Master's thesis

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

Iben Andrea Bøyum Huus
Rikke Kjenes Paulsen

Securing Safety in the Norwegian Petroleum Industry with Digital Twins

Master's thesis in Communication Technology and Digital Security
Supervisor: Maria Bartnes
Co-supervisor: Lars Bodsberg, Roy Thomas Selbæk Myhre
June 2022

NTNU
Norwegian University of Science and Technology

Iben Andrea Bøyum Huus
Rikke Kjenes Paulsen

Securing Safety in the Norwegian Petroleum Industry with Digital Twins

Master's thesis in Communication Technology and Digital Security
Supervisor: Maria Bartnes
Co-supervisor: Lars Bodsberg, Roy Thomas Selbæk Myhre
June 2022

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

NTNU
Norwegian University of
Science and Technology

Title:	Securing Safety in the Norwegian Petroleum Industry with Digital Twins
Student:	Iben Andrea Bøyum Huus
	Rikke Kjenes Paulsen

Problem description:

The fourth industrial revolution (I4.0) defines a shift towards advanced automation, decentralization, and augmented decision-making. This shift facilitates a more connected and digital operation and management of critical infrastructures, i.e., the Oil&Gas-industry. While the industry has traditionally been concerned with isolating components and control systems of operational technology (OT) from information technology (IT), I4.0 brings these domains together, allowing interoperability and connectivity between assets.

Simulation, emulation, digital twin (DT), and asset administration shell (AAS) are a set of new and old terms that encompass a trending aspect of industrial I4.0. These technologies benefit the industry with data generation and visualization that improve efficiency and production, while also reducing costs. Furthermore, this technology's effect on cybersecurity and safety, both as a tool to increase resilience against cyber threats and as a potential source of new vulnerabilities, is an emerging area of interest to the industry.

This work aims to introduce and analyze state-of-the-art AAS technology from a cybersecurity perspective. We will examine how the AAS can affect resilience against threats as a part of the cybersecurity barrier management process while also considering its limitations. The objective is to contribute with valuable insights on the effect of the technology to ensure and increase safety and security in the critical infrastructure of Norway's offshore oil and gas industry.

Date approved:	2022-02-23
Responsible professor:	Maria Bartnes, IIK and SINTEF
Supervisor(s):	Lars Bodsberg, SINTEF
	Roy Thomas Selbæk Myhre, Sopra Steria

Abstract

The Norwegian petroleum industry is subject to stringent requirements for control and safety. This is due to incidents with consequences spanning loss of equipment, environmental and financial degradation, and loss of life. Information Technology (IT)/Operational Technology (OT) convergence and sophisticated cyber attacks make the sector more vulnerable to cyber threats. The Norwegian Petroleum Safety Authority (PSA) implies that a high level of safety must be a priority when introducing new technology, motivating the term *secure safety*. The Digital Twin is an emerging technology in Industry 4.0 (I4.0), facilitating Machine-to-Machine (M2M) communication, analysis, and visualization of physical and digital assets. In the Norwegian petroleum industry, Equinor has implemented the Digital Twin mainly for predictive maintenance. However, these characteristics also make the Digital Twin an interesting research area as an asset for cybersecurity, addressing current challenges regarding legacy systems and IT/OT convergence. To follow the PSA requirements, one must ensure that the implementation of new technologies is not compromising security and, consequently, safety.

This work explores how the Norwegian Oil&Gas industry can benefit from the Digital Twin in a cybersecurity context while still addressing *secure safety*. A qualitative research approach involving interviews and literature reviews on the topics of Digital Twin, cybersecurity, and barrier management is used to analyse and answer the research questions. The aim of the work is to identify possible use areas and challenges for the technology and to discuss these in the context of barrier management. This context intends to emphasize the convergence between safety and security.

We have derived four recommended use areas for an initial implementation of the Digital Twin for cybersecurity. These findings includes system status monitoring, security patching, intrusion detection, and training and awareness. Both technical and cultural challenges and limitations regarding the technology were identified. These involves legacy systems, data quality- and bottleneck, lack of standardization and awareness, and cyber culture. Analyzing use areas and challenges at the upper maturity levels of the Digital Twin and designing sub models for an Asset Administration Shell (AAS) presents a new perspective for future work and considerations.

