry faces shortcomings concerning security. There are several guidelines and standards for actors to utilize, but when it comes to addressing cyber security across the sector in a more holistic way, there are few resources. Therefore, the design science problem presented in this thesis can be framed as creating an artifact that effectively addresses the challenges posed by the problem context. In other words, it involves the design of both technological and non-technological solutions aimed at enhancing transparency and equipping the petroleum industry with effective tools to manage cyber security threats. The newly proposed artifact should effectively address the challenges that limited the effectiveness of original risk assessment methods, thereby providing a more robust solution.

Design science is a research approach that often is used when developing IT solutions by creating innovative artifacts to solve people's problems when working with ICT. On the other hand, design focuses on the visual and functional aspects of the artifact, while design science employs scientific methods and theories to create practical and scientifically grounded artifacts. It bridges the gap between theory and practice by addressing real-world problems. According to Johannesson and Perjons [JP14], this differentiation between design science and design necessitates three additional requirements in design science research:

Table 3.1: Requirements for Design Science

1. The use of rigorous research methods to generate knowledge of general interest.
2. Ensuring the new knowledge is connected to an existing knowledge base to guarantee its soundness and originality.
3. Communicating the new findings to both practitioners and researchers.

So, how do these requirements translate to the studies of this thesis? First, a research strategy and methods for data collection have to be chosen, including interviews, as well as analyzing the collected data. Additionally, the project must evaluate the artifact using appropriate research strategies and methods. For the master's thesis, qualitative research and semi-structured interviews have been chosen which can be read more about later in this chapter 3.4. Secondly, the project should connect its results with existing knowledge in the petroleum sector, including models, standards and guidelines, and practices. This allows for assessing the originality and validity of the project's findings. This master's thesis aims to present its results 4 in regard to the background knowledge acquired in the previous chapter (Sec. 2). Thirdly, the project should share its results with researchers and people within the sector through publications, presentations at conferences and fairs, and other relevant events. The master's thesis will be sent to all interviewees before publication for revisiting, and also be presented for SINTEF and their project on cyber security barrier management [SINb].

Another book on design science, by Wieringa [Wie14], highlights that the overall goal of design science is to reach the research goal, and for this thesis, it involves answering the RQs. Figure 3.1 shows the different aspects which are needed to reach this goal. For this study, the goal is to get an overview of the state of the art of the petroleum industry to improve the methods of assessing and managing cyber security risks going forward. The design problem in this context, as previously mentioned,

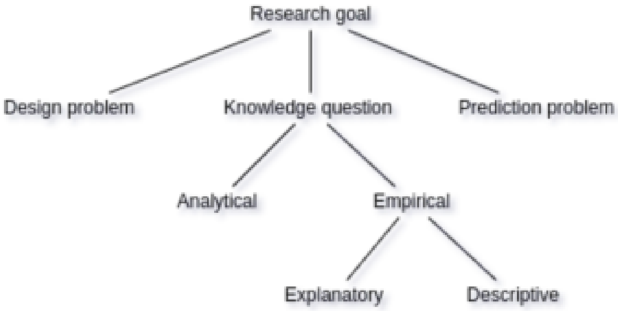


Figure 3.1: Design science architecture. Figure adapted from [Wie14].

is the development of an effective artifact, in the form of improved methods and models for assessing cyber security risks in the petroleum industry. Furthermore, the prediction problem is the difficulty in forecasting the ever-evolving nature of cyber threats to the petroleum industry's ICT infrastructure. When it comes to the knowledge questions, they serve a vital role in design science by providing additional knowledge that contributes to accomplishing the research goal. As shown in figure 3.1, knowledge questions can be classified into two main categories: analytical and empirical. Analytical knowledge questions are addressed through logical reasoning, conceptual analysis, and the utilization of existing theories or models [Wie14]. In contrast, empirical knowledge questions involve gathering and analyzing real-world data to draw conclusions and gain insights. Empirical knowledge can be divided into two types: explanatory and descriptive. Explanatory knowledge aims to answer the question of why a certain event occurred, while descriptive knowledge focuses on providing a straightforward account of what happened and when it took place. The choice between analytical and empirical approaches depends on the specific nature of the knowledge question and the availability of suitable resources and methodologies.

Due to the critical and sensitive nature of its operations and infrastructure, the petroleum sector typically maintains a level of discretion about its cyber security measures. This master's thesis involves reviewing articles, papers, standards, guidelines, and reports regarding the petroleum sector 2, but also valuable information gathering from interviewees with knowledge and experience in the sector. Therefore, most knowledge questions will have an empirical nature and answers, like for instance how the perceived shortcomings of the current cyber security measure are in the industry. Also, some knowledge questions will be answered analytically. In cases of ICS security standards not being up to date with the vulnerabilities locally identified, it requires analytical answers based on the architecture of the ICS. The architecture and the first of the three listed requirements will be combined going forward with this master's thesis to help derive new knowledge.

3.3 Literature Review

A literature review is carried out prior to conducting interviews for this thesis. The literature review serves as a foundation for gaining familiarity and knowledge about the research topic. By exploring relevant works, the literature review establishes a strong basis for understanding. Additionally, it aids in crafting insightful interview questions, thereby enhancing the overall quality and depth of the interviews. Figure 3.2 lists five steps for conducting a literature review according to the research guide from Georgia State University [Uni23b]. The five steps are also listed below:

Table 3.2: Literature Review Process

1. Choose your topic
2. Identify databases & resources
3. Search and refine
4. Read & analyze
5. Write the review

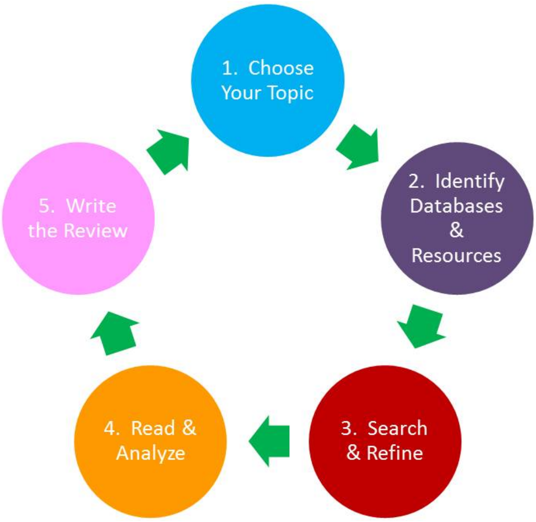


Figure 3.2: Overview of how to conduct a literature review according to Georgia State University. Adapted from [Uni23b].

1. Choose Your Topic

For the first step, we had to choose the topic. Our first step for our master's thesis was to choose a topic proposal, and the one we decided on was «Industrial cyber safety - securing critical infrastructure». However, already after the first meeting with our supervisors, we decide to scope it down to the petroleum sector. This has further been reduced to addressing cyber security in the petroleum sector on an operator level. This subject is timely and relevant given the increasing threats faced by the petroleum industry and the importance of cyber security in protecting resources, data, and infrastructure.

2. Identify Databases & Resources

Our main source of resources has been articles, papers, and reports relevant to both the petroleum industry and cyber security provided by our supervisors. These have been reviewed and presented in the related work section 2.7 in chapter 2. Since this literature is used at SINTEF and in projects like the Cybersecurity Barrier Management (CBM) project [SINb], it shows the relevance and reliability of those resources. We have cross-checked the credibility of the sources using other databases where they appear online, and Table 2.4 and Table 2.5 shows the identified resources. Furthermore, we have also identified databases like Google Scholar as a tool for searching a broad spectrum of articles across disciplines. Lastly, we have used standard.no to get familiar with standards, e.g. IEC 62443, but also used other resources to familiarize ourselves with other, different guidelines and recommendations presented in Section 2.4.

3. Search and Refine

Our primary literature has been the resources provided by our supervisors. We have also searched for secondary and supplementary materials within the databases and resources mentioned above. However, within the landscape of industrial cyber security, numerous participants produce valuable resources that may not be accessible via traditional academic search engines typically used for literature exploration. To find relevant background material, we considered various actors in the field of industrial cyber security, and have presented the types of these actors along with examples in Table 3.3, which were used during our literature search.

So, we have not used the method of literature review in terms of defining initial keywords for searching and refining our searches [Uni23a]. This has mainly been done in this manner due to the problem mentioned above, but also because this thesis' main area of data generation is down to interviewing different stakeholders in the petroleum industry. The literature review can give us insight into the state of the art of the sector, but since the industry is so complex it will not be complete without empirical results from the interviews. Therefore, we have chosen to not strictly follow the literature review guide provided by Georgia State University, but rather use valuable resources produced by actors mentioned in Table 3.3. The corresponding literature can be viewed in Chapter 2 and Table 2.3, Table 2.4, and Table 2.5.

Table 3.3: Actors in Industrial Cyber Security

Type of Actor	Examples
Private corporations in ICS cyber security	DNV, Sopra Steria
Private firms in threat intelligence	Dragos
Institutions in ICS cyber security	SINTEF
Organizations setting ICS cyber security standards	IEC, ISA, ISO
Organizations recommending ICS cyber security guidelines	Offshore Norge
Governmental agencies in national ICS cyber security	PSA, NIST
Norwegian Intelligence Services	NSM, PST, E-tjenesten

4. Read & Analyze

Even though we did not do the searching according to [Uni23b], the reading and analysis of the material have been extensive. This part has been one of the most significant parts of the literature review giving us sufficient knowledge and insight into how the petroleum sector operates. It has laid the foundation for our understanding before the interviews but also helped us feel comfortable enough to conduct semi-structured interviews where follow-up questions are a big part of the method. Additionally, the knowledge obtained will contribute to a more fluent dialogue and hopefully help the interviewees be more expressive when we as interviewers are familiar with the field of expertise.

5. Write the Review

The process of constructing our literature review can be broken down into two distinct phases. The initial phase involved acquiring a substantial body of knowledge before even beginning to draft the background chapter. This foundational work allowed us to provide a comprehensive overview of the Norwegian petroleum sector, highlight potential risks, and offer a discussion of relevant previous work. We highlighted these findings in Table 2.5, where we have summarized various reports and highlighted the existing gap between safety assessment and security assessment in the industry. Additionally, we read the material in Table 2.4 to help get an overview of the sector.

The second phase of our literature review process played a vital role in constructing our interview guide. The guide is not included in the thesis due to the disclosure of information regarding some of the questions. While this guide was initially developed based on our pre-existing knowledge, it underwent refinement and iterative enhancement after each interview, drawing on the insights we gathered. However, the literature review, as a foundational element, remained a pivotal component in the formulation of our interview questions. The entirety of the literature review process has been a crucial aspect of our research, shaping our comprehension of the present state of affairs and directing our exploration within this crucial sector.

3.4 Interview Process

The cornerstone of the data collection in this thesis lies in the insights gathered from key individuals involved in the Norwegian petroleum sector. Articles, papers, standards, and reports serve as useful resources providing plenty of background information about the sector's operations and its current stance on cyber security risk assessment. However, they can not entirely encapsulate the unique viewpoints of those directly operating within the industry. Understanding the complexities of cyber security measures and identifying opportunities for progress in an environment continuously shaped by evolving cyber threats necessitates direct dialogue with these key individuals. Their firsthand perspectives offer a valuable lens through which we can deeply understand the current cyber security state in the petroleum sector and pinpoint possibilities for innovative, effective solutions. Our second research question, concerning future directions for addressing cyber risk, will particularly benefit from these insights. However, the first research question, focused on addressing present-day cyber security, will also gain a more comprehensive understanding by providing a detailed overview of the current risk assessment strategies employed in the petroleum industry. This direct engagement will complement the literature review and will provide a more thorough answer to our research questions.

3.4.1 Qualitative Research

The first requirement mentioned in Table 3.1 emphasizes the importance of employing rigorous research methods to generate knowledge that is of general interest. In this context, qualitative research plays a significant role. Qualitative research has continually evolved since Paul Felix Lazarsfeld presented his perspective at the beginning of the 20th century, and he has subsequently been called *the father of qualitative research* [Bai14]. Through this master's thesis, we have experienced the considerable sensitivity of qualitative research to the context in which it is conducted. The use of qualitative methods is preferred as they provide a more descriptive understanding of the topic rather than simply presenting numerical data. Moreover, the importance of adjusting our own project, approach, ideas, and actions when encountering the sector and field we have studied has become evident [Tjo17]. In this thesis, we have chosen to work with semi-structured interviews, which we will explain now.

Semi-Structured Interviews

In the field of qualitative research, structured interviews and unstructured interviews sit at opposite ends of the spectrum. The former utilizes a rigid, preset list of questions, facilitating easy comparison across participants but restricting depth and adaptability. In contrast, the latter operates like a free-flowing conversation, offering great flexibility for deep dives into responses and unique insights, but it poses challenges when comparing data across different interviews.

Semi-structured interviews, *the best of both worlds* [Geo22], blend the advantages of both styles. They start with a preset list of questions but also grant the interviewer the liberty to delve deeper and explore unexpected areas of discussion. This method maintains a measure of consistency and comparability, while also providing the richness and flexibility of open-ended responses. The decision to use any of these styles hinges on the objectives of the research, the nature of the participants, and the resources at hand.

We assessed a variety of interview methodologies for our research. Initially, we considered structured interviews, but these were deemed excessively rigid, providing more of a numerical insight than a qualitative one. Given our literature review, we believed that such a formal approach may not deliver the right insights and the analytic knowledge questions could already be answered thanks to the literature review. On the flip side, we contemplated unstructured interviews, but these posed the risk of potentially overlooking key topics, as the interviewer could diverge from the main track. After this careful evaluation, we opted for semi-structured interviews. This format, with its balanced blend of structure and flexibility, ensures comprehensive coverage of all essential topics, while also granting participants the opportunity to introduce novel thoughts and ideas [Tjo17]. Furthermore, incorporating this form of qualitative research method can contribute to addressing the empirical knowledge questions outlined in Section 3.2. This, in turn, supports the overall research objective.

3.4.2 Data Management and Privacy

After settling on semi-structured qualitative interviews as our preferred data collection method, we proceeded to the following stages of the interview process: crafting an interview guide, registering our planned interviews with Sikt (formerly known as the Norwegian Centre for Research Data [NSD21]), identifying potential interviewees, conducting the interviews, and processing the resultant data. The interview guide is not provided due to privacy concerns relating to certain questions. Some questions are specific to the organization or individual being interviewed, and sharing these could potentially lead to the disclosure of sensitive information.

According to Wilson [Wil12], qualitative interviews can be executed in various ways, including in-person, via video call, or through voice call. The choice of video calls offered cost-effectiveness and convenience, eliminating the need for travel time and expenses. However, conducting interviews in a digital format does introduce potential challenges in communication due to the absence of physical cues, but also due to network issues. Given the geographical distance between us and our interviewees, most of our interviews were carried out via video calls using Microsoft Teams. Every interview was recorded, subject to the consent of the interviewees. The recordings were securely stored on NTNU's servers until the completion of the analysis, after which they were promptly deleted.

3.4.3 Selection of Interviewees

For selecting interview candidates, our primary approach involved utilizing the network established through the CDS-forum, as mentioned in Section 3.1. Initially, we sought assistance from our supervisors to acquire contact information, which proved to be effective in most cases. By leveraging both the CDS-forum and LinkedIn platforms, we identified individuals within relevant organizations whom we believed would be suitable for our study. Our key criteria for candidate selection revolved around their expertise and experience in the field, encompassing both cyber security and safety. We aimed to gain insights from these individuals regarding potential areas for improvement within the sector.

During interviews, we routinely inquired whether the interviewee possessed any contact information for individuals who were relevant to our research topic and were discussed during the conversation. This approach allowed us to expand our pool of interviewees and subsequently conduct interviews with a few additional individuals. Out of the desired participants, we were unable to engage with everyone we had initially intended to include. Nonetheless, we successfully gathered a diverse group of 10 participants for our study. Their selection was based on the valuable range of perspectives they could offer, and we were grateful that they agreed to be interviewed and share their experiences.

