NTNU – Trondheim
Norwegian University of
Science and Technology

A Gap Analysis of Implemented Barriers and Recommended Best Practices in Oil and Gas Cyber Security

A Case Study on a Major Oil and Gas Company on the Norwegian Continental Shelf

Eivind Høydal

Submission date: June 2020
Responsible professor: Maria Bartnes, IIK & SINTEF
Supervisor: Lars Bodsberg, SINTEF

Norwegian University of Science and Technology
Department of Telematics

Title: A Gap Analysis of Implemented Barriers and Recommended Best Practices in Oil and Gas Cyber Security

Student: Eivind Høydal

Problem description:

The trend of implementing Internet Protocols (IP) on operational technology (OT) networks exposes Industrial Control Systems (ICS) to new vulnerabilities. This convergence of Information Technology (IT) and OT will increase the number of attack vectors on ICS, and likely increase the number of cyberattacks on ICS. Several sophisticated cyber attacks have been launched on ICS [HEF18], and security professionals report increased activity by threat actors targeting ICS [DRA19]. A cyberattack on an oil platform may cause considerable disruption of production and may result in loss of human life, which gives reason to be cautious.

Bridging the gap between safety and cyber security practices in ICS on oil and gas installations on the Norwegian Continental Shelf (NCS) is challenging. Still, organisations on the NCS are required to work with cyber security barriers. It is challenging to quantify a level of risk-reduction for cybersecurity measures. In cybersecurity, attacks maybe accidental or with intent, and consequently estimating probability becomes more challenging. Bridging the gap from safety to security is a challenge. Operators struggle to answer how well they are protected.

The overall goal of this thesis is to evaluate the effect (risk reduction) of cyber security barriers on safety-related control functions on the NCS. Evaluating barriers will be done through a threat modelling of offshore platforms on the NCS. A cyber security barrier can be technical, organisational, or process-oriented.

Responsible professor: Maria Bartnes, IIK & SINTEF
Supervisor: Lars Bodsberg, SINTEF

Abstract

The increased use of Information Technology (IT) in Industrial Control Systems (ICS) exposes ICS to previously unencountered threats. Consequently, cyber security has gained recognition as a barrier responsible for safeguarding Health, Safety, and Environment (HSE) on the Norwegian Continental Shelf (NCS). The sophisticated cyber attacks, Stuxnet, Industroyer, and Trisis, have shown the advanced capabilities of threat actors targeting ICS. With sophisticated threat actors capable of disrupting oil and gas installations through cyber attacks, there is consequently a need to understand how installations should be protected. This master thesis aims to determine how implemented cyber security barriers on the NCS align with selected best practices for ICS cyber security.

A gap analysis was performed between the implemented cyber security barriers of an operator on the NCS, and three selected ICS cyber security guidelines and best practices. The gap analysis was conducted as a single-case holistic case study on the documentation of cyber security barriers of the operator. The three selected best practices were the NIST Cybersecurity Framework, the Center for Internet Security (CIS) Controls, and the IEC 62443 3-3. Additionally, five inadequately addressed cyber security activities from the gap analysis are examined in detail, and a literature review was performed to create a threat landscape for the NCS.

The gap analysis shows that there are gaps between the operator's requirements to cyber security barriers and the guidelines, where NIST CSF had 53 out of 108 subcategories covered (49%), CIS Controls had 46 out of 190 sub-controls (24%) covered, and IEC 62443 3-3 had 20 out of 51 system requirements covered (39%). These three results show significant gaps between the implemented cyber security barriers of the operator and the recommendations of all three guidelines, and the cyber security requirements of the operator cannot be regarded as fully aligned with best practices. Additionally, by examining five inadequately addressed cyber security activities, it was discovered that the cyber security barrier elements should be updated. Consequently, there is a need for further research to create a comprehensive cyber security barrier model aligned with the best practices.

Sammendrag

Den økte bruken av informasjonsteknologi (IT) i industrielle styringssystemer (ICS) utsetter ICS for tidligere ukjente trusler. Følgelig har cybersikkerhet blitt en del av barrierestyringen som er ansvarlig for å ivareta helse, sikkerhet og miljø (HMS) på norsk kontinentalsokkel. De sofistikerte cyberangrepene, Stuxnet, Industroyer og Trisis, har vist at trusselaktører målrettet angriper ICS. Med et trusselbilde der sofistikerte trusselaktører er i stand til å forstyrre olje- og gassinstallasjoner gjennom cyberangrep, er det følgelig behov for å forstå hvordan installasjoner på norsk sokkel bør beskyttes mot cyberangrep. Denne masteroppgaven tar sikte på å bestemme hvordan implementerte cybersikkerhetsbarrierer på norsk sokkel er i samsvar med utvalgte veiledninger for cybersikkerhet i industrielle styringssystemer.

For å svare på problemstillingen ble en gap-analyse gjennomført mellom de implementerte cybersikkerhetsbarrierene hos en operatør på norsk kontinentalsokkel, og tre utvalgte veiledninger for cybersikkerhet i industrielle styringssystemer. Gap-analysen ble gjennomført som en case-studie av en enkelt virksomhet hvor virksomhetens dokumentasjon av cybersikkerhetsbarrierer dannet grunnlaget for gap-analysen. De tre utvalgte veiledningene var NIST Cybersecurity Framework, Center for Internet Security (CIS) Controls, og IEC 62443 3-3. I tillegg ble fem utvalgte barrierer med identifiserte gap diskutert i detalj. Masteroppgaven inkluderer også et litteratursøk som ble brukt til å utforme et trusselbilde for norsk kontinentalsokkel.

Gap-analysen viser at de interne kravene til barrierer i virksomheten dekker 53 av 108 (49%) subkategorier i NIST CSF, 46 av 190 subkontroller (24%) i CIS Controls, og 20 av 51 (39%) system krav i IEC 62443 3-3. Disse tre resultatene viser signifikante gap mellom de implementerte cybersikkerhetsbarrierene og tiltakene som foreslås i de tre veiledningene. Av den grunn konkluderer masteroppgaven med at dokumentasjonen av virksomhetens cybersikkerhetsbarrierer ikke samsvarer fullt ut med de anbefalinger som presenteres i de tre veiledningene. Videre, ved å undersøke de fem barrierene med identifiserte gap, konkluderes det med at cybersikkerhetsbarrieremodellen bør oppdateres. Følgelig er det behov for videre forskning for å lage en komplett cybersikkerhetsbarrieremodell tilpasset anbefalingene fra veiledninger for cybersikkerhet i industrielle styringssystemer.

Preface

This thesis is the final deliverable of a Master of Science in Communication Technology at the Norwegian University of Technology (NTNU). This thesis was done in the specialisation Information Security. The work and the report itself has been produced between January and June 2020.

First of all, I would like to thank my supervisors for their continued support in this rollercoaster of a thesis. I am grateful to both my responsible professor Maria Bartnes and my supervisor Lars Bodsberg. I would also like to sincerely thank the company Alpha, which will continue to be anonymous, for participating in my thesis.

Finally, I want to thank my good friends Aleksander Walde, Bendik Aalmen Markussen, Jakob Kok, Nils Folvik Danielsen and Per Kristian Gravdal for managing to live and work together in a 100 square meters apartment through a global pandemic.

Eivind Høydal
Trondhiem, June 2020

Contents

Appendices

List of Figures

List of Tables

List of Acronyms

APT Advanced Persistent Threat.

CABS Cyber Attack Barrier Strategy.

CAPS Cyber Attack Performance Standard.

CERT Computer Emergency Response Team.

CIS Center for Internet Security.

COTS Commercial-Off-The-Shelf.

CSIRT Computer Security Incident Response Team.

ENISA European Union Agency for Cybersecurity.

ESD Emergency Shutdown.

F&G Fire & Gas Detection.

HMI Human-Machine Interface.

HSE Health, Safety and Environment.

ICS Industrial Control Systems.

IEC International Electrotechnical Commission.

IO Integrated Operations.

IT Information Technology.

NCS Norwegian Continental Shelf.

NIST National Institute of Standards and Technology.

NOG Norwegian Oil and Gas Association.

NSM Norwegian National Security Authority.

OS Operating System.

OT Operational Technology.

PAGA Public Address and General Alarm.

PERA Purdue Enterprise Reference Architecture.

PLC Programmable Logic Controller.

PRA Probabilistic Risk Assessments.

PSA Norwegian Petroleum Safety Authority.

PSD Process Shutdown.

PST Norwegian Police Security Service.

SCADA Supervisory Control And Data Acquisition.

SIF Safety Instrumented Function.

SIL Safety Integrity Level.

SIS Safety Instrumented System.

SL Security Level.

SuC System under Consideration.

TTP Tactics, Techniques and Procedures.

Chapter 1 Introduction

1.1 Motivation

Through the last 40 years, the oil and gas sector has experienced several catastrophic accidents. Alexander L. Kielland, Piper Alpha, and Deepwater Horizon are some of the most well known. These significant accidents have resulted in a stringent focus on Health, Safety and Environment (HSE), which on the Norwegian Continental Shelf (NCS) is enforced through proactive and reactive barriers on the oil and gas installations.

The Norwegian oil and gas sector has increased its reliance on Information Technology (IT) since the adoption of Integrated Operations (IO) from 2004 and onwards. Partial control of industrial processes from onshore through IO has evolved into unmanned platforms on the NCS which are completely remotely controlled [Equ17]. This trend in Industrial Control Systems (ICS) is often named the convergence of IT systems and Operational Technology (OT) systems [MJV17], and this results in complex architectures and systems [GMR$^+$18]. The increased connection between IT and OT means ICS are exposed on operators' computer networks to a greater extent than before. This increased connectivity increases the area of the attack surface and thereby increases the number of possible vulnerabilities in the cyber security domain of the Norwegian oil and gas sector. The connection of IT to industrial processes on the NCS is not a new problem in academia, already in 2009, there was proposed a solution to ensure secure remote access to Safety Instrumented System (SIS) [JLG09].

Cyber security has gained recognition as a barrier part of barrier management on the NCS due to the increased connectivity. Already in 2007, the first recommended guideline on information security was created by the Norwegian Oil and Gas Association (NOG), NOG 104 [NOG16]. However, since the creation of the guideline, the threat landscape of ICS cyber security has seen a significant change. ICS have historically been less targeted by threat actors compared to traditional IT, but this is changing. Threat intelligence on groups specifically targeting ICS [DRA19] shows that the threat against critical infrastructure is increasing. Besides, there have been three significant attacks on ICS where the threat actor have made a physical impact on the industrial processes in the last ten years:

1. In 2010, Stuxnet was discovered. Stuxnet is the first publically known malware that targets ICS. The malware utilises several zero-days to attack machines using Microsoft Windows to control Siemens Step7 Programmable Logic Controllers (PLCs). This resulted in the destruction of centrifuges used to enrich uranium by manipulating their frequency [MRHM20, FMC11].

2. In 2016, Industroyer was discovered. Industroyer is the first-ever known malware designed to attack electrical grids. Industroyer is unique in how it does not take advantage of any technical vulnerability or exploit in ICS, but instead takes advantage of how the electric grid is designed. The attack on the Ukrainian electrical grid on the 17th of December 2016 used this malware [LAC17, Dra17a].

3. In 2017, Trisis was discovered. It is the first malware to target safety systems, SIS specifically. The malware was delivered into a petrochemical facility in the Middle East. It marks an escalation of cyber threats against ICS as its design has the potential to threaten human lives [Dra17b, JCK$^+$17].

These three sophisticated cyber attacks show the advanced capabilities of threat actors targeting ICS. With sophisticated threat actors capable of disrupting oil and gas installations through cyber attacks, there is consequently a need to understand how installations should be protected. There exist numerous guidelines and best practices for ICS cyber security suitable to the NCS. These guidelines and best practices provide detailed information on how operators should protect their systems against threat actors. However, there is little specific knowledge of the implemented cyber security barriers on the NCS and how these barriers compare to recommendations found in guidelines and best practices.

1.2 Objectives

As stated in the project description, *the overall goal of this thesis is to evaluate the effect (risk reduction) of cyber security barriers*[1] *on safety-related control functions on the NCS. Evaluating barriers will be done through a threat modelling of offshore platforms on the NCS.* The following research question (RQ) was created to facilitate this goal.

[1] In this thesis, the terms barriers, controls, and countermeasures are used interchangeably in the context of cyber security.

Research question: How are implemented cyber security barriers on the Norwegian Continental Shelf aligned with Industrial Control Systems cyber security standards and best practices?

Addressing the effectiveness of cyber security barriers on the NCS is currently an open research question. The problem space of the research goal is vast, and consequently, the RQ was created to have a feasible goal in the limited time available for this master thesis. Exploring the alignment between cyber security barriers on the NCS and ICS cyber security guidelines and best practices provide a picture of the current state of implemented cyber security barriers, and how they compare to best practices. While the association between the RQ and research goal is not exhaustive, answering the RQ provides new knowledge in the area of the research goal. It is helpful to have an overview of which cyber security barriers are in place and how they are organised before a method to evaluate them is designed. Additionally, as cyber security in ICS is a developing discipline, comparing selected standards and best practices to the implemented barriers provide knowledge of the cyber security maturity on the NCS.

The project description also states how the overall research goal will be reached through threat modelling. As this thesis does not fully answer the research goal, threat modelling was not done to the extent initially intended. Instead, threat modelling and related terms are discussed in the background before a threat landscape of the NCS is presented in later a later section.

1.3 Scope and Limitations

As ICS exists in numerous organisations in various industries and sectors, the focus of this thesis is confined to the Norwegian petroleum industry, and specifically the offshore installations. In this way, it is possible to conduct more specific and in-depth research. The term NCS is used throughout the thesis to emphasise the sectorial and geographical scope of the thesis. Still, the results could be relevant for both companies in the petroleum industry across the globe, and other industries where ICS cyber security is relevant.

There is a multitude of threats facing operators on the NCS, and to further narrow the scope, the thesis will only explore adversarial threats. In other words, threats originating from deliberate attackers targeting ICS.

There are three principal types of barrier elements on the NCS according to the Norwegian Petroleum Safety Authority (PSA). These are technical, organisational and operational barriers. All three types are in the scope of the thesis. However, the vast majority of the barriers discussed are technical and operational as the selected best practices have primarily technical and operational countermeasures rather than organisational controls.

On the NCS, there are many different assets. In this thesis, the assets of interest are the ones related to the production and processing of hydrocarbons and maintaining safety on oil and gas installations. Assets related to office systems and IT are out of scope.

1.4 Outline

The master thesis has the following structure:

Chapter 2 Background gives the necessary definitions and introduces the relevant background, ICS and SIS, standards and guidelines, and basics of risk analysis and threat modelling. Further, the threat landscape on the NCS is presented together with how threat actors attack ICS.

Chapter 3 Methodology explains how the study was conducted in terms of choice of method and research design. The chapter also reflects on challenges and limitations of this research.

Chapter 4 Case presents the operator subject to examination and the operator's documentation of implemented cyber security barriers.

Chapter 5 Results present the findings from the gap analysis between the operator's cyber security requirements and the selected ICS cyber security guidelines.

Chapter 6 Discussion presents and discusses the results related to the research questions. Furthermore, this chapter presents some recommendations to Alpha based on the results in 5. Lastly, a discussion on the validity of the research is included.

Chapter 7 Conclusion and Future Work presents a brief conclusion of the master thesis, together with reflections on future research in the field of cyber security barriers on the NCS.

Chapter 2
Background

This chapter presents relevant background information on the ecosystem of ICS and SIS, and ICS is formally defined in 2.1. Further, the concept of barrier management is presented in section 2.3, together with the relevant regulations on the NCS. An overview of the relevant standards and guidelines is presented in 2.4. Following is a section on the concept of risk management in cyber security in section 2.5. Next, threat modelling and related terms is presented in 2.6 before a threat landscape on the NCS is presented in 2.7. Finally, how threat actors attack ICS is presented in section 2.8.

2.1 Industrial Control Systems

Operational Technology (OT), Industrial Control Systems (ICS), and Industrial Automation and Control Systems (IACS) are three different terms used to describe the control systems used to control physical processes. Physical processes range from power generation and distribution, gas and water supply, factory automation, traffic control technology, to oil and gas operations. In this thesis, the term ICS is used exclusively, and the definition from National Institute of Standards and Technology (NIST)'s *Guide to Industrial Control Systems (ICS) Security* is used to define ICS:

> "Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures" [NIS15b].

2.1.1 Requirements to ICS

ICS is inherently different from IT. There are unique requirements to everything from delay and jitter to change management. These requirements impact how cyber security has been addressed in ICS historically and how it should be addressed in the future. The NIST's Guide to Industrial Control Systems (ICS) Security [NIS15b] presents the different requirements in an orderly manner, and the requirements are presented in table 2.1 sorted by separate categories.

The nature of physical processes controlled by ICS makes safety and the correct and continuous operation the primary concerns in ICS. Thus, ICS are engineered with strict requirements for reliability. ICS are generally time-critical, with requirements to low delay and jitter. Consequently, the primary security objective in ICS is the availability of information. This is the opposite of IT systems, where confidentiality has traditionally been the primary security objective [NIS15b].

Category	**IT system**	**ICS**
Priority of security objectives	1. Confidentiality 2. Integrity 3. Availability	1. Availability 2. Integrity 3. Confidentiality
Risk impact	• Financial losses • Information disclosure • Delay of operations	• Loss of life • Environmental losses • Financial losses
Change management	Upgrades are straightforward	Upgrades must be carefully made and thoroughly tested
Component lifetime	3-5 years	10-15 years
Performance requirements	• Non-real-time • Demands high throughput • Delay and jitter acceptable	• Real-time • Modest throughput is acceptable • Delay and jitter unacceptable
Resource constraints	Enough resources to support additional security	Constrained memory and computing
Communications	Standard communication protocols	Proprietary and standard communication protocols

Table 2.1: Summary of key differences between IT and ICS. Based on table 2-1 in [NIS15b].

The nature of ICS also impacts risk management. While cyber security in IT is primarily concerned with the protection of information, cyber security in ICS protects the physical process. Thus, risk management in ICS are primarily concerned with human safety to prevent loss of life, possible environmental damage, and loss of production. Any cyber security measure or control that impairs safety is unacceptable in ICS.

Historically, ICS had little resemblance to IT systems in that ICS were isolated systems running proprietary control protocols using specialised hardware and software. As ICS was isolated or air-gapped from other systems, cyber security was of little concern. As IT and OT converges (see section 1.1), efforts to address cyber security in ICS must be increased. The lifetime of ICS is also considerably longer than IT systems, where ICS components are in use several times the lifespan of IT. However, ICS architecture and system requirements force cyber security to be tailored to ICS, rather than implementing Commercial-Off-The-Shelf (COTS) IT cyber security solutions. Applications and Operating Systems (OSs) running in the ICS may not operate correctly with COTS solutions due to the specialised ICS architecture [NIS15b]. Finally, cyber security measures or controls should not degrade the reliability of the ICS as this could impact safety.

2.1.2 Architecture of ICS

To be able to describe and discuss system architecture in ICS, the recognised Purdue Enterprise Reference Architecture (PERA) model is used as the reference architecture. The PERA is used in the International Electrotechnical Commission (IEC)'s standard for IACS security, known as the IEC 62443 series [IEC09]. The model is used to describe the different hierarchies in ICS and separates ICS into a hierarchy of five different levels (six levels with level 3.5, DMZ). The model of the different levels is illustrated in figure 2.1.

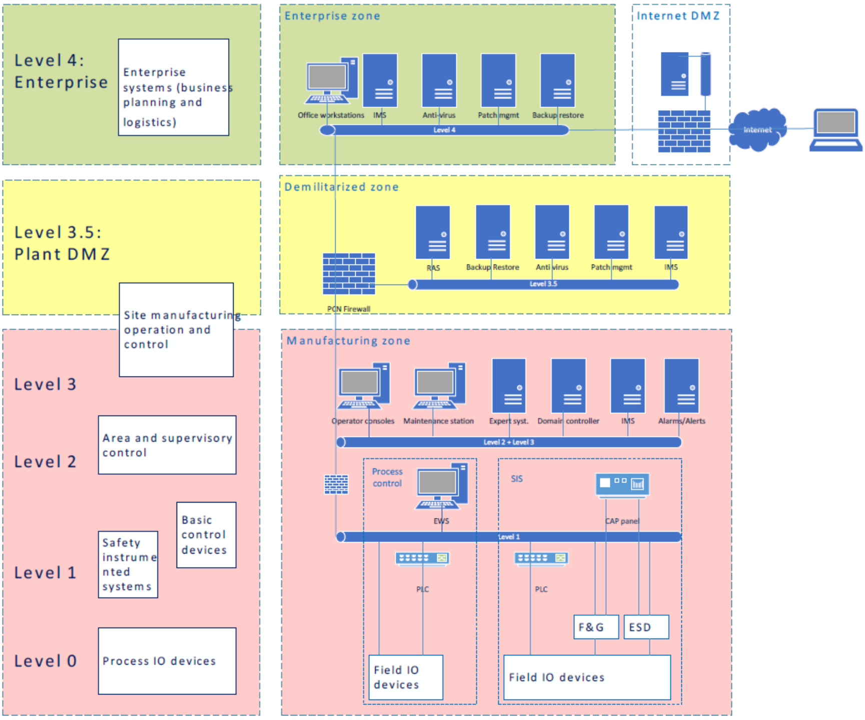


Figure 2.1: PERA's functional separation of ICS into a hierarchy of levels [DNV17, p. 19].

2.2 Safety Instrumented Systems

A SIS is a designated system that implements the required safety functions necessary to achieve or maintain a safe state for some industrial equipment. The overall safety-philosophy for the handling of unwanted severe events is to go to a safe state. Going to a safe state will, in many cases, mean to shut down the ongoing production and processing in the installation.