Sammendrag

Norsk petroleumindustri er underlagt strenge krav til kontroll og sikkerhet. Dette skyldes at hendelser kan ha konsekvenser som tap av utstyr, miljømessig og økonomisk forringelse og tap av liv. Informasjons Teknologi (IT)/Operasjonell Teknologi (OT)-konvergens og sofistikerte cyberangrep gjør sektoren mer sårbar for cybertrusler. Petroleumstilsynet (PSA) spesifiserer at et høyt sikkerhetsnivå må prioriteres ved introduksjon av ny teknologi, noe som motiverer begrepet *cybersikker sikkerhet (secure safety)*. Digital Tvilling er en ny teknologi innen Industri 4.0 (I4.0), som muliggjør Maskin-til-Maskin (M2M) kommunikasjon, analyse og visualisering av fysiske og digitale eiendeler. I norsk petroleumsnæring har Equinor implementert teknologien hovedsakelig for prediktivt vedlikehold. Imidlertid gjør disse egenskapene også Digital Tvilling til et interessant forskningsområde innen cybersikkerhet, og kan tenkes å adressere nåværende utfordringer angående eldre systemer og IT/OT-konvergens. For å følge PSA-spesifikasjonene må man sørge for at implementeringen av nye teknologier ikke går på bekostning av cybersikkerheten og følgelig sikkerheten (safety).

Dette arbeidet utforsker hvordan norsk petroleum-industri kan dra nytte av den Digitale Tvillingen i en cybersikkerhetskontekst, samtidig som den oppfyller PSA-spesifikasjonene. En kvalitativ forskningstilnærming bestående av intervjuer og litteratur studier på temaene Digital Twin, cybersikkerhet og barrierehåndtering brukes til å analysere og svare på forskningsspørsmålene. Målet med arbeidet er å identifisere mulige bruksområder og utfordringer for teknologien og diskutere disse i sammenheng med barrierehåndtering. Denne konteksten har til hensikt å understreke konvergensen mellom cybersikkerhet og sikkerhet.

Vi har utledet fire anbefalte bruksområder for en innledende implementering av Digital Twin for cybersikkerhet. Disse funnene inkluderer systemstatusovervåking, sikkerhetsoppdatering, inntrengningsdeteksjon, og opplæring og bevissthet. Både tekniske og kulturelle utfordringer og begrensninger knyttet til teknologien ble identifisert. Disse involverer eldre systemer, datakvalitet- og flaskehalser, mangel på standardisering og bevissthet, og cyberkultur. Å analysere bruksområder og utfordringer på de øvre modenhetsnivåene til Digital Twin og utforme undermodeller for et Asset Administration Shell (AAS) presenterer et nytt perspektiv for fremtidig arbeid og overveielser.

Preface

This master thesis is the final delivery of the Master of Science in Communication Technology and Digital Security degree at the Norwegian University of Science and Technology (NTNU). The research was conducted in the time period from January 2022 until June 2022, and was based on the work performed the previous fall during the pre-project.

We would like to thank our supervisors Maria Bartnes, Lars Bodsberg, and Roy Thomas Selbæk Myhre for guidance throug the pre-project and subsequent thesis. A big thank you must also be given to interview participants, all of which provided valuable insight and opinions on the research topics.

Finally, we would like to thank our friends and family for supporting us through our studies, and particularly during the masters thesis work process.

Iben Andrea Bøyum Huus
Rikke Kjenes Paulsen
Trondheim, June 2022

Contents

List of Figures

List of Tables

List of Acronyms

AAS Asset Administration Shell.

AI Artificial Intelligence.

APT Advanced Persistent Threat.

AR Augmented Reality.

CBM Cybersecurity Barrier Management.

CCE Consequence-driven Cyber-informed Engeneering.

CPC Core Process Control.

CPS Cyber Physical System.

CSF Cybersecurity Framework.

DNV Det Norske Veritas.

DoS Denial of Service.

I3.0 Industry 3.0.

I4.0 Industry 4.0.

IACS Industrial Automation and Control Systems.

ICT Information and communication technology.

IDS Intrusion Detection System.

IEC International Electrotechnical Commission.

IIoT Industrial Internet of Things.

IoT Internet of Things.

IPS Intrusion Prevention System.

IRP Incident response plan.

ISBR Information Security Baseline Requirement.

IT Information Technology.

M+O Monitoring and Optimization.

M2M Machine-to-Machine.

NIST National Institute of Standards and Technology.