3.4.4 Arrangement of Interviews

After deciding the participants the arrangement of the interviews had to be decided. As mentioned earlier, video calls were used to conduct the interviews. Since we worked on the master's thesis full-time, we only needed the participants to find a time slot that worked for them. Based on this we used our NTNU mail to facilitate and invited them to a meeting through Microsoft Teams.

When including personal information in academic work, it is essential to obtain the required permissions from Sikt, formerly known as Norsk senter for forskningsdata

(NSD). Therefore, at the start of our work, we sent an application to Sikt and got it approved. In Appendix A the application can be viewed with the approval in Appendix B. Before the interviews, we provided information and a declaration of consent to each participant to make sure that all formalities were in order, as can be seen in Appendix C.

To effectively plan the interviews, we worked to develop an interview guide with relevant and targeted questions that would help address our research questions. Our approach involved initially identifying our own areas of curiosity, based on the literature review, and the specific information we sought to gather from both groups of interviewees: non-operator companies and operators. Throughout this process, we remained mindful of our research objectives.

Next, we structured the questions within the guide according to each research question, while also incorporating additional relevant inquiries as needed. While some questions were applicable to all participants, irrespective of their role as an authority or an operator, we ultimately divided the interview guide into two distinct parts. This division allowed us to tailor the questions to the unique perspectives and experiences of each group, resulting in separate sections for commercial actors/government representatives and operators within the guide.

3.4.5 Conducting the Interviews

Our chosen methodology for our project is semi-structured interviews, also known as in-depth interviews [Tjo17], as it appropriately aligns with our research questions that necessitate the collection of empirical data. This format is especially beneficial as it provides flexibility for questions that may arise spontaneously during the dialogue, which we as interviewers may not have conceived prior to the conversation. Such emergent inquiries could be essential for asking the interviewee to elaborate on certain topics they may touch upon during the conversation.

The semi-structured interview, as described by Tjora [Tjo17], follows a three-phase structure: the warm-up phase, the reflection phase, and the round-off phase. This can be seen in Figure 3.3. During the initial warm-up phase, the objective is to create an informal and comfortable environment for the interviewee [Tjo17]. The questions posed during this phase are intended to be simple and concrete, with little requirement for reflection. This phase includes preliminary steps such as seeking consent for recording the interview, presenting ourselves and our study, and asking the interviewee to provide their background.

Next, we move into the reflection phase, which serves as the core of the interview [Tjo17]. This phase seeks to engage the interviewee through open-ended questions, offering the interviewee an opportunity to share their experiences and knowledge.

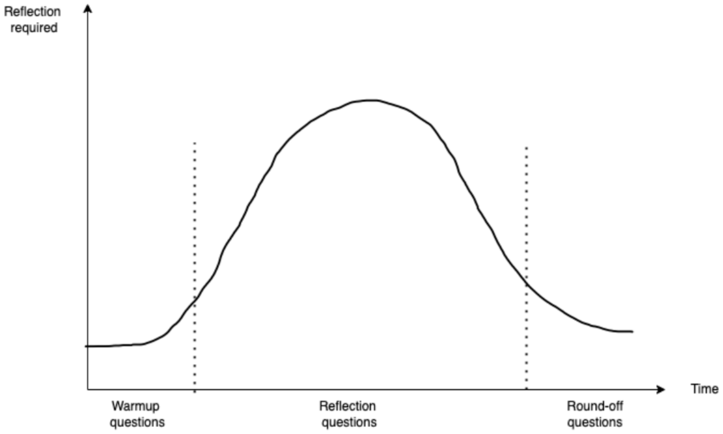


Figure 3.3: The interview process during a semi-structured interview. Figure adapted from [Tjo17].

According to Tjora [Tjo17], the estimated number of questions is three to six during an hour-long interview in this phase. Most of our interviews lasted between 45-75 minutes, and we had around 10 questions in total. Some of them can be categorized as a warmup or round-off questions, while some may also include follow-up questions to further clarify or delve deeper into the topics under discussion. Even though we had more questions than recommended, we are under the impression that we got answers to every question we had in all the interviews. This phase is crucial to thoroughly cover all research questions and ensure the reliability of results by asking the same set of questions to all informants. However, based on the specific categories the informants belong to, authorities/commercial actors or operators, we have tailored the interview guide, including category-specific questions and potential follow-up questions based on the organization.

In the last section of our interview, the round-off phase, we aim to lighten the conversation after the more in-depth reflection phase [Tjo17]. Any lingering uncertainties or misunderstandings are resolved here. We discuss what is next in the project, and if there would be a need for future discussions. Interviewees can voice any final thoughts or questions about the thesis or the interview process. Post-interview, we clarify how we plan to utilize their data and propose to share the segments of the thesis where their data appears. We strive to ensure they are satisfied with its representation. After each session, we review our approach, refining our questions for better clarity in subsequent interviews.

3.5 Data Analysis

Our data analysis drew inspiration from one of the methods described by Tjora in [Tjo17], a step-wise inductive methodology, to be able to present the result. In Figure 3.4, the first two steps are based on the methodology presented by Tjora, while the next steps are how we worked in the process of conveying our results.

As previously stated, the initial step follows [Tjo17]'s guidelines, focusing on the crafting and formulation of the interview guide. How it was developed and refined can be viewed in Section 3.4.4. The subsequent step involved performing the interviews. Throughout these sessions, we took notes, and dialogues were recorded, providing us with empirical data for later analysis. After we finished an interview we revisited the interview guide, incorporating interviewee feedback and refining any questions that were unclear to the respondents.

The third step represents our first deviation from [Tjo17], who proposes that interviews should be transcribed at this stage. Given our dual interviewer setup, one of us took the lead in conducting the interview, while the other focused on note-taking. This arrangement enabled us to promptly summarize the interviews immediately upon their conclusion, potentially providing a more holistic vision than transcribing the interviews at a later time. This approach was motivated by our initial impressions and emotions from the interview, first individually and then combined into a joint summary. We believe this approach resulted in richer empirical data. It encapsulated not only the interviewee's responses but also our insights and perceived understandings as observers and interviewers.

According to [Tjo17], the fourth and final step before the results and conclusion, is to code the transcribed interviews. As per Linneberg and Korsgaard [LK19], coding qualitative data involves the process of transforming raw data into a coherent and meaningful representation. This is achieved by identifying key topics and elements within the data and assigning labels or codes to words, paragraphs, and sentences that capture the essence of their content. However, in our analysis, we left out the coding and changed it into steps four and five in Figure 3.4. In our process, the fourth step is to draw parallels between the different interviews to gather the main themes. To do this we worked together to define the main points based on the summaries done in step three. Step five is to use the key findings from step four to find relevant citations and quotes from the participants. Here, we played the interviews back, noting down the most common and most important citations brought up in the different interviews. Afterward, we sorted the citations based on the key points we found in step four. These findings and citations are the basis of our results and discussion presented in later chapters.

Upon completing our step-by-step analysis, we started working on the results.

Here we sorted the key findings into different sections pretty easily due to the work done in the previous steps. The combination of our findings and the background information presented in Chapter 2 established the foundation of our discussion. Here, we collaborated to choose the best citations and findings to help us argue why the methods we had chosen would benefit the risk assessment of cyber security in the petroleum sector.

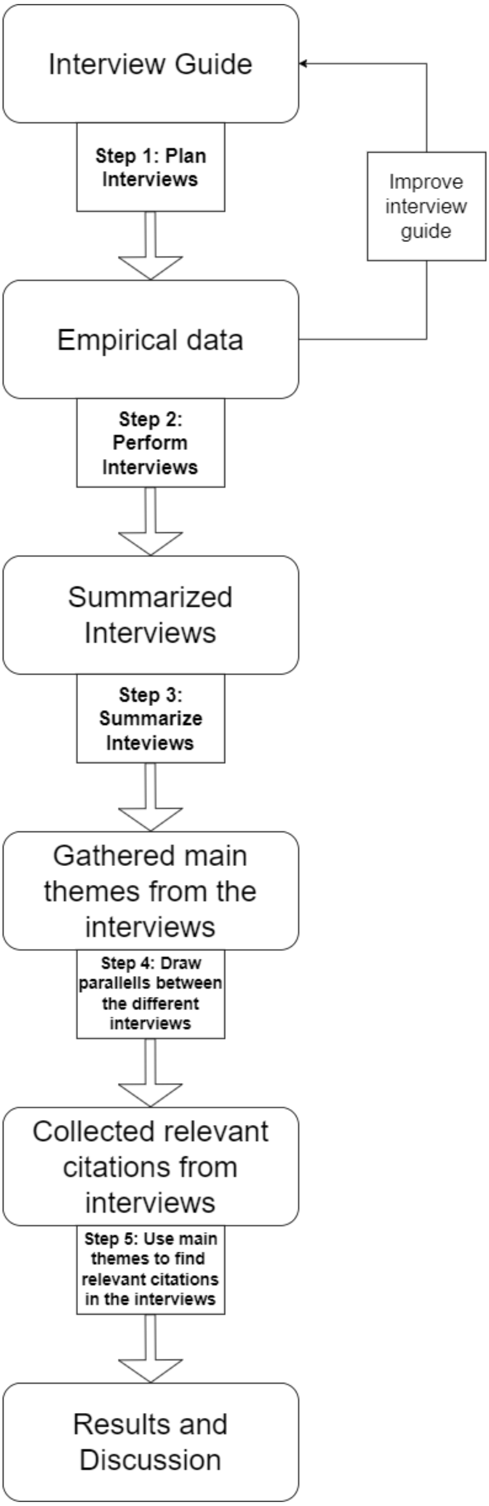

Interview Guide
Step 1: Plan Interviews
Improve interview guide
Empirical data
Step 2: Perform Interviews
Summarized Interviews
Step 3: Summarize Inteviews
Gathered main themes from the interviews
Step 4: Draw parallells between the different interviews
Collected relevant citations from interviews
Step 5: Use main themes to find relevant citations in the interviews
Results and Discussion

Figure 3.4: Step-wise inductive methodology used in the data analysis.

3.6 Challenges and Limitations

This thesis seeks to evaluate how risk associated with cyber security in the petroleum sector is addressed today and how it can be addressed going forward (RQs). Based on the methodology used, possible challenges and limitations connected with this are outlined in this section to give the research credibility. The trustworthiness of the qualitative research is addressed first, followed by the presentation of specific examples of challenges and limitations encountered in this study.

3.6.1 Trustworthiness

This subsection focuses on evaluating the credibility of the research methods employed in order to address any potential biases, limitations, and errors. Often are the three factors reliability, validity, and generalizability used as indicators to secure the trustworthiness of qualitative research according to [Tjo17].

Reliability

As stated by Tjora [Tjo17], reliability is related to the internal consistencies within a research project and their reflection in the reporting. It refers to the reproducibility of study results, allowing others to replicate the research and obtain consistent findings and interpretations. In the context of qualitative research, ensuring reliability requires transparency and providing comprehensive descriptions of the employed research methods and analytical strategies [Tjo17]. Thus, maintaining good documentation becomes essential in achieving research reliability.

To enhance the reliability of our study, we have provided a comprehensive description of our research methodology. The databases, articles, reports, and papers utilized during the literature review process are clearly identified and referenced throughout the thesis. Additionally, we have presented relevant information about the interviewees' company affiliations and backgrounds, which can aid in replicating our interviews. However, due to the sensitive nature of cyber security, and to ensure good qualitative responses from the interviewees, names and the operator companies have been pseudonymized. These details are explained later in Section 4.1. Additionally, the information provided to the interviewees prior to the interviews are available in Appendix C. While it may be challenging to reproduce the exact responses due to the nature of qualitative data collection through conversations, presenting the interviewees in a clear manner enables the identification of individuals with similar backgrounds.

Validity

Validity, defined by Tjora [Tjo17], «is associated with the question of whether the answers we find in our research are actually answers to the questions we ask». The accuracy of information provided by a source can be influenced by their knowledge and experience regarding the phenomenon being investigated. Additionally, the willingness of the source to provide accurate information plays a crucial role. To ensure this, we decided to pseudonymize the interviewees and their responses. Validity is reinforced when information is sourced from multiple independent sources.

One approach to ensuring a strong level of validity is through triangulation. Triangulation involves utilizing multiple methods or data sources in qualitative research to obtain a comprehensive understanding of phenomena [CBD+14]. In this master's thesis, we have used both a literature review and semi-structured interviews, with the interviews involving individuals working in various roles within the industry. By using this approach, we have been able to compare our findings with existing literature and safeguard against potential biases, thus strengthening the validity of the results.

Another method for increasing the level of validity is ensuring that we interviewed individuals with extensive knowledge within the field of oil and gas or cyber security or both. It was anticipated that these sources would have a genuine interest in contributing to research within their respective domains, increasing the likelihood of obtaining accurate information. However, there is a potential challenge if the representatives wish to present their company in the best possible light, potentially omitting problematic factors. To mitigate this, we conducted interviews with a diverse range of ten participants, presented in Section 4.1, representing various actors within the industry.

Unfortunately, our interviews were limited to only three operators as we were not able to get responses from more operators. This raises concerns about the representativeness of our research findings for the entire sector. Nevertheless, we believe that the combination of these interviews with our extensive literature research offers a realistic portrayal of the sector as a whole. While acknowledging the limitation in terms of the sample size, we are confident that the insights gathered from our study, encompassing both primary and secondary sources, contribute to a comprehensive understanding of the sector's dynamics.

Generalizability

Tjora distinguishes between two types of generalizability: moderate and conceptual [Tjo17]. Moderate generalizability involves determining the specific situations where research findings are valid, considering factors like time, place, and context. Conceptual generalizability applies to qualitative research and involves developing concepts, typologies, or theories that have relevance beyond the specific cases studied, making them applicable to other situations or contexts.

In simpler and combined terms, the question is whether the results can be applied to areas beyond the ones specifically studied. Determining the applicability of our findings beyond the petroleum sector presents challenges as this study primarily focused on the Norwegian petroleum industry, collecting interview data exclusively from that sector. However, the literature review included knowledge from various critical infrastructure sectors and technologies, making it more applicable.

Taking comprehensive measures to address trends in cyber risk levels is essential for all sectors. While the interviews in this study focused on the petroleum industry, the diverse backgrounds of the participants enhance the generalizability of the findings. The interviewees displayed a favorable response to the suggestion of finding a better way of assessing trends in cyber risk levels. Nonetheless, it is crucial to acknowledge the limitations imposed by a relatively small sample size, making it challenging to determine the widespread generalizability of the findings across various sectors.

3.6.2 Specific Examples

Below we outline the specific challenges and limitations encountered during the course of our research.

Logistic of Interviews

One of the primary challenges we encountered was related to the logistics of conducting interviews. Firstly, the overall time it took to complete the interviews proved to be considerable. We had our first interview in late January and our last in late April. However, an even greater challenge than anticipated was finding suitable time slots for the interviews. This was primarily due to the busy schedules of the interviewees, who held high positions within their respective companies. As a result, their calendars were often tightly packed. In many instances, it took approximately 2-3 weeks from the initial email contact to the actual interview taking place. Despite these challenges, we were fortunate to successfully interview a total of ten highly knowledgeable individuals who provided valuable insights and contributed to the overall depth of this thesis.

Classified Information

One limitation experienced during several interviews was the constraint imposed by the confidentiality of classified information. Some interviewees had to exercise caution and think twice before sharing certain information, resulting in the potential incompleteness or inaccuracy of the gathered data. However, we fully understand the reasons behind this constraint, as the consequences of leaked information could provide a competitive advantage to other actors while also exposing vulnerabilities to attackers. Therefore, we have a comprehensive understanding of why certain information was withheld from us. Although the inclusion of this withheld information could have contributed to a deeper analysis, it becomes challenging to present it in a thesis that will be publicly available.

3.7 Ethics

In this process, we spoke with several industry representatives. Through these conversations, we gained insight into corporate information and potential vulnerabilities to systems from the interviewees. The potential disclosure of confidential information was mitigated by not transcribing and adding the interviews as appendices to this thesis. To gather the necessary information, we employed the methods outlined in Figure 3.4. Instead of transcribing the entire interview, we summarized the most crucial information and identified sufficiently generalized quotes that could be used in our further writing.