In IEC 61508 a SIS is defined as: *SIS is a distinct, reliable system used to safeguard a process to prevent a catastrophic release of toxic, flammable, or explosive chemicals* [IEC10a]. The specific control functions performed by an SIS are called Safety Instrumented Functions (SIFs). Each SIF has a Safety Integrity Level (SIL) which is defined as a relative level of risk-reduction provided by the SIF. IEC 61508 defines four levels of SILs. Minimum requirements for SILs on the NCS can be found in NOG guideline 070 [NOG18]. The guideline defines SILs in the areas of process shutdown (PSD), emergency shutdown (ESD), fire and gas functions (F&G), some blowout preventer (BOP) functions, and specific workover functions [NOG18].

As hydrocarbons are highly flammable, SISs are a crucial part of operations on the NCS. Figure 2.2 show the relation of SIS to process control and other protective measures. While SIS is used to protect in situations that could lead to failures, accidents, and hazards, the SIS can itself fail. Failures of SISs can either be safe or dangerous failures. Additionally, a failure can be detected or undetected by tests, which leaves four different types of failures. An undetected dangerous failure is the most severe, and how this particular scenario relates to cyber attacks is of great interest.

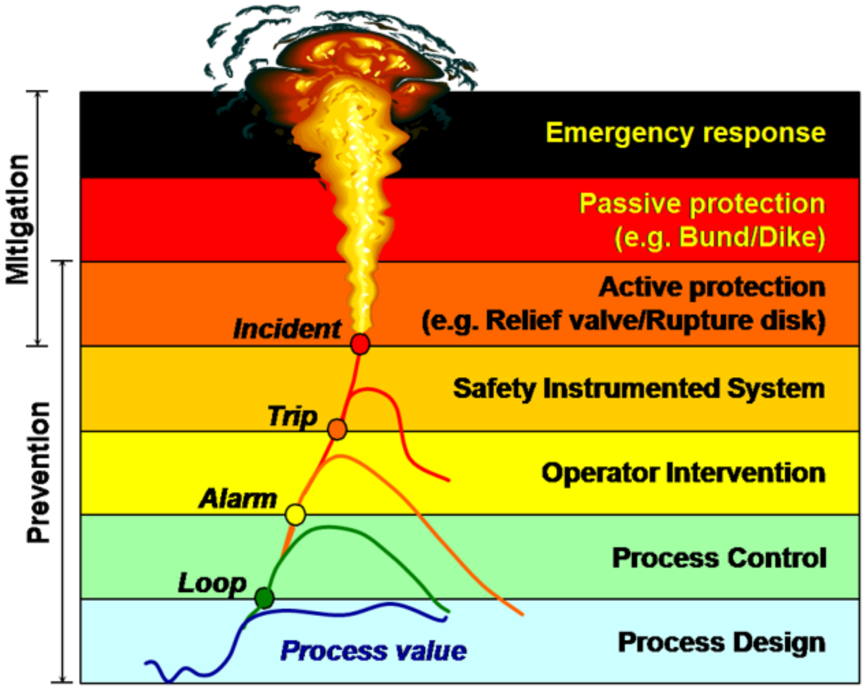


Figure 2.2: The different layers of protection in industrial processes [ARC].

2.3 Barrier Management

The very nature of oil and gas makes safety a real concern on the NCS. Operators are facing the risk of accidents with disastrous consequences, while the likelihood of these accidents is low [HO16]. Consequently, regulating HSE is vital. The PSA enforces five sets of regulations related to HSE, and there are several additional laws and regulations relevant to operators on the NCS [Nor19]. This regulation enforced by the PSA sets requirements to how operators are to protect their installations.

Safety is maintained through the concept of barriers. The PSA defines a barrier as the following in *Principles for barrier management in the petroleum industry: Barrier Memorandum 2017*:

> "Technical, operational and organisational elements which are intended individually or collectively to reduce possibility/ for a specific error, hazard or accident to occur, or which limit its harm/disadvantages" [Nor17].

A barrier is, in other words, a countermeasure that reduces either the likelihood or the consequence of a specific error, hazard or accident to occur. The management regulations regulate barriers, and §5 states the following:

> "Barriers shall be established that at all times can
>
> (a) identify conditions that can lead to failures, hazard and accident situations,
>
> (b) reduce the possibility of failures, hazard and accident situations occurring and developing,
>
> (c) limit possible harm and inconveniences.
>
> Personnel shall be aware of what barriers have been established and which function they are intended to fulfil, as well as what performance requirements have been defined in respect of the concrete technical, operational or organisational barrier elements necessary for the individual barrier to be effective" [Nor15].

The last paragraph of §5 sets requirements to barriers. A barrier has a defined function and consist of the barrier elements necessary for the barrier to fulfil its function. The elements of a barrier can either be technical, operational or organisational. SIS are crucial barriers when protecting ICS to ensure their correct and safe operation. Barrier management is the process of establishing and maintaining the barriers and barrier elements.

It is easy to see the similarities between the concept of barriers and cyber security countermeasures. However, neither requirements to cyber security nor cyber attacks are explicitly mentioned in the regulation. The PSA has adopted a practice where cyber security is implied from the regulations. It interprets existing regulations to cover the need for cyber security barriers. In a recent report by the company DNV

GL for the PSA, DNV GL assesses the PSA's regulations concerning cyber security in ICS. The overall assessment of the regulations is that *it works well in preventing technical problems in critical systems from contributing to major accidents, but that it needs to be strengthened with respect to cyber threats* [DNV20].

2.4 Standards and Guidelines

This section presents the frameworks, guidelines and standards discussed in this thesis. There are several standards and guidelines applicable to cyber security in ICS on the NCS. The NIST Cybersecurity Framework (CSF) and the IEC 62443 series of standards are more or less tailored to cyber security in ICS, where the NIST CSF is made for critical infrastructure [NIS18], and the IEC 62443 is made for cyber security in ICS [IEC09]. Further, the NOG has guideline 104, which is recommended baseline requirements for information security [NOG16]. The company DNV GL has created a guide for implementing IEC 62443 in the oil and gas industry through a joint industry project [DNV17].

Additionally, other standards and guidelines are governing safety-related systems on the NCS, both from the IEC and NOG. Safety influences cyber security in that no cyber security countermeasure should impact the safety of the installation.

The regulation on the NCS does not name any standard nor guideline as an official industry standard. However, according to the Norwegian Industry Forum for Cybersecurity of Industrial Automation and Control Systems (CDS-forum) the IEC 62443 is becoming the de facto industry standard on the NCS [Sin]. A driver in this development is the company DNV GL with the previously mentioned guide for implementing IEC 62443 in the oil and gas industry [DNV17].

Still, there are other frameworks and guidelines for cyber security, both general and tailored to ICS, which are relevant for operators on the NCS. The CIS has a guideline with twenty different controls used in IT environments, but there is a corresponding guideline for adopting the CIS Controls in an ICS environment.

2.4.1 IEC 62443

The IEC 62443 series of cyber security standards are multi-industry standards listing cyber security protection methods and techniques in industrial communication networks. The standard covers all relevant roles, product suppliers, system integrators, and asset owners. The goal of the standard is to provide a holistic cyber security scheme for a plant in operation. A holistic scheme encompasses policies and procedures, functional security measures, and the competency of the people in the organisation. The standard focuses on defence-in-depth as the strategy to achieve the goal, a holistic cyber security scheme [IEC09]. As the standard is a series, it consist of standards in four different categories, general, policies & procedures, system, and component. The four categories with their respective standards are presented in figure 2.3.

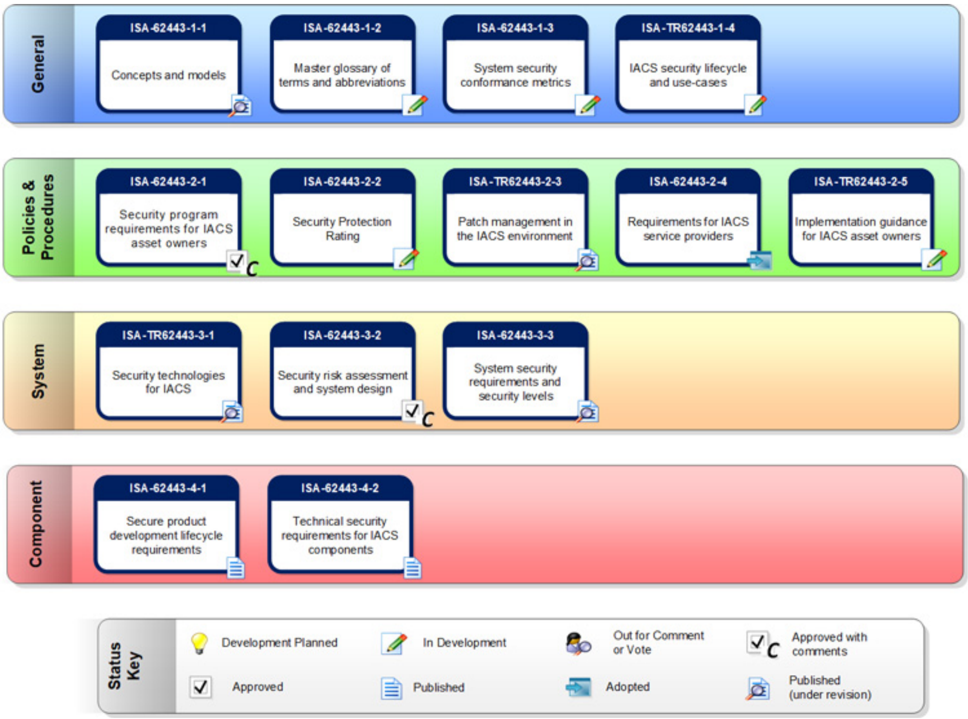

General
ISA-62443-1-1
Concepts and models
ISA-62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security conformance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
ISA-62443-2-1
Security program requirements for IACS asset owners
ISA-62443-2-2
Security Protection Rating
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Requirements for IACS service providers
ISA-TR62443-2-5
Implementation guidance for IACS asset owners
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security risk assessment and system design
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Secure product development lifecycle requirements
ISA-62443-4-2
Technical security requirements for IACS components
Status Key
Development Planned
In Development
Out for Comment or Vote
Approved with comments
Approved
Published
Adopted
Published (under revision)

Figure 2.3: The various work products in the IEC 62443 series of IACS standards and technical reports [Int]

The recommended practice *Cyber security in the oil and gas industry based on IEC 62443* (DNVGL-RP-G108) from DNV GL combines IEC 62443 3-2, 3-3, and 2-4 to a single manageable document [DNV17]. The recommended practice (RP) was created through a joint industry project with eleven different stakeholders from the NCS. The RP is structured after the elements in the lifecycle of an oil and gas installation, Concept, FEED (Front End Engineering Design), Project, and Operations. It is explicitly created for securing ICS in the oil and gas sector.

IEC 62443 3-3

This particular standard part of the IEC 62443 series sets system security requirements and security levels for ICS. 51 detailed technical control system requirements (SRs) are associated with seven functional requirements (FRs) [IEC13]. Each SR has a corresponding Security Level (SL), which define the security capability of the SR. The SL is similar in function to SIL in IEC 61511 (discussed in 2.2). SLs come in four different levels (1-4) where each level has a definition of the security capability it provides. An SL equal to 0 is implicitly defined as no SRs. SL-1 is the most basic requirement, and each additional level provides the capability to protect the system against increasingly skilful and motivated threat actors.

In DNVGL-RP-G108, the recommended best practice is to use SL-1 as a minimum level, exposed solutions like the remote access solutions should have SL-3, and high criticality systems in the ICS should have minimum SL-2 [DNV17]. Note that an ICS can be divided into multiple System under Consideration (SuC) where each SuC has a defined SL. This means an ICS does not need to have SL-4 in all subsystems to protect against the most advanced threat actors. SL-4 in all SuC would neither be feasible nor provide efficient protection of the ICS. Of the 51 SRs, 37 are SL-1, 12 are SL-2, 2 are SL-3, and zero are SL-4. Additionally, a large part of the SRs have requirement enhancements (REs) which are additional requirements belonging to a higher SL. As an example, SR 7.1 belong to SL-1, but it has two REs belong to SL-2 and SL-3, respectively. Considering IEC 62443 3-3 with all SRs with all REs there is a total of 100 requirements.

The seven different FRs are presented in table 2.2 with the number of unique SRs in each FR.

Functional requirement	Number of SRs
FR 1 - Identification and authentication control (IAC)	13
FR 2 - Use control (UC)	12
FR 3 - System integrity (SI)	9
FR 4 - Data confidentiality (DC)	3
FR 5 - Restricted data flow (RDF)	4
FR 6 - Timely response to events (TRE)	2
FR 7 - Resource availability (RA)	8
Total	51

Table 2.2: The seven FRs with the corresponding number of SRs in IEC 62443 3-3.

2.4.2 IEC 61508 and IEC 61511

IEC 61508 and IEC 61611 are two related series of standards. The IEC 61508 consists of methods on how to apply, design, deploy and maintain automatic protection systems called safety-related systems [IEC10a]. The standard is named *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE).*

IEC 61511 covers the design and management requirements for SISs throughout the entire safety life cycle [IEC16]. IEC 61511-1 has been developed as a process sector implementation of IEC 61508:2010.

2.4.3 NOG 070

NOG 070 is a guideline for the *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (recommended SIL requirements)* [NOG18]. The overall purpose of the document is to standardise and simplify the application of IEC 61508 and IEC 61511 on the NCS. This is done through a detailed guideline where NOG 070 provides SIL requirements (presented in section 2.2) for the different SIFs on SISs.

2.4.4 NOG 104

NOG 104 is the Norwegian Oil and Gas Association's recommended guideline on information security baseline requirements for process control, safety and support ICT systems [NOG16]. It was first published in 2007 and made cyber security part of the agenda for operators on the NCS. The latest revision was in 2016 to bring the guideline up to date with a changed threat picture and new modes of operation [NOG16]. The guideline consists of 19 different Information Security Baseline Requirements (ISBR).

2.4.5 NIST Cybersecurity Framework

The framework is voluntary guidance, based on existing standards, guidelines, and practices for organisations to better manage and reduce cyber security risk. The framework consists of three parts, a framework core, implementation tiers, and framework profile. The core of the framework is different cyber security activities to increase cyber security resilience. The core is structured with five functions as the control categories, 23 categories as the control objectives and 107 subcategories as the cyber security activities or countermeasures. The five functions are: Identify, Protect, Detect, Respond, and Recover. The goal of the five functions is together to *"provide a high-level, strategic view of the lifecycle of an organisation's management of cyber security risk"* [NIS18].

The implementation tiers *"provide context on how an organisation views cybersecurity risk and the processes in place to manage that risk"* [NIS18]. However, the framework does not provide tiers on each countermeasure in the framework core. Instead, it defines how an organisation can determine its desired tier. The framework profiles *"are an organisation's unique alignment of their organisational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core"* [NIS18]. However, the framework does not include any profile templates.

2.4.6 CIS Controls

The CIS Controls are *a prioritised set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks against systems and networks* [CIS19]. According to the SANS Institute, a *"principal benefit of the Controls is that they prioritise and focus a smaller number of actions with high pay-off results"* [SAN]. In total, there are 20 controls divided into three groups, basic, foundational, and organisational controls. The controls are based on the most common attack patterns highlighted in the leading threat reports and vetted across a vast community of government and industry practitioners [SAN]. Each control has several detailed sub-controls, and each sub-control is mapped to an implementation group (IG). The IGs are three subsets of the CIS Controls tailored to different types of enterprises, where IG1 are the essential controls all enterprises should consider. Each IG builds upon the previous one, IG2 includes IG1, and IG3 includes both IG1 and IG2. CIS recommends that implementation of CIS Controls are prioritised after the IGs [CIS18]. Only larger organisations dealing with a broader threat landscape and risk profile should consider implementing all the controls.

Additionally, CIS has created a guideline for implementing the CIS Controls in an ICS environment. The *Implementation Guide for Industrial Control Systems* presents the applicability of each CIS control in ICS, and considerations the organisation should assess on each CIS control. Table 2.3 presents the 20 different CIS Controls.

2.5 Risk Assessment in Cyber Security

Risk management is a crucial part of conducting business in all modern organisations. As a part of risk management, organisations must conduct risk assessments to identify risks. There are three main approaches to estimate the levels of risk in risk assessments, qualitative, semi-quantitative, and quantitative. In their basic form, all three methods involve estimating the probability or likelihood of a risk scenario and the related consequence of the scenario. Likelihood refers to the possibility of a risk occurring measured in qualitative values, while probability is a quantitative measurement of outcome. The ultimate goal of risk assessments is to get an overview of the risk an organisation is facing. If the risk is considered too high, then risk-reducing countermeasures are needed.

Number	Description
1	Inventory and Control of Hardware Assets
2	Inventory and Control of Software Assets
3	Continuous Vulnerability Management
4	Controlled Use of Administrative Privileges
5	Secure Configurations for Hardware and Software on Devices, Laptops, Workstations, and Servers
6	Maintenance, Monitoring, and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitations and Control of Network Ports, Protocols, and Services
10	Data Recovery Capabilities
11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Implement a Security Awareness and Training Program
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

Table 2.3: The 20 CIS Controls

Briefly explained, qualitative risk assessment uses expert judgement to assign levels from descriptive scales. Semi-quantitative uses qualitative scales to assign numerical values to risk. Quantitative risk assessments (QRA) involves assigning numerical values to risk through statistical methods or other means. The choice of method depends both on the application and the data available. Another important factor is the type of risk scenario. A risk can be intentional (a deliberate harmful action), unintentional (human mistake), or accidental (nature).

There is no clear answer to which of the three approaches suit deliberate harmful actions. Some argue it is too difficult, or not even relevant, to address probability when considering this kind of threat. The Norwegian National Security Authority (NSM) supports this view in their guide to risk assessments for securing critical infrastructure *(Risikovurdering for sikring)* [Nat16]. They recommend using the triangle of threat, vulnerability and asset. NSM consider this approach more useful as it can highlight risks which would not be caught by other models [Nat16]. This method is based on the Norwegian standard NS 5832:2014 [Nor14]. The model does not address likelihood explicitly, but both the threat and vulnerability can be seen as metrics which together can describe the likelihood of the risk materialising. Threat, vulnerability and consequence can also be used as the triangle. A consequence is closely related to an asset as a consequence will affect the asset. Thus the two triangles are similar.

The IEC 62443 series of standards states that an operator shall choose a risk assessment methodology *that identifies and prioritises risks based upon the security threats, vulnerabilities, and consequences related to their IACS assets* [IEC10b, p. 19]. This supports the use of a risk assessment method which utilise the triangle of threat, vulnerability and consequence.

2.6 Threats, Vulnerabilities and Assets

This section is a continuation from the last section where key concepts within cyber security risk assessment were presented. The following subsections are based on a literature review conducted, as outlined in section 3.2. The fundamental terms threat, threat actor, and threat model are explored before the threat landscape of the NCS are established in section 2.7.

Threats

The terms threat, threat actor, and threat model are related. To be able to explore the terms, a definition of the term *threat* should be established. However, the term is used somewhat differently by different actors and organisations in the field of ICS cyber security. In their glossary, European Union Agency for Cybersecurity (ENISA) defines *threat* as *"Any circumstance or event with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data, and/or denial of service"* [Eura]. In DNVGL-RP-G108 *cyber threat* is defined as *"a circumstance or event that has, or indicates, the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organisational operations, organisational assets (including information and information systems), individuals, other organisations, or society"* [DNV17]. In the Information security risk management standard ISO 27005 *threat* is defined as: *"A potential cause of an incident, that may result in harm of systems and organization"* [NEK18]. In other words, a threat can be seen as an event with the potential to cause harm.

Threats can either occur through nature or individuals. Individuals can form threats through deliberate malicious acts or failures and accidents. The ENISA

Threat Taxonomy [Eurb] presents a complete view of relevant threats in table 2.4. A check-mark is used to mark the threats relevant to this thesis which are the adversarial threats, as presented in the scope in section 1.3. Adversarial threats are the threats which originate from threat actors which intentionally attack an asset. Consequently, environmental and accidental threats are disregarded from the threat landscape. As the topic of the thesis is cyber security, physical attacks are as well disregarded, with the exception where physical access is used as an attack vector for a cyber attack.

Threat	Relevance in thesis
Physical attack (deliberate/ intentional)	×
Unintentional damage / loss of information or IT assets	×
Disaster (natural, environmental)	×
Failures/ Malfunction	×
Outages	×
Eavesdropping/ Interception/ Hijacking	✓
Nefarious Activity/ Abuse	✓
Legal	×

Table 2.4: ENISA Threat Taxonomy.

Threat modelling is an important concept in the area of cyber security. Shostack defines threat modelling as *"The use of abstractions to aid in thinking about risk"* [Sho14]. Bodeau *et al.* defines cyber threat modelling as *Cyber threat modelling is the process of developing and applying a representation of adversarial threats (sources, scenarios, and specific events) in cyberspace"* [BMF18]. Further, Bodeau *et al.* presents a comprehensive overview of different methodologies to threat modelling and their differences. Note that the paper primarily presents threat modelling methodology oriented to IT systems, and does not go into depth on methodology oriented to ICS. There are several methods for threat modelling mentioned in the paper, such as COBIT, STRIDE, OCTAVE, and various NIST special publications. Even if some methods mentioned by Bodeau *et al.* are labelled with low complexity by the authors, it was deemed infeasible to do a complete threat modelling in this thesis without changing the RQ. Instead, this thesis presents a threat landscape with relevant threat actors, vulnerabilities, and assets for the NCS.

Threat Actors

The terms *Threat actor* and *Threat agent* are closely related to the term threat. NIST defines a *Threat Actor* as *an individual or a group posing a threat* [NIS16]. In DNVGL-RP-G108 *Threat Agent* is defined as a *causative agent of a threat action*

[DNV17]. The term threat actor is used to describe both threat agents and actors in the rest of this thesis. Threat actors are the individuals or organisations that intend to cause harm, the actors responsible for cyber attacks. They are usually grouped in categories where the actors with the least resources, the lowest capability, are labelled as script kiddies, and the most advanced actors are state-sponsored actors, or the nation-states themselves. This last category of actors is called Advanced Persistent Threats (APTs). These actors have the most resources and can be persistent over long periods. The Tactics, Techniques and Procedures (TTP) used in cyber attacks are used to identify threat actors as APTs. Cyber security companies and researchers give the groups various aliases which can create confusion as distinct APTs end up with multiple aliases. As an example, the group APT29 is also known under the aliases YTTRIUM, The Dukes, Cozy Bear, and CozyDuke [MITa].