NOA NAMUR Open Achitecture.

NOG Norwegian Oil and Gas Association.

OPC UA Open Platform Communications United Architecture.

OT Operational Technology.

PCSS process control, safety and support.

PSA Norwegian Petroleum Safety Authority.

RAMI 4.0 Reference Architecture Model Industry 4.0.

RP Recommended Practice.

SAS Safety and Automation Systems.

SIL Safety integrity level.

SIS Safety Instrumented System.

VR Virtual Reality.

Chapter 1
Introduction

The petroleum industry is a critical infrastructure with a significant global presence, impacting societal functions, the economy, and the environment [Gil21]. It is the most prominent industry in Norway, contributing to the economy with a value creation of approximately NOK 15,700 billion in total [18b]. Accidents occurring on offshore Oil&Gas installations can have consequences spanning loss of equipment, environmental and financial degradation, and loss of life [18a; OBH+22; Gil21]. These consequences make the industry subject to stringent requirements for control and safety [18a]. The Norwegian Petroleum Safety Authority (PSA) has issued the Barrier Memorandum to encounter these safety requirements, where a *barrier* is an action that deliberately influences a sequence of events to prevent or limit damage or loss [Nor17].

The exposure to cyber threats in Industrial Automation and Control Systems (IACS) and Operational Technology (OT) systems have traditionally been small. The limited exposure has made unintentional and safety-related incidents the main focus when designing barriers [Gil21]. However, assets and systems within the petroleum industry have experienced a shift towards digitalization, introducing Information Technology (IT) components to the previously isolated OT networks [21c]. This aggregation of OT data provides opportunities for new services and technologies [ZPG12]. On the other hand, the convergence between the two domains increases the overall vulnerability of the system by intertwining safety oriented OT assets with high availability requirements and cybersecurity oriented IT equipment designed for confidentiality [Gil21]. New threats and vulnerabilities stress the need for comprehensive cybersecurity awareness and improved barriers to meet the PSA requirements for safety [ENI21; ZL21]. An ongoing research project initiated by SINTEF aims to increase the focus on *securing safety* by introducing cybersecurity barriers, and their management in the existing Barrier Memorandum for safety [21b].

Recent attacks and reports show that cyber incidents can have severe safety-related consequences [MRB+22]. However, cybersecurity competence, awareness, and

preparedness among personnel remain low [Dra21a; MRB+22]. Mittal, Slaughter, and Zonneveld (2017) emphasize the need for new solutions and innovative thinking to address challenges in the petroleum industry. Existing challenges include security patching, intrusion detection, and cyber hygiene [DNV17]. One of the emerging technologies in the industry is the *Digital Twin* with benefits including increased effectiveness, cost reduction, and improved resource management [TTAA18; IBM20]. The Digital Twin uses manufacturing documents, logs, requirements, and real-time data to represent a physical asset virtually. It uses the Industrial Internet of Things (IIoT) to enable communication between previously isolated components, giving access to the real-time status of the component and system on a control panel [IBM20].

The Digital Twin, especially of higher maturity levels, has mainly been studied and implemented on a small scale in the health and retail industry and the manufacturing industry for predictive maintenance [BFP+18]. To our knowledge, the industry has yet to implement the Digital Twin for cybersecurity purposes. However, the attributes and capabilities of the Digital Twin offer promising implications for several domains, including cybersecurity in the petroleum industry [HPM+21; BFP+18]. This motivate our exploratory research on Digital Twins for enhanced resilience, cybersecurity barriers, and cybersecurity awareness in the Norwegian petroleum Industry.