In addition to this, all data gathered from the interviews is anonymized or pseudonymized as mentioned in Section 4.1. The identities of individuals were completely anonymized, while descriptions of a person's experiences were shared in broad terms. Official organizations and non-operating companies are not anonymized due to the significance of understanding the context of their views and contributions. However, it should be noted that despite the non-anonymization of the companies, the identities of the interviewees within these organizations are kept confidential, thereby limiting any potential exposure of their personal identities.

Chapter 4 Results

This chapter presents the results and findings from the semi-structured interviews and literature review. Before presenting the research results, section 4.1 provides background information on the individuals interviewed so that the statements can be contextualized. Since semi-structured interviews need to be understood based on the individual's perspective, our study aimed to provide insights into the experiences and beliefs of each participant rather than simply focusing on their explicit responses. An important part of addressing cyber security risks is risk assessment. Section 4.2 provides an overview of the current risk assessment practices in the sector, including incident reporting and the state of exercises and incident response plans. In Section 4.3, the audits conducted by the PSA are presented, along with the suggestion of introducing an «audit light» approach. Finally, Section 4.4 explores the sharing of information within the sector and highlights the impact of relevant laws and regulations. The findings are evaluated and used to answer the research questions:

RQ1: How is risk associated with cyber security in the petroleum sector addressed today?

RQ2: How can risk associated with cyber security across the petroleum sector be effectively addressed going forward?

4.1 Who Are the Interviewees?

This section provides an introduction of the interviewees and describes why their thoughts and input are relevant to this thesis. For privacy reasons and due to the sensitive nature of cyber security, all identities have been pseudonymized. We will therefore refer to the interviewees as Interviewee A from PSA, Interviewee B from Company 1, and so on. The official organizations and non-operator companies are not pseudonymized because we consider this information as non-sensitive and important to understand the background of their thoughts and input. By doing so, it is easier for the reader to follow what interviewee a statement comes from.

4.1.1 Official Organizations and Non-operator Companies

The interviewees from official organizations and non-operator companies come from diverse professional backgrounds within the oil industry and possess extensive knowledge gained through years of involvement in related fields. They provide a view from outside the sector and are more objective than the individuals from the operator companies.

Interviewee A is a chief engineer at PSA.

Interviewee B is also a chief engineer at PSA.

Interviewee C is a consultant and specializes in the field of industrial IT/OT and cyber security.

Interviewee D is also a consultant who specializes in the field of cyber security and works for a different company.

Interviewee E is a senior advisor at the NSM and specializes in, amongst others, cyber security for industrial systems, risk management, ICS and OT. They have previously worked at PSA.

Interviewee F is a security analyst at KraftCERT.

Interviewee G is a consultant specializing in information- and cyber security.

4.1.2 Operating Companies

The interviewees from operating companies have many years of experience in the field and some of them have also worked in official organizations within the sector. They provide an inside view and through them, we have gotten to better understand how risks associated with cyber security are actually handled in the field.

Interviewee H, Company 1 is a lead automation engineer in a small operator company.

Interviewee I, Company 2 is a manager in a small operating company.

Interviewee J, Company 3 is an OT engineer in a large operator company.

4.2 Risk Assessment and Incident Reporting

This section provides an overview of the findings from the interviews and literature review regarding the current practices of conducting risk assessments, including threat analysis, in the sector. Further, incident reporting and exercises within the sector are presented. Additionally, the section briefly describes how the size of operator companies affects these practices.

4.2.1 Risk Assessment Today

During the initial phase of our research, we discovered that each operating company bears responsibility for its own cyber security and the associated risks. However, various cyber security organizations and petroleum sector authorities are involved in different aspects of risk assessment. To facilitate risk analysis, there exist multiple standards, guidelines, and frameworks, some of which are referenced in 2.4.

An article by NRK [NRK22] highlights that Equinor and Gassco were subjected to the Security Act (Sikkerhetsloven) last summer. We were informed that there could be additional organizations that have undergone this process. However, this information is not publicly accessible. These organizations are required to receive recommendations from supervisors at NSM. Additionally, they are granted access to NSM's technical systems, including Allvis NOR, a tool used for scanning internet-exposed services for vulnerabilities, and «Varslingssystem for digital infrastruktur» (VDI), which consists of network sensors monitoring the network traffic to detect suspicious activity and threats based on known patterns. However, it has been observed that these tools do not effectively identify all vulnerabilities and do not detect new and unknown attacks and threats. They are also unable to monitor encrypted traffic, which comprises the majority of today's network traffic [Rik23]. Utilizing these tools can potentially pose a risk to organizations, as they may provide a false sense of protection.

Conversely, operators not subject to the Security Act do not receive the same guidance. Nonetheless, this disparity does not imply that they are any less important. As emphasized by interviewee E, «An attacker will jump over the fence where it is lowest, and the consequences can still be quite substantial». This underscores the necessity for a method to address cyber risk across all operators in the sector.

According to interviewee B, «The operators have significantly increased their focus on cyber security in the past three years, with greater implementation in their routines. Recent incidents have made it clearer what the potential costs can be». While the operators have made progress, there is still room for improvement and further advancements to be made when it comes to addressing cyber security risks.

4.2.2 Threat Analysis

Threat analysis is another crucial aspect of risk assessment, and it is primarily the responsibility of each operator. During the interviews, it became evident that all interviewees perform this analysis individually. They have access to various resources and gather information from entities such as Dragos, KraftCERT, NSM, PST, the NIS, LinkedIn, and their vendors. Interviewee H emphasizes, «There are many sources and various perspectives. What is interesting to us is OT». Moreover, they mention casually encountering interesting articles while sitting at home on the couch with a cup of coffee in the evening. This highlights the extensive and unstructured nature of the task at hand.

Interviewee H also points out that the public reports from NSM, PST, and the NIS lack specific details due to their sensitivity, thus limiting their usefulness. This indicates that despite the presence of multiple threat intelligence sources, there is room for improvement in terms of their practical value. Interviewee C strengthens this by stating that «The yearly risk and threat reports from NSM, PST, and the NIS are not addressing industrial IT and OT in a sufficient manner. They have forgotten that a lot of the industry in Norway is run on digital technology». KraftCERT plays a role in enhancing this aspect by issuing an annual threat assessment in June. This assessment serves as an intelligence product more specifically for OT and offers insights into how companies perform risk assessments. NSM also provides a classified report to individuals who hold the necessary security clearance. This is usually given to CEOs or other key personnel in larger companies. Unfortunately, we have been unable to access these reports due to their confidential nature.

Additionally, KraftCERT notifies its members of vulnerabilities, including criticality assessments and recommended countermeasures. It then becomes the responsibility of each operator to determine whether their systems or equipment are affected. Given the complexity of the petroleum sector, where each operator owns numerous systems and equipment, keeping track of everything becomes a challenging task. Notably, not all operators have effective solutions in place to maintain control over their inventory.

According to KraftCERT, they aim to «ensure good, secure, and efficient incident management and information sharing between relevant companies nationally and internationally» [Kra]. However, there are numerous service providers offering solutions related to the threat landscape. «It is overwhelming with so many different sources and repetition of the same information, but presented in various ways. There are many who are selling services related to the threat landscape since it is a hot topic at the moment. They also have something to gain by hyping up the threat landscape. It is important to obtain relevant information and not too much information», states interviewee I. The participants find it valuable to have concise summaries or similar sources of information that compile emerging threats or vulnerabilities. This approach provides them with an easier means of assessing the relevance of the information at hand.

Regardless of the size of the operator, the task of threat analysis remains equally challenging. However, the availability of resources to carry out this work differs significantly. Large operators, such as interviewee H's company, have dedicated cyber security departments and find this job more manageable. On the other hand, smaller operators as interviewee I's company, may face resource constraints when it comes to threat analysis. Limited financial means, expertise, and technological infrastructure can pose significant challenges in effectively addressing cyber security risks. These operators might have to rely on external resources to a greater extent, such as third-party service providers or industry collaborations, to augment their threat analysis capabilities. While they may still possess a strong commitment to cyber security, the absence of dedicated cyber security departments can make the task more demanding and require strategic prioritization.

Interviewee C mentions that their consulting firm has a high focus on cyber security in the petroleum sector and regularly performs threat assessments. Their objective is to engage with large enterprises at a strategic level, addressing emerging trends, threats, and vulnerabilities. The primary goal is to enhance awareness, demonstrate a serious commitment, allocate resources, establish priorities, and foster a more tactical and operational approach. They also mention that their firm's expertise in conducting threat assessments is utilized by multiple operators, primarily the larger companies due to the associated costs.

4.2.3 Incident Reporting

Following the PSA's guidelines on Regulation on Management [10, § 29], which concerns notification and reporting, ICT incidents are required to be reported to the PSA. This regulation has been in effect since 2011. However, as mentioned in Subsection 2.2.3, the PSA has delegated KraftCERT the responsibility of servings as the sector-specific CERT for the petroleum sector and should receive reports of ICT incidents that are less important than those reported to the PSA. According to interviewee B, the reporting of security-related incidents to KraftCERT has been in place since mid-2022. However, the number of reported incidents is not as high as expected. According to Interviewee F, establishing a culture of trust and incident reporting takes time, but there is also a need for more and improved reporting tools on a national level. The purpose of incident reporting is to obtain an overview of incidents within the sector. The collected data is then shared with NSM to provide a comprehensive view of security incidents across various sectors. Interviewee C highlights that there is a risk of underreporting or reporting on non-significant matters due to the obligation to report. Operators may choose to neglect certain incidents to avoid reporting them, while others may report every minor incident out of concern for meeting the reporting obligation.

In addition to KraftCERT, there are several other entities that gather information on incidents. Large companies like Microsoft, Google, and Cisco, as well as specialized firms like Dragos, which focuses on ICS, are examples of such actors.

4.2.4 Exercises and Incident Response Plans

When it comes to incidents, it is not sufficient to solely report them. Having a well-defined incident response plan and conducting regular exercises are crucial. During our interviews with various operators, we found that they all have established incident response plans and engage in some exercises. These plans outline the appropriate actions to be taken during incidents, and the operators are aware of whom to contact in such situations. However, it is worth noting that the interviewees were not directly involved in the creation of these plans, and their participation in exercises varies as not all concern OT systems. This comes from that a lot of the exercises are related to HSE, thus leaving less time and resources for exercises related to cyber security.

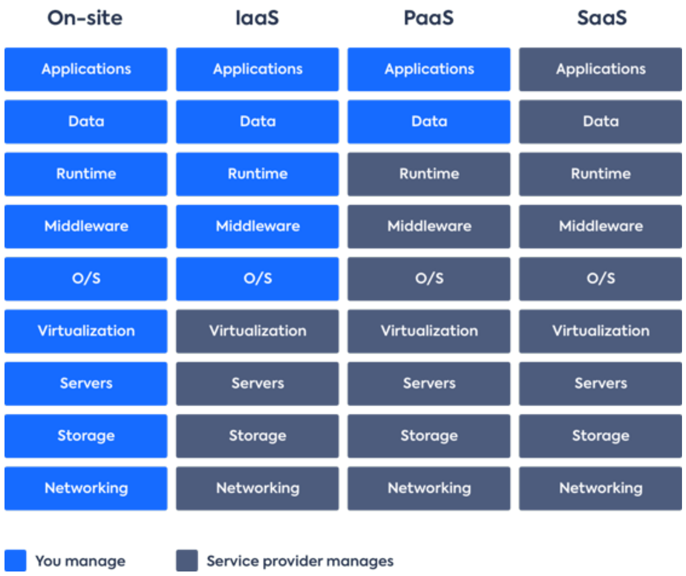
According to interviewee E, only a few operators have comprehensive plans and exercises in place specifically for OT-related security incidents. While exercises of varying scales are conducted, they primarily focus on higher-level scenarios. Interviewee E suggested that there should be greater involvement of major vendors in both exercises and the development of incident response plans.

Although the operators demonstrate a good level of emergency preparedness, interviewee B noted that cyber security is often treated differently during training and exercises. This comes from the delicate and complex nature of the ICSs and how they can negatively affect production. Nonetheless, valuable insights and discoveries often emerge during these exercises, underscoring their importance. Throughout our interviews, it became apparent that the operators believe they engage in exercises too infrequently.

4.2.5 Size of the Operator Companies

The size of operator companies has an impact on their organizational structure and how they address risks. Smaller companies, constrained by limited resources, often opt to outsource various functions. Figure 4.1 illustrates the distinctions between IaaS, PaaS, and SaaS, highlighting the shift in responsibility resulting from different IT outsourcing strategies. Although this example specifically relates to IT, the key takeaway is how this shift in responsibility impacts the organization's risk perception. While the organization remains primarily accountable for security even after outsourcing, the service provider typically assumes some level of responsibility.

The exact description of these responsibilities is a complex legal matter beyond the scope of this thesis. However, the main point to consider is that the size of operator companies influences how they approach and manage risks.



On-site	IaaS	PaaS	SaaS
🟦 Applications	🟦 Applications	🟦 Applications	▨ Applications
🟦 Data	🟦 Data	🟦 Data	▨ Data
🟦 Runtime	🟦 Runtime	▨ Runtime	▨ Runtime
🟦 Middleware	🟦 Middleware	▨ Middleware	▨ Middleware
🟦 O/S	🟦 O/S	▨ O/S	▨ O/S
🟦 Virtualization	▨ Virtualization	▨ Virtualization	▨ Virtualization
🟦 Servers	▨ Servers	▨ Servers	▨ Servers
🟦 Storage	▨ Storage	▨ Storage	▨ Storage
🟦 Networking	▨ Networking	▨ Networking	▨ Networking

🟦 You manage ▨ Service provider manages

Figure 4.1: Illustration of the differences between IaaS, PaaS, and SaaS and the level of vendor management with each service model. The figure is taken from [Leab].

During an interview with a smaller operator company, it was revealed that they have a dedicated department responsible for assessing security. However, their focus is primarily on IT systems rather than OT systems. The assessment of OT systems is predominantly the responsibility of each operating facility. It is worth noting that many operating companies have a presence in multiple countries. The location of their primary operations significantly influences the organizational culture and their approach to cyber security and risk management.

This geographical diversity poses challenges, particularly in countries where the operators have limited facilities. In such instances, these operators may find themselves with fewer resources and support, leading to a greater sense of isolation in addressing cyber security and risk concerns.

4.3 Audits

Audits, introduced in 2.2.1, are conducted on an irregular basis based on the need for supervision. This means that some companies are being audited more often than others. Audits can cover different areas where cyber security is one of them, and the one we have focused on. At PSA they have a dedicated division working with cyber security and related audits. Both interviewees A and B from PSA are working in the particular division. This division has expanded from 1 to 4 members in recent years. The expansion was a result of the Norwegian Board of Audit's (Riksrevisjonen) revision of how the PSA follows up on health, safety, and environment in the petroleum sector [Rik19], where they recommended that the PSA follow up on cyber security in the petroleum sector in a better way. The Norwegian Board of Audit was satisfied with the expansion. The PSA has increased the focus on cyber security audits and has as of now conducted audits with the focus on cyber security at all operators operating on the NCS. They have been conducted over a 10-year period, according to interviewee B.

Interviewee E expressed that «The audits are fulfilling their purpose; however, they could be expanded to not only focus on regulatory compliance but also on enhancing robustness, understanding, and culture within the companies». This is further confirmed by interviewee I, stating that «audits are very superficial, only looking at regulations». This raises the question of the purpose of audits. While ensuring compliance with regulations is important, these regulations are broad and subject to interpretation. The main objective of the audits is to verify the effective functioning of the management system and associated documents. This is achieved through a combination of reviewing documentation and engaging in dialogue with key personnel within the organization. The audits also cover areas such as technical installations, inventory control, and processes related to vulnerability alerts. Often, weaknesses in human factors, such as lack of competence and training, are identified. Many operators, both large and small, often lack sufficient control over their systems and lack a systematic approach to effectively address vulnerabilities.