Intel's Threat Agent Library list 18 different threat agents to help differentiate attackers based on their resources, skill level, objective, visibility, primary goal (outcome), and limits [Cas07]. Bugeja *et al.* created an overview of malicious threat agents targeting smart homes based on the ICS CERT taxonomy, which include six types of threat agents sorted by capability [BJD17]. CIS uses the labels Insiders, Cybercriminals, Hacktivists, Terrorist Organisations, and Nation-State actors to describe threat actors [Cen]. The five actors are not differentiated by capability, but by their motivation, affiliation and common TTP. Mateski *et al.* created a cyber threat matrix where threat agents are assigned a threat level from 1 to 8 where the assignment of a threat level is based on the commitment and resources of the threat [MFV+12]. Interestingly, Mateski *et al.* argues that the use of semi-descriptive labels (such as script kiddies and hacktivists) undermine a clear understanding of capabilities. However, as this thesis tries to provide a comprehensive overview of threats, not provide a solution, the descriptive labels of threat actors are included. Table 2.5 presents an overview of different threat actors classified by their capability. The table is based on Bugeja *et al.*, but thieves are replaced with cyber criminals from the table as thieves (physical attacks) are considered out of scope in this thesis.

Alongside the capability of threat actors, motivation is often used to differentiate threat actors. Bodeau *et al.* divides the adversary goal (motivation) into financial gain, personal motives, geopolitical advantage, and positional/stepping-stone [BMF18]. CIS does not have a taxonomy for motivation, but rather describes each actor individually. The terms used are similar to Bodeau *et al.*, but geopolitical advantage are divided into political, ideological, espionage, and military [Cen]. Intel has defined ten elements used in their motivation parameter in their threat taxonomy. Ideology, Organizational Gain, Personal Financial Gain, Dominance, Disgruntlement, Unpredictable, and Notoriety are the seven defining motivations used to differentiate the 18 previously mentioned threat agents [Cas15]. The motivation was excluded from table 2.5 as threat actors can have several motivations, and it did not help to

Name	Other Aliases	Capability
Advanced Persistent Threats	State sponsored actors, Nation states	High
Cyber terrorists		High
Organised crime		Moderate
Hacktivist		Low
Cyber criminals		Low
Script kiddies		Low

Table 2.5: Different threat actors sorted by their capability. Adopted from [BJD17].

differentiate the threat actors further. However, motivation will be discussed later in the context of the NCS.

2.7 Threat Landscape on the NCS

In this section the threat landscape on the NCS is presented. The threat landscape includes relevant threats, vulnerabilities and assets on the NCS, and it will be used in the discussion to discuss cyber security barriers in the context of the threat landscape.

Threats on the NCS

While several known cyber attacks targeting oil and gas have been geographically constrained to the Middle East [HEF18], cyber attacks are not unheard of the NCS. In 2014, the Norwegian petroleum sector experienced a large-scale cyber attack with more than 50 Norwegian oil and energy companies attacked in a coordinated phishing campaign [Nas14]. Muller *et al.* examines the challenges in securing the Norwegian petroleum sector in a digital age within a geopolitical context [MGF18]. Russia is presented as a potential threat as it has the capability to conduct advanced cyber attacks, an interest in petroleum activities, and has targeted Western countries in cyber operations [MGF18]. However, Muller *et al.* emphasises that different threat actors within Russia should be differentiated.

There are several identified groups of APTs relevant for companies operating on the NCS. The industrial cyber security company Dragos follows eleven different activity groups targeting ICS. Five out of the eleven groups are known to target oil and gas companies [DRA20]. The cyber security company FireEye has observed at least 16 different APTs targeting companies in the energy sector. An unknown number of the groups are suspected to be Russian-based threat groups conducting reconnaissance of ICS and Supervisory Control And Data Acquisition (SCADA) systems [Fir16].

Reliable supplies of oil and gas are strategic concerns of national importance for states all over the globe. Hence oil and gas supply is of particular interest to intelligence services of both allies and potential adversaries. Additionally, as Norway supplies between 20 and 25 per cent of the EU gas demand [Nor], the threats to the NCS must be viewed in a greater geopolitical context [MGF18].

The threat assessments and risk analysis from the three Norwegian governmental bodies, The Intelligence Service (E-tjenesten), The Norwegian Police Security Service (PST) and NSM, calls attention to the risk of threat actors targeting operators on the NCS. In its 2019 threat assessment, PST states the following:

> "Actors within the petroleum and energy sector also have to take into account that they will be targeted by advanced network operations in 2019" [Pol19].

In their 2020 threat assessment, PST list oil and gas as one of the sectors which are particularly exposed to foreign states intelligence services [Pol20]. The NSM considers that companies in the defence sector, space, maritime, petroleum and power are at risk to threat actors in their 2020 risk assessment [Nas20]. It should be noted that the primary activities conducted by threat actors are reconnaissance and information gathering. However, these activities could be preparation for future sabotage of critical infrastructure [Nas20].

Regarding motivation, threat actors could have several motives, as previously mentioned. Muller *et al.* attributes political or financial objectives as the primary motivation behind cyber attacks that could harm the Norwegian petroleum sector [MGF18]. It should be noted that a financially motivated cyber attack could still impact the ICS. As an example, ransomware could encrypt devices in the ICS, which could cause safety functions in the ICS to fail or production to stop.

Based on the strategic importance of petroleum and threat intelligence from both Norwegian intelligence services and private cyber security companies, operators on the NCS are identified as potential targets for APTs. However, operators should still consider the rest of the threat actors in table 2.5 as there is no evidence to neglect the rest of the actors. However, protecting against threat actors with the highest capability would imply protection from threat actors with lower capability, which are considered less skilful and persistent. Consequently, operators on the NCS must consider the whole spectrum of potential threat actors when defending their systems and networks against threats.

Assets on the NCS

Briefly explained, assets are any elements a threat actor is interested in attacking. Assets in the context of cyber security are physical assets themselves, information stored on them, or the services provided by them. Assets can as well be intangible, an example being reputation.

On the NCS, there are many different assets. In this thesis, the assets of interest are the ones related to the production and processing of hydrocarbons on oil and gas installations. All equipment related to safety is also essential assets as protecting both humans, and the installation itself is vital. In the PERA model (figure 2.1, this correlates to almost all devices and systems contained within level 0 (field devices) to level 3.5 (DMZ). It is important to note that some assets are more critical than others. However, deciding which assets are the most critical is the responsibility of the operator, and usually part of risk analysis. As an example, if safety is deemed more important than production, then assets related to safety are more critical than assets related to production.

Assets related to office systems like human resources (HR), procurement, and accounting are important for an organisation operating on the NCS. Nevertheless, they are out of scope in this thesis. The assets in scope are the equipment in and services provided by the ICS.

Known Vulnerabilities on the NCS

In 2015, the Official Norwegian Report Digital Vulnerabilities in Society (NOU 2015: 13) was published where digital vulnerabilities in the Oil and Gas sector were discussed [Reg15]. The report presented the most common vulnerabilities at the different stages of the petroleum value chain and measures to handle the identified vulnerabilities. The company DNV GL created the underlying report used in the chapter concerning oil and gas in the NOU 2015: 13, *Digital Vulnerabilities in Oil & Gas* [DNV15]. The list below are the top ten identified vulnerabilities in the sector but note that these vulnerabilities are not sorted according to criticality [DNV15].

1. Lack of cyber security awareness and training among employees
2. Remote work during operations and maintenance
3. Using standard IT products with known vulnerabilities in the production environment
4. A limited cyber security culture among vendors, suppliers and contractors
5. Insufficient separation of data networks

6. The use of mobile devices and storage units including smartphones
7. Data networks between on- and offshore facilities
8. Insufficient physical security of equipment such as data rooms and cabinets
9. Vulnerable software
10. Outdated and ageing control systems in facilities.

Additionally, DNV GL discusses some broader themes outside of the top ten vulnerabilities. The authors point out that the complexity of the digital supply chain is a challenge for cyber security [DNV15]. With several dependencies between subcontractors and sub-subcontractors, it is hard to establish each company's responsibility for securing the final systems. Further, the majority of the equipment on installations (such as hardware components, control systems, and software) was designed with a lifespan of 15-25 years. Many of these systems have gotten approved extensions of their time on the platforms, which means the software is outdated [DNV15]. There is no Computer Emergency Response Team (CERT) nor an environment for operational cooperation on incident response in the cyber security domain of the petroleum sector [DNV15]. There are additional themes discussed in the DNV GL report, but these are not included as the themes are deemed out of the scope of this master thesis.

2.8 Attacking ICS

The steps of a cyber attack can be modelled with a kill chain. In 2011 Lockheed Martin created the Cyber Kill Chain [HCA11]. It consists of seven steps the attacker needs to accomplish to mount a successful attack. Observing the steps of the kill chain makes a defender able to identify where he can implement measures to break the chain. There is one kill chain model customised to the nature of ICS, the ICS Cyber Kill Chain created by Michael J. Assante and Robert M. Lee in 2015 [AL15]. This is an adoption of the Lockheed Martin Cyber Kill Chain to an industrial environment. The new framework consists of two stages, the first representing a traditional cyberattack against IT to establish a foothold, and the second stage the process of conducting a successful attack against ICS. The different stages are presented in figure 2.4.

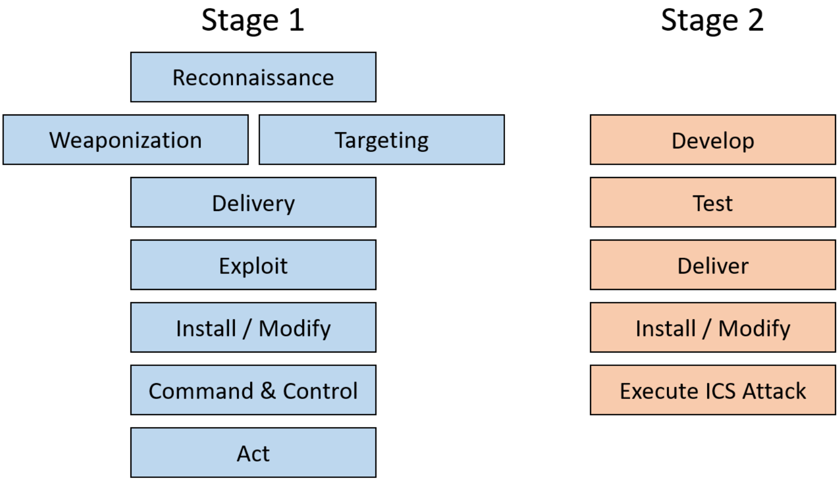


Figure 2.4: The two stages of the ICS Kill Chain with its various steps. Adopted from [Slo20].

The first step of an attack on ICS is to establish access. As mentioned above, this can be done through an attack on the IT environment to establish a foothold. However, cyber attacks limited to IT is out of scope in this thesis. Still, there are several techniques to get direct access to the ICS environment. MITRE ATT&CK for ICS presents ten techniques used to get initial access to the ICS [MIT20]. These techniques are presented in a list below.

1. Data Historian Compromise
2. Drive-by Compromise
3. Engineering Workstation Compromise
4. Exploit Public-Facing Application
5. External Remote Services
6. Internet Accessible Device
7. Replication Through Removable Media
8. Spearphishing Attachment
9. Supply Chain Compromise
10. Wireless Compromise

Cyber attacks on ICS can be divided into two main categories after the end objective of the attack, information gathering and disruption of the physical processes. Of the known cyber attacks, malware, campaigns, and cyber-threat groups targeting ICS, the first category is the most common [HEF18], but the second is the most critical as the consequences are more severe. Consequences could be a stop to production, loss of human life, damage to equipment, and environmental damages due to spillage.

Cyber attacks with a physical impact can be further differentiated based on the techniques used. A cyber attack on ICS can focus on immediate process disruption, such as turning off the power or shutting down a plant. Nevertheless, an examination of the history and potential of known ICS intrusions shows a far more alarming attack vector [Slo19]. Rather than seeking immediate disruption, attackers undermine the integrity of an industrial environment, by targeting the process accuracy or process safety. Undermining the integrity can achieve impacts with more significant results than merely disrupting the process like degrading the production over an extended period.

Slowik presents in detail how the cyber attacks Stuxnet, Industroyer and Trisis all are integrity-based cyber attacks in [Slo19]. Stuxnet is the first known ICS-targeting malware, and other integrity-based attacks mimic its behaviour. Rather than seeking direct disruption, Stuxnet sought to undermine process integrity by altering the functionality of the plant in question while concealing effects to operators. Since then, the industrial community faced a long period where attacks focused only on direct disruption until the emergence of Industroyer in 2016 and the safety-system targeting TRISIS. Each of these sought in specific ways to undermine the very reliability of underlying processes to produce potentially disastrous outcomes.

Knowledge of the industrial process in question is required to attack ICS successfully and cause a physical impact. Green *et al.* show how specific knowledge of the industrial process in question is necessary to manipulate process variables successfully [GKA17]. Understanding what information is necessary for the attacker in order to achieve its desired completeness of process comprehension, is critical for planning defence activities.

2.8.1 MITRE ATT&CK for ICS

MITRE ATT&CK for ICS is a knowledge base useful for describing the actions an adversary may take while operating within an ICS environment [MIT20]. The knowledge base can be used to better characterise and describe post-compromise adversary behaviour. The framework consists of eleven different tactics, and 81 techniques used by adversaries. As an example, Hooking, Module Firmware, Program Download, Project File Infection, System Firmware, and Valid Accounts are the six techniques that make up the technique Persistence. All the techniques are based on real observations of either adversaries or proof of concepts from researchers. Each of these techniques can be considered as a threat to the ICS, and selected techniques are used in the discussion in chapter 6 to give concrete evidence on threat actors attack ICS.

Tactic	Description
Initial Access	The adversary is trying to get into your ICS environment.
Execution	The adversary is trying to run malicious code.
Persistence	The adversary is trying to maintain their foothold in your ICS environment.
Evasion	The adversary is trying to avoid being detected.
Discovery	The adversary is trying to figure out your ICS environment.
Lateral Movement	The adversary is trying to move through your ICS environment.
Collection	The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.
Command and Control	The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.
Inhibit Response Function	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
Impair Process Control	The adversary is trying to manipulate, disable, or damage physical control processes.
Impact	The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment.

Table 2.6: The 11 MITRE ATT&CK for ICS Tactics

Chapter 3 Methodology

This chapter presents the research methodology applied in this master thesis. The idea is to describe and explain the research methods used together with the considerations made. First, the research goal and research question are presented in detail, together with the reasoning behind the choice of method in section 3.1. Then, the methods for data collection, literature review and gap analysis, are presented in sections 3.2 and 3.3 respectively. Further, some ethical considerations concerning the research method and study subject are presented in section 3.4. Finally, potential pitfalls with the research method are presented in section 3.5. An overall figure of the methodology is shown in figure 3.1 in section 3.1.

3.1 Research Question and Research Design

According to Edgar *et al.* the field of cyber security research contends with numerous unique issues, such as a high-speed environment evolution, adversarial behaviour, and the merging of natural and social science phenomena [EM17]. The research method should be tailored to account for the issues above and the type of phenomena under examination.

The project description states that *The goal of this research is to evaluate the effect (risk reduction) of cyber security barriers on safety-related control functions on the NCS. Evaluating barriers will be done through a threat modelling of offshore platforms on the NCS.* This means the result of this master thesis should provide new knowledge on the state of cyber security in the Norwegian oil and gas sector. The research goal was based on initial discussions with both the supervisor and the responsible professor after attending an industry conference on cyber security in ICS on the NCS[1] in October 2019.

[1] CDS-forum - Industry Forum for Cybersecurity of Industrial Automation and Control Systems, https://www.sintef.no/projectweb/cds-forum/

The research question (RQ) presented in section 1.2 was formulated during the spring of 2020 and is derived from the research goal. RQ:

> *How are implemented cyber security barriers on the Norwegian Continental Shelf aligned with Industrial Control Systems cyber security standards and best practices?*

With this research question, the researcher wanted to provide new knowledge on what barriers are currently implemented on the NCS, and how these barriers align with acknowledged guidelines, standards, frameworks and best practices. As the RQ is a 'how' question, the result should be a description of how current cyber security barriers cover standards and best practices used in cyber security in ICS.

Robson and McCartan propose fixed and flexible designs as approaches to the design of a study [RM16]. A fixed design study is a study where the design is fixed before the main stage of the data collection takes place. Flexible design, on the other hand, evolves during the data collection, and it usually corresponds to using qualitative research methods, but this is not a requirement. Using a flexible design will give the researcher more flexibility. This thesis utilised a flexible design as it was not entirely clear how the RQ was best answered before the data collection.

A significant part of the research is to acquire knowledge about the research area before answering the RQ. Thereby, it is reasonable to consider that a single research method can not be sufficient for the entirety of the master thesis. A literature review was conducted to examine reliable and informative sources before the research question was answered with a second method. The literature review examined literature related to ICS cyber security guidelines, and threats and vulnerabilities on the NCS.

The second research method used in this thesis was a gap analysis. Gap analysis has not been used in the field of cyber security on the NCS before, but have seen previous applications in cyber security [MMST16, KFA^{+}11]. As the objective of the RQ is to answer how implemented barriers are aligned with best practices, a gap analysis is suited to find this alignment or non-alignment. The literature review influenced the selection of ICS cyber security guidelines in the gap analysis.

Case Study

In this thesis, the gap analysis is performed as a case study. A case study can be done on a single entity or multiple entities to investigate the phenomena under examination [Yin09]. Investigating one phenomenon across multiple entities will make the study more generalised, and conclusions can more easily be drawn beyond the study. However, it is more resource consuming to investigate details in several entities. On the contrary, a single entity case study enables the researcher to investigate the particular details of the phenomenon investigated. However, the results are specific to the entity, and conclusions may not be generalisable in a broader context.

To be able to do a detailed gap analysis of the cyber security barriers of an operator on the NCS, it is necessary to go into depth. Consequently, in this thesis, a single case is examined. The study subject is a single organisation, an operator on the NCS. The case involves a single unit of analysis which is examining the documentation on implemented barriers. This type of case study is a holistic single-case design [Yin09]. Analysing subsets of the documentation in greater detail would have made the case into an embedded case study with multiple units of the analysis. However, there was no evidence to select particular subsets from the documentation rather than examining the full documentation.

A single-case holistic case study implies that the result of this thesis does not apply to other organisations. However, the thesis should be relevant to other organisations in the same sector, other operators on the NCS. Still, no conclusions on other operators can be drawn. How these operators implement and document cyber security barriers is not examined, and subsequently, the results are not directly applicable.

It is common to perform several data collections in a case study [Yin09]. However, external factors explained in section 3.5 impacted the number of available methods for data collection for this thesis. Consequently, the study relied entirely on the analysis of the documentation provided by the operator, which is a weakness of the research method. Still, due to the narrow scope of the research question, the method should be adequate. Mapping three different best practices give more credibility to the research compared to mapping from one best practice as conclusions are drawn from more sources of evidence.

Final Research Design

In summary, the research design of the thesis consists of two research methods, literature review and gap analysis. Additionally, the research is a single-case holistic case study as the documentation on cyber security barriers of a single operator on the NCS is examined. The study was a flexible design, but due to external factors and abundant information received from the operator, no additional data collection was performed. Figure 3.1 presents a flowchart of the methods used to answer the research question.

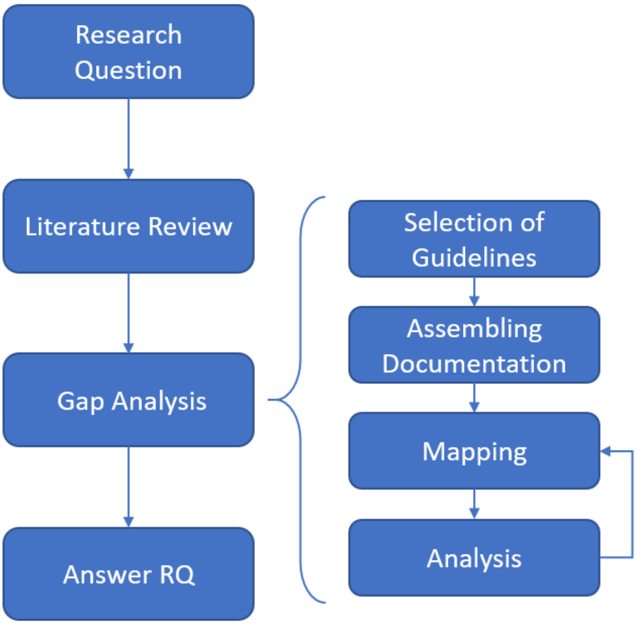


Figure 3.1: A flowchart presenting the steps of the selected research method.

3.2 Literature Review

As outlined in figure 3.1, a literature review is performed before the gap analysis. The literature review is used as a basis for both acquiring knowledge about the research area, and examining ICS cyber security guidelines before performing the gap analysis. The paper *Undertaking a literature review: a step-by-step approach* [CRC08] by Cronin *et al.* outlines a step-by-step approach to literature reviews which consists of the following elements:

1. Selecting a review topic.
2. Searching the literature.
3. Gathering, reading and analysing the literature.
4. Writing the review. Literature found relevant is included in chapter 2.
5. References. All literature used is referenced and stored in Bibtex.

The research goal and research question influenced the review topics selected. The goal of the literature review was to gather information on standards and guidelines used in ICS cyber security, and to create a threat model for the NCS. The exact terms used in the search are presented in table 3.1. Synonyms were extensively used to obtain all relevant sources.