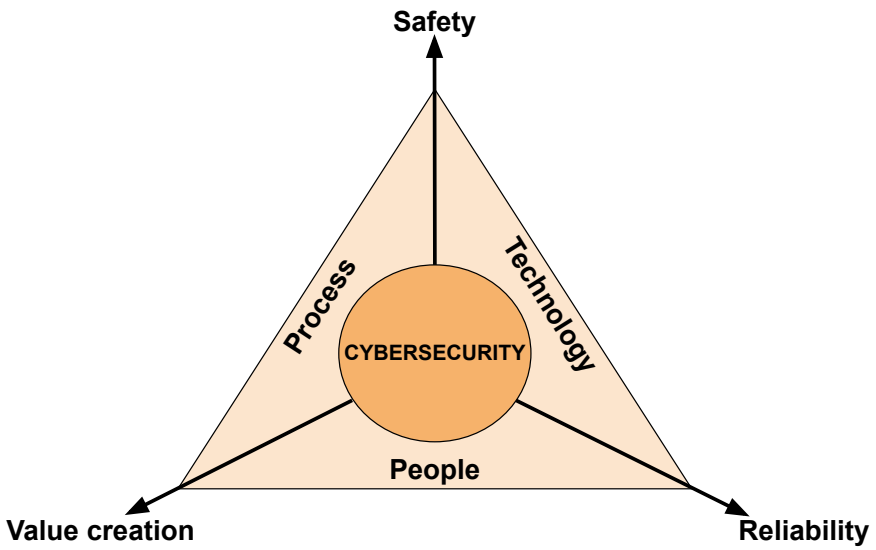

Figure 1.1: Cybersecurity involves processes, technology, and people, and enables value creation, reliability and safety. Adopted from [MSZ17] and [DNV17].

1.1 Scope and Research Questions

This work aims to explore current Digital Twin research and industry insights for cybersecurity to see how the petroleum industry's security and safety can be improved or affected by its implementation. We used the Scopus database to search for the term "Digital Twin" and found over 1400 papers in 2022. However, when including the term "cybersecurity," we only encompassed 23 papers. The initial search implies that the technology is explored for several applications. However, the focus has not been on cybersecurity. In addition to the current issues in the industry and the indicated benefits of the technology, this observation motivated us to try to answer the following research questions:

RQ1: *How can the Digital Twin technology be used to improve cybersecurity in the Norwegian petroleum industry?*

RQ2: *What are the challenges that limit the industry from utilizing Digital Twins for cybersecurity?*

The research gap this thesis addresses involve how the Norwegian petroleum industry can implement Digital Twins to improve its cybersecurity, barriers, and cybersecurity awareness while still conforming with PSA requirements regarding securing safety [18a; 21b]. The ongoing Cybersecurity Barrier Management (CBM) project addresses the convergence between safety and security. As this presents a current industry focus area, we will use terminology and concepts from the safety Barrier Memorandum to present our findings. However, CBM is not yet a published concept, and it is not in the scope of this thesis to provide a comprehensive presentation and definition of its concepts. This work uses the International Electrotechnical Commission (IEC) 62443-1-1's definition of a security countermeasure when referring to a *cybersecurity barrier*:

action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken [09a].

Due to the time constraint of 21 weeks, we further limited the scope. The Digital Twin is not yet a standardized concept, and it spans many capabilities and technologies. It is not in the scope of this thesis to present all possible enabling technologies, even if these differences affect the potential use areas and limitations of the technology. The name Asset Administration Shell (AAS) is used by the German Plattform Industrie 4.0 for the implementation of the Digital Twin in the industry, and it was also used in our problem description. This concept limits our study of enabling technologies presented in Chapter 2. However, the term Digital Twin

will be used throughout the thesis to increase readability and because of the work's exploratory purpose. Due to time constraints, we have not included storage or data processing in the cloud or edge as part of the scope when answering research question RQ2.

The analysis will identify possibilities and challenges with the technology when adopted for cybersecurity purposes on offshore Oil&Gas installations. Other potential benefits excluded from the research are its possibilities within the areas of remote control- and access technologies, increased production efficiency, and economics [HPM+21]. These areas are highly relevant, and other Digital Twins assessments should consider these perspectives. Additional challenges and considerations outside the scope involve the ethical and economic aspects of the implementation, which require further research [HPM+21]. We chose to focus on the offshore Oil&Gas installations because of the high safety impact of successful cyber attacks. The initial scope of this work is comprehensive and not limited to a single use case or a subset of the technology. This decision was based on the intention to explore a broad set of use areas to motivate the industry to exploit the Digital Twin for cybersecurity.

1.2 Contribution

The thesis' primary objective is to enhance the industry's focus and awareness of cybersecurity by providing recommended use areas for Digital Twins as cybersecurity barriers while using familiar safety barrier concepts to facilitate secure safety.