In contrast, there are other benefits of the audits. The interviewees from the operator companies emphasized the usefulness of audits as they compel them to thoroughly review their routines and systems. The external oversight provided by audits is highly valuable. While not all vulnerabilities and regulatory noncompliance are deemed critical, the PSA effectively distinguishes between different levels of criticality in relation to vulnerabilities. Interviewee J mentioned that «prior to the situation in Ukraine, obtaining resources for improvements was not always straightforward due to a lack of clear understanding of the consequences, and it was more cost-effective to take risks. In such cases, the PSA played a helpful role by providing deviations and directives». This underscores how audits compel management to prioritize cyber security matters. As the interviewee pointed out, the ongoing war in Europe has also heightened the focus on cyber security.

The PSA places great importance on ensuring the safety of petroleum activities and establishing the necessary regulatory framework. As stated by the PSA, their core responsibility is to develop HSE regulations and oversee companies' compliance with them [Pet21]. This underscores their commitment to safety, which is further supported by the findings from the interviews. While they acknowledge the increasing significance of security, their main focus lies on safeguarding OT rather than IT, as the latter falls outside their mandate, as mentioned by interviewee A. With the growing digitalization and the diminishing separation between IT and OT, critical systems face an expanded attack surface. The PSA addresses this concern by evaluating the effectiveness of measures implemented to maintain the air gap, typically achieved through firewall protection. While the PSA does not carry out penetration tests themselves and lacks the authority to require operators to do so, they can provide recommendations in favor of conducting such tests.

4.3.1 «Audit Light»

Due to the sporadic nature of audits based on specific needs, operators often undergo infrequent cyber security audits. As a result, the PSA has limited knowledge about the subject between audits. Without a clear understanding of the current status, it becomes challenging to address the PSA's main issue for 2023, which includes «security against deliberate attacks in all phases of the petroleum industry» [Pet23]. To address this, we propose the establishment of a lighter form of audit, referred to as an «audit light». This approach would ensure that cyber security remains a continuous focus rather than solely being addressed during specific cyber security audits. As stated by interviewee A, «The notification letter is half the audit». This indicates that when the companies receive the notification, they address known issues. This shows how the operators may work with cyber security sporadically rather than continuously, which is unfortunate. Furthermore, this shows the importance of the audits in which they indirectly ensure the implementation of measures and address weaknesses. The light audits will supplement regular audits and will also be reported to the PSA.

The purpose of the light audits is to provide a more comprehensive overview. Regular audits focus on actual practices, while light audits concentrate on how management addresses cyber security and the evolving threat landscape. Both threats and vulnerabilities, as well as their impact, can be assessed. The effectiveness of measures in addressing changes in the risk level can also be evaluated.

Interviewee J's company already conducts self-assessments based on NOG104. In contrast to audits, these self-assessments are less formal and involve more dialogue, allowing for meaningful discussions on addressing challenges rather than solely evaluating the current state. This indicates that these self-assessments are valuable not only for gaining an overview but also for addressing challenges being discovered.

Additionally, it is possible to assess how operators are addressing new threats and vulnerabilities. This can be accomplished in combination with the annual self-assessments based on NOG104, either more frequently as the threat landscape evolves or at the same interval. Since NOG104 is generic and static, addressing the changing threat landscape will result in enhanced comprehension of the cyber security status of the operators.

According to interviewee B, the PSA experimented with survey-based self-assessments in the past but found that they did not provide an in-depth analysis of the cyber security status. Instead, interviews were deemed more valuable as they revealed the actual practices. This comes from that quantitative data is less rich than qualitative data. To enrich the self-reporting, interviews can be incorporated into the light audits as needed, particularly when the self-assessment does not provide a clear understanding of how threats and vulnerabilities are addressed. To ensure the self-assessments reflect reality, concrete examples of how threats or vulnerabilities are addressed can be included.

4.4 Information Sharing

Sharing of information and knowledge within the sector is taking place to some extent. In terms of cyber security, information is not considered a competitive advantage. However, there is a sensitive nature to this information as it may reveal vulnerabilities that could be exploited by malicious actors. Official organizations such as NSM, PST, NIS, KraftCERT, and Dragos, as described in Section 4.2.2, share information through reports and notifications. This section will focus more on alternative forms of communication for information sharing, rather than reports.

Due to the relatively small size of the OT community in Norway, a significant amount of information is shared both formally and informally. This has been confirmed through interviews, and there is for instance an informal OT forum that includes several operators. However, not all interviewees are aware of this forum and are therefore not part of it. Ideally, all operators should have the opportunity to participate in information sharing. Interviewee H stated that this OT forum works well, with fruitful conversations and meetings held approximately twice a year to discuss up-to-date topics and common challenges. Additionally, interviewee C mentioned that informal information sharing is quite common, where one operator can contact another operator's Security Operations Center (SOC) to notify about unusual incidents. Interviewee J highlighted the importance of more information and knowledge sharing, both among operators and with vendors. These forums could be facilitated by relevant actors such as SINTEF, KraftCERT, or others, providing a platform to discuss incidents, vulnerabilities, threats, and new technologies. However, one key success factor for these forums is that there are no official minutes of the meetings, allowing participants to express their genuine opinions without fear of consequences from official organizations.

A report from Sopra Steria [GTA+22] concludes that «more informal forums and meeting places should be established to develop knowledge about incidents, vulnerabilities, threats, and assets across specialist groups, companies, sectors, and government authorities». Our research aligns with this finding.

Regarding formal forums, there are several options available. KraftCERT organizes an annual forum that lasts for 2-3 days, while the CDS-forum, hosted by SINTEF, takes place twice a year. We attended two CDS-forums and found them to be informative and valuable for participants from various organizations, operators, and vendors who share a passion for cyber security. Through our interviews, we recognized the significant value of information sharing, particularly for smaller operators with limited resources for testing new technologies and increased reliance on outsourcing. Although it may be less evident how larger operators benefit from information sharing, several entities are eager to share their experiences, enhancing their reputation and fostering meaningful discussions and diverse perspectives.

The diagram in Figure 4.2 illustrates the process of interpreting data and its significance in generating information. By correctly understanding and contextualizing data, meaningful information is derived. This information then forms the basis for acquiring knowledge, making informed decisions, and taking subsequent actions. Sharing information among various stakeholders amplifies the pool of data and information, thereby broadening the foundation upon which wisdom can be built. Additionally, forums and meetings that bring together participants from different companies foster extensive and in-depth discussions, contributing to more enriched decision-making processes, actions, and overall knowledge advancement.

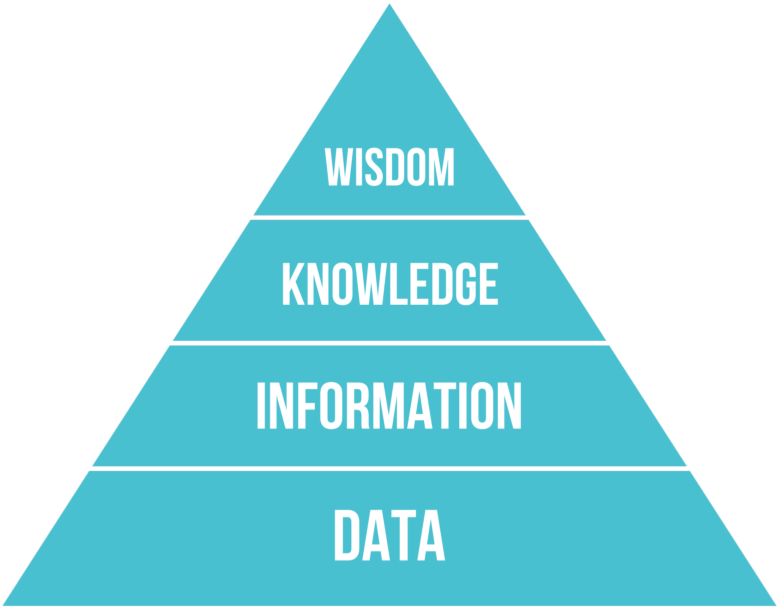


Figure 4.2: The DIKW-pyramid, showing how data can be transformed into wisdom. Figure adapted from [Leaa].

The report by Sopra Steria highlights the need for a more effective and comprehensive platform or channel in the oil and gas sector to share information and knowledge about vulnerabilities. Specifically, they suggest the establishment of a clearer and more centralized mechanism, like KraftCERT, for spreading information related to vulnerabilities [GTA+22]. While incident reporting to KraftCERT has been implemented, there is still room for improvement in addressing the issue of sharing vulnerability information effectively.

Currently, NSM plays a role in distributing general information about ongoing attacks, vulnerabilities, and affected systems through their website [Nas]. However, this information tends to be more general in nature and lacks the necessary specificity for the petroleum sector. On the other hand, KraftCERT provides sector-specific vulnerability information for both the petroleum and electric power sectors. However, this information often remains with technicians and may not receive sufficient attention from management.

To fully grasp the implications of vulnerabilities and their potential impact on other systems and production, it is essential to consider the broader context. This entails ensuring that the information is accessible to individuals who possess the required expertise and understanding of the system context. Currently, the flow of information from KraftCERT is primarily unidirectional, with limited opportunities for reporting vulnerabilities. As a result, the sharing of vulnerability information mostly occurs through informal forums, where discussions and exchanges take place among relevant stakeholders.

In conclusion, while efforts have been made to share information and knowledge about vulnerabilities in the oil and gas sector, there is still a need to establish a more robust and inclusive platform that addresses the specific challenges and requirements of the industry. This would enable effective sharing of vulnerability information, foster a better understanding of the broader context, and facilitate more comprehensive discussions and actions among stakeholders.

4.4.1 Laws and Regulations

Laws and regulations is a complex matter and we are only touching this briefly. To our understanding, the PSA has comprehensive knowledge within this field. According to the letter «Informasjon om håndtering av IKT-sikkerhet» [Pet19], the PSA states that the paragraphs mentioned in table 4.1 are relevant for cyber security. These are also the paragraphs that are the basis for cyber security audits. A report from DNV [GL20b] discusses the advantages and shortcomings of having a function-based regulation rather than a prescriptive one. Some of the key findings are that a function-based regulation is dependent on trust between the PSA and the operators, as well as a broad and deep understanding among auditors. This complexity makes it challenging for the PSA to obtain a comprehensive view and address cyber security in an appropriate manner. According to interviewee A, this works well because the operators have a significant economic interest in avoiding cyber incidents. The implementation of function-based regulations can also present challenges when dealing with operators that have ownership in different countries but are operating on the NCS. Cultural differences may influence how these operators approach and manage cyber security risks. Another significant challenge with these audits is that a substantial portion of the results is exempt from public disclosure under the Freedom of Information Act, Section 23 [06, § 3]. This limitation hinders the sharing of information within the sector. The issue of information sharing is addressed in Section 4.4 and discussed in 5.3.

Table 4.1: Paragraphs in regulations that are relevant for cyber security according to the PSA.

Paragraph	**The PSA's understanding of relevance for cyber security**
Regulation on Management §4 Risk Reduction: The responsible party [shall] choose technical, operational, and organizational solutions that reduce the probability of harm, errors, and hazardous and accident situations from occurring.	This implies that solutions for ICT security are chosen to reduce the probability of ICT attacks that cause harm, errors, or hazardous situations.
Regulation on Management §4 Risk Reduction: The responsible party (shall) choose technical, operational, and organizational solutions that reduce the probability of harm, errors, and hazardous and accident situations from occurring.	This implies that solutions for ICT security are chosen to reduce the probability of ICT attacks that cause harm, errors, or hazardous situations.
Regulation on Management §8 Internal Requirements: The responsible party shall establish internal requirements that specify the requirements in the regulations and contribute to achieving the goals for health, environment, and safety.	Requirements must be set for how ICT security is handled, both technically, operationally, and organizationally.

Continued on next page

Table 4.1 – continued from previous page

Paragraph	**The PSA's understanding of relevance for cyber security**
Regulation on Facility Design §32-34 Safety Systems: The system should be able to perform its intended functions independently of other systems. Guidance: The system may have interfaces with other systems if it cannot be negatively affected by system failures, errors, or individual events in those systems.	The requirement that interfaces with other systems should not have a negative impact means that even ICT attacks should not prevent the systems from performing their intended functions.
Regulation on Facility Design §34a Control and Monitoring Systems: Guidance: In addition, Norwegian Oil and Gas Guideline No. 104 should be used as a basis for protection against ICT-related hazards.	The guidance refers to recognized guidelines, but other standards can also be used.
Regulations on Activity §21 Competence: The responsible party shall ensure that personnel at all times have the necessary competence to perform activities in accordance with health, environment, and safety legislation. In addition, personnel should be able to handle hazardous and accident situations.	The requirement for competence is also relevant for those who are responsible for handling hazardous situations related to ICT incidents with the industrial control and safety systems.

Continued on next page

Table 4.1 – continued from previous page

Paragraph	**The PSA's understanding of relevance for cyber security**
Regulation on Activity §23 Training and Exercises: The responsible party shall ensure that necessary training and exercises are conducted so that personnel is always capable of effectively managing operational disruptions and hazardous and accident situations.	The requirement for training and exercises is also relevant for those who are responsible for handling hazardous situations related to ICT incidents with industrial control and safety systems, as well as interacting with response teams.
Regulation on Activity §45 Maintenance: The responsible party shall ensure that facilities or parts of them are maintained so that they are capable of performing their required functions throughout their entire lifespan.	Updating and patching software when security vulnerabilities are discovered is considered maintenance.
Regulation on Activity §48 Planning and Prioritization: A comprehensive plan for the execution of maintenance programs and corrective maintenance activities shall be prepared.	The requirement for planning involves a systematic approach to how the company maintains control over which updates are relevant and which equipment components require maintenance programs.
Regulation on Management §29 Notification and Reporting: Guidance: situations where the normal operation of control or safety systems is disrupted by unplanned work (ICT incident).	The notification of an ICT incident, as stated in the guidance, is information provided to us about the situation. If sensitive information is associated with the incident, the text must be labeled so that this part can be exempt from disclosure. The framework provided by NSM, as mentioned above, describes how incidents in critical infrastructure/-critical societal functions should be handled.

In the petroleum sector, there are numerous ongoing legal processes pertaining to cyber security. Since Norway is part of the European Economic Area (EEA) and consequently a member of the European Union (EU), EU laws and regulations can be applicable to Norway. Specifically, this applies to the Directive on Security of Network and Information Systems (NIS) and its revised version, NIS2. It is important to note that the NIS acronym used in this context should not be confused with the abbreviation NIS used elsewhere in the thesis.

According to the Norwegian government [Nor23], the NIS directive came into effect on February 3rd, 2023 in the EEA and its requirements will be implemented in Norway through «Digitalsikkerhetsloven» [Reg22]. However, the Norwegian Petroleum Safety Authority (PSA) believes that it will not have a significant impact on the petroleum sector, as the sector's existing laws and regulations already address the requirements outlined in the directive. On the other hand, NIS2, which is an extension of NIS, is expected to be implemented at a later date. This extension aims to strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more strict supervisory measures and stricter enforcement requirements. It is worth noting that both directives apply to companies involved in or responsible for essential services, including the petroleum sector. However, these directives primarily encompass medium and large businesses. Because the NIS directive is already in effect in the EEA and NIS2 is in effect in the EU but not yet in the EEA, we will briefly describe NIS2.

Table 4.2 describes the areas covered by NIS2 that are most relevant to this thesis. Additionally, DNV has published a whitepaper on the NIS2 directive, examining its implications for industrial companies and presenting a three-step approach to achieving compliance [DNV23].

Table 4.2: Table of important areas the NIS2-directive [Eur22b] covers

Area	**Article(s) in NIS2-directive**
Report on the state of cyber security in the Union	18
Peer reviews	19
Cyber security risk-management measures	21
Reporting obligations	23
Information sharing	29, 30

Chapter 5 Discussion

In Chapter 4, current risk assessment practices, information sharing, incident reporting, audits, and the state of exercises and incident response plans were identified. This mainly answers out RQ1 and the introduction of audits light is more focused towards RQ2. This chapter will further discuss how risk associated with cyber security can be addressed going forward. Section 5.1 discusses different approaches to assessing risk, analyzing threats, and briefly touches on incident reporting and exercises. Next, audits and audits light are discussed in Section 5.2. Reflections regarding information sharing in the sector are discussed in 5.3.