Search terms		
threat	model	norwegian continental shelf
		oil and gas
		petroleum
cyber security	threats	norwegian continental shelf
		oil and gas
		petroleum
cyber security	vulnerabilities	norwegian continental shelf
		oil and gas
		petroleum
cyber security	guideline	norwegian continental shelf
		oil and gas
		industrial control systems
cyber security	best practice	norwegian continental shelf
		oil and gas
		industrial control systems
cyber security	standard	norwegian continental shelf
		oil and gas
		industrial control systems

Table 3.1: Search terms used in the literature review. The terms are divided into two themes, threats and best practices for cyber security.

In the ecosystem of industrial cyber security, many actors publish valuable material which is not necessarily found in academic search engines which are traditionally used to find relevant literature [CRC08]. To be able to find relevant background material, the following actors were also considered when finding literature:

- Private companies working with ICS cyber security (Dragos Inc and DNV GL).
- Private companies publishing threat intelligence on the oil and gas sector (FireEye Inc, and Dragos Inc).
- Institutions working with ICS cyber security (SANS Institute, ENISA, and SINTEF).
- Organisations which create the international standards governing ICS cyber security (IEC and ISA).

- Governmental bodies which develop national guidelines for ICS cyber security (NIST and PSA).
- Norwegian Intelligence Services publishing threat intelligence (NSM, PST, and E-tjenesten).

However, before selecting any literature, three inclusion criteria were formulated to find relevant research and to reduce the total number of articles and sources to a manageable level. The following list presents the different inclusion criteria used in selecting literature.

- *Setting*: The research should be scoped to ICS cyber security.
- *Geographic location*: The research should be scoped to the NCS, or at minimum cyber security in oil and gas.
- *Time*: Research concerning threats and vulnerabilities on the NCS should be reasonably recent.

The academic search engines used include Microsoft Academic (MA) and Google Scholar. MA was primarily used to gather research articles as it provides the researcher with the ability to query a semantic search engine rather than just searching the web. Using a semantic search engine reduces the number of results from searches while keeping the most relevant results. Searching "threat model ICS" in MA provides 316 results compared to 340 000 results in Google Scholar. A disadvantage of MA is that it only considers peer-reviewed or conference papers and books. This is a disadvantage due to the limited amount of research in the field of ICS cyber security on the NCS. Consequently, Google Scholar was used to finding relevant sources from other actors, as mentioned previously.

Next, in gathering, reading and analysing the literature, the different inclusion criteria were considered when deciding on the applicability of a source. Headline, abstract, summaries and keywords were used to decide if the source was relevant. All included literature is presented in chapter 2. The chapter presents background information as well as establishing a threat landscape on NCS. The literature review forms the basis for the sources included in sections 2.4, 2.6, 2.7, and 2.8. Finally, all literature is referenced and managed through Bibtex.

3.3 Gap Analysis

The thesis builds on a gap analysis between three selected best practices and the cyber security requirements of an operator on the NCS. In general, a gap analysis serves the purpose of identifying the difference (gap) between the current and the target state of affairs. In this thesis, the current state refers to the implemented cyber security barriers of the operator, while the target state is the countermeasures proposed by the three best practices. The difference between the two states is the gap, and the gap will be used to answer the research question. The following sections present the steps used to perform the gap analysis.

This method accommodates the research question presented in section 1.2 as the gap identifies too which degree the implemented cyber security barriers of the operator are aligned with categories and controls in the selected best practices.

The process of selecting best practices is presented in 3.3.1. In order to do a gap analysis, the researcher obtained documentation on the cyber security barriers implemented by an operator on the NCS. The process of assembling documentation is presented in 3.3.2, while the operator and the documentation are presented in chapter 4. Due to confidentiality considerations (ethical considerations are presented in section 3.4), the operator is anonymised and given the pseudonym "Alpha". How the mapping was conducted is presented in 3.3.3, and how the analysis was performed in 3.3.4. A second iteration of both mapping and analysis was done to reduce the risk of mistakes and decide on uncertain mappings left from the first iteration.

For clarity, the word requirement always refers to a cyber security requirement from the documentation of the operator. In contrast, the word control refers to the countermeasures presented in the best practices.

3.3.1 Selection of Guidelines

In cyber security, there are numerous different guidelines, frameworks, standards, and best practices expressing the countermeasures organisations should implement to protect their assets against threats. As the scope of this thesis is ICS on the NCS, the focus was on best practices tailored to industrial cyber security in the oil and gas sector.

Through discussion with both supervisors, it was decided that the gap analysis should consider three different best practices. The best practices chosen were the NIST CSF, the IEC 62443 3-3, and the CIS Controls. The standards and guidelines are presented in section 2.4. The choice of guidelines was based on the following two judgements. Firstly, based on talks at the aforementioned CDS-forum where the supervisors also participated (see section 3.1). The talks provided a view on which cyber security guidelines are in use on the NCS today. Secondly, the choice was based on the *SANS 2019 State of OT/ICS Cybersecurity Survey*, which includes a presentation of the top ten regulations, standards, and best practices used to map OT/control systems [FW19]. The list is presented in table 3.2.

Rank	Document	Percentage
1	NIST CSF	38,1%
2	ISO 27000 series	32,0%
3	NIST 800-53	31,4%
4	NIST 800-82	30,9%
5	IEC 62443 series	30,4%
6	CIS Controls	29,9%
7	NERC CIP	23,7%
8	GDPR	15,5%
9	C2M2 (Cybersecurity Capability Maturity Model)	10,3%
10	NIS Directive (EU)	8,3%

Table 3.2: Top 10 Regulations, Standards, Best Practices Used in ICS. *Which cyber security standards, regulations or best practices do you map your OT/control systems to? Select all that apply.* Derived from [FW19].

In the table, the most used regulations, standards or best practices from the survey can be observed. The most used document is the NIST Cyber Security Framework (CSF), followed by the ISO 27000 series and NIST Special Publication 800-53. The ISO 27001 provides best practice recommendations on information security management [NEK18], but the series is not tailored to ICS nor oil and gas. NIST 800-53 provides a catalogue of security and privacy controls for all U.S. federal information systems [NIS15a], but is neither tailored to ICS or oil and gas. The fourth entry on the list is NIST 800-82, Guide to Industrial Control Systems (ICS) Security. NIST 800-82 is tailored to ICS as it customises the controls in NIST 800-53 to ICS [NIS15b]. However, based on the talks as mentioned earlier at CDS-forum, it was apparent that there is a substantially higher interest in IEC 62443 and the CIS Controls. The CIS Controls are created for traditional Enterprise IT environments [CIS19], but the CIS Controls have a guideline for adopting the controls in ICS [CIS18]. In section 2.4.1, it is presented how IEC 62443 have numerous different sub-standards as part of the series. As this thesis primarily focuses on the technical aspect of cyber security, IEC 62443 3-3 was selected as the sub-standard to map. IEC 62443 3-3 presents the documentation for setting *System security requirements and security levels.* Consequently, NIST CSF, CIS Controls, and IEC 62443 3-3 were chosen as the documents to examine in a gap analysis.

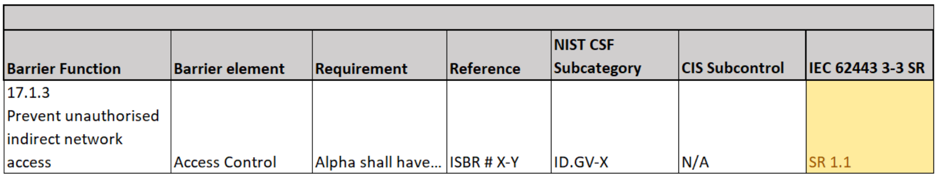
3.3.2 Assembling Documentation

It is necessary to examine cyber security barriers in place on the NCS to answer the research question. As the study is structured as a holistic single-case study, a single operator on the NCS was contacted. The operator agreed to participate in the study and provided the necessary documentation. The documentation provided was a barrier strategy and a corresponding Performance Standard which sets requirements to the barrier elements in the barrier strategy. The Performance Standard states all controls the operator implements to protect against and minimise the effect of cyber attacks in ICS. Additionally, the operator held a presentation introducing the two documents and how it approaches cyber security in ICS. In chapter 4, the two documents are discussed in detail, as well as presenting the necessary information on the operator. As previously mentioned, the operator will be anonymised throughout the thesis, and necessary ethical considerations are addressed in section 3.4.

3.3.3 Mapping

The main part of the gap analysis is mapping the requirements in the Performance Standard to each of the ICS cyber security guidelines. The mapping was done in Microsoft Excel. Each requirement from the Performance Standard was represented in a distinct row in the Excel sheet. Then the subcategories, sub-controls, and system requirements in NIST CSF, CIS Controls, and IEC 62443 were mapped separately against the 125 requirements in the Performance Standard. Figure 3.2 presents the structure of the Excel sheet used in the mapping.

Mapping a requirement to a control involves examining the description of the requirement and then finding a corresponding control in the guideline currently being mapped. The mapping of a particular requirement results in the requirement either being covered by one control, covered by several controls in the particular guideline or not covered by any controls in the guideline. The mapping was aided by the use of keyword search and existing mappings between the selected best practices to reduce the workload.



Barrier Function	Barrier element	Requirement	Reference	NIST CSF Subcategory	CIS Subcontrol	IEC 62443 3-3 SR
17.1.3 Prevent unauthorised indirect network access	Access Control	Alpha shall have...	ISBR # X-Y	ID.GV-X	N/A	SR 1.1

Figure 3.2: The structure of the Excel sheet used in the mapping with an example. N/A are used on requirements not covered by any controls in the guideline. Yellow coloured cells mark mappings subject to a second review.

One issue that needs to be addressed is if the requirement only partly covers the control under examination. In this case, it will be challenging to map the requirement as the association between control and requirement is not exhaustive. This scenario will materialise in the mapping when requirements have a different level of detail or include only parts of the scope of the control. A requirement can be more specific than a control, or the control can be more specific than the requirement. In these cases of doubt, the control was marked for a second review with a yellow colour.

The second review was performed during the second iteration of mapping and analysis. In the second review, it was examined if the requirement satisfies the goal of the control sufficiently. As one iteration of mapping and analysis had been performed, it was possible to examine these cases of doubt in a broader context as all requirements and controls had by then been examined once.

3.3.4 Analysis

Finally, the result of the mapping was analysed. The three outcomes of each mapping are presented in figure 3.3. After each mapping, there will be non-mapped requirements in the Performance Standard (unless all requirements are mapped), requirements mapped to controls, and non-mapped controls in the ICS cyber security guideline (unless all controls are mapped). The extent of coverage of each guideline will be calculated by looking at the ratio of mapped and non-mapped controls. The coverage will include both the total coverage, but also the coverage of each category in each ICS cyber security guideline. This analysis will provide tables which present the areas of the guidelines that are covered, and which areas that are not. Note that the requirements that are not mappable to any of the controls in any of the three ICS cyber security guidelines will be identifiable after the mapping. These non-mapped requirements will also be presented in chapter 5, and discussed in chapter 6.

Based on the mapping, a single table with the coverages of the three mapped best practices will be presented as an answer to the research question. These coverages, both in absolute number and percentage, will show the alignment of the implemented cyber security barriers to the selected cyber security standards and best practices. This result will be presented in chapter 5, and discussed in chapter 6.

To provide some new knowledge concerning the overall research goal of this thesis (see section 3.1) the character of the non-mapped controls was examined. Considering that the goal of both the implemented barriers and the controls in the best practices is to prevent threat actors from performing successful cyber attacks, it is reasonable to believe that barriers which are missing controls are less effective in preventing the successful cyber attacks. Note that this reasoning is based on the assumption that the best practices provide efficient protection.

After the three gap analyses were completed, the results were reviewed in a simple process to find the cyber security activities not covered by the Performance

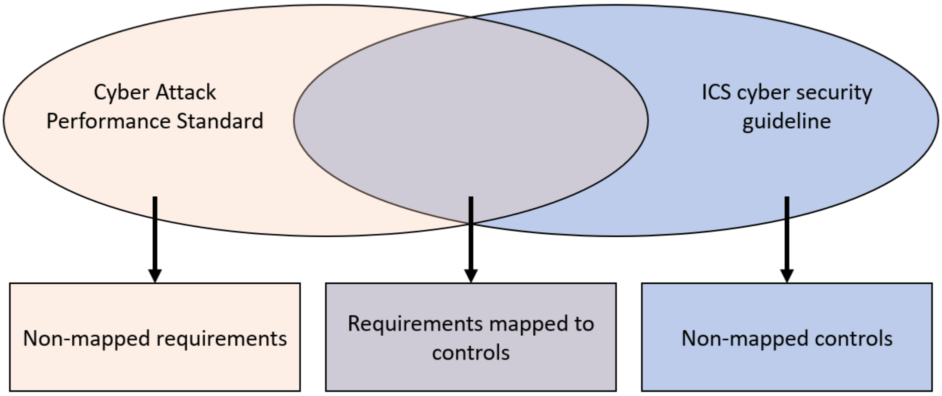

Cyber Attack Performance Standard
ICS cyber security guideline
Non-mapped requirements
Requirements mapped to controls
Non-mapped controls

Figure 3.3: The three outcomes when mapping an ICS cyber security guideline to the requirements in the performance standard.

Standard. The non-mapped controls were given categories based on their purpose, which corresponds to a cyber security activity. Next, triangulation was used to identify the activities that all three best practices identify as non-mapped. Finally, five cyber security activities were selected, and they are presented in 5.5, and discussed in 6.2. The criteria for selection was activities with a substantial gap, and it was desired to select activities which collectively associate to both proactive and reactive barriers. Five was used as a limit as discussing all non-mapped controls, and the following implications were judged excessive.

Finally, it will be determined which guideline is the most complete in covering the requirements in the Performance Standard based on the non-mapped requirements. This calculation follows the same approach as the calculation of the guidelines as mentioned above. This result is presented in 5.6.

3.4 Ethical Considerations

The main ethical concern related to the research method is the potential revealing of confidential information from the organisation participating in the case study. The researcher had to sign a Non Disclosure Agreement (NDA) before any confidential material was provided to the researcher. The participating organisation was given a pseudonym in the thesis to protect their identity. The organisation was also given the final draft of this thesis to comment on any information in conflict with the NDA, which were subsequently removed. Leaking the identity of the organisation could expose the operator to targeted cyber attacks, and consequently, measures to protect its identity was implemented.

The results of the thesis were also provided to the operator through a presentation in June 2020. Presenting the results made sure the identified gaps were presented to key personnel in the organisation. Additionally, the Excel sheet used in the gap analysis was provided to the operator.

The full documentation from Alpha and the Excel sheet used in the gap analysis are not included in any appendix of this thesis as this would conflict with the NDA.

3.5 Challenges and Limitations

Possible biases and limitations of the research are addressed in this section to give the research credibility. The generalisability, reliability and validity of the research are discussed together with external factors impacting the master thesis.

The thesis is relying on a single organisation in the case study. Examining a single organisation enables the researcher to discuss countermeasures in great detail, but all results are drawn from a single source of information. There is no triangulation of results between different organisations which makes the generalisability of the thesis weaker. However, studying several organisations on the required level of detail would not be feasible in the limited time available for conducting the master thesis. Triangulation can also be achieved by having several sources of data collection, such as conducting experiments, interviews, and surveys [Yin09]. However, this proved difficult due to external factors explained below. Considering other operators on the NCS, the thesis should still have some applicability in their context as they are facing similar challenges in cyber security as the organisation in the case study.

All mappings are challenging to work with as the standards have different objectives, perspectives and divisions. Requirements and controls may seem somewhat coinciding, but upon close examination of the rationale text, it can be seen that there may be significant differences between the text in the requirement and the control. The challenge of correctly mapping requirements and controls impacts the reliability and replicability of the analysis and the result. Additionally, when mapping a requirement, the researcher can be tainted with biases which impact the mapping. The mapping was done twice to reduce the risk of errors, but there will still be a notable residual risk for errors in the mapping.

The research question does not meet the research goal in its entirety, but the gap analysis provides knowledge helpful to evaluate the effectiveness of cyber security barriers. Evaluating the effect of all barriers even for a single operator on the NCS is a considerable amount of work, and the work would rely heavily on free access to stakeholders and the necessary information in the organisation. Free access was deemed unfeasible because of two external factors. With the corona-crisis and historically low oil prices during the spring of 2020, it proved difficult to get external actors, i.e. operators on the NCS, invested in the thesis. This difficulty resulted in a reshaping of the thesis to be solely based on a gap analysis of selected ICS cyber security guidelines.

Chapter 4 Case

This chapter presents the cyber security barriers implemented by the organisation which participated in the case study. The organisation is anonymised for confidentiality reasons, and the master thesis will refer to the fictitious company "Alpha" and its offshore oil platform "Bravo". Operator "Alpha" is an operator on the NCS with the responsibility of operating the offshore oil platform "Bravo". The following section presents the documentation received from Alpha as stated in section 3.3.2.

The study subject is the ICS on Bravo with the related safety-related control systems. The safety-related control systems, in this case, are the Fire & Gas Detection (F&G), Emergency Shutdown (ESD), Process Shutdown (PSD), and Public Address and General Alarm (PAGA) on the platform. The safe operation of Bravo is of critical importance, and these systems are significant parts in keeping operations safe.

4.1 Alpha's Implemented Cyber Security Barriers

The operator Alpha has a barrier strategy in line with the barrier model used on the NCS, and this model is presented in the *Barrier Memorandum 2017* authored by the PSA [Nor17]. The strategy is tailored to the platform, Bravo. Barrier management requirements and practices are presented in 2.3 together with relevant regulations. Figure 4.1 presents the barrier model used on the NCS. Functions to identify, reduce the likelihood of, and reduce the consequence of failure, hazard and accident situations outside of normal operations should be in place. The part of the diagram showing functions to reduce the likelihood and reduce consequence, as well as the incident itself, is called a bow-tie diagram.

Cyber security is identified as part of the barriers on Alpha's installation, Bravo, and cyber security barrier elements are in place to reduce both the likelihood and consequence of a successful cyber attack in the ICS environment. The organisation has created a Cyber Attack Performance Standard (CAPS) which set requirements to

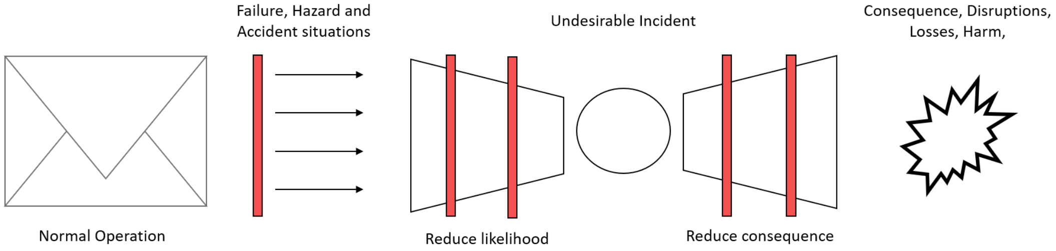

Failure, Hazard and Accident situations
Undesirable Incident
Consequence, Disruptions, Losses, Harm,
Normal Operation
Reduce likelihood
Reduce consequence

Figure 4.1: Traditional barrier diagram showing functions (in red) to handle failure, hazard and accident situations outside of normal operations. Adopted from [Nor17].

the technical, operational and organisational countermeasures (barriers) implemented to protect the overall safety of the installation. The CAPS show which activities are required to maintain the correct function of a countermeasure.

Of the many performance standards, one governs the case of a cyber attack, and there is one corresponding barrier strategy for the case of a cyber attack. The CAPS sets the requirements for the barriers in the Cyber Attack Barrier Strategy (CABS). The relationship between the PSA barrier management model and CABS is presented in figure 4.2. The CABS is split in two parts which align with the two main functions of the PSA barrier management model. Reducing the likelihood of incidents is changed to reducing the probability of a successful cyber attack, and reducing the consequence is changed to mitigating the consequences of a successful cyber attack.

As mentioned above, the CABS presents barriers for two different situations, reducing the probability of a successful cyberattack, and mitigating the consequences of a successful cyberattack. Figure 4.4 shows the relationship between reducing the probability of a successful cyberattack and all the barrier elements in the CABS and figure 4.5 show the relationship between mitigating the consequence of a successful cyberattack and the different barrier elements. The relevant barrier function is shown in yellow while the barrier element are shown in light green. Each barrier function has at least one requirement in the CAPS .

The CAPS consist of 125 different requirements, and the requirements are derived from two different guidelines:

1. The *recommended guidelines on information security baseline requirements for process control, safety and support ICT systems* from Norwegian Oil and Gas (NOG 104) [NOG16]. NOG 104 is presented in section 2.4.4.

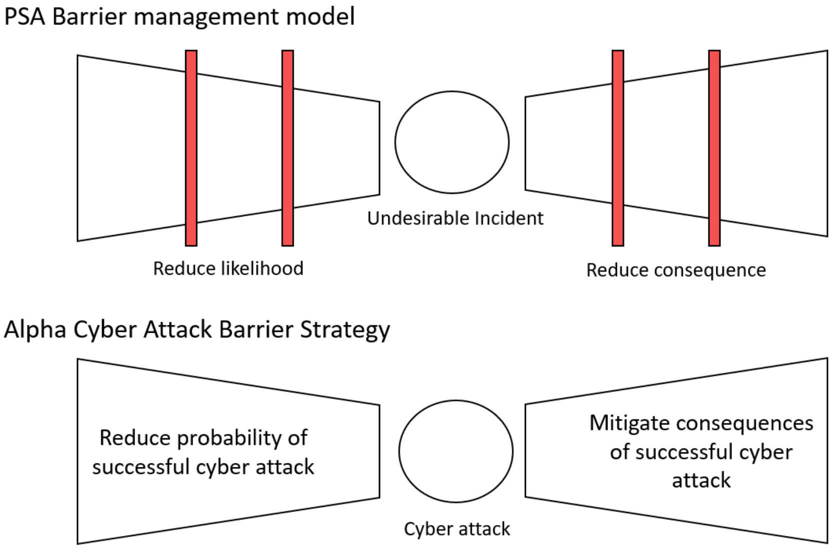
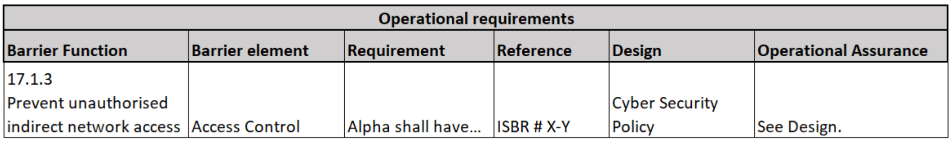

PSA Barrier management model
Undesirable Incident
Reduce likelihood
Reduce consequence
Alpha Cyber Attack Barrier Strategy
Reduce probability of successful cyber attack
Mitigate consequences of successful cyber attack
Cyber attack

Figure 4.2: PSA barrier management model compared with Alpha's two-pronged Cyber Attack Barrier Strategy.