5.1 Risk Assessment

Based on the initial findings of our research and the information we have gathered so far, it is apparent that each operating company carries its own responsibility for managing cyber security and its related risks. To support this responsibility, multiple standards, guidelines, and frameworks are available, some of which have been mentioned in Section 2.4. This decentralized approach allows for flexibility, given the unique situations of each operator, but also may introduce inconsistencies in the quality and accuracy of risk assessment across the sector. Agreeing on minimum standards of cyber security practices may be beneficial. Other key aspects of our findings regarding the risk assessment today and going forward are discussed further in this section.

5.1.1 The Security Act (Sikkerhetsloven)

The Security Act has mandated heightened cyber security standards for organizations such as Equinor and Gassco, providing them with access to technical systems for threat detection and vulnerability scanning. However, it is crucial to acknowledge the limitations of these tools, as they may not detect new and unknown threats. Therefore, over-reliance on these tools could foster a false sense of security. Meanwhile, operators not under the Security Act's jurisdiction face a disparity in guidance and support, which could make them vulnerable to attacks. As one of our interviewees correctly pointed out, attackers often exploit the weakest link in a network, and even if that link belongs to a single operator, the resulting consequences can be substantial for the broader petroleum sector. This situation tells us that all companies, whether they are under the Security Act or not, need to manage cyber risks better. This means improving the tools they use to spot threats and making sure all companies follow good cyber security practices.

5.1.2 The VTS Model

In Section 2.5, we discussed the VTS model, which focuses on assets, threats, and vulnerabilities. However, according to [Mat20], this model possesses specific shortcomings.

Another article introduces a comparison between the VTS model and the ROS model (Risiko- og sårbarhetsanalyse in Norwegian) [Jan21]. It triggers a discussion on the most appropriate model for risk assessments or the potential need to use both models. It becomes evident throughout the article that the «traditional» ROS model falls short of meeting the requirements set by the new Security Act. This model, concentrating on the likelihood of events and their consequences, must evolve to address the new Act's demands, which necessitates an analysis encompassing value, threat, probability, vulnerability, and consequence. The integration of these five factors signals a more comprehensive and potentially superior approach to risk assessment.

The VTS model is preferred by NSM in their «Risk assessment for ICT-systems». It is based on NS 5832:2014, which is a standard describing ICT risk as a relationship between a specific threat and the targeted value's vulnerability [NSMa]. Instead of attempting to quantify the difficult-to-estimate likelihood of occurrence, it emphasizes mitigating vulnerabilities to reduce the overall ICT system risk. This three-factor or «risk triangle» approach assessing value (V), threats (T), and vulnerabilities (S) is the NSM's preferred model. However, contrasting viewpoints presented in [Mat20] and [Jan21] may challenge its relevance, suggesting a possible need for updating the standard to address the evolving risk landscape.

The firstly mentioned article, [Mat20], underscores this by declaring both models as inadequate. There are two different models, but neither of them provides sufficient risk analysis to meet the Security Act's requirements. While ROS focuses on probability and consequence, VTS centers on value, threat, and vulnerability. However, according to the law, an effective analysis must incorporate all five of these factors [Mat20].

5.1.3 The Risk Equation

As noted in Section 2.5, IEC 62443 highlights threats, vulnerabilities, and consequences when selecting a method for assessing risk related to IACS. This standard employs a risk estimation methodology that involves the use of the following formula:

$$Risk = Threat \times Vulnerability \times Consequence \tag{5.1}$$

During a conference in 2016, Michael Hayden referred to it as «The Classic Risk Equation» [TTI16]. In his presentation, he stated that:

«Most of the history of what we call cyber security has been in that middle factor – vulnerability reduction. In the new paradigm, however, the consequence is what matters most. Breaches are an inevitability. They are going to get in. Get over it».

It is important to highlight that this presentation focused on cyber security in general. However, when applying this thinking to the petroleum sector, this paradigm shift raises a crucial question: should the industry, undergoing a radical digitalization, be focusing more on the potential consequences of a breach rather than investing heavily in vulnerability reduction? According to Hayden's perspective, while efforts to reduce vulnerabilities are important, they may not be sufficient to prevent breaches, necessitating a shift in focus toward mitigating the potential impacts of inevitable security breaches.

For instance, consider the example of an ICS that manages the production process in a petroleum refinery, which serves as the asset in this scenario. Threats might include cyber-attacks designed to disrupt these systems and cause production to stop or safety incidents. Examples of vulnerabilities could be software bugs in the ICS or weak network security. If the focus is solely on reducing these vulnerabilities, the company would likely employ software patch management processes, harden network security, and segregate the ICS network from others.

However, the consideration of consequences, such as a production stoppage or a safety incident, brings a different perspective to risk management. In addition to reducing vulnerabilities, the company might also invest in redundant systems that can quickly take over in case of a disruption, safety systems that can bring the process to a safe state, and emergency plans to manage any production loss.

Despite the emphasis on consequences, it does not imply that threats and vulnerabilities should be overlooked. On the contrary, a balanced approach that considers all parameters of the risk equation – threat, vulnerability, and consequence – is essential. Can we assume that reducing vulnerabilities will necessarily reduce the likelihood of threats exploiting them, leading to fewer consequences? This might not always be the case, as it can depend on the complexity of the threat landscape and the nature of the vulnerabilities present. Hence, it's crucial to view risk as a holistic concept involving all these factors.

In Section 2.5, we explored how assets, threats, and vulnerabilities form the triangle in the VTS model. Similarly, another triangle can be formed by threat, vulnerability, and consequence. But if we were to substitute consequences for assets, does this offer a new perspective on how we approach risk assessment? After all, consequences directly impact the functionality and integrity of assets. Thus, the two triangles bear similarities. This prompts companies to evaluate what is of utmost importance to them, directing their focus towards safeguarding it, whether it pertains to assets or consequences, or even both.

5.1.4 Risk Assessment Going Forward

Improving risk assessment in the future is crucial as cyber security and its associated threats continue to evolve. To enhance risk management practices going forward, we recommend the following suggestions:

Continuously updating and refining risk assessment strategies

Cyber threats are a moving target. New vulnerabilities are discovered daily, and cybercriminals are constantly developing new methods of attack. Therefore, organizations must be cautious and continuously update their risk assessment strategies to keep up with this ever-evolving landscape. Regular cyber security audits and threat assessments should be conducted to identify new vulnerabilities and potential threats. These findings can then be incorporated into the existing risk assessment strategy, ensuring it remains relevant and effective.

Adopting a proactive approach to risk assessment

Traditionally, many organizations have taken a reactive approach to cyber security, responding to incidents after they occur. However, a proactive approach that focuses on identifying potential threats and consequences before they happen can be more effective in preventing breaches. This might involve regular threat-hunting exercises, investing in advanced threat detection technologies, or using predictive analytics to identify potential future threats.

Developing robust emergency plans

Even with the best cyber security measures in place, the possibility of a breach cannot be entirely eliminated. Therefore, it is important to have robust emergency plans in place to manage the impact of potential security breaches. These plans should detail the steps to be taken in the event of a breach, including incident response, communication strategies, and recovery plans. Regular drills should be conducted to ensure all stakeholders are familiar with their roles in the event of a breach.

Utilize external expertise

Cyber security is a specialized field, and it may not always be feasible for organizations to have all the necessary expertise in-house. Therefore, it can be beneficial to use external expertise where necessary. This might involve partnering with threat intelligence companies, hiring cyber security consultants, or participating in information sharing forums or similar. Such partnerships can provide organizations with valuable insights into the latest threat trends and best practices in cyber security.

Building a strong cyber security culture

Cyber security is not just a technical issue, but also a cultural one. It is important for all staff, not just those in IT, to understand their role in maintaining security. This involves regular training and awareness programs to ensure all staff knows how to recognize potential threats and how to respond. It is also important to foster a culture where staff feel comfortable reporting potential security issues, without fear of blame.

Regularly reviewing and updating cyber security measures

Technology is always advancing, and so are the methods used by cybercriminals. Therefore, it is important for organizations to regularly review and update their cyber security measures to ensure they are using the latest and most effective technologies available for their company. This might involve upgrading outdated security software, implementing new security protocols, or investing in emerging technologies such as artificial intelligence or machine learning for threat detection.

Our research emphasizes the need for every operating company to manage cyber security risks. Different models like the VTS, Risk and Vulnerability Analysis (ROS), and the Risk Equation provide unique risk assessment perspectives, suggesting that focusing solely on reducing vulnerabilities is not sufficient. Rather, a balanced approach considering threats, vulnerabilities, and assets/consequences is required. Future risk assessments should be dynamic, proactively identifying threats and regularly updating risk strategies. The petroleum sector needs to strive for a balanced, coordinated risk assessment strategy that involves increased cyber security awareness, improved tools, standardized practices, and shared best practices across the industry.

5.1.5 Threat Analysis

Several important elements regarding the state of threat analysis in the petroleum sector are presented in our results. These will be discussed here.

Individual and Unstructured Threat Analysis

It appears that all operators perform threat analysis individually and unstructured, some even during leisure time. While this shows dedication and informal awareness, it raises questions about the consistency and comprehensiveness of these efforts. The lack of a standardized approach could potentially lead to missed threats or disparities in assessment quality. We think that it is unnecessary that all operators are conducting the same task and that there is great potential for centralizing this task.

Insufficiency of Existing Threat Intelligence Reports

The findings point towards the insufficiency of public reports from entities like NSM, PST, and NIS for practical application, particularly in the realm of industrial IT and OT. While these reports provide threat intelligence, their lack of specificity due to sensitive information and limited focus on industrial IT and OT reduces their effectiveness. To enhance this aspect, interviewee E stated that «The NSM are able to present how their report is relevant for the petroleum sector in a forum». We think measures like this will increase the value of the existing reports. The PSA also have a responsibility with interpreting and conveying this information to the sector, so they could be facilitating this.

Restricted Access to Information

The restricted access to classified reports creates an uneven distribution of information, hindering stakeholders from being fully informed about vulnerabilities. As this mostly affects the smaller operators, this is unlucky because they are also the ones with the least resources to carry out risk assessments in the first place, creating even more unbalance in the sector. This will further «lower the fence» and make these operators a more attractive target for cyber attacks.

Overwhelming Number of Service Providers

The rise in threat landscape-related service providers seems to be a double-edged sword. While these services can potentially help operators, especially smaller ones, the repetitive information presented in varying manners can be overwhelming. This, coupled with the potential incentive these providers have to over-hype the threat landscape, makes it necessary for operators to be perceptive.

Need for Summary Sources

The previous point and feedback from interviewees indicate the necessity for concise and consolidated sources of information concerning emerging threats and vulnerabilities. These summaries would assist operators in evaluating the relevance of information without being overwhelmed by the extensive volume of available data. While KraftCERT currently provides vulnerability notifications, our findings suggest that these notifications are not functioning optimally and can be improved. They cover both the electric power and the petroleum sector. Some of the systems can be similar, but there are distinct differences too, making notifications of vulnerabilities and recommendations superficial and not optimal. A similar approach is undertaken by Dragos, where they issue concise and informative weekly notifications. We believe it would be advantageous for KraftCERT to adopt a similar approach. An example report from Dragos can be found in [Inc22b].

Resource Disparity and External Dependence

The varying sizes and resources of operators seem to significantly affect their ability to perform comprehensive threat analysis. Smaller operators, due to financial, technological, and expertise constraints, rely more on external resources, such as third-party service providers and industry collaborations. This dependence may introduce additional risk as these external entities themselves may be targeted, leading to vulnerabilities for the smaller operators. Furthermore, smaller operators may have less control over the quality of threat analysis provided by these external entities.

Strategic Engagement by Consulting Firms

Consulting firms, including the one mentioned by interviewee C, offer a valuable service by engaging with large enterprises at a strategic level. These firms can contribute to a more tactical and operational approach to threat analysis. However, the drawback is that the costs associated with their services often limit accessibility to larger companies, highlighting the resource disparity between larger and smaller operators. Is it feasible for the entire sector to benefit from the valuable threat analysis services provided by these firms? One possibility is to explore a collaborative engagement at the sector level. This would require a thorough assessment of the feasibility of such an approach, and we encourage key decision-makers to engage in further discussions on this matter.

The findings indicate a requirement for an improved, coordinated, and readily available approach to threat analysis in the petroleum sector. Enhancing collaboration and information sharing, both internally within the sector and with external entities such as NSM, KraftCERT, and consulting agencies, can alleviate some of these challenges. Additionally, the development of targeted threat intelligence tailored to the sector's specific needs would be advantageous. These findings make a valuable contribution to the ongoing discourse on enhancing cyber security in the petroleum sector with the rapid changes in the threat landscape.

5.1.6 Incident Reporting and Exercises

Incident Reporting

The primary objective of incident reporting is to obtain a comprehensive overview of incidents occurring within the sector. Operators are legally obligated to report incidents to the appropriate entities, as outlined in Subsection 4.4.1. However, it is crucial to establish effective frameworks and reporting tools to ensure that this reporting process does not create additional liabilities for the operators.

It is important to acknowledge that incident reporting, limited to the NCS, provides only a partial understanding of the overall situation within the sector. Relying solely on NCS data can present a narrow perspective and may not capture the complete picture of incidents occurring throughout the entire industry. Considering the existence of other prominent companies that engage in incident reporting on a larger scale, it can be argued that the current incident reporting lacks the desired level of usefulness.

Given these factors, it is recommended to explore alternative approaches by allocating resources and efforts toward utilizing other specialized sources that can provide a more comprehensive overview of incidents within the sector. By leveraging these additional sources, the petroleum sector can potentially gain a broader and more accurate understanding of the incidents occurring across the industry. However, it is crucial to maintain compliance with regulations and laws, and not solely rely on external actors to gain an overview of incidents in the sector. Balancing the utilization of specialized sources while fulfilling regulatory obligations is a critical consideration.

A comprehensive assessment is needed to determine the most effective approach for handling incident reporting within the sector. This assessment should explore the allocation of resources, evaluate the reliability and usefulness of various sources, and ensure compliance with existing and new regulations. By conducting a thorough evaluation, the industry can establish a more robust incident reporting framework that strikes a balance between regulatory requirements and gaining a comprehensive understanding of incidents occurring within the petroleum sector.

Exercises and Incident Response Plans

Based on our research, it has become evident that a significant number of operators in the petroleum sector do not have robust incident response plans in place, nor do they regularly conduct exercises specifically focused on cyber incidents. This lack of emphasis on cyber security in incident response and exercises raises concerns and highlights the need for a stronger focus on addressing cyber threats.

Having comprehensive incident response plans is crucial for effectively managing and mitigating cyber incidents. These plans outline the appropriate actions to be taken when an incident occurs, ensuring a swift and coordinated response. However, our findings indicate that many operators have yet to develop comprehensive plans that specifically address cyber security incidents.

Furthermore, regular exercises play a vital role in assessing an organization's preparedness and ability to respond effectively to cyber incidents. Unfortunately, our research reveals that exercises related to cyber incidents are not conducted frequently enough in the petroleum sector. This lack of regular exercises constrains the operators' ability to identify weaknesses, improve their response procedures, and enhance their overall cyber security maturity.

To address these shortcomings, it is crucial for operators to place a higher priority on cyber security in their incident response planning and exercises. This entails developing comprehensive incident response plans that specifically address cyber incidents and conducting regular exercises that simulate cyber attack scenarios. By doing so, operators can enhance their readiness to handle cyber incidents effectively and minimize the potential impact on their operations and critical infrastructure.

Ultimately, a stronger focus on cyber security in incident response planning and exercises will contribute to a more resilient and secure petroleum sector, better equipped to mitigate and respond to the evolving cyber threats that pose a significant risk to the industry. As a recommendation, we will encourage them to allude to the master's thesis by Skytterholm and Hotvedt [SH21], which delves deeper into this topic.

5.2 Audits

Our findings explore the practice of cyber security audits in the petroleum sector. The irregularity of the audits based on supervision needs prompts further discussion as it could potentially expose vulnerabilities due to varying frequencies of audits among operators.

Expansion of Cyber Security Division

The expansion of the cyber security division at PSA indicates a growing recognition of the increasing importance of cyber security in the petroleum industry. This highlights the industry's acknowledgment of the evolving threat landscape and the need to prioritize cyber security measures to safeguard critical operations and assets. However, we suggest that further expansion of the division should be considered due to the limited capacity to conduct audits.

Current Audit Practices and the Purpose of Audits

The observations by interviewees E and I suggest that audits may not yet be comprehensive or in-depth enough to fully assess and ensure robustness, understanding, and cyber security culture within companies. This highlights a core question around the purpose of audits: should they merely ensure compliance, or should they also foster a deeper understanding and improvement of systems and processes? While compliance with regulations is crucial, a more proactive approach could be beneficial, particularly as it is evident that many operators lack systematic control over their systems and lack effective approaches to addressing cyber security vulnerabilities. The feedback from operator companies suggests that audits have the added benefit of compelling them to thoroughly review their systems further. This reinforces the idea that audits can serve as catalysts for improvement, not just compliance checks. A report from Sopra Steria [GTA+22] concluded that «... supervision inadequately identifies the instances in which management systems and internal control do not function in the manner in which they are often presented by the companies». This is interesting because the report is based on interviews with operators, whereas interviewee E is a former PSA-employee. This highlights some of the difficulties of having function-based rather than prescriptive regulations. The conflict between function-based and prescriptive regulations poses an interesting dilemma. While function-based regulations may offer flexibility, they could also lead to a lack of clarity and specificity, making it difficult to enforce and assess compliance.

The Prioritization of OT over IT

The prioritization of OT over IT within the audits, given the growing convergence of these domains, presents another point of contention. As digitalization continues to blur the lines between IT and OT, there's a significant risk that IT vulnerabilities could impact OT systems. It could be advantageous to consider auditing these aspects as a unified, interconnected system, rather than separate entities. We believe this could be justified under Petroleumsloven § 9-3. The usefulness of penetration tests to identify vulnerabilities is well-noted but the lack of authority to require such tests could be a point of potential improvement in the auditing process. Requiring such tests would enhance the overall cyber security in the sector.

Overall, our findings reveal the dynamic and complex nature of audits in the petroleum sector, particularly within the context of cyber security. While significant strides have been made in expanding the role and frequency of these audits, the findings suggest there is still much room for improvement to ensure more thorough and comprehensive audits, increased focus on the interplay between IT and OT, and perhaps most importantly, an emphasis on audits as a tool for continuous improvement rather than just a compliance check.

5.2.1 «Audit Light»

Our results propose the introduction of a lighter form of audit, referred to as «audit light», in the petroleum sector. This is meant to ensure a continuous focus on cyber security and presents an innovative and practical solution. It directly addresses the PSA's main issue for 2023 related to security against deliberate attacks in all phases of the petroleum industry. This proposal integrates the idea of self-assessment as a crucial part of maintaining cyber security standards. However, some points can be discussed further.

Frequency and Timing of Audits

Though the proposed «audit light» is aimed to make the cyber security measures more continuous, it is essential to consider the optimal frequency and timing of these audits. Annual self-assessments might be a start, but given the dynamic nature of cyber threats, more frequent assessments may be needed to remain updated with the rapidly evolving cyber threat landscape.

Reliability and Validity of Self-Assessments

One potential concern here could be the reliability of self-assessments. Given the importance of cyber security in the petroleum sector, it is crucial to ensure that self-assessments accurately reflect the reality of the cyber security measures in place. Furthermore, self-assessments may suffer from bias, as operators might be inclined to present their security posture in a better light. Our findings propose the inclusion of concrete examples of how threats or vulnerabilities are addressed to ensure the self-assessments reflect reality. While this is a step in the right direction, some form of external validation might still be required to ensure objectivity. One approach to achieving this could involve conducting interviews with a randomly selected group of operators in each round. Another approach could be to further investigate operators where the self-assessment raises unanswered questions.

Audit Light Framework

The proposed light audits could benefit from a clear framework to guide companies through the process. The NOG104 guideline, discussed in Section 2.4, can serve as a valuable resource for audits as it is widely adopted by both operators and the PSA. According to interviewee J, NOG104 provides a structured approach to conducting assessments and offers a more feasible alternative to evaluating against the comprehensive and challenging IEC 62443 standards. It presents a straightforward method for identifying major vulnerabilities in the system. However, it is important to acknowledge that NOG104 has certain limitations. Firstly, its documentation explicitly states that it is not intended for external reporting purposes. Additionally, interviewees have pointed out that NOG104 may not necessarily uncover major vulnerabilities and that it is outdated in some aspects. This suggests that adjustments should be considered if NOG104 is to be effectively utilized.

Furthermore, we have learned that NSM is in the process of developing a set of fundamental principles for OT, which is likely to be launched later this year. It would be advisable to evaluate these principles and assess their suitability as a framework for the audit guidelines. Incorporating the latest industry standards and guidelines, such as those being developed by NSM, would enhance the relevance and effectiveness of the audit process.

While the NOG104 guideline offers a starting point, a more detailed and specific structure could facilitate consistency across the sector and ensure important areas are not overlooked.

«Audit Light» and Regular Audits

Balancing between regular audits and the proposed light audits might present a challenge. An analysis of how these two types of audits could complement each other, avoiding redundancy, and ensuring that all necessary aspects are covered would be valuable.

Evolving Threat Landscape

Given that the threat landscape in cyber security is constantly changing, the assessments should not only include current threats but also anticipate future vulnerabilities and threats. This will require continuous updating of the assessment tools and a proactive approach to cyber security. An option to consider is incorporating newly emerging threats within the evolving landscape and assessing how operators are managing them.

Training

There may be a need for additional training for staff to conduct these light audits effectively. This could potentially involve a comprehensive understanding of the framework used, cyber threats, and best practices in cyber security. To facilitate this, the PSA could explore various approaches such as developing an online training module, conducting on-site visits to operators, or organizing workshops to initiate the implementation of light audits.

Implementation and Regulatory Oversight

The implementation of light audits may involve a significant investment of time and resources, especially in the initial phases. It is essential to examine the long-term cost-effectiveness of this approach compared to other methods of enhancing cyber security management at a sector level. Additionally, the role of regulatory bodies such as the PSA should be explored. Should they perform periodic checks to validate self-assessments? What sanctions or incentives could be implemented to ensure compliance and the effectiveness of these light audits?

The proposition of audits light presents a starting point for addressing the issue of sporadic cyber security audits in the petroleum industry. By providing these points of discussion, the idea can be further refined and developed into a comprehensive solution.

5.3 Information Sharing

Our research provides a thorough exploration of information sharing in the Norwegian petroleum sector, highlighting the crucial role of both formal and informal communication channels. From the analysis, there are several key points worthy of further discussion.

Informal vs. Formal Communication

Our findings demonstrate that information sharing in the petroleum sector occurs both formally and informally. An interesting observation was that informal forums were preferred for their flexibility and discretion. There is a clear need to strike a balance between these communication forms. While informal methods foster open discussions without fear of repercussions, formal channels can provide structure, reach a broader audience, and ensure valuable information does not get lost in the fray. A further examination of how more information can be shared, both formally and informally, should be conducted.

Understanding and Contextualizing Information

Additionally, our findings underscore the importance of properly interpreting and contextualizing data to convert it into meaningful information. This process is critical in ensuring the knowledge and wisdom built from the data are accurate and applicable. Information sharing channels, therefore, need to not just distribute data but also provide the necessary support and resources to help operators understand and apply it in their specific contexts.

The Role of NSM and KraftCERT

Following, both NSM and KraftCERT play a significant role in spreading cyber security-related information. However, our findings suggest a need for improvement in sharing more sector-specific and context-specific vulnerability information. KraftCERT is doing well in providing notifications and suggested measures, but this often only reaches technicians and is not given the attention it needs by management. We propose that KraftCERT focuses on enhancing their notifications, as discussed in Subsection 5.1.5.

Establishment of Robust Information Sharing Platform

Our research aligns with the Sopra Steria report in calling for more comprehensive information sharing mechanisms [GTA+22]. This includes the need for more inclusive and focused platforms tailored to the specific needs of the petroleum sector. A platform that encourages dialogue, exchange of ideas, and distribution of vulnerability-specific knowledge could provide significant benefits. This would also guarantee that the sharing of information is conducted in a secure manner.

In conclusion, it is evident that there have been advancements in improving communication within the Norwegian petroleum sector. However, there are still opportunities for further improvement. By strengthening formal communication channels, establishing reliable and inclusive platforms for sharing information, and maintaining a focus on secure information exchange, the sector can continue to promote its cyber security efforts and enhance cyber security at a sector-wide level.

5.3.1 Cyber Security in RNNP

Our research initially focused on extending the application of the RNNP framework to include cyber security trends. However, we soon realized that this approach would be challenging and less effective than intended. The RNNP framework is designed to present historical data to prevent similar unwanted events, which works well for safety considerations since the threat landscape is relatively predictable. However, when it comes to cyber security, relying solely on historical data and trends does not provide the same value due to the rapidly changing and unpredictable nature of the threat landscape. It must be assumed that threat actors are continuously developing new methods to target critical infrastructure, making it difficult to predict future attacks.

One possible way to incorporate cyber security into the RNNP framework is by leveraging the results from the proposed «audits light». These results can be anonymized and used to present trends in the risk level related to cyber security. However, the specific implementation of this approach requires further assessment. Different operators use different vendors and systems, making it challenging to create a meaningful representation of the data. Quantification of cyber security risks can also be complex. Moreover, the limited number of operators raises concerns about the potential disclosure of sensitive information if the pseudonymized data is attributed to specific sources. Therefore, a careful examination is needed to determine if and how cyber security can be integrated into the RNNP framework.

Chapter 6 Conclusion and future work

6.1 Conclusion

In conclusion, this study has provided valuable insights into how risk associated with cybersecurity in the petroleum sector is currently addressed (RQ1), as well as proposed strategies for its effective management in the future (RQ2).

In response to RQ1, the study provides insights into how risk associated with cyber security in the petroleum sector is currently addressed. It highlights the existing risk assessment practices, incident reporting, and exercises in the industry. The audits conducted by the PSA play a crucial role in verifying compliance with regulations and identifying weaknesses. However, the research also emphasizes the need for a more comprehensive and continuous approach to cyber security beyond sporadic audits. The sharing of information within the sector, although taking place to some extent, can be further improved in terms of more structured and inclusive forums.

The study then moves onto RQ2, proposing several strategies to effectively address cybersecurity risks in the future. First, the establishment of «audit light» approaches, along with regular audits, can provide a more comprehensive overview of cyber security practices. These lighter audits can focus on management's approach to cyber security, the evolving threat landscape, and the effectiveness of measures in addressing changes in risk levels. Additionally, more informal and formal forums should be established to develop knowledge and facilitate information sharing about incidents, vulnerabilities, threats, and assets across specialist groups, companies, sectors, and government authorities. This will promote collaboration, enable the exchange of best practices, and enhance overall cyber security awareness in the sector.

In summary, addressing risk associated with cyber security in the petroleum sector requires a comprehensive and dynamic approach. By combining proactive measures, continuous evaluation, improved information sharing, and the introduction of an «audit light» approach, the sector can effectively mitigate cyber security risks and ensure the protection of critical infrastructure.

6.2 Future Research Directions

The results presented in this thesis are derived from interviews conducted with key individuals in the Norwegian petroleum industry. To delve deeper into the current state of risk assessment and explore strategies for addressing cyber security in the future, several avenues for future research can be considered.

Cyber Security Barrier Management (CBM-Project)

Our master's thesis contributes to the ongoing CBM Project conducted by SINTEF. The overall objective of this project is to contribute new knowledge and guidance for the continuous process of cyber security barrier management. This includes addressing both technical and non-technical aspects and bridging the domains of safety and cyber security [SINa]. It aims to provide insights and recommendations for effective cyber security barrier management throughout the development and operation of ICS. The CBM Project is scheduled to continue until the end of 2025 [SINb], and we hope that our research contributes positively to its progress and outcomes.

Expanding to Include the Supply Chain

One way of further exploration is to extend the focus of this work to encompass addressing risk associated with cyber security throughout the entire supply chain in the industry. In this thesis, the scope has been limited to operators due to time constraints. However, for a more comprehensive understanding of the real-world scenario, it is crucial to include the complete supply chain, including suppliers, vendors, and other actors involved in providing IT and OT equipment and solutions. Addressing cyber security across the entire supply chain, from A to Z, is essential to establish the optimal prerequisites for protecting against emerging threats and vulnerabilities. This represents a potential future task to be pursued.

Keeping up-to-date on the Landscape

At the time of writing, the threat landscape aligns with the findings presented in the mentioned threat assessments in Subsection 2.6.2. However, it is important to recognize that the landscape is dynamic and constantly evolving. As this thesis is published, new threats and attack vectors may have emerged, emphasizing the need for ongoing research and awareness in critical infrastructure such as the petroleum sector. The annual threat assessment from KraftCERT is coming later in June, giving more insight into the threat landscape. Future work should focus on analyzing and addressing the evolving threat landscape, ensuring that cyber security measures remain up-to-date and effective. Additionally, evaluating the impact and effectiveness of the contributions made in this thesis will help determine if adjustments or alternative approaches are necessary to address the ever-changing realm of cyber security.

References

[06] «Act relating to the right of access to documents held by public authorities and public undertakings (freedom of information act)», Lovdata. (2006), [Online]. Available: https://lovdata.no/dokument/NLE/lov/2006-05-19-16 (last visited: May 14, 2023).

[10] «Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften)», Lovdata. (2010), [Online]. Available: https://lovdata.no/dokument/LTI/forskrift/2010-04-29-611 (last visited: May 13, 2023).

[Bai14] L. F. Bailey. «The origin and success of qualitative research». (2014), [Online]. Available: https://journals.sagepub.com/doi/pdf/10.2501/IJMR-2014-013 (last visited: Apr. 26, 2022).

[Ben08] A. Benjamin, «Audit: How to do it in practice», vol. 336, 2008, https://www.bmj.com/content/bmj/336/7655/1241.full.pdf.

[BJD17] J. Bugeja, A. Jacobsson, and P. Davidsson, «An analysis of malicious threat agents for the smart connected home», in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017, pp. 557–562.

[CBD+14] N. Carter, D. Bryant-Lukosius, *et al.*, «The use of triangulation in qualitative research», *Oncology Nursing Forum*, vol. 41, no. 5, pp. 545–547, 2014.

[Con16] W. A. Conklin, «It vs. ot security: A time to consider a change in cia to include resilience», in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 2642–2647.

[DAN21] L. Dhirani, E. Armstrong, and T. Newe. «Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap». (2021), [Online]. Available: https://www.researchgate.net/figure/Timeline-and-history-of-ICS-cybersecurity-attacks_fig3_352152549 (last visited: Apr. 28, 2023).

[Dig18] Digital21. «Digitale grep for norsk verdiskaping,» (2018), [Online]. Available: https://www.regjeringen.no/contentassets/d018d0b1a7374cdf894b4cf7ff4fea81/digital21_endeligversjon.pdf (last visited: May 11, 2023).

[DMT+19] M. C. De Maggio, M. Mastrapasqua, M. Tesei, *et al.*, «How to improve the security awareness in complex organizations», *Eur J Secur Res*, vol. 4, pp. 33–49, 2019. [Online]. Available: https://doi.org/10.1007/s41125-017-0028-2.

[DNV17] DNV, «Cyber security in the oil and gas industry based on iec 62443», DNVGL, Tech. Rep. Recommended practice — DNVGL-RP-G108, 2017, Amended 2021.

[DNV19] DNV GL, «Håndtering av innsiderisiko», Technical Report, 2019. [Online]. Available: https://www.ptil.no/contentassets/d0de842c25b84fcebda5c24fe6daa6fa/handtering-av-innsiderisiko-rev-1.pdf (last visited: May 27, 2023).

[DNV22] DNV. «The cyber priority». Available at: https://www.dnv.com/cybersecurity/cyber-insights/thecyberpriority.html. (2022), (last visited: May 27, 2023).

[DNV23] DNV GL. «DNV GL». (2023), [Online]. Available: https://brandcentral.dnv.com/original/gallery/10651/files/original/5a2853da-dd83-4fa1-8071-253d93767198.pdf (last visited: May 28, 2023).