2. The recommended practice *Cyber security in the oil and gas industry based on IEC 62443* (DNVGL-RP-G108) from DNV GL [DNV17]. DNVGL-RP-G108 is presented in section 2.4.1.

The requirements are devised to meet the overall objective of the CAPS, which is to describe operational assurance activities to protect against and minimise the effect of cyber attacks. A secondary objective is to fulfil the operational requirements in NOG 104. The CAPS lists the requirements and gives a high-level description of how the requirements are fulfilled. The structure of the columns in the CAPS is shown in figure 4.3. The CAPS groups the requirements after the Information Security Baseline Requirements (ISBRs) found in NOG 104, and presents the barrier function and element related to the group (ISBR). Each ISBR has a number of requirements, and the requirements are named as *ISBR # X-Y* where *X* is the corresponding ISBR and *Y* is the requirement's number in the group. As an example, there are eleven requirements belonging to ISBR 1, and they are numbered from *ISBR # 1-1* to *ISBR # 1-11*, where all eleven requirements are part of the barrier element access control. Of the 125 requirements, 114 are based on NOG 104, and the remaining 11 are based on DNVGL-RP-G108. DNVGL-RP-G108 is used for requirements in areas where Alpha identified a lack of requirements in NOG 104. Each requirement has corresponding fields in the CAPS named design and operational assurance which is how Alpha satisfies the requirement. The ISBR *Information security in engineering, procurement and commissioning processes* (ISBR 8) is omitted from the CAPS as it covers requirements outside of operation. The CAPS is compared to three other relevant standards and guidelines in chapter 5 through a gap analysis.



Operational requirements					
Barrier Function	**Barrier element**	**Requirement**	**Reference**	**Design**	**Operational Assurance**
17.1.3 Prevent unauthorised indirect network access	Access Control	Alpha shall have...	ISBR # X-Y	Cyber Security Policy	See Design.

Figure 4.3: The six different columns forming the CAPS with an example in the third row.

It should be noted that a significant part of the requirements in the CAPS is covered by the access control system used by Alpha, given the pseudonym "Aegis" in this thesis. Aegis controls all access to resources in the ICS based on work-orders from a central management system which forces all access to the ICS to be both time-limited and role-based. This gives visibility and traceability of all actions in the ICS, which is a valuable foundation for implementing countermeasures against cyber attacks.

While the CAPS contain 125 requirements, the vast majority of the requirements belong to barrier elements assigned to reduce the probability of a successful cyber attack. The CAPS does not contain a detailed mapping of each requirement to each barrier element which would make it possible to calculate the exact number of requirements to each barrier element. Instead, there is a coarse mapping between each group of requirements and the corresponding barrier element. This stands for all ISBRs except the last ISBR where the mapping is detailed. The exception mentioned has requirements to all the seven barrier elements in mitigating the consequence of a successful cyber attack, and one of the barrier elements in reducing the probability of a successful cyber attack. 97 out of 125 (78%) requirements belong to barrier elements in place to reduce the probability of a successful cyber attack, and the remaining 28 (22%) requirements belong to barrier elements in place to mitigate the consequence of a successful cyber attack. This shows that the majority of the effort put in countermeasures are fixed on reducing probability, assuming each requirement is weighted equally.

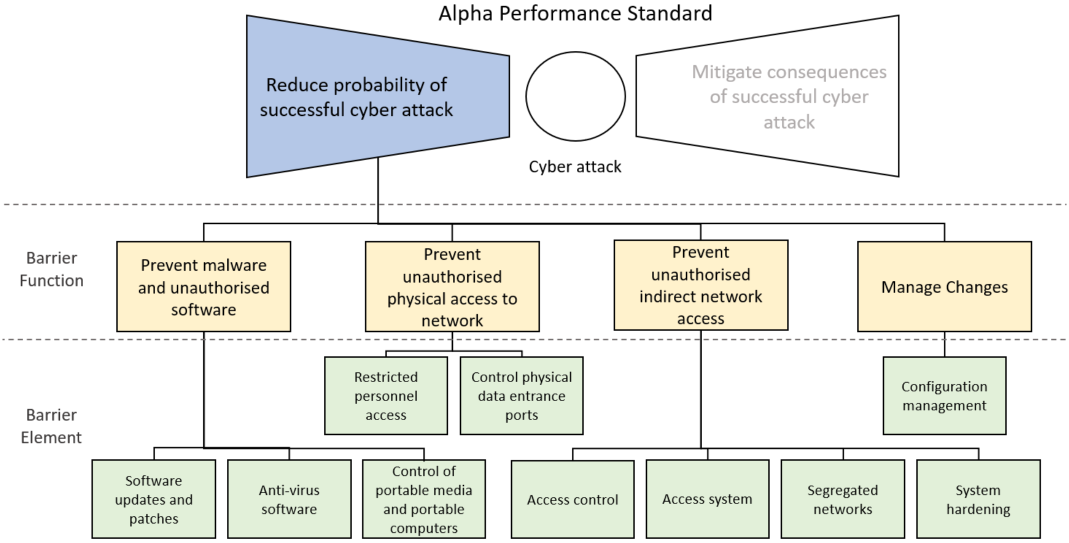

Alpha Performance Standard
Reduce probability of successful cyber attack
Cyber attack
Mitigate consequences of successful cyber attack
Barrier Function
Prevent malware and unauthorised software
Prevent unauthorised physical access to network
Prevent unauthorised indirect network access
Manage Changes
Barrier Element
Restricted personnel access
Control physical data entrance ports
Configuration management
Software updates and patches
Anti-virus software
Control of portable media and portable computers
Access control
Access system
Segregated networks
System hardening

Figure 4.4: Overview of the proactive barrier functions with the associated barrier elements reducing the probability of a successful cyber attack.

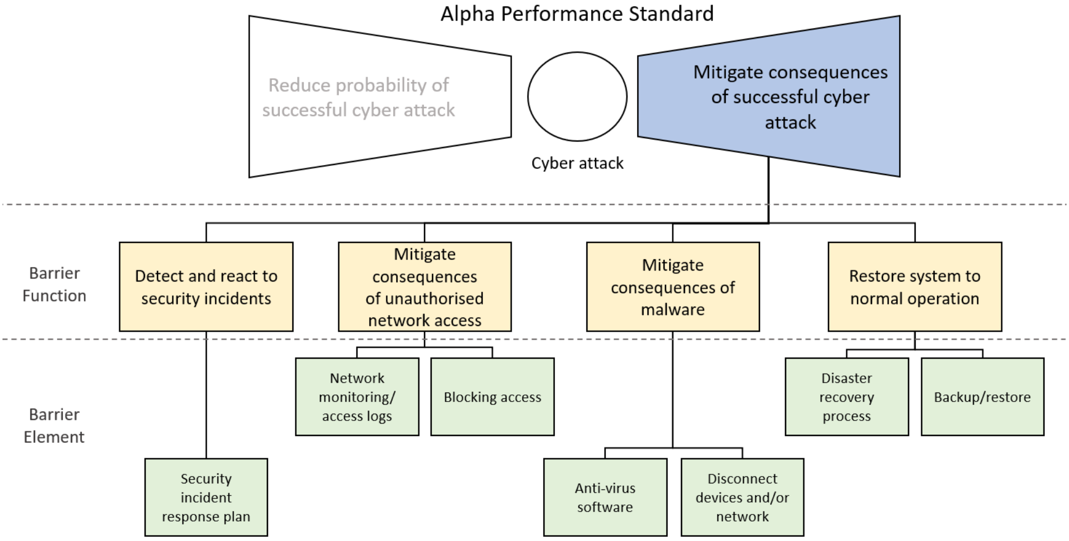

Alpha Performance Standard
Reduce probability of successful cyber attack
Cyber attack
Mitigate consequences of successful cyber attack
Barrier Function
Detect and react to security incidents
Mitigate consequences of unauthorised network access
Mitigate consequences of malware
Restore system to normal operation
Barrier Element
Network monitoring/ access logs
Blocking access
Disaster recovery process
Backup/restore
Security incident response plan
Anti-virus software
Disconnect devices and/or network

Figure 4.5: Overview of the reactive barrier functions with the associated barrier elements mitigating the consequence of a successful cyber attack.

Chapter 5 Results

This chapter presents the results of the gap analysis to answer the research question. First, the relation between NOG 104 and the CAPS is presented in section 5.1. The results of mapping NIST CSF are presented in section 5.2. CIS Controls follows in section 5.3. Next, the results of mapping IEC 62443 3-3 are presented in section 5.4. Further, five cyber security activities identified as inadequately addressed by the gap analysis are presented in section 5.5. Finally, the gap analysis shows which of the three guidelines that gives the best coverage of the CAPS in section 5.6.

To reiterate, the research question of this thesis is: *How are implemented cyber security barriers on the Norwegian Continental Shelf aligned with Industrial Control Systems cyber security standards and best practices?*

In order to identify the alignment of cyber security barriers on the NCS to ICS cyber security standards and best practices, a gap analysis was performed. The gap analysis followed the method presented in section 3.3. The gap analysis was done between the Cyber Attack Performance Standard (CAPS) of operator Alpha and the three selected guidelines. The three selected guidelines are the NIST Cybersecurity Framework (CSF) [NIS18], the CIS Controls [CIS19], and the standard IEC 62443 3-3 [IEC13], which is presented in sections 2.4.5, 2.4.6, and 2.4.1 respectively. The documentation received from Alpha is presented in section 4.1.

The subcategories, sub-controls and system requirements from the guidelines NIST CSF [NIS18], CIS Controls [CIS19], and the standard IEC 62443 3-3 [IEC13] was mapped sequentially to the different requirements in the CAPS. The three relevant standards and guidelines to the CAPS have slightly different objectives, and subsequently, they have different approaches to managing cyber security. Following the method for the analysis presented in 3.3.4, there are three outcomes of each mapping. A mapping will result in non-mapped requirements in the CAPS (unless all requirements are mapped), requirements mapped to controls, and non-mapped controls in the ICS cyber security guideline (unless all controls are mapped).

5.1 The relationship between CAPS and NOG 104

As mentioned in section 4.1, the CAPS is primarily based on NOG 104. In NOG 104, there is a figure placing the NIST CSF functions as proactive and reactive barrier functions in relation to the barrier management model used on the NCS [NOG16]. Figure 5.1 shows that Identify, Protect, and Detect are regarded as proactive barriers, while Respond and Recover are regarded as reactive barriers. The figure also shows how the functions in the NIST CSF framework provide a coherent approach to cyber security.

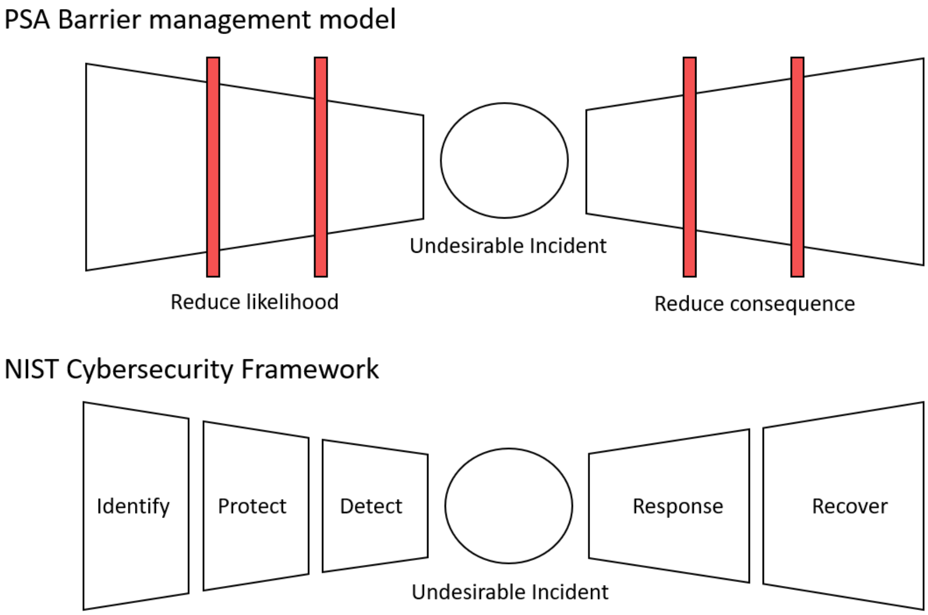


Figure 5.1: Similarity between PSA barrier management model and NIST CSF. Adopted from [NOG16, p. 12]

The vast majority of the requirements in the CAPS are requirements based on NOG 104. However, the CAPS is not based on the current edition of NOG 104, and this is the first finding of this thesis. The CAPS covers 16 different Information Security Baseline Requirements (ISBRs), while the current version of NOG 104 has 19 different ISBRs. NOG 104 was updated in December 2016, after the creation of the CAPS, but before the latest revision of the CAPS.

The three missing baseline requirements are *Hardware and software inventory* (ISBR 17), *Remote access* (ISBR 18), and *Access management* (ISBR 19). Additionally, several of the existing ISBRs underwent minor changes.

The newest version of NOG 104 provides a link between each Information Security Baseline Requirement (ISBR) in NOG 104 and categories in NIST CSF deemed relevant [NOG16]. A table is included in Appendix A that shows the mapping between all the NIST CSF categories and the ISBRs in NOG 104 according to NOG 104 (table A.1). Of the 23 NIST CSF categories, the ISBRs maps to 17 of the NIST CSF categories. Supply Chain Risk Management (ID.SC), Detection Processes (DE.DP), Communications (RS.CO), Analysis (RS.AN), Mitigation (RS.MI), and Improvements (RS.IM) are the six missing categories. Of the five functions in NIST CSF, Respond is the least covered by the ISBRs with four out of five categories not covered. This existing mapping was used as a starting point, but **not** as a solution for the mapping.

5.2 NIST Cybersecurity Framework Gap Analysis

The mapping examined all the requirements of the CAPS in the context of the NIST CSF subcategories. In total, there are 108 subcategories in 23 different categories and five different functions in NIST CSF. These subcategories were mapped against the 125 requirements in the CAPS. The CAPS covers 53 of 108 subcategories in NIST CSF. This leaves 55 subcategories as not covered by any requirement in the CAPS. Note that the NIST CSF does not cover all requirements in the CAPS. The gap analysis show that 39 requirements in the CAPS are not covered by subcategories in NIST CSF. Figure 5.2 presents the three outcomes of the mapping in an orderly manner.

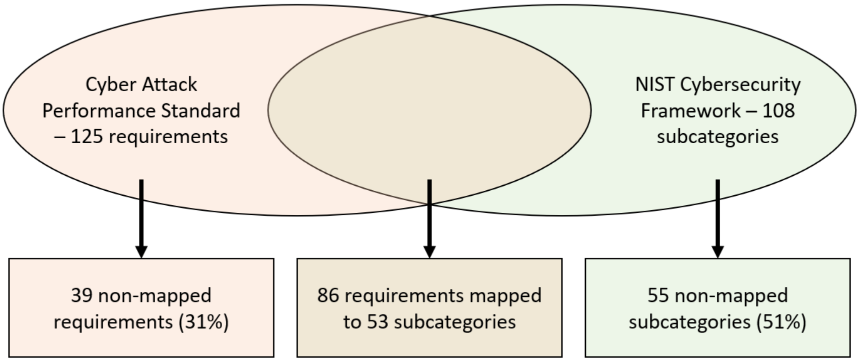

Cyber Attack Performance Standard – 125 requirements
NIST Cybersecurity Framework – 108 subcategories
39 non-mapped requirements (31%)
86 requirements mapped to 53 subcategories
55 non-mapped subcategories (51%)

Figure 5.2: The three outcomes of the gap analysis between the NIST CSF subcategories and the requirements in the CAPS.

In the following sections the result of the gap analysis of NIST CSF is examined in detail. Table 5.1 present the result of the mapping as the coverage of the five NIST CSF functions. The next paragraphs will present similar tables for each NIST CSF function and present the findings in each category.

Function	Covered / All subcategories	Percentage covered
Identify	17/29	59%
Protect	24/39	62%
Detect	9/18	50%
Respond	2/16	13%
Recover	1/6	17%
Total	53/108	49%

Table 5.1: Total coverage of the NIST CSF functions by the CAPS.

5.2.1 Identify

The first of the five functions in the NIST CSF is Identify. The five functions together *provide a high-level, strategic view of the lifecycle of an organization's management of cyber security risk* [NIS18]. The goal of Identify is to *Develop an organizational understanding to manage cyber security risk to systems, people, assets, data, and capabilities* [NIS18].

The CAPS covers 59% of the subcategories in Identify, 17 out of 29 subcategories. Identify is the function where the CAPS is the most compliant; all other functions have a lower percentage of mapped subcategories. From table 5.2 it is apparent that Supply Chain Risk Management (ID.SC) is the least covered subcategory. This could be contributed by the fact that ID.SC was added in the 1.1 revision of the NIST CSF published in 2018, i.e. three years later than the CAPS was created. However, requirements in the CAPS could still have covered the subcategories in ID.SC.

The CAPS lack requirements for addressing risk management in the supply chain explicitly (ID.SC-1), conducting risk assessment of the cyber supply chain (ID.SC-2), assessing suppliers through audits (ID.SC-4), and including suppliers in response and recovery planning (ID.SC-5). It should be noted that Alpha has marked several of the requirements in the CAPS as included in the service contract with the ICS equipment vendor, which means subcategory ID.SC-3 is covered.

Alpha has requirements for risk management in the production environment. However, these do not mention any use of cyber threat intelligence (ID.RA-2) nor if the role of the installation in critical infrastructure or a sector-specific risk analysis impact Alpha's risk tolerance (ID.RM-3). There is no mention of Alpha's role in the supply chain (ID.BE-1) being identified or Alpha's place in critical infrastructure being identified and communicated (ID.BE-2).

The subcategories in Identify are mapped to the barrier elements access control, system hardening, and a part of software updates and patches. The barrier elements above are all part of reducing the probability of a successful cyber attack. The first group of requirements is related to information security policy, and the second group is related to information security risk management. Both these groups are part of the barrier element access control, but the requirements in these two groups have a broader impact than the barrier function, preventing unauthorised indirect network access. The third group of requirements are mapped to the barrier element system hardening, but the third group is related to system and information owner.

A general note on the requirements in Identify, the CAPS is not the only governing document in the organisation. There could be other documents covering some of the non-mapped subcategories in Identify. This fact could apply to the other NIST CSF functions as well. However, the subcategories in Identify are focused on governance, risk assessment, risk management, and the business environment, areas that are not unique to managing cyber security in an organisation.

	Category in Identify	Covered / All subcategories	Percentage covered
ID.AM	Asset Management	5/6	83%
ID.BE	Business Environment	2/5	40%
ID.GV	Governance	2/4	50%
ID.RA	Risk Assessment	6/6	100%
ID.RM	Risk Management Strategy	2/3	67%
ID.SC	Supply Chain Risk Management	1/5	20%
	Total	17/29	59%

Table 5.2: Total coverage of the NIST CSF subcategories in the Identify function by the CAPS.

5.2.2 Protect

The goal of Protect is to *Develop and implement appropriate safeguards to ensure delivery of critical services* [NIS18]. The requirements in the CAPS covers 59,0% of the 39 subcategories in Protect. Protect is the function greatest in size if measured in the number of different subcategories, and the CAPS coverage of the different categories is presented in table 5.3.

Data Security (PR.DS) is the least compliant category of the six categories with 25,0% coverage. The CAPS lack requirements for protecting data at rest (PR.DS-1), and the only protection of data in transit (PR.DS-2) is through the design of the network topology, i.e. the network is segmented, and all traffic between different zones go through controlled gateways. There is no mention of cryptography nor integrity checking to protect data in transit in the ICS. Further, devices could be vulnerable to denial of service attacks as there are no requirements for availability (PR.DS-4), and the integrity of software and firmware (PD.DS-6) on devices nor the integrity of the hardware (PD.DS-8) is checked.

Awareness and training (PR.AT) have a 60,0% coverage, but this is due to NIST CSF having divided understanding roles and responsibilities into unique subcategories for privileged users, third-party stakeholders, senior executives, and cyber security personnel. The CAPS do not have the same distinction, which impacts the coverage. However, the subject is addressed in another Performance Standard (PS), which means the CAPS does not provide the full picture as relevant details to awareness and training could exist in this other PS.

Alpha lacks requirements on issuing unique credentials to each verified user, device, and process interacting with the ICS (PR.AC-6), and protecting transactions in the ICS based on a risk assessment and implementing the authentication mechanisms required (PR.AC-7). Further, Alpha is missing requirements on improving its protection processes (PR.IP-7), and there is no mention of implementing resilience mechanisms to achieve resilience requirements in both normal and adverse situations (PR.PT-5).

The subcategories in Protect are mapped to 10 out of the 15 groups of requirements Alpha have in the CAPS. This means that subcategories in Protect map to requirements in the majority of the barrier elements in place. This is not surprising as Protect has the highest number of subcategories, and three-fourths of the requirements in the CAPS is related to reducing the probability of cyber attack. A general finding in Protect is that the requirements in the CAPS are more high-level than the subcategories in NIST CSF. NIST CSF goes into more depth and is more explicit in the measures required to protect ICS.