[Eur22a] Euronews. «Fears grow as more suspicious drones appear above Norway's offshore facilities». (2022), [Online]. Available: https://www.euronews.com/2022/10/23/fears-grow-as-more-suspicious-drones-appear-above-norways-offshore-facilities (last visited: Mar. 21, 2023).

[Eur22b] European Parliament and Council of the European Union. «Directive (EU) 2022/2555 of the European Parliament and of the Council». (2022), [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN (last visited: May 28, 2023).

[FG21] J.-M. Flaus and J. Georgakis, «A systemic approach for preliminary risk analysis of cybersecurity of industrial control systems», esrel2021-paper, Singapore: Research Publishing, 2021.

[Geo22] T. George. «Semi-structured interview | definition, guide & examples». (2022), [Online]. Available: https://www.scribbr.com/methodology/semi-structured-interview/ (last visited: Nov. 15, 2022).

[GL20a] D. GL, «Cyber security sis og egensikre komponenter, kommunikasjonsprotokoller», DNV GL, 2019-0826, 2020, Available at: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/dnv-gl---cyber-security-sis.pdf.

[GL20b] D. GL, «Regelverk og tilsynsmetodikk», DNV GL, 2019-0824, 2020, Available at: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/dnv-gl---regelverk-og-tilsynsmetodikk.pdf.

[GL20c] D. GL, «Resiliens mot cyberhendelser og kan blokkjede bidra?», DNV GL, 2019-0825, 2020, Available at: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/dnv-gl---resiliens-mot-cyberhendelser-og-kan-blokkjede-bidra.pdf.

[Gre15] A. Greenberg. «Hackers can disable a sniper rifle—or change its target». (2015), [Online]. Available: https://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/ (last visited: May 22, 2023).

[GTA+22] A. Grefsrud, K. Titlestad, *et al.*, «Protection of data at rest and in transit», Sopra Steria, 2022.

[Hah16] A. Hahn, «Operational technology and information technology in industrial control systems», in *Cyber-security of SCADA and Other Industrial Control Systems*, E. J. M. Colbert and A. Kott, Eds. Cham: Springer International Publishing, 2016, pp. 51–68. [Online]. Available: https://doi.org/10.1007/978-3-319-32125-7_4.

[HOJ+21] G. K. Hanssen, T. Onshus, *et al.*, «Principles of digitalisation and it-ot integration», SINTEF Digital, 2021:00057, 2021, Available at: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/sintef---report---principles-of-digitalisation-and-it-ot-integration.pdf.

[Inc17] D. Inc., «CRASHOVERRIDE: Analysis of the threat to electric grid operations», Report, 2017.

[Inc22a] D. Inc. «CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS)». (2022), [Online]. Available: https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/ (last visited: May 27, 2023).

[Inc22b] D. Inc. «Dragos worldview report sample 2022». (2022), [Online]. Available: https://www.dragos.com/wp-content/uploads/2023/02/dragos-worldview-report-sample-2022-44-TLP-CLEAR-1.pdf (last visited: May 24, 2023).

[Inc23] D. Inc. «ICS/OT Cybersecurity Year In Review 2022». (2023), [Online]. Available: https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Report-2022.pdf?hsLang=en (last visited: Feb. 14, 2023).

[Int09] International Electrotechnical Commission (IEC), *Industrial communication networks - network and system security - part 1-1: Terminology, concepts and models*, 2009.

[Int10] International Electrotechnical Commission (IEC), *Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program*, 2010.

[Int12] S. E. International. «Puerto rico smart meters believed to have been hacked – and such hacks likely to spread». (2012), [Online]. Available: https://www.smart-energy.com/regional-news/north-america/puerto-rico-smart-meters-believed-to-have-been-hacked-and-such-hacks-likely-to-spread/ (last visited: May 22, 2023).

[Int19] International Electrotechnical Commission (IEC), *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*, 2019.

[Int20] International Electrotechnical Commission (IEC), *Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design*, 2020.

[Jan21] Jan Terje Sæterbø. «Ros eller vts – eller begge deler?» (2021), [Online]. Available: https://f24.com/no/ros-eller-vts-eller-begge-deler/ (last visited: May 27, 2023).

[JP14] P. Johannesson and E. Perjons, *An Introduction to Design Science*. Springer, 2014. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-07374-3_4.

[JWBK21] M. G. Jaatun, E. Wille, *et al.*, «Grunnprinsipper for ikt-sikkerhet i industrielle ikt-systemer», SINTEF Digital, 2021:00055, 2021, Available at: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id4-grunnprinsipper-for-ikt-sikkerhet_sintef-rapportnr-2021-00055-feb---signert.pdf.

[Kar21] S. Kardon. «Florida water treatment plant hit with cyber attack». (2021), [Online]. Available: https://www.industrialdefender.com/blog/florida-water-treatment-plant-cyber-attack (last visited: May 22, 2023).

[Ker22] S. M. Kerner. «Colonial pipeline hack explained: Everything you need to know». (2022), [Online]. Available: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know (last visited: May 30, 2023).

[Kje22] Kjetil Malkenes Hovland. «Norsk olje og gass skifter navn: Skal hete offshore norge», e24. (2022), [Online]. Available: https://e24.no/energi-og-klima/i/mrkv64/norsk-olje-og-gass-skifter-navn-skal-hete-offshore-norge (last visited: May 29, 2023).

[Kra] KraftCERT. «KraftCERT - Norwegian Energy CERT», KraftCERT. (), [Online]. Available: https://www.kraftcert.no/en/# (last visited: May 22, 2023).

[Kre11] KrebsOnSecurity. «Cyber intrusion blamed for hardware failure at water utility». (2011), [Online]. Available: https://krebsonsecurity.com/2011/11/cyber-strike-on-city-water-system/ (last visited: May 22, 2023).

[Leaa] C. Leadership. «Dikw model». (), [Online]. Available: https://conversational-leadership.net/dikw-model/ (last visited: May 25, 2023).

[Leab] LeanIX. «Saas vs. iaas vs. paas». (), [Online]. Available: https://www.leanix.net/en/wiki/saas/iaas-vs-paas-vs-saas (last visited: May 22, 2023).

[LGAH19] H. Lu, L. Guo, *et al.*, «Oil and gas 4.0 era: A systematic review and outlook», *Computers in Industry*, vol. 111, pp. 68–90, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361519302064.

[LK19] M. Linneberg and S. Korsgaard, «Coding qualitative data: A synthesis guiding the novice», *Qualitative Research Journal*, May 2019.

[Mat20] G. Mathisen, *Ros og vts-modeller - ingen er gode nok*, Aktuell Sikkerhet, 2020. [Online]. Available: https://www.aktuellsikkerhet.no/bjorn-melandso-kjelsaas-dss-guri-kjorven/ros-og-vtsto-modeller--ingen-er-gode-nok/619844 (last visited: May 30, 2023).

[MBFA06] M. McQueen, W. Boyer, *et al.*, «Quantitative risk reduction estimation tool for control systems: Suggested approach and research needs», Idaho National Lab. (INL), Idaho Falls, ID (United States), Tech. Rep. INL/CON-06-01255, Mar. 2006. [Online]. Available: https://doi.org/10.2172/911635.

[Mne21] Mnemonic AS, «Security report 2021», mnemonic AS, Technical Report, 2021. (last visited: May 27, 2023).

[MOL+21] T. Myklebust, T. Onshus, *et al.*, «Datakvalitet ved digitalisering i petroleumssektoren», SINTEF Digital, 2021:00053, 2021, Available at: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id2-datakvalitet-ved-digitalisering_sintef-rapportnr-2021-00053---signert.pdf.

[Mor19] C. Morgan. «Your data at risk: Fbi cyber division shares top emerging cyber threats to your enterprise». (2019), [Online]. Available: https://www.reliaquest.com/blog/your-data-at-risk-fbi-cyber-division-shares-top-emerging-cyber-threats-to-your-enterprise/ (last visited: May 27, 2023).

[MTE+21] P. Meland, S. Tokas, *et al.*, «A systematic mapping study on cyber security indicator data», *Electronics*, vol. 10, no. 9, p. 1092, 2021. [Online]. Available: https://doi.org/10.3390/electronics10091092.

[Nas] Nasjonalt cybersikkerhetssenter. «Varsler fra NCSC». (), [Online]. Available: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/ (last visited: May 26, 2023).

[Nat16] National Security Authority of Norway (NSM). «Håndbok: Risikovurdering for sikring». (2016), [Online]. Available: https://www.nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf (last visited: May 27, 2023).

[Nat18] National Institute of Standards and Technology, «Framework for improving critical infrastructure cybersecurity, version 1.1», Tech. Rep., 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[NIS09] NIST. «About nist». Last updated 2022. (2009), [Online]. Available: https://www.nist.gov/about-nist (last visited: Jun. 1, 2023).

[NIS23] NIS Norwegian Intelligence Service, «Fokus 2023 - etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer», Technical Report, 2023. (last visited: May 27, 2023).

[Nor15] NorSIS, *Kommune cert–utredning av behov og muligheter*, 2015. [Online]. Available: https://norsis.no/content/uploads/2022/06/KommuneCSIRT-print.pdf (last visited: May 31, 2023).

[Nor16] Norwegian Oil and Gas Association, «104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems», Tech. Rep., 2016.

[Nor17] P. Norway, «Principles for barrier management in the petroleum industry barrier memorandum 2017», Petroleum Safety Authority Norway, Tech. Rep., 2017.

[Nor23] Norwegian Ministry of Justice and Public Security. «Nis-direktivet». (2023), [Online]. Available: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/ (last visited: May 26, 2023).

[NRK22] NRK. «Sikkerhetslovens far: - oljebransjen er ikke godt nok forberedt». (2022), [Online]. Available: https://www.nrk.no/norge/sikkerhetslovens-far_-_-oljebransjen-er-ikke-godt-nok-forberedt-1.16129483 (last visited: May 15, 2023).

[NSD21] NSD. «Strukturendring i kunnskapssektoren». (2021), [Online]. Available: https://www.nsd.no/artikkel/strukturendring-i-kunnskapssektoren/ (last visited: Jun. 1, 2023).

[NSMa] NSM, *Risikovurdering av ikt-systemer.* [Online]. Available: https://nsm.no/getfile.php/136603-1625054089/NSM/Filer/Bildegalleri/Bilder%5C%20til%5C%20grunnprinsipper/Risikovurdering%5C%20av%5C%20IKT-systemer.pdf (last visited: May 30, 2023).

[NSMb] N. N. S. A. NSM. «About the norwegian national security authority». (), [Online]. Available: https://nsm.no/about-nsm/about-the-norwegian-national-security-authority/ (last visited: May 8, 2023).

[NSM23] NSM Norwegian National Security Authority, «Risiko 2023», Technical Report, 2023. (last visited: May 27, 2023).

[NTN] NTNU. «Ttm4502 - communication technology, specialization project». (), [Online]. Available: https://www.ntnu.edu/studies/courses/TTM4502#tab=omEmnet (last visited: May 16, 2023).

[Nær22] Næringslivets Sikkerhetsråd, «Mørketallsundersøkelsen 2022», Næringslivets Sikkerhetsråd, 2022, Available at: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen. (last visited: May 11, 2023).

[OBH+21] T. Onshus, L. Bodsberg, *et al.*, «Ict security and independence», SINTEF Digital, 2021:01387, 2021, Available at: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/sintef---report---ict-security-and-independence.pdf.

[OBH+22] T. Onshus, L. Bodsberg, *et al.*, «Security and independence of safety systems», *J. Cybersecur. Priv.*, vol. 2, pp. 20–41, 2022, https://doi.org/10.3390/jcp2010003.

[oFin20] T. M. of Finance Norway. «Meld. st. 2 - melding til stortinget - revidert nasjonalbudsjett 2020». (2020), [Online]. Available: https://www.regjeringen.no/contentassets/f7f31a9baf3e49c1ad1fa72da5585003/no/pdfs/stm201920200002000dddpdfs.pdf (last visited: May 11, 2023).

[Pau20] K. Paul. «What you need to know about the biggest hack of the us government in years». (2020), [Online]. Available: https://www.theguardian.com/technology/2020/dec/15/orion-hack-solar-winds-explained-us-treasury-commerce-department (last visited: May 27, 2023).

[Peta] N. Petroleum. «Companies». (), [Online]. Available: https://www.norskpetroleum.no/en/facts/companies-production-licence/ (last visited: May 11, 2023).

[Petb] N. Petroleum. «State organisation of petroleum activities». (), [Online]. Available: https://www.norskpetroleum.no/en/framework/state-organisation-of-petroleum-activites/ (last visited: May 13, 2023).

[Pet19] Petroleumstilsynet (PTIL), *Brev - handtering av ikt-sikkerhet*, https://www.ptil.no/contentassets/cdf45185805f4c14bc7caf03f6853d08/2019_1176-brev-handtering-av-iktsikkerhet.pdf, 2019. (last visited: Jun. 5, 2023).

[Pet21] Petroleum Safety Authority Norway. «PTIL - Role and Responsibility». (2021), [Online]. Available: https://www.ptil.no/om-oss/rolle-og-ansvarsomrade/ (last visited: May 22, 2023).

[Pet23] Petroleum Safety Authority Norway. «Main issue 2023 - technical competence». (2023), [Online]. Available: https://www.ptil.no/en/technical-competence/main-issue-2023/ (last visited: May 23, 2023).

[PSAa] PSA. «OM RNNP». (), [Online]. Available: https://www.rnnp.no/om-rnnp/ (last visited: May 31, 2023).

[PSAb] T. P. S. A. N. PSA. «Audit reports». (), [Online]. Available: https://www.ptil.no/en/supervision/audit-reports/ (last visited: May 8, 2023).

[PSA19] PSA. «The psa's role and area of responsibility». (2019), [Online]. Available: https://www.ptil.no/en/about-us/role-and-area-of-responsibility/ (last visited: Mar. 22, 2023).

[PSA20] T. P. S. A. N. PSA. «Ict security – robustness in the petroleum sector». (2020), [Online]. Available: https://www.ptil.no/en/technical-competence/explore-technical-subjects/reports-from-projects/2020/ict-security--robustness-in-the-petroleum-sector/ (last visited: May 14, 2023).

[PSA21a] T. P. S. A. N. PSA. «Ict security – robustness in the petroleum sector ii». (2021), [Online]. Available: https://www.ptil.no/en/technical-competence/explore-technical-subjects/reports-from-projects/2021/ict-security--robustness-in-the-petroleum-sector-ii/ (last visited: May 14, 2023).

[PSA21b] T. P. S. A. N. PSA. «Industrial ict systems». (2021), [Online]. Available: https://www.ptil.no/en/technical-competence/explore-technical-subjects/news/2021/ict-security---robustness-in-the-industry/ (last visited: May 14, 2023).

[PST20] PST Norwegian Police Security Service, «Etteretningstrusselen mot norsk petroleumssektor», The Norwegian Police Security Service, Technical Report, 2020. (last visited: May 27, 2023).

[PST23] PST Norwegian Police Security Service, «Nasjonal trusselvurdering 2023», Technical Report, 2023. (last visited: May 27, 2023).

[Reg22] Regjeringen. «Prop. 109 l (2022–2023)». (2022), [Online]. Available: https://www.regjeringen.no/no/dokumenter/prop.-109-ls-20222023/id2975558/?ch=1 (last visited: May 31, 2023).

[Rik19] Riksrevisjonen, «Riksrevisjonens undersøkelse av petroleumstilsynets oppfølging av helse, miljø og sikkerhet i petroleumsvirksomheten», 2019. [Online]. Available: https://www.riksrevisjonen.no/globalassets/rapporter/no-2018-2019/petroleumstilsynet.pdf (last visited: May 14, 2023).

[Rik23] Riksrevisjonen. «Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor». (2023), [Online]. Available: https://www.riksrevisjonen.no/globalassets/rapporter/NO-2022-2023/myndighetenes-samordning-av-arbeidet-med-digital-sikkerhet-i-sivil-sektor.pdf.

[SFS11] K. Stouffer, J. Falco, and K. Scarfone. «Guide to industrial control systems (ics) security», NIST. (2011), [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf (last visited: May 11, 2023).