	Category in Protect	Covered / All subcategories	Percentage covered
PR.AC	Identity Management and Access Control	5/7	71%
PR.AT	Awareness and Training	3/5	60%
PR.DS	Data Security	2/8	25%
PR.IP	Information Protection Processes and Procedures	8/12	67%
PR.MA	Maintenance	2/2	100%
PR.PT	Protective Technology	4/5	80%
	Total	24/39	62%

Table 5.3: Total coverage of the NIST CSF subcategories in the Protect function by the CAPS.

5.2.3 Detect

The goal of Detect is to *Develop and implement appropriate activities to identify the occurrence of a cyber security event* [NIS18]. The requirements in the CAPS cover 44,4% of the requirements to Detect, which corresponds to 8 out of 18 subcategories. All three subcategories have coverages between 40 and 50 per cent. The lack of compliance is due to NIST CSF being significantly more detailed and exhaustive in the activities described concerning Detect.

Logging is implicitly required through requirement 6-1 and 13-2. 6-1 states that the *Acceptable use of each of the critical PCSS/ICT system shall be documented.* Logging is required in the *Design-column*, how Alpha answers the requirement, which is: *All network-attached use of critical PCSS/ICT systems is logged.* Requirement 13-2 states that *The PCSS ICT network shall be monitored on its various levels to detect potential cyber security events*, where monitoring can be regarded as implying the collection of logs. However, the following subcategory in Security Continuous Monitoring, *The network is monitored to detect potential cyber security events* (DE.CM-1), is not mapped as a gap. While specific requirements for logging are lacking, logging is required in the CAPS. However, there are other identified gaps in relation to logging. There is no mention of requirements on monitoring the physical environment (DE.CM-2) or monitoring all personnel activity (DE.CM-3).

There is a requirement to collect, report, preserve and correlate alarms and events from the ICS through a Security Information and Event Management System (SIEM). However, there is no requirements for the testing of detection (DE.DP-3), nor determining the impact of events (DE.AE-4), nor creating a baseline of network operations and expected data flows for users and systems (DE.AE-1).

Requirement 13-2 states that *The PCSS ICT network shall be monitored on its various levels to detect potential cyber security events.* This and five other requirements are included in the service contract with the ICS equipment vendor. This shows that some of the requirements in the CAPS are covered by the service providers. From the six requirements it can be established that the service provider has responsibility for several cyber security activities in the ICS.

The subcategories in the three Detect-categories are mapped to three groups of requirements belonging to six different barrier elements. Anomalies and Events (DE.AE) is mapped to the barrier elements blocking access and security incident response plan, which both are part of mitigating the consequence of a successful cyber attack. Security Continuous Monitoring (DE.CM) is mapped to the barrier elements segregated networks, system hardening, anti-virus software, configuration management, and security incident response plan. These barrier elements are all related to reducing the probability of a successful cyber attack, except for the security incident response plan. Detection Processes (DE.DP) is mapped to the barriers anti-virus software and security incident response plan.

	Category in Detect	Covered / All subcategories	Percentage covered
DE.AE	Anomalies and Events	3/5	60%
DE.CM	Security Continuous Monitoring	4/8	50%
DE.DP	Detection Processes	2/5	40%
	Total	9/18	50%

Table 5.4: Total coverage of the NIST CSF subcategories in the Detect function by the CAPS.

5.2.4 Respond

The goal of Respond is to *Develop and implement appropriate activities to take action regarding a detected cyber security incident* [NIS18]. Respond is the NIST CSF function with the least coverage by the CAPS with only two out of 16 requirements covered, 12,5%. The initial requirement in the CAPS concerning Response is *There shall be requirements for handling a cyber-security incident, including a response plan.* However, this requirement corresponds to Protect, *Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery* *and Disaster Recovery) are in place and managed* (PR.IP-9), in other words having a response plan is part of protection. The NIST CSF function Respond is concerned with the contents of the response plan and all the related activities. It should be noted that Alpha has both a business continuity plan and an IT disaster recovery plan. However, these documents are more aligned to the NIST CSF function Recover, which is discussed in coming paragraphs.

By examining the requirements concerning Response in the CAPS, it is clear that Alpha bases its incident response on manual reporting of incidents. Requirement 16-5, *Alpha shall have developed templates, have intranet pages, or specific applications for the users to report information security incidents.* Moreover, requirement 16-7, *Alpha shall have documented requirements for the users to report information security incidents.* RS.CO-2 maps to these two requirements, *Incidents are reported consistent with established criteria.* There are no requirements for sharing information (RS.CO-3), nor coordinating with stakeholders (RS.CO-4).

The final requirement is 16-9, *Reported information security incidents shall be registered and followed up.* This corresponds to RS.AN-1, *Notifications from detection systems are investigated.* However, there are no requirements to understand the impact of the incident (RS.AN-2), performing forensics (RS.AN-3), containing the incident (RS.MI-1), nor mitigating the incident (RS.MI-2). There is no mention of how a response plan incorporates lessons learned (RS.IM-1), nor updating the response strategy (RS.IM-2).

	Category in Respond	Covered / All subcategories	Percentage covered
RS.RP	Response Planning	0/1	0%
RS.CO	Communications	1/5	20%
RS.AN	Analysis	1/5	20%
RS.MI	Mitigation	0/3	0%
RS.IM	Improvements	0/2	0%
	Total	2/16	13%

Table 5.5: Total coverage of the NIST CSF subcategories in the Respond function by the CAPS.

5.2.5 Recover

The goal of Recover is to *Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident* [NIS18]. Recover consists of just six subcategories, but the CAPS covers only one subcategory. A disaster recovery process is one of the barrier elements in mitigating the consequence of a cyber attack, and have four corresponding requirements. Due to the design of the NIST CSF, three out of these four requirements are mapped to subcategories in Protect. A disaster recovery plan is managed and documented (PR.IP-9), and the plan is required to be tested (PR.IP-10). The plan shall be maintained and updated (RS.IM-2), but the rest of the subcategories in Recover are not covered. Incorporating lessons learned (RC.IM-1) and executing the recovery plan during or after an incident (RC.RP-1) are missing. The lack of coverage in Recover is largely due to that none of the three subcategories concerning communication (RC.CO) are covered. There is no mention of managing public relations (RC.CO-1) nor repairing reputation (RC.CO-2) after an incident.

	Category in Recover	Covered / All subcategories	Percentage covered
RC.RP	Recovery Planning	0/1	0%
RC.IM	Improvements	1/2	50%
RC.CO	Communications	0/3	0%
	Total	1/6	17%

Table 5.6: Total coverage of the NIST CSF subcategories in the Recover function by the CAPS.

5.3 CIS Controls Gap Analysis

The CIS Controls are a prioritised set of actions defenders should implement to protect systems and networks against common attacks. The CIS Controls are all action-based; there are no controls requiring risk management nor risk assessment of industrial cyber security. The controls were initially made for Enterprise IT environments, but there is a guideline for applying the controls in ICS environments [CIS18].

The mapping compared all the 190 sub-controls belonging to the 20 different CIS Controls to the 125 requirements in the CAPS. Figure 5.3 presents the three outcomes of the mapping in an orderly manner. The mapping shows that there is a significant gap in the CAPS coverage of the CIS Controls in all the three implementation groups (IG) of the CIS Controls. The mapping also shows that coverage of IG1 is significantly higher than both IG2 and IG3. Table 5.7 presents the coverage of the sub-controls in IG1 while table 5.8 presents the coverage of all CIS sub-controls. Note that the CIS Controls are long way from covering all requirements in the CAPS.

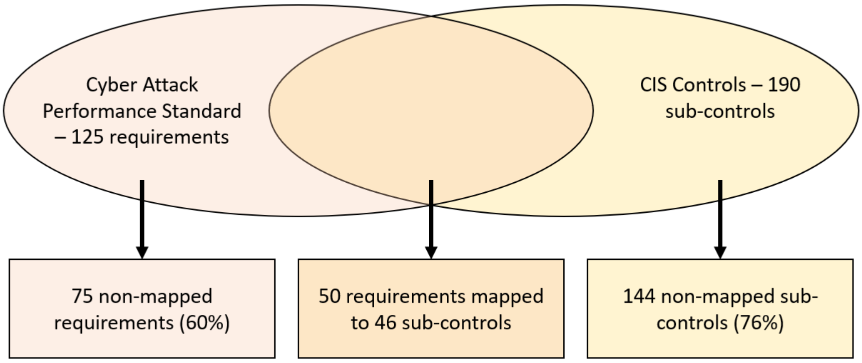

Cyber Attack Performance Standard – 125 requirements
CIS Controls – 190 sub-controls
75 non-mapped requirements (60%)
50 requirements mapped to 46 sub-controls
144 non-mapped sub-controls (76%)

Figure 5.3: The three outcomes of the gap analysis between the CIS Controls sub-controls and the requirements in the CAPS.

The CIS Controls *Implementation Guide for Industrial Control Systems* presents sub-controls that may not be applicable in ICS. The percentage of coverage would be higher if these sub-controls were removed from the mapping. However, it was decided to not remove any controls as there are considerations to be made before any of these sub-controls are deemed irrelevant. These considerations could be done by personnel in Alpha with first-hand knowledge of both the CAPS and the ICS on Bravo. It should be noted that the goal of the mapping is not to show Alpha's compliance of the CIS Controls, but rather identifying areas where Alpha's barriers are inadequate. When presenting sub-controls of interest from the CIS Controls, sub-controls belonging to IG1 have been prioritised.

	CIS Control	Covered IG1 / Number of IG1	%
1	Inventory and Control of Hardware Assets	1/2	50%
2	Inventory and Control of Software Assets	2/3	67%
3	Continuous Vulnerability Management	0/2	0%
4	Controlled Use of Administrative Privileges	0/2	0%
5	Secure Configurations for Hardware and Software on Devices, Laptops, Workstations, and Servers	1/1	100%
6	Maintenance, Monitoring, and Analysis of Audit Logs	1/1	100%
7	Email and Web Browser Protections	0/2	0%
8	Malware Defenses	2/3	67%
9	Limitations and Control of Network Ports, Protocols, and Services	1/1	100%
10	Data Recovery Capabilities	2/4	50%
11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	1/1	100%
12	Boundary Defense	2/2	100%
13	Data Protection	1/3	33%
14	Controlled Access Based on the Need to Know	1/1	100%
15	Wireless Access Control	0/2	0%
16	Account Monitoring and Control	2/3	67%
17	Implement a Security Awareness and Training Program	1/6	17%
18	Application Software Security	0	
19	Incident Response and Management	1/4	25%
20	Penetration Tests and Red Team Exercises	0	
	Total	19/43	44%

Table 5.7: Total coverage of the sub-controls in CIS Controls belonging to IG1 by the CAPS.

	CIS Control	Covered sub-controls / Number of sub-controls	%
1	Inventory and Control of Hardware Assets	2/8	25%
2	Inventory and Control of Software Assets	3/11	27%
3	Continuous Vulnerability Management	3/8	38%
4	Controlled Use of Administrative Privileges	1/10	10%
5	Secure Configurations for Hardware and Software on Devices, Laptops, Workstations, and Servers	1/6	17%
6	Maintenance, Monitoring, and Analysis of Audit Logs	4/9	44%
7	Email and Web Browser Protections	0/11	0%
8	Malware Defenses	3/9	33%
9	Limitations and Control of Network Ports, Protocols, and Services	1/6	17%
10	Data Recovery Capabilities	3/6	50%
11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	1/8	13%
12	Boundary Defense	8/13	62%
13	Data Protection	3/10	30%
14	Controlled Access Based on the Need to Know	3/10	30%
15	Wireless Access Control	0/11	0%
16	Account Monitoring and Control	6/14	43%
17	Implement a Security Awareness and Training Program	1/10	10%
18	Application Software Security	0/12	0%
19	Incident Response and Management	3/9	33%
20	Penetration Tests and Red Team Exercises	0/9	0%
	Total	46/190	24%

Table 5.8: Total coverage of the sub-controls in CIS Controls by the CAPS.

Four of the CIS controls have a zero per cent coverage by the CAPS when considering all sub-controls, but these are also controls which are less relevant to ICS and consist mostly of sub-controls belonging to IG2 and IG3. Email and Web Browser Protections (Control 7) are less relevant in ICS as this functionality is less common in ICS as access between the ICS and internet is often limited. Wireless

Access Control (Control 15) would be relevant if there were wireless devices in the ICS, but this is not mentioned in the CAPS, and consequently no sub-controls map. Application Software Security (Control 18) would be relevant if Alpha had in-house software or applications used in the ICS on Bravo, but this is not the case as Alpha relies on third-party vendors and suppliers. Penetration Tests and Red Team Exercises (Control 20) is only relevant for operators with a highly mature cyber security program as there are strict requirements for doing penetration tests in ICS. Additionally, none of the sub-controls belongs to IG1.

The highest coverage is found in the CIS Controls 6, 10, 12, and 16. Still, the controls are far from fully covered, and there are several sub-controls missing in Alpha's requirements. Maintenance, Monitoring and Analysis of Audit Logs (Control 6) still lack coverage of sub-controls related to timestamps (6.1), detailed logging (6.3) and adequate storage for logs (6.4). Data Recovery Capabilities (Control 10) lacks coverage on sub-controls to ensure the protection of backups (10.4), and there is no requirement mentioning offline storage of at least one backup (10.5). The non-mapped sub-controls in Boundary Defense (Control 12) are less applicable in ICS, but Alpha does not mention scanning for unauthorised connections (12.1) nor denying communication with known malicious IP addresses (12.2). In Account Monitoring and Control (Control 16), there is no indication of requirements to protect the transmission of usernames and authentication credentials (16.5), nor storing all authentication credentials either encrypted or hashed with salt (16.4).

Inventory and Control of Hardware and Software Assets are CIS Control 1 and 2. Alpha does not require the integration of its software and hardware inventories (2.5), nor are there any explicit requirements for addressing unauthorised assets (1.6) nor unauthorised software (2.6). There is no requirement on using tools for asset discovery, either active or passive (1.1, 1.2). However, this could impact the function of the ICS and consequently, discovery tools should only be used with the correct precautions in place. Alpha has a single requirement in the CAPS on vulnerability management,

Controlled Use of Administrative Privileges (Control 4) is related to account management, and Alpha does not have any requirements in place regarding the prohibiting of default passwords (4.2), requiring unique passwords (4.4), maintaining an inventory of administrative accounts (4.1), nor having dedicated administrative accounts (4.3).

5.4 IEC 62443 3-3 Gap Analysis

The IEC 62443 series consist of several standards, and of them, the IEC 62443 3-3 sets system security requirements and security levels to the ICS environment. Although the requirements are technical and similar to the CIS Controls, IEC 62443 3-3 does not cover risk assessment nor risk management. However, these areas are covered by other standards in the IEC 62443 series, such as IEC 62443 2-1 which covers risk management, and IEC 62443 2-3 which covers patch management. This means the controls in NOG 104 not covered by IEC 62443 3-3 could be covered by other standards in the IEC 62443 family.

The mapping of IEC 62443 3-3 to the requirements in the CAPS show that there is a significant gap in the coverage of the standard. Figure 5.4 presents the three outcomes of the gap analysis in an orderly manner. The coverage of IEC 62443 3-3 is presented in detail in table 5.9. It should be noted that the system requirements in the IEC 62443 3-3 is more detailed and have a smaller scope compared to NIST CSF. Using the existing mapping between NIST CSF and IEC 62443 3-3 in NIST CSF [NIS18], an examination shows that 80,4% of the 51 system requirements map to at least one subcategory belonging to the NIST CSF function Protect. This means the IEC 62443 3-3 is predominantly used for system protection and reducing the likelihood of a successful cyber attack. Except for the functional requirement of timely response to events (TRE), all the functional requirements are mapped to Protect. TRE is mapped to Detect and has full coverage by the CAPS, which means that Alpha has the technical requirements for responding to incidents in place according to IEC 62443 3-3.

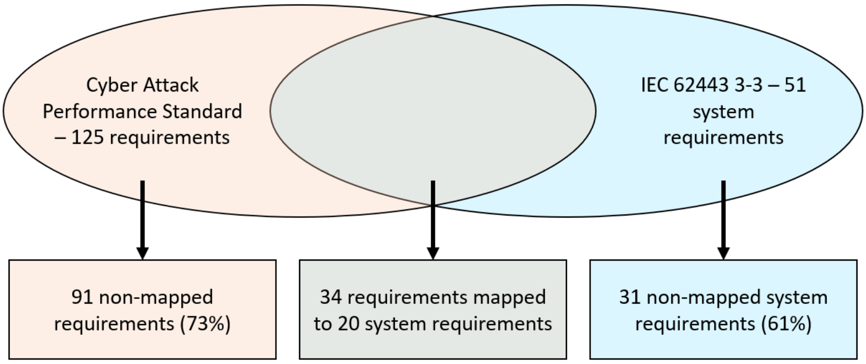


Figure 5.4: The three outcomes of the gap analysis between the IEC 62443 3-3 system requirements and the requirements in the CAPS.

Functional requirement	Covered SRs / Number of SRs	Percentage covered
FR 1 - Identification and authentication control (IAC)	5/13	38%
FR 2 - Use control (UC)	4/12	33%
FR 3 - System integrity (SI)	2/9	22%
FR 4 - Data confidentiality (DC)	0/3	0%
FR 5 - Restricted data flow (RDF)	2/4	50%
FR 6 - Timely response to events (TRE)	2/2	100%
FR 7 - Resource availability (RA)	5/8	63%
Total	20/51	39%

Table 5.9: Total coverage of the IEC 62443-3-3 functional requirements in number of system requirements (SRs) by the CAPS .

The CAPS only covering 39,2% of the IEC 62443 3-3 SRs can be attributed to the highly detailed system requirements. In the functional requirement of identification and authentication control (IAC), eight of the system requirements (SRs 1.1-1.5 & 1.7-1.9) are related to access control. Because of the level of detail in IEC 62443 3-3, the CAPS do not cover each of the SRs even if the CAPS have several requirements related to access control. Alpha is missing requirements for providing identifying and authenticating software processes and devices (SR 1.2), authentication of users to prove identity (SR 1.5), wireless access management (SR 1.6), and rules for password-based authentication (SR 1.7).

The same pattern of highly detailed requirements is seen in the functional requirements Use Control (UC), System Integrity (SI), Restricted Data low (RDF), and resource availability (RA) where there are a significant number of non-mapped requirements. While the requirements in TRE are covered, some related requirements in other FRs are not. Alpha lacks requirements on the contents of the logs to be able to monitor the ICS environment successfully. The CAPS lack requirements to the type of events logged (SR 2.8), information included in each event logged (SR 2.8), the log storage capacity (SR 2.9), response to audit processing failures (SR 2.10), and having timestamps in the logs (SR 2.11).

Concerning the functional requirement SI, Alpha lacks requirements to the integrity of transmitted communication in the ICS (SR 3.1), validating the input used in process control (SR 3.5), and protecting the integrity of sessions (SR 3.8). There is no mention of the control system having the capability to operate in a degraded mode during denial of service (DoS) attacks (SR 7.1), and limiting the use of resources by the control system security functions to prevent resource exhaustion (SR 7.2).

Not a single requirement of data confidentiality (DC) is covered. Confidentiality is the ICS security objective with least precedence, but this is not equivalent to neglecting confidentiality completely. The CAPS have requirements for appointing owners of critical data. However, no requirement is found in the CAPS to protect this data at rest or in transit (SR 4.1), removing critical data from decommissioned devices (SR 4.2), or any requirements on the use of cryptography (SR 4.3).

Finally, two requirements from the functional requirement of restricted data flow (RDF) lack coverage. Alpha lacks requirements to restrict or prohibit general person-to-person communication (SR 5.3) in the ICS, and there is no mention of supporting the partitioning of data, applications and services based on criticality (SR 5.4). General person-to-person communication includes but is not limited to email systems, social media or any messaging system that permit the transmission of any executable file.

5.5 Result and Inadequately Addressed Cyber Security Activities

The mapping shows that there are significant gaps in the CAPS' coverage of all three guidelines. Table 5.10 present the CAPS coverage of the three guidelines. The most significant gap is found in the CIS controls, with only 24% of the sub-controls mapped as covered. This result is discussed in section 6.1 in the discussion, together with the coverage of NIST CSF and IEC 62443 3-3.

Guideline	CAPS Coverage	Percentage covered
NIST CSF	53/108	49%
CIS Controls	46/190	24%
IEC 62443 3-3	20/51	39%

Table 5.10: The CAPS total coverage of the three mapped guidelines.

The gap analyses found numerous controls in the three guidelines not covered by the requirements in the CAPS. As mentioned in 3.3.4 the methodology, inadequately addressed cyber security activities can be identified by comparing the non-mapped controls in these three guidelines. As the coverages were between 24% and 49%, there are numerous non-mapped controls to address. The research question of this thesis was not to identify all inadequate barrier elements but to examine the alignment of implemented barriers with selected best practices. Still, to provide some context to the research goal of the thesis, the following paragraphs present five cyber security activities identified as not explicitly addressed in the three gap analyses. Note that these five activities relate to a subset of the total number of non-mapped controls. There are other activities with non-mapped controls.

A cyber security activity can be viewed as similar in concept to the barrier functions and barrier elements in the CABS. However, the terms barrier functions and barrier elements are not used as these refer to the implemented barriers in the CABS. The importance of these five identified cyber security activities is discussed in section 6.2.

Asset Identification

Identifying and keeping records on all devices and processes is a countermeasure in all three guidelines. Alpha should evaluate the importance of guideline controls not covered in the CAPS. While Alpha requires assets deemed critical to be documented, there is evidence this is not sufficient. If Alpha has complete control on all devices in the ICS, then any unauthorised device or process in the ICS should be easier to detect. Asset identification is part of the system hardening barrier element in the CAPS, but the requirements in the CAPS are mostly focused on declaring owners of critical systems and information.

Identity and Access Management

As presented in section 4.1, Alpha has a work order based access control system in the ICS. This system provides a protective boundary with time-limited role-based access. Still, Alpha lacks several requirements related to IAM. As presented in 2.1.1, cyber security countermeasures should under no circumstances be able to degrade safety. Subsequently, requirements to access control need to be tailored to the system or device in question. Identity and access management is part of the access control barrier element, the barrier element with the highest number of requirements in the CAPS. Still, there were several identified areas of potential improvement in the sections above.

Data Protection

After the mapping, it is apparent that Alpha has a gap in its requirements for data protection and data integrity. In section 2.1.1, it is presented how confidentiality is the least prioritised cyber security attribute in ICS, but this is not a reason to completely dismiss it. Both the NIST CSF category Data Security (PR.DS), the CIS Control Data Protection (13), and the functional requirements SI and DC in IEC 62443 3-3 discusses the importance of protecting information. However, Alpha has few safeguards in this area. There are no requirements to protect the confidentiality or integrity of data in transit or at rest. This area does not have a corresponding barrier element nor a barrier function.

Logging and Detection

While there are requirements for logging and monitoring in Alpha's CAPS, these requirements have a different level of detail than comparable controls in the three guidelines. The detection of attacks will be challenging if the information provided from logging is insufficient. All three guidelines specify the need for requirements on what type of information should be logged. The requirements in place concerning logging are part of the barrier function, mitigating consequences of unauthorised network access, which is part of the reactive barrier on the right side of the bowtie, mitigating consequences of a successful cyber attack. The barrier element of network monitoring/access logs is in place, but there is a significant gap between the CAPS and the ICS cyber security guidelines.

Alpha has one requirement on monitoring the network in the ICS, and another requirement on detection of cyber security events. However, both NIST CSF and CIS Controls specify additional controls. Alpha is missing requirements on identifying an incident, and estimating the potential impact of the incident. A baseline of normal network operations and expected data flows will provide Alpha with the capability to identify attackers based on the attacker using techniques outside of the recorded baseline. The relevant barrier element is network monitoring/access logs, but as with logging, there is a significant gap identified.

Incident Handling

Overall, the response plan of Alpha in the ICS environment misses several controls in both NIST CSF and CIS Controls. Incident handling is not a control in IEC 62443 3-3, as the standard only has technical requirements. The most substantial gap in the mapping of the NIST CSF functions is found in Response, as Alpha lacks 14 out of 16 controls in the function.

The incident handling of Alpha is primarily focused on disaster recovery, not responding to the active incident. While an incident handling plan is required, the corresponding operational assurance is a business continuity plan and an IT disaster recovery plan. Blocking access is the corresponding barrier element, but this barrier has only a single requirement.

5.6 The Guidelines' Coverage of the CAPS

The mapping of the three guidelines to the CAPS gave nine findings as each mapping give three findings, illustrated in section 3.3.4 by figure 3.3. There are the CAPS coverage of each ICS cyber security guideline, the mapping between controls and requirements, and the coverage of the requirements in the CAPS by the guidelines. The mapping of NIST CSF to the CAPS showed that there was a significant number of requirements not covered by the framework. This finding was reinforced when mapping the CIS Controls and the IEC 62443 3-3, which both cover even fewer requirements in the CAPS. Table 5.11 presents the coverage of the CAPS by each of the three guidelines.

Guideline	Covered / Total requirements	Percentage of CAPS covered
NIST CSF	86/125	69%
CIS Controls	50/125	40%
IEC 62443 3-3	34/125	27%

Table 5.11: Coverage of the requirements in the CAPS by the three guidelines.

An examination of the 39 requirements not covered by NIST CSF was subsequently done to identify any potential pattern in the non-mapped requirements. This examination is presented in the following paragraphs. NIST CSF is used as it was the guideline with the highest coverage.

The requirements not covered by NIST CSF falls in one of two groups. Group one are the requirements which are specific and highly detailed to certain aspects of the installation, Bravo. As an example, three requirements state three different ways the employees in the production environment are to be informed about information security, intranet, e-mail, and general meetings. No subcategory in NIST has this kind of detail, and consequently, the three requirements are mapped as not covered by NIST.

Further, six of these requirements are related to documentation of various production procedures, configuration, and contracts. Five of the remaining requirements are related to time, i.e. they state how frequent activities need to be conducted. Three of the remaining non-mapped requirements relate to which systems or scope are applicable for the requirement. Finally, there are five remaining requirements which are specific requirements to the ICS. Of these five, four are derived from DNVGL-RP-G108, which shows the relevance of this document to specific use cases in ICS. The requirements are related to patch management in ICS and account management in ICS.

Group two are the requirements the three guidelines have difficulties in covering because of how they are fashioned. These requirements are requirements referring to the previous requirement and then stating some additional conditions to be fulfilled. One example is requirement 16-7 in the CAPS, *Alpha shall have documented requirements for the users to report information security incidents.* The following requirement is 16-8, *This requirement shall be fulfilled.* This requirement is not covered by any subcategory in NIST CSF, sub-control in CIS Controls, nor system requirement in IEC 62443 3-3. The controls in NIST CSF, CIS Controls and IEC 62443 3-3 do not have any controls mappable to this type of requirement. Other specific requirements belonging to group one are listed below:

1. "This requirement shall be fulfilled."
2. "These procedures shall be adhered to."
3. "This overview shall be complete and updated."
4. "This document shall be maintained and kept updated."
5. "Every PCSS/ICT system shall be configured to comply with this requirement."

Removing requirements on these five forms previously mentioned reduces the total number of requirements from 125 to 109. Consequently, it increases the coverage of all the three guidelines as none of them mapped to any of the requirements listed above. This increase in coverage is presented in table 5.12.

Guideline	Covered / Total requirements	Percentage of CAPS covered
NIST CSF	86/109	79%
CIS Controls	50/109	46%
IEC 62443 3-3	34/109	31%

Table 5.12: Coverage of the requirements in the CAPS by the three guidelines after non-mappable requirements are removed.

Chapter 6
Discussion

In chapter 5, there was identified a gap between the requirements in Alpha's CAPS and the different controls mentioned in the three guidelines mapped in the gap analysis. This chapter discusses the results of the gap analysis in section 6.1, and the inadequately addressed cyber security activities are discussed in section 6.2. Next, cyber security barrier management is discussed in section 6.3. Reflections on the requirements in Alpha's CAPS which did not map to any of the guidelines is discussed in section 6.4. Finally, the validity of the results and other limitations are discussed in section 6.5.

6.1 Results of Gap Analysis

This section discusses the answer to the research question and discusses the findings from the gap analysis, as presented in section 5.5. To reemphasise, the research question of the thesis is *"How are implemented cyber security barriers on the NCS aligned with ICS cyber security standards and best practices?"* The specific case examined in this thesis shows that the cyber security barriers in place on a distinct installation on the NCS covers between 24 and 49 per cent of the controls in the three mapped guidelines. NIST CSF had 53 out of 108 subcategories covered (49%), the CIS Controls had 46 out of 190 sub-controls covered (24%), and IEC 62443 3-3 had 20 out of 51 system requirements covered (39%). This shows that the implemented cyber security barriers of Alpha should be improved before it can be regarded as fully aligned with any of the three guidelines.

However, the percentages themselves should not be used to answer the research question alone. The unique features of each guideline are discussed below to give more context to interpret the result. The underlying research method for the results is qualitative, which impacts the validity of the mapping and subsequently, the results. Discussion on the difficulties of mapping correctly are found in section 3.5, and the use of percentages is found in section 6.5.

Considering the five functions of NIST CSF as a model of the lifecycle of cyber security countermeasures, there is identified significant gaps in all functions. By percentage, the most significant gaps were found in Respond and Recover. However, this does not reflect that the majority of the subcategories are found in Identify and Protect. Protect had a higher number of non-mapped controls (16) compared with Respond (14). The inadequately addressed cyber security activities are found in all NIST CSF functions except recover. Based on the results, there are improvements to be made in both preventive (likelihood-reducing) and reactive (consequence-reducing) barrier elements.

The CIS Controls have the lowest coverage of the three guidelines. The low coverage could be contributed by the CIS Controls being tailored to Enterprise IT and not ICS. While there exists a guideline on how to apply the controls in ICS (section 2.4.6), the guideline is not removing or adding sub-controls, it presents sub-controls that could be removed and could be added. As each ICS is unique, removing or adding sub-controls is left to the operator of the ICS. No controls were removed before mapping following this logic. Still, even with removed sub-controls, there would be a considerable gap. The mapping also showed that Alpha has more of the sub-controls belonging to IG1 covered, than the rest of the sub-controls. CIS recommends that organisations prioritise their implementation of the Controls by following the IGs [CIS19]. Consequently, Alpha should first consider implementing sub-controls from IG1 before the rest of the controls.

IEC 62443 3-3 have a coverage between the two other guidelines. The results in section 5.6 show that IEC 62443 3-3 covers the least amount of the requirements in the CAPS. This shows that the scope of the requirements in the CAPS is broader than the system requirements in IEC 62443 3-3. To create a CAPS based on the standards in IEC 62443, the operator must consider more standards than only 3-3. *Part 2-1: Establishing an industrial automation and control system security program* [IEC10b] could be considered relevant to cyber security barriers as subcategories in NIST CSF it is mapped against IEC 62443 2-1 in the documentation of NIST CSF. Still, more parts of IEC 62443 could be relevant to create a complete CAPS. A note on IEC 62443 3-3 compared to the two other guidelines, is how it addresses how system requirements should not conflict with unique requirements to the ICS in the description of the controls.

The gap analysis did not use the Requirement Enhancements (REs) part of IEC 62443 3-3 in the gap analysis. Using the REs would have increased the number of total requirements in IEC 62443 3-3 from 51 to 100. As the CAPS' coverage of the IEC 63443 3-3 was 39% with the original 51 system requirements, there is no indication that adding the REs would increase the CAPS' coverage of the IEC 63443 3-3. Adding 49 REs would add 41 system requirements belonging to SL-3 and SL-4, which would likely further decrease the level of alignment.

6.2 Inadequately Addressed Cyber Security Activities

The following list presents the areas identified as inadequately addressed in section 5.5. The five elements will be discussed together with the relevant research from the field of cyber security on the NCS previously presented in this thesis, and selected techniques from MITRE ATT&CK for ICS [MIT20]. MITRE ATT&CK for ICS is included to show how the findings relate to known techniques used to exploit vulnerabilities in ICS by threat actors.

- Asset Identification
- Identity and Access Management
- Data Protection
- Logging and Detection
- Incident Handling

Asset Identification

Asset identification is an important area as it acts as a prerequisite step to prevention, detection, and response. There is no way to protect assets which are not known. The gap analysis in chapter 5 shows that there are controls Alpha lack in this area from all three guidelines. The requirements in the CAPS are focused on identifying critical assets and establishing asset owners. While critical assets are the most important to manage, based on the gap analysis, Alpha should consider identifying all assets in the ICS. All devices and software are relevant when threat actors look to escalate privileges or move laterally in the system. Asset identification is also necessary to later manage assets in vulnerability and patch management. Currently, asset identification and asset management is part of the system hardening barrier element. Alpha should consider if asset identification and asset management should be part of any other barrier functions as it does not only relate to preventing unauthorised indirect network access, but also preventing malware and unauthorised software.

Identity and Access Management

According to the received documentation, Alpha has a state of the art access control system, which is in accordance with the controls in the three guidelines. The solution is a good practice as every access is granted from work orders, and the permission is revoked when the work is finished [DNV17]. Still, Alpha has missing controls related to access control. Even if access is work order based, a threat actor could still do considerable harm to the ICS if the threat actor gets control of an account through social engineering or other means. Alpha should have requirements to passwords, and prohibit the use of default passwords. Threat actors use these techniques to get persistent access and to move laterally in the ICS [MITb].

Additionally, passwords used in the ICS should have requirements for storage. A threat actor with limited access could escalate privileges if passwords are stored in cleartext and the threat actor can steal a valid account [MITg]. Access control belongs to the access control barrier element, but the inclusion of the access system barrier element in the CAPS may create some confusion. This barrier element has no requirements, and it is interchangeable with access control. Consequently, Alpha should consider removing it for clarity.

Alpha should also consider detaching the three first groups of requirements in the CAPS from the access control and system hardening barrier elements and create a new barrier element or a new barrier function. Asset management and risk assessment could both be new barrier elements. The first group of requirements is related to information security policy, the second group is related to information security risk management, and the third group of requirements is related to appointing system and information owners.

Data Protection

As identified in the results in chapter 5, data protection is an area where Alpha should consider new barrier elements. In the area of data protection, measures to protect the integrity and authenticity of information and data flows in the ICS are included. While availability is the primary security objective in ICS (see section 2.1.1), integrity and confidentiality should still be addressed. Protecting the integrity of the data flows in the ICS is of great importance. If no measures to protect integrity are in place, a threat actor will have many avenues of further escalation as information flows are not protected, and there is little to stop the threat actor from tampering with communication in the ICS. Without integrity and authenticity, a threat actor can send commands to a PLC as a spoofed control server or Human-Machine Interface (HMI). APTs are known to utilise integrity-based cyber attacks against ICS. This technique was used in the Industroyer malware [MITc].

Having requirements to the confidentiality of data at rest or transit would limit the available techniques a threat actor can use to exfiltrate confidential information from the ICS. Malware targeting ICS are known to gather information like AutoCAD and Visio files (files that likely contain operational information) [MITe]. This information is also valuable to threat actors as it can be used in future operations. If information at rest is encrypted, then threat actors can not exfiltrate readable data. There is no current barrier element that implements requirements to confidentiality, integrity or authenticity. Alpha should consider creating a new barrier function to prevent unauthorised change or reading of data where data protection should be a corresponding barrier element. Alpha should consider requiring all devices to be authenticated, but this could conflict with requirements to the performance of the ICS as presented in section 2.1.1.

Logging and Detection

Logging, monitoring and detection are three related areas in cyber security. To be able to detect incidents in the ICS, the network must be monitored, and to be able to monitor, logs must be collected from the devices and gateways in the ICS. The requirements in these areas in the CAPS can be described as lacking. The barrier elements exist, but the gap analysis revealed that there are only a couple of requirements related to each barrier element. To be able to detect threat actors giving legal, but potentially damaging commands to devices in the ICS, Alpha should add the controls mentioned in chapter 5 to the requirements. Then alarms can be triggered if control parameters are outside expected boundaries or other potential damaging commands. An alarm should be triggered if a PLC download new program logic [MITd] or controllers are placed into an alternate mode of operation [MITf] .

The barrier element of Network monitoring/access logs is part of the barrier function Mitigate the consequences of unauthorised network access. However, it is easy to argue that a comprehensive logging and monitoring program also reduces the likelihood of successful incidents. In NOG 104, the NIST CSF function Detect is placed on the left side of the bowtie, as in figure 5.1. While a threat actor may have gained initial access in the ICS, this does not mean the threat actor has executed a successful cyber attack as the CABS suggest. Alpha should consider removing "successful" from "successful cyber attack" in the bowtie of the CABS. The barrier functions in *Mitigate consequences of successful cyber attack* can reduce both the probability and consequence of a successful cyber attack. The success of a cyber attack is dependent on the goal of the threat actor, and consequently if the threat actor reaches the objective. The barrier functions *Detect and react to security incidents*, *Mitigate consequences of unauthorised network access*, and *Mitigate consequences of malware* can prevent a threat actor from reaching the objective.

Alpha has a significant gap in detection where the existing requirements can be characterised as lacking sufficient details. Implementing the missing controls in Detect and Maintenance, Monitoring, and Analysis of Audit Logs (CIS Control 6) would provide Alpha with a powerful barrier element in combating threat actors as its theoretical detection capability would increase.

Incident Handling

A detailed course of action on stopping an identified attack in the ICS is not found in the CAPS. One of the cyber security areas identified as vulnerable in the NOU 15: 13 was incident response [Reg15]. There is no sector-wide CERT nor Computer Security Incident Response Team (CSIRT) on the NCS, but some operators are cooperating with KraftCERT [Reg15]. Alpha has few requirements on how ongoing incidents are responded to, and there is no mention of a CERT nor a CSIRT. Consequently, incident handling was found as an inadequate barrier element in the results chapter, and the sector-wide vulnerability from NOU 2015: 13 is observed in Alpha. Alpha should consider adding the requirements presented under Respond in section 5.2.4 and relevant sub-controls from the CIS Controls in 5.3 to the barrier element *Security incident response plan*, which only have a couple of requirements.

Alpha should consider creating a more detailed response plan tailored to ICS with the missing controls in *Respond* and the CIS Control Incident Response and Management (CIS Control 19). The lack of coverage of the controls in *Respond* is not surprising as the requirements in the CAPS are based on NOG 104. In section 5.1, it was shown how NOG 104 lack coverage of 4 out of 5 categories in *Respond.*

6.3 Cyber Security Barrier Management

This section discusses the results in relation to barrier management, the threat landscape on the NCS presented in section 2.7 and how threat actors attack ICS, presented in section 2.8.

Barrier elements may either be technical, organisational or operational. In the PSA Barrier Memorandum 2017, the barrier function is divided into barrier sub-functions, which is further divided into technical, organisational or operational barrier elements. In other words, it is common to divide the barrier elements after its function. Currently, Alpha has barrier elements that have more than one function. Examining the barrier element of Access Control in the CAPS, it is apparent that it consists of requirements belonging to both technical and organisational barrier functions. To fully adopt the barrier management model for the implemented cyber security barriers on Bravo, Alpha should consider dividing the barrier elements by their barrier function. Dividing existing barrier elements would increase their number, but the functionality of the barrier should be more understandable when the underlying requirements are accommodating one single barrier function.

Evaluating cyber security barriers alone is ineffective in the context of preventing major accidents, as the goal of a cyber security barrier should not be only to prevent a cyber attack, but to be a part of the prevention of major accidents. If a threat actor with access to the ICS could manipulate control to increase temperature or pressure, the consequence could be catastrophic. When Alpha has decoupled the cyber security barrier management from safety, this relationship between cyber security and safety is challenging to grasp. However, if the goal is to prevent a cyber attack, the current approach seems both manageable and practical. It is also essential to understand how the barriers will not have an equally weighted contribution to risk reduction, which increases uncertainty in their perceived effectiveness.

In 2015, NOU 2015: 13 was published. The findings of the report are presented in section 2.7. The report presented the most common vulnerabilities at the different stages of the petroleum value chain and measures to handle the identified vulnerabilities. When it comes to barriers, the report highlight how barriers mitigating consequences of incidents is far less numerous than barriers reducing the likelihood of incidents [Reg15]. The findings in chapter 5 support this view, Alpha has far more preventive barriers than reactive barriers. However, according to the Barrier Memorandum 2017, likelihood-reducing measures should be given priority over consequence-reducing measures [Nor17]. Consequently, it can be observed that the cyber security barriers of Alpha are in line with the Barrier Memorandum.

Of the relevant areas identified in NOU 2015: 13 as vulnerable, it is difficult to assess if Alpha is vulnerable. On the areas mentioned, Alpha has many requirements in place, but the areas are still potential vulnerabilities. As an example, remote work during operations and maintenance is still an area exposed to threat actors even if Alpha has requirements in place. The areas mentioned in NOU 2015: 13 has not been sufficiently examined to draw more definite conclusions as this thesis only relies on a gap analysis of documents provided by Alpha. The actual ICS with interfaces must likely be audited to assess these vulnerabilities. Still, countermeasures to these vulnerabilities exist in the guidelines examined in this thesis.

Mapping the cyber security requirements of Alpha to the three selected guidelines provide a baseline of cyber security protection and a gap to the complete implementation of each guideline. Both CIS Controls and IEC 62443 3-3 use a form of levels of protection, implementation groups and SLs respectively. Higher SLs are related to threat actors with higher capabilities, and higher implementation groups are related to organisations with a broader risk picture. Based on the literature review presented in 2.7, there is a credible threat of APTs targeting operators on the NCS. Considering this threat landscape, Alpha should consider implementing more controls to contend with threat actors with high capabilities on the NCS.

Alpha does not mention using different SLs in the different network-segments of the ICS, or any other subsets of the ICS. As an example, DNVGL-RP-G108 recommends SL-3 to the remote access solution and SL-2 to high criticality systems such as SIS [DNV17]. However, no similar distinctions are made in the requirements in the CAPS. It is not observed that any SIS or remote access solution lack protection, but Alpha should consider using different SLs in their requirements to make sure critical assets are adequately addressed concerning their criticality.

Previously it was presented how the majority of Alpha's cyber security barrier belongs to preventive barriers, rather than reactive. In section 2.8, the ICS cyber kill chain is briefly mentioned, and it explains how APTs use multiple steps to achieve their objective when attacking. As APTs use multiple steps to attack, defence-in-depth is a common principle used in protecting ICS and IT. If Alpha added more requirements to reactive barriers, there is potential to increase the overall defence-in-depth.

6.4 Reflections on Mapping

The last finding in chapter 5 was the the three guidelines' coverage of the CAPS, as opposed to the rest of chapter 5 which discussed the CAPS' coverage of the three guidelines. Of the 125 requirements in the CAPS, NIST CSF covered 86 (69%) requirements, CIS Controls covered 50 (40%) requirements, and finally IEC 62443 3-3 covered 34 (27%) requirements. The findings are also found in table 5.11 in section 5.6.

The reason why the guidelines do not fully cover the CAPS can be attributed to two factors. Firstly, two of the guidelines have a smaller scope than the requirements in the CAPS. The overall objective of the CAPS is to describe operational assurance activities to protect against and minimise the effect of cyber attacks. The CIS Controls and IEC 62443 3-3 do not cover all these activities and subsequently cover less than half of the requirements in the CAPS.

Secondly, as discovered in section 5.6, Alpha has numerous requirements not mapped to any controls in the three guidelines. This can be attributed to some highly specific requirements, and some requirements referencing other requirements in the CAPS. However, Alpha has tailored the CAPS to its needs when managing cyber security barriers. The PSA state explicitly that barriers should be maintained, verified, and followed up on by the operator [Nor17], and consequently Alpha must tailor the CAPS to barrier management. These requirements referencing other requirements could exist to be able to verify the correct function of barrier elements, as well as following them up. As the ICS cyber security guidelines do not follow the same philosophy, it is reasonable that none of the guidelines are fully aligned with the CAPS.