[SH21] A. N. Skytterholm and G. Hotvedt, «Preparedness exercises for cyber attacks against industrial control systems in the petroleum industry», M.S. thesis, NTNU, 2021.

[SINa] SINTEF. «Cds-forum». (), [Online]. Available: https://cds-forum.com/ (last visited: May 16, 2023).

[SINb] SINTEF. «Cybersecurity barrier management». (), [Online]. Available: https://www.sintef.no/en/projects/2021/cybersecurity-barrier-management/ (last visited: May 22, 2023).

[Slo19] J. Slowik, *Stuxnet to crashoverride to trisis: Evaluating the history and future of integrity-based attacks on industrial environments*, Dragos, 2019. [Online]. Available: https://www.dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf.

[SW21] S. Shackelford and M. Wade. «Colonial pipeline forked over $4.4m to end cyberattack – but is paying a ransom ever the ethical thing to do?» (2021), [Online]. Available: https://theconversation.com/colonial-pipeline-forked-over-4-4m-to-end-cyberattack-but-is-paying-a-ransom-ever-the-ethical-thing-to-do-161383 (last visited: May 30, 2023).

[Tjo17] A. Tjora, *Kvalitative forskningsmetoder i praksis.* Gyldendal Norsk Forlag AS, 2017.

[TTI16] TTI/Vanguard. «Gen michael hayden - cybersecurity and intelligence». (Oct. 2016), [Online]. Available: https://www.youtube.com/watch?v=am-0nKhkBuA (last visited: May 30, 2023).

[Uni23a] G. S. University. «Literature reviews: 3. search the literature». (2023), [Online]. Available: https://research.library.gsu.edu/c.php?g=115595&p=818161 (last visited: May 22, 2023).

[Uni23b] G. S. University. «Research guides, literature reviews: Introduction». (2023), [Online]. Available: https://research.library.gsu.edu/litrev (last visited: May 14, 2023).

[Wie14] R. Wieringa, *Design Science Methodology for Information Systems and Software Engineering.* Jan. 2014, pp. 1–332.

[Wil12] V. Wilson, «Research methods: Interviews», *Evidence Based Library and Information Practice*, pp. 96–98, 2012.

[Wil15] M. Williams. «Bmw cars found vulnerable in connected drive hack». (2015), [Online]. Available: https://www.pcworld.com/article/431610/bmw-cars-found-vulnerable-in-connected-drive-hack.html (last visited: May 22, 2023).

[Wil20] J. Williams. «What you need to know about the solarwinds supply-chain attack». (2020), [Online]. Available: https://www.sans.org/blog/what-you-need-to-know-aboutthe-solarwinds-supply-chain-attack/ (last visited: May 27, 2023).

[Zio16] E. Zio, «Critical infrastructures vulnerability and risk analysis», *European Journal for Security Research*, vol. 1, Oct. 2016.

[ZL21] P. Zhu and J. Liyanage, «Cybersecurity of offshore oil and gas production assets under trending asset digitalization contexts: A specific review of issues and challenges in safety instrumented systems», *European Journal for Security Research*, vol. 6, Dec. 2021.

[ØBJ+21] K. Øien, L. Bodsberg, *et al.*, «Regulation of ict security in the petroleum sector», SINTEF Digital, 2021:00054, 2021, Available at: https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/sintef---report--regulation-of-ict-security-in-the-petroleum-sector---en.pdf.

Appendix A
Sikt/NSD Application

When including personal information in academic work, it is necessary to obtain the required permissions as mandated by Sikt. Sikt was formerly know as the Norwegian Center for Research Data (NSD).The following information was filled out in the application to Sikt/NSD.

Sikt

Meldeskjema / Masteroppgave / Eksport

Meldeskjema

Referansenummer
122600

Hvilke personopplysninger skal du behandle?

- Navn (også ved signatur/samtykke)
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

Beskriv hvilke bakgrunnsopplysninger du skal behandle

Stilling og arbeidsområde for utvalget hvor relevant informasjon angående risikovurdering i deres bedrift vil bli behandlet samt lydopptak av stemme

Prosjektinformasjon

Prosjekttittel

Masteroppgave

Prosjektbeskrivelse

Masteroppgave ved IIK NTNU, Risikovurdering i petroleumssektor

Begrunn hvorfor det er nødvendig å behandle personopplysningene

Opptak av intervju med utvalget for riktig sitering og informasjon rettet mot masteroppgave. Utvalget og bedriften de jobber for vil bli anonymisert gjennom masteroppgaven med mindre det er strengt nødvending (meget usannsynlig) å nevne. Det vil i så fall bli gjort en avtale med den/de det gjelder angående bruk av navn/stilling og/eller bedrift hvis dette skulle være aktuelt. Intervjuguiden, vedlagt for Utvalg 1, vil gå mer inn på behandlingen av personopplysninger og hva utvalget får av informasjon om deres opplysninger.

Prosjektbeskrivelse

Specialization_project_Simen_Andreas.pdf

Ekstern finansiering
Ikke utfyllt
Type prosjekt
Studentprosjekt, masterstudium

Kontaktinformasjon, student
Andreas Johan Nyland, andreas.johan.nyland@gmail.com, tlf: 40765765

Behandlingsansvar

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)
Maria Bartnes, maria.bartnes@ntnu.no, tlf: 45218102

Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?
Nei

Utvalg 1

Beskriv utvalget

Ledere og personer med toppstillinger innenfor petroleumssektor når det kommer til cybersikkerhet.

Beskriv hvordan rekruttering eller trekking av utvalget skjer

Rekrutteringen skjer i et nettverk innenfor petroleumssektoren i Norge hvor personene jobber eller har jobbet innenfor sektoren med relevans til risikovurdering av informasjonsteknologi.

Alder
25 - 80

Personopplysninger for utvalg 1

- Navn (også ved signatur/samtykke)
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

Hvordan samler du inn data fra utvalg 1?

Personlig intervju

Vedlegg

Intervjuguide.pdf

Grunnlag for å behandle alminnelige kategorier av personopplysninger
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Informasjon for utvalg 1

Informerer du utvalget om behandlingen av personopplysningene?
Ja

Hvordan?
Skriftlig informasjon (papir eller elektronisk)

Informasjonsskriv

Informasjon til deltakere.pdf

Tredjepersoner

Skal du behandle personopplysninger om tredjepersoner?
Nei

Dokumentasjon

Hvordan dokumenteres samtykkene?

- Elektronisk (e-post, e-skjema, digital signatur)

Hvordan kan samtykket trekkes tilbake?

Skriftlig (e-post) og muntlig

Hvordan kan de registrerte få innsyn, rettet eller slettet personopplysninger om seg selv?

Vil utveksle kontaktinformasjon med registrerte hvor de har mulighet til å få tilsendt personopplysningene og lydopptakene. Skal også la de registrerte få sjekke sitater.

Totalt antall registrerte i prosjektet
1-99

Tillatelser

Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?
Ikke utfyllt

Behandling

Hvor behandles personopplysningene?

- Ekstern tjeneste eller nettverk (databehandler)

Hvem behandler/har tilgang til personopplysningene?

- Student (studentprosjekt)
- Databehandler

Hvilken databehandler har tilgang til personopplysningene?

Da dataene er interne vil NTNUs skytjenester være tilstrekkelige for lagring og behandling av data. Dermed vil databehandler være Office 365, nærmere bestemt Teams og OneDrive.
Ref: https://i.ntnu.no/wiki/-/wiki/Norsk/Lagringsguide

Tilgjengeliggjøres personopplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?
Nei

Sikkerhet

Oppbevares personopplysningene atskilt fra øvrige data (koblingsnøkkel)?
Ja

Hvilke tekniske og fysiske tiltak sikrer personopplysningene?

- Adgangsbegrensning
- Flerfaktorautentisering
- Endringslogg
- Adgangslogg
- Andre sikkerhetstiltak

Hvilke

Automatisk tastelås på PC etter kort tid

Varighet

Prosjektperiode
09.01.2023 - 02.06.2023

Hva skjer med dataene ved prosjektslutt?
Data slettes (sletter rådataene)

Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?
Ja

Begrunn

Vil kunne forekomme referanser til intervjuer og samtaler med personer i oljesektoren og hva de sier angående risikovurdering i sin bedrift. Dette er kun aktuelt ved samtykke.

Tilleggsopplysninger

Angående masteroppgaven så blir denne skrevet sammen med Simen Endre Bergset som også studerer Kommunikasjonsteknologi og Digital Sikkerhet på NTNU. Siden vi jobber på samme prosjekt vil også han ha tilgang til dataene vi samler inn og er underlagt de retningslinjene som er beskrevet gjennomgående her. Dette vil også gjelde våre veileder, Maria Bartnes, Thor Buan og Roy Myhre som vi vil diskutere funnene våre med.
Angående behandlingen av data har vi som studenter ved NTNU private PCer. Derfor vil vi bruke våre private PCer til å gjøre opptakene men lagre de i NTNU sin skytjeneste for oppbevaring.

Appendix B
Sikt/NSD Approval

The appendix below includes the requisite approval from Sikt/NSD, granting permission for the utilization of personal information in this thesis, provided that the usage aligns with the specifications outlined in the application found in Appendix A.

Sikt

Meldeskjema / Masteroppgave / Vurdering

Vurdering av behandling av personopplysninger

Referansenummer	**Vurderingstype**	**Dato**
122600	Automatisk ?	13.01.2023

Prosjekttittel
Masteroppgave

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig
Maria Bartnes

Student
Andreas Johan Nyland

Prosjektperiode
09.01.2023 - 02.06.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 02.06.2023.

Meldeskjema

Grunnlag for automatisk vurdering
Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
  - Rasemessig eller etnisk opprinnelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - Genetiske data
  - Biometriske data for å entydig identifisere et individ
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

Informasjon til de registrerte (utvalgene) om behandlingen må inneholde

- Den behandlingsansvarliges identitet og kontaktopplysninger
- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)
- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)

- Hvor lenge personopplysningene vil bli behandlet
- Retten til å trekke samtykket tilbake og øvrige rettigheter

Vi anbefaler å bruke vår mal til informasjonsskriv.

Informasjonssikkerhet
Du må behandle personopplysningene i tråd med retningslinjene for informasjonssikkerhet og lagringsguider ved behandlingsansvarlig institusjon. Institusjonen er ansvarlig for at vilkårene for personvernforordningen artikkel 5.1. d) riktighet, 5. 1. f) integritet og konfidensialitet, og 32 sikkerhet er oppfylt.

Appendix C
Information to participating interviewees

The following document was sent to the interviewees prior to their participation. The document is written in Norwegian, and approved by NSD.

Vil du delta i forskningsprosjektet "*Protecting the Norwegian Petroleum Sector: A Study on Incorporating Cybersecurity into the Risk Assessment*"?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å samle inn data knyttet til risikovurdering rundt cybersikkerhet i petroleumssektoren, med formål om å bruke innsikt fra dette til å forstå hvordan denne risikovurderingen gjøres i dag og hvordan den kan forbedres. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse innebærer for deg.

Formål

Formålet med dette prosjektet er å hente innsikt fra representanter som jobber med cybersecurity i petroleumssektoren. Formålet er å forstå hvordan risikovurdering knyttet til cybersikkerhet foregår i dag, både i selskaper og i sektoren som en helhet. Problemstillingen i dette prosjektet baserer seg på at petroleumssektoren historisk har vært flinke til å vurdere safety - risiko knyttet til hendelser som påvirker menneskeliv og miljø, men ikke i like stor grad fokusert på risikovurdering av cybersecurity. Forskningsspørsmålene i oppgaven tar derfor for seg hvordan risikovurderingen av cybersecurity gjøres i dag og hvordan selskaper i sektoren opplever dette. Videre vil vi også hente innspill til forslag om forbedringer til risikovurderingen. Basert på funnene ønsker vi å få god forståelse av hvordan risikovurdering knyttet til cybersecurity utføres i dag og hvilke eventuelle utfordringer og mangler dagens metode innehar.

Ønsket er å utarbeide et forslag til hvordan risikovurdering av cybersikkerhet i petroleumssektoren kan utføres på en måte slik at det enkelt kan tilpasses fremtidige endringer i trusselbildet og infrastrukturen.

Prosjektet er en del av masterstudiet ved NTNU, og kommer ikke til å brukes til andre formål enn å fullføre masteroppgaven.

Hvem er ansvarlig for forskningsprosjektet?

Maria Bartnes ved Institutt for informasjons- og kommunikasjonsteknologi ved NTNU er ansvarlig for prosjektet. Thor Buan ved Ren Røros og Roy Myhre ved Sopra Steria er veiledere, men prosjektet utføres for NTNU, og har ikke noe ytterligere å gjøre med verken Sintef, Ren Røros eller Sopra Steria. Prosjektet utføres av Simen Bergset og Andreas Nyland, som med dette prosjektet vil fullføre sin mastergrad ved NTNU.

Hvorfor får du spørsmål om å delta?

Vi har bedt deg om å delta grunnet din stilling og innsikt i hvordan risikovurdering knyttet til cybersecurity gjøres enten i sektoren eller i en bedrift. Prosjektet vårt avhenger av innsikt i hvordan denne risikovurderingen gjøres og erfaringer knyttet til den og dette er grunnen til at vi mener at det har stor verdi at du deltar i dette forskningsprosjektet.

Hva innebærer det for deg å delta?

Deltakelse innebærer at vi ønsker å utføre et eller flere intervjuer med deg, der lydopptak av intervjuet vil lagres for å sikre god flyt i intervjuet. Intervjuet kommer til å bestå av spørsmål rundt risikovurdering knyttet til cybersikkerhet i petroleumssektoren med fokus på hvordan dette gjøres og erfaringer og meninger rundt metoden.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern - hvordan vi oppbevarer og bruker dine opplysninger

Vi vil kun bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

De som vil ha tilgang til opplysningene du oppgir vil være veilederne Maria Bartnes, Thor Buan og Roy Myhre, samt Simen Bergset og Andreas Nyland, som skriver den aktuelle masteroppgaven. Selv om personopplysningene, spesielt stilling/rolle kan være relevant for erfaringer og vurderinger, vil navn og annen personlig informasjon i utgangspunktet anonymiseres slik at vedkommende ikke kan bli gjenkjent. Om det derimot skulle være nødvendig at navn og/eller annen personlig informasjon publiseres vil vi komme tilbake med spørsmål og opplysninger rundt hva som eventuelt vurderes til å være nødvendig for publisering. Vi følger NTNUs retningslinjer for lagring av forskningsdata, og derfor vil datamaterialet lagres på NTNUs servere. Du som deltaker vil i utgangspunktet *ikke* kunne gjenkjennes i publikasjonen vår, med mindre dette er strengt nødvendig og vi innhenter samtykke på et senere tidspunkt. Dette har du naturligvis full bestemmelsesrett over selv og det er mulig å trekke tilbake samtykke før publiseringen.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres til prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er i begynnelsen av juni. Etter prosjektslutt vil personopplysninger og lydopptak fra intervju slettes.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

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

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- NTNU ved Maria Bartnes (maria.bartnes@sintef.no), veileder for prosjektet, eller studentene Simen Bergset (simeneb@stud.ntnu.no) og Andreas Nyland (andreajn@stud.ntnu.no).
- Vårt personvernombud: Thomas Helgesen (epost: thomas.helgesen@ntnu.no, telefon: 930 79 038)

Hvis du har spørsmål knyttet til Personverntjenester sin vurdering av prosjektet, kan du ta kontakt med:

- Personverntjenester på e-post (personverntjenester@sikt.no)

Med vennlig hilsen

Maria Bartnes
(Forsker/veileder)

Simen Bergset
(Student)

Andreas Nyland
(Student)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Assessment of risk associated with cyber security in the petroleum sector,* og har fått anledning til å stille spørsmål. Jeg samtykker til:

- □ å delta i *intervju*
- □ *at opplysninger om meg publiseres slik at jeg kan gjenkjennes - hvis dette blir aktuelt*

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

—---
(Signert av prosjektdeltaker, dato)

NTNU

Norwegian University of
Science and Technology