As seen in table 5.12, the coverage increase when these previously mentioned un-mappable requirements are removed. Nevertheless, as discussed above, there is a basis to believe the CAPS is structured in this way to accommodate barrier management.

Based on the non-mapped requirements in the CAPS, it can be determined that NIST CSF is the most complete in covering the existing requirements in the CAPS. However, some requirements in the CAPS are identified as not related to cyber security, and subsequently out of scope for the NIST CSF subcategories. Nevertheless, neither NIST CSF, CIS Controls, or IEC 62443 3-3 are fully aligned to the requirements in the CAPS.

6.5 Limitations

In this section, limitations regarding the validity and reliability of the findings are discussed. Challenges and limitations of the method are addressed in section 3.5, but during the gap analysis, additional factors influencing validity and reliability was discovered.

The results in chapter 5 rely entirely on two documents. Several of the requirements in the CAPS point to other documents further specifying a requirement, or other documents as the operational assurance of the requirements. Concerning incident handling, an IT disaster recovery plan and a business continuity plan are the operational assurance maintaining the requirement. These documents were not examined in the gap analysis. A complete examination of all documentation related to cyber security in Alpha would likely show that some of the identified gaps in the CAPS are only gaps in the CAPS, not in Alpha.

However, not collecting all relevant information on cyber security barriers in the CAPS could be regarded as a weakness. The PSA stresses how "A structured approach" to barrier management is important [Nor17]. Collecting all information on cyber security barriers in one document would make it easier to assess the implemented cyber security barriers. Nonetheless, the validity of the results in this thesis would be impacted if there exists substantial information on countermeasures implemented by Alpha outside of the received information.

Further, Alpha could have cyber security barriers in place without adequately documenting the function of the barrier in the CAPS. Barriers in place without full documentation in the CAPS would influence the validity of the findings because the actual gap between implemented cyber security barriers and the ICS cyber security guidelines would be smaller. However, the Barrier Memorandum of the PSA emphasises the importance of ensuring and maintaining barrier performance, measuring and verifying the barriers' performance, and following up the barrier management system [Nor17]. In other words, barriers must be sufficiently documented to be able to meet the requirements relating to barriers.

Next, the certainty of the findings could be misinterpreted when reading this thesis, as results are given as percentages in tables. Each percentage have some uncertainty as the underlying mappings can contain errors. The challenge of mapping correctly was discussed in Challenges and Limitations in section 3.5. As the method used in the thesis was qualitative, estimating this uncertainty as a quantity is challenging. Consequently, instead of focusing on the exact percentages listed in the tables as the sole result, the percentages should be viewed in a greater context. A higher percentage implies that this area is a cyber security activity Alpha addresses and is recognised as a barrier element, while a low percentage implies the opposite.

Finally, relying entirely on the two documents made one of the original goals of this thesis challenging to achieve. There was a wish to discuss SISs specifically, but as SISs is not explicitly mentioned in the requirements in the CAPS, this proved difficult.

Chapter 7 Conclusion and Future Work

In this thesis, both implemented cyber security barriers on the NCS, and best-practice cyber security barriers were explored. Previous research in the area of oil and gas cyber security on the NCS is limited. The field is mainly populated with official reports from Norwegian governmental institutions and white papers from cyber security companies and organisations. This study has examined how an operator on the NCS aligns with three selected best practices on ICS cyber security. The results and discussion indicate that there is a need for future studies, which is suggested below.

The thesis was structured as a gap analysis between the documentation of implemented cyber security barriers of one operator on the NCS and three widely used cyber security best practices. Additionally, a comprehensive review of background material was included, where a substantial part of the background is an examination of the threat landscape on the NCS. The result of the gap analysis reveals that the operator covered 53 out of 108 subcategories (49%) in NIST CSF, 46 out of 190 sub-controls (24%) in CIS Controls, and 20 out of 51 system requirements covered (39%) in IEC 62443 3-3. Consequently, there were significant gaps in Alpha's barrier requirements compared to the three guidelines, and the cyber security requirements of Alpha can not be regarded as fully aligned with the best practices.

It should be noted that the thesis results are based on limited documentation from Alpha. A complete examination of all documentation related to cyber security in Alpha would likely show that some of the identified gaps in the CAPS are only gaps in the CAPS, not in Alpha.

The threat landscape on the NCS is characterised by highly capable threat actors motivated by possible financial and political gain. However, the main objectives of threat actors on the NCS have seemingly been information gathering and reconnaissance of networks, rather than sabotage. Additionally, the identified gaps between the CAPS and the three guidelines were used to present five areas where Alpha could make adjustments to the barrier elements in the CABS.

This thesis has brought light to the current state of implemented cyber security barriers of an operator on the NCS. Besides, the thesis has outlined a process for future gap analysis in the field of oil and gas cyber security. Hopefully, this study can aid Alpha to evaluate its current cyber security barriers and implement additional barrier elements based on the identified gaps and threat landscape.

Future Work

There are three main avenues for future work. As discussed in the limitation of the results in 6.5, the results in this thesis are based on the analysis of the received documentation; no additional data collection was performed. To further study the state of implemented cyber security barriers of Alpha, the limitations in data collection could be addressed. Addressing the limitations would gather a more complete picture of Alpha's alignment to the three guidelines in contrast to this thesis which explored the alignment between the CAPS and the three guidelines. Additionally, there was identified a need to improve the existing CABS of Alpha. Creating a comprehensive cyber security barrier model aligned with best practices and with the proper division between technical, organisational and operational barriers would be a significant contribution to the research in the field.

Secondly, research on the general state of cyber security barriers in the sector is needed in order to conclude the level of alignment to best practices in ICS cyber security on the NCS.

Finally, to be able to answer the overall research goal of evaluating the effect of cyber security barriers, additional research is needed. A feasible way to evaluate the effect must be established before any cyber security barriers are evaluated. As one of the goals of barrier management is avoiding major accidents, it is suggested that such a method is suited to evaluating a cyber security barrier's contribution to reducing the risk of a major accident on the NCS.

References

[AL15] Michael J. Assante and Robert M. Lee. The Industrial Control System Cyber Kill Chain. *SANS Institute*, October 2015.

[ARC] ARC Advisory Group. SIS Layers of Protection. Available at https://www.arcweb.com/sites/default/files/Images/blog-images/Layers-of-Protection.png. [Online, .png], Last accessed 03.06.20.

[BJD17] Joseph Bugeja, Andreas Jacobsson, and Paul 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)*, pages 557–562, 2017.

[BMF18] Deborah J. Bodeau, Catherine D. McCollum, and David B. Fox. Cyber Threat Modeling: Survey, Assessment, and Representative Framework. *The Homeland Security Systems Engineering and Development Institute (HSSEDI)*, April 2018.

[Cas07] Timothy Casey. Threat Agent Library Helps Identify Information Security Risks. *Intel Information Technology White Paper*, September 2007.

[Cas15] Tim Casey. Understanding Cyberthreat Motivations to Improve Defense. *Intel Security and Privacy Office White Paper*, 2015.

[Cen] Center for Internet Security®. Cybersecurity Spotlight – Cyber Threat Actors. Available at https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cyber-threat-actors/. [Online], Accessed 04.06.20.

[CIS18] CIS Controls. Implementation Guide for Industrial Control Systems. Guideline, Center for Internet Security, 2018.

[CIS19] CIS Controls Version 7.1. CIS Controls. Guideline, Center for Internet Security, April 2019.

[CRC08] Patricia Cronin, Frances Ryan, and Michael Coughlan. Undertaking a literature review: a step-by-step approach. *British journal of nursing*, 17(1):38–43, 2008.

[DNV15] DNV GL. Digitale Sårbarheter Olje & Gass (Digital Vulnerabilities in Oil & Gas). *2015-0462 Rev. 1*, 04 2015.

[DNV17] DNV GL. Cyber security in the oil and gas industry based on IEC 62443. *DNVGL-RP-G108*, 2017.

[DNV20] DNV GL. Regelverk og tilsynsmetodikk (Regulatory and supervisory methodology). *2019-0824 Rev. B*, 02 2020.

[Dra17a] Dragos Inc. CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations. Available at https://dragos.com/wp-content/uploads/CrashOverride-01.pdf, June 2017. [Online].

[Dra17b] Dragos Inc. TRISIS Malware, Analysis of Safety System Targeted Malware. Available at https://dragos.com/wp-content/uploads/TRISIS-01.pdf, 2017. [Online].

[DRA19] DRAGOS Inc. Global Oil and Gas Cyber Threat Perspective, ASSESSING THE THREATS, RISKS, AND ACTIVITY GROUPS AFFECTING THE GLOBAL OIL AND GAS INDUSTRY. Available at https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf, August 2019. [Online].

[DRA20] DRAGOS Inc. 2019 Year In Review: THE ICS LANDSCAPE AND THREAT ACTIVITY GROUPS. Available at https://www.dragos.com/year-in-review-2019/, January 2020. [Online], Last accessed 28.05.20.

[EM17] Thomas W. Edgar and David O. Manz. Chapter 2 - Science and Cyber Security. In Thomas W. Edgar and David O. Manz, editors, *Research Methods for Cyber Security*, pages 33 – 62. Syngress, 2017.

[Equ17] Equinor. Norway's first platform to be remotely-operated from land. Available at https://www.equinor.com/en/news/09nov2017-valemon-remote.html, November 2017. [Online] Accessed: 24.02.20.

[Eura] European Union Agency for Cybersecurity. Glossary. Available at https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary. [Online] Accessed 15.04.20.

[Eurb] European Union Agency for Cybersecurity. Threat Taxonomy. Available at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy. [Excel Worksheet] Accessed 15.04.20.

[Fir16] FireEye, Inc. CYBER THREATS TO THE ENERGY INDUSTRY. Available at https://www.fireeye.com/current-threats/reports-by-industry/energy-threat-intelligence.html, 2016. [Online], Last accessed 28.05.20.

[FMC11] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32.Stuxnet Dossier. Available at https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, February 2011.

[FW19] Barbara Filkins and Doug Wylie. SANS 2019 State of OT/ICS Cybersecurity Survey. *SANS Institute*, June 2019.

[GKA17] Benjamin Green, Marina Krotofil, and Ali Abbasi. On the significance of process comprehension for conducting targeted ics attacks. *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*, pages 57–67, November 2017.

[GMR^{+}18] Leif Gressgård, Kjersti Melberg, Martin Risdal, Jon Tømmerås Selvik, and Ruth Skotnes. Digitalisering i petroleumsnæringen - utviklingstrender, kunnskap og forslag til tiltak. *IRIS-rapport 2018/001*, March 2018.

[HCA11] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Lockheed Martin Corporation*, 2011.

[HEF18] Kevin E. Hemsley and Dr. Ronald E. Fisher. A history of cyber incidents and threats involving industrial control systems. In *International Conference on Critical Infrastructure Protection*, pages 215–242, 2018.

[HO16] Stein Hauge and Knut Oeien. Guidance for barrier management in the petroleum industry. *SINTEF A27623*, 2016.

[IEC09] IEC/TS 62443-1-1:2009. Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models. Standard, International Electrotechnical Commission, 2009.

[IEC10a] IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements. Standard, International Electrotechnical Commission, 2010.

[IEC10b] IEC 62443-2-1:2010. Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program . Standard, International Electrotechnical Commission, 2010.

[IEC13] IEC 62443-3-3:2013. Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Standard, International Electrotechnical Commission, 2013.

[IEC16] IEC 61511-1:2016. Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements. Standard, International Electrotechnical Commission, 2016.

[Int] International Society of Automation (ISA). ISA99, Industrial Automation and Control Systems Security. Available at https://www.isa.org/isa99/. [Online], Last accessed 23.05.20.

[JCK^{+}17] Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, and Christopher Glyer. Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure). Available at https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, December 2017. [Online], accessed 24.01.20.

[JLG09] Martin Gilje Jaatun, Maria B. Line, and Tor Olav Grotan. Secure remote access to autonomous safety systems: A good practice approach. *International Journal of Autonomous and Adaptive Communications Systems*, 2(3):297–312, 2009.

[KFA+11] Nishchal Singh Kush, Ernest Foo, Ejaz Ahmed, Irfan Ahmed, and Andrew Clark. Gap analysis of intrusion detection in smart grids. In *Proceedings of the 2nd International Cyber Resilience Conference*, pages 38–46, 2011.

[LAC17] Robert M. Lee, Michael J. Assante, and Tim Conway. ICS Defense Use Case No. 6: Modular ICS Malware. Available at https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf, 8 2017. [Online].

[MFV+12] Mark Mateski, Jason Frye, Cynthia Veitch, John Michalski, James Harris, Cassandra Trevino, and Scott Maruoka. Cyber threat metrics. *Sandia National Laboratories, SANDIA REPORT SAND2012-2427*, March 2012.

[MGF18] Lilly Pijnenburg Muller, Lars Gjesvik, and Karsten Friis. Cyber-weapons in International Politics. Possible sabotage against the Norwegian petroleum sector. *NUPI Report 3 / 2018*, 2018.

[MITa] MITRE ATT&CK®. APT29. Available at https://attack.mitre.org/groups/G0016/. [Online], Accessed 04.06.20.

[MITb] MITRE ATT&CK® for Industrial Control Systems. Default Credentials. Available at https://collaborate.mitre.org/attackics/index.php/Technique/T812. [Online] Accessed 30.05.20.

[MITc] MITRE ATT&CK® for Industrial Control Systems. Manipulation of Control. Available at https://collaborate.mitre.org/attackics/index.php/Technique/T831. [Online] Accessed 30.05.20.

[MITd] MITRE ATT&CK® for Industrial Control Systems. Program Download. Available at https://collaborate.mitre.org/attackics/index.php/Technique/T843. [Online] Accessed 30.05.20.

[MITe] MITRE ATT&CK® for Industrial Control Systems. Theft of Operational Information. Available at https://collaborate.mitre.org/attackics/index.php/Technique/T882. [Online] Accessed 30.05.20.

[MITf] MITRE ATT&CK® for Industrial Control Systems. Utilize/Change Operating Mode. Available at https://collaborate.mitre.org/attackics/index.php/Technique/T858. [Online] Accessed 30.05.20.

[MITg] MITRE ATT&CK® for Industrial Control Systems. Valid Accounts. Available at https://collaborate.mitre.org/attackics/index.php/Technique/T859. [Online] Accessed 30.05.20.

[MIT20] MITRE Corporation. ATT&CK® for Industrial Control Systems. Available at https://collaborate.mitre.org/attackics/index.php/Main_Page, March 2020. [Online], Last accessed 22.04.20.

[MJV17] Glenn Murray, Michael N. Johnstone, and Craig Valli. The convergence of IT and OT in critical infrastructure. *The Proceedings of 15th Australian Information Security Management Conference*, December 2017.

[MMST16] Julien Mineraud, Oleksiy Mazhelis, Xiang Su, and Sasu Tarkoma. A gap analysis of Internet-of-Things platforms. *Computer Communications*, 89-90:5 – 16, 2016.

[MRHM20] Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho. Stuxnet Under the Microscope (Revision 1.31). Available at https://www.welivesecurity.com/media_files/white-papers/Stuxnet_Under_the_Microscope.pdf, undated, accessed 24.01.20. [Online].

[Nas14] Nasjonal sikkerhetsmyndighet - NSM (National Security Authority). Varsler om datainnbrudd (Data breach notifications). Available at https://www.nsm.stat.no/aktuelt/varsler-om-datainnbrudd/, August 2014. [Online], Last accessed 28.05.20.

[Nas20] Nasjonal sikkerhetsmyndighet - NSM (National Security Authority). RISIKO 2020 (Risk 2020), April 2020.

[Nat16] National Security Authority of Norway (NSM). Håndbok: Risikovurdering for sikring. Available at https://www.nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf, 2016. [Online], accessed 02.03.2020.

[NEK18] NEK ISO/IEC 27005:2018. Information technology - Security techniques - Information security risk management . Standard, Norsk Elektroteknisk Komite, 2018.

[NIS15a] NIST Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations. Guideline, National Institute of Standards and Technology, 2015.

[NIS15b] NIST Special Publication 800-82 Revision 2. Guide to Industrial Control Systems (ICS) Security. Guideline, National Institute of Standards and Technology, 2015.

[NIS16] NIST Special Publication 800-150. Guide to Cyber Threat Information Sharing. Guideline, National Institute of Standards and Technology, 2016.

[NIS18] NIST. Cybersecurity Framework Version 1.1. Guideline, National Institute of Standards and Technology, April 2018.

[NOG16] NOG 104. Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems. Guideline, Norwegian Oil and Gas Association, 2016.

[NOG18] NOG 070. Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements). Guideline, Norwegian Oil and Gas Association, 2018.

[Nor] Norsk Petroleum (Norwegian Petroleum). Exports of oil and gas. Available at https://www.norskpetroleum.no/en/production-and-exports/exports-of-oil-and-gas/. [Online], Last accessed 29.05.20.

[Nor14] Norsk Standard NS 5832:2014. Societal security - Protection against intentional undesirable actions - Requirements for security risk analysis. Standard, Standard Norge, 2014.

[Nor15] Norwegian Petroleum Safety Authority. The Management Regulations, §5 Barriers. Available at https://www.ptil.no/en/regulations/all-acts/the-management-regulations3/II/5/, 2015. [Online], Last accessed 22.04.20.

[Nor17] Norwegian Petroleum Safety Authority. Principles for barrier management in the petroleum industry: BARRIER MEMORANDUM 2017. *Version 3*, 03 2017.

[Nor19] Norwegian Petroleum Safety Authority. About the regulations. Available at https://www.ptil.no/en/regulations/acts/about-the-regulations/, February 2019. [Online], Last accessed 03.06.20.

[Pol19] Politiets Sikkerhetstjeneste - PST (The Norwegian Police Security Service). Threat Assessment 2019, February 2019.

[Pol20] Politiets Sikkerhetstjeneste - PST (The Norwegian Police Security Service). Nasjonal trusselvurdering 2020 (National threat assessment 2020), February 2020.

[Reg15] Regjeringen. Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden (Digital Vulnerabilities in Society). *Norsk Offentlig Utredning 2015: 13 (Official Norwegian Report 2015: 13)*, 2015.

[RM16] Colin Robson and Kieran McCartan. *Real World Research: A Resource for Users of Social Research Methods in Applied Settings.* Wiley, 4th edition, 2016.

[SAN] SANS. CIS Critical Security Controls. Available at https://www.sans.org/critical-security-controls/. [Online], Last accessed 15.05.20.

[Sho14] Adam Shostack. *Threat Modeling: Designing for Security.* Wiley, 2014.

[Sin] Sintef. Industry forum for cybersecurity of industrial automation and control systems. Available at https://www.sintef.no/projectweb/cds-forum/. [Online] Accessed 20.03.20.

[Slo20] Joe Slowik. Evolution of ICS Attacks and the Prospects for Future Disruptive Events. *Dragos Inc.*, undated, accessed 10.06.20.

[Slo19] Joe Slowik. Stuxnet to CRASHOVERRIDE to TRISIS: Evaluating the History and Future of Integrity-Based Attacks on Industrial Environments. *Dragos Inc.*, 2019.

[Yin09] Robert K. Yin. *Case study research : design and methods*, volume vol. 5 of *Applied social research methods series.* Sage, Thousand Oaks, Calif, 4th ed. edition, 2009.

Appendix A
Mapping of NIST CSF categories and NOG 104 ISBRs

NOG 104 provides references to relevant NIST CSF categories for each Information Security Baseline Requirement (ISBR) [NOG16]. These references was used to create a mapping between all ISBRs and all categories in NIST CSF. Table A.1 presents this mapping. Of the 23 NIST CSF categories, the ISBRs maps to 17 of the categories. Supply Chain Risk Management (ID.SC), Detection Processes (DE.DP), Communications (RS.CO), Analysis (RS.AN), Mitigation (RS.MI), and Improvements (RS.IM) are the six missing categories. Of the five functions in NIST CSF, Respond is the least covered by the ISBRs with four out of five categories not covered.

NIST CSF Category	Description	NOG 104 ISBR
ID.AM	Asset Management	3 System and information owners 11 Network topology 17 Hardware and software inventory
ID.BE	Business Environment	3 System and information owners 8 (omitted from CAPS)
ID.GV	Governance	1 Information security policy 9 Service and support levels 8 (omitted from CAPS)
ID.RA	Risk Assessment	2 Information security risk management 17 Hardware and software inventory
ID.RM	Risk Management Strategy	2 Information security risk management 17 Hardware and software inventory
ID.SC	Supply Chain Risk Management	×
PR.AC	Identity Management and Access Control	4 Segmented networks 14 Access requests 18 Remote access 19 Access management
PR.AT	Awareness and Training	5 User training and awareness
PR.DS	Data Security	4 Segmented networks 15 Operational and maintenance procedures
PR.IP	Information Protection Processes and Procedures	6 Designated use of systems 9 Service and support levels 10 Change management and work permit procedures 15 Operational and maintenance procedures
PR.MA	Maintenance	6 Designated use of systems 10 Change management and work permit procedures 12 Security patches 15 Operational and maintenance procedures
PR.PT	Protective Technology	4 Segmented networks 10 Change management and work permit procedures 12 Security patches 13 Malicious software 18 Remote access
DE.AE	Anomalies and Events	13 Malicious software 16 Reporting information security events
DE.CM	Security Continuous Monitoring	11 Network topology 13 Malicious software 16 Reporting information security events
DE.DP	Detection Processes	×
RS.RP	Response Planning	13 Malicious software
RS.CO	Communications	×
RS.AN	Analysis	×
RS.MI	Mitigation	×
RS.IM	Improvements	×
RC.RP	Recovery Planning	7 Preparedness for disaster recovery
RC.IM	Improvements	7 Preparedness for disaster recovery 13 Malicious software
RC.CO	Communications	7 Preparedness for disaster recovery

Table A.1: The mapping between the 23 different NIST CSF categories and the 19 NOG 104 ISBRs according to NOG 104. The red crosses mark NIST CSF categories not covered by NOG 104.