This thesis contributes with insight into the state-of-the-art Digital Twin technology and how the Norwegian petroleum industry can utilize the technology to address the current and future cybersecurity threat landscape. Literature studies and semi-structured interviews with the industry provides us with the foundation to answer the research questions. Discussing the findings in the context of cybersecurity barriers was motivated due to the current industry interest in this area. Exploring the concepts of cybersecurity barriers and Digital Twins in light of each other is not previously done, motivating the use of a qualitative research approach involving analysis of literature and interview data. The work is structured to identify initial use areas for the industry to increase its robustness against cyber attacks using Digital Twins for cybersecurity barriers while also emphasizing the limitations and challenges of the technology.

1.3 Outline

This section provides an outline of the thesis. Each chapter's content is summarized in short.

Chapter 1: Introduction introduces the research area of the project. It includes the reasoning behind the chosen topics and formulates the objectives, research questions, and scope.

Chapter 2: Background presents the background information that is used to understand and discuss the research area. It contains definitions of terms and concepts from literature and standards utilized throughout the project.

Chapter 3: Methodology present the research methodology used throughout the conducted research. It presents the different methods and their execution.

Chapter 4: Results presents the data collected and generated through the conducted literature study and parallel interviews with the industry. The data is analyzed to identify recommended use areas and limitations for the Digital Twin in cybersecurity.

Chapter 5: Discussion analyses and discusses the data presented in the previous chapter. The chapter is structured using the research questions. The chapter concludes with by addressing the study's limitations.

Chapter 6: Conclusion and Future Work concludes the paper by summarising the work that have been done and the derived results.

Chapter 2
Background

This thesis aims to answer, "*How can the Digital Twin technology be used to improve cybersecurity in the Norwegian petroleum industry?*" and "*What are the challenges that limit the industry from utilizing Digital Twins for cybersecurity*". The following chapter will provide the theoretical basis needed to substantiate and understand the main research areas relevant to the results and discussion. The Barrier Management Memorandum issued by the PSA stresses *barrier management* as an essential activity for industrial safety in Norway. It is also an important part of the discussion of this work to facilitate *secure safety*. Section 2.1 provides an overview of cyber attacks targeting critical infrastructures, emphasizing the need for improved cybersecurity. Next, Section 2.2 present the terminology and parts of the memorandum relevant to the later discussion about cybersecurity barriers (Sec. 5.2). Further on, Section 2.3 presents standards, guidelines, and frameworks used in Norway to ensure compliance with security and safety requirements. Digital Twins is the fundamental technology explored in this work. Section 2.4 explains the concept of the Digital Twin in the area of I4.0 (Sec.2.4.2), the AAS (Sec. 2.4.3), and the plant life cycle (Sec. 2.4.4). The term *plant* is used as a synonym for offshore Oil&Gas installations. The technology's potential and challenges are investigated in depth during the literature study presented in Chapter 4.

2.1 Cyber attacks targeting critical infrastructures

Over the last two decades, the number of cyber attacks targeting critical infrastructures, Cyber Physical Systems (CPSs) and IACS has increased, with *ransomware as a service* as a trending concept amongst adversaries [Dra21a; ZL21]. This section highlights some significant incidents from the last decade. The first three are examples of attacks targeting the increasingly vulnerable and exposed IACS [oAut20], illustrating the consequences cyber attack has on the entire infrastructure across domains and not solely IT. Industry awareness and statistics regarding this concludes this section, stressing the need for improvements.

Stuxnet The Stuxnet attack targeted a power facility in Iran between 2009 and 2011. The attack included a worm exploiting four zero-day vulnerabilities to damage centrifuges used to enrich uranium. The attack is an example of infrastructure sabotage that managed to manipulate and apply damage to systems through malware. It targeted the company's OT systems, which, as discussed, are heavily interconnected with IT, thus affecting both domains was possible [21c].

NotPetya Maersk, a Danish shipping company, became the victim of the large-scale crypto-ransomware named NotPetya in 2017. The malware encrypted data beyond repair, forcing the company to replace all the infected computers. Notpetya stood out from regular ransomware as it managed to spread independently through computers, locking all data it came across. The event cost Maersk an estimated sum of $300 million, and the global cost of the malware, which also crippled power plants, banks, and metro systems, added up to around $10 billion [Gre18].

Triton The Triton malware attacked the OT infrastructure, specifically the Safety Instrumented System (SIS). With SIS being the last line of defense, such compromise could be fatal. The previous perception and naivety that safety systems were off-limits as this directly targets human life was refuted in this cyber attack[Gil19].

Colonial fuel pipeline A recent cyber attack targeting the Oil&Gas-industry was the attack on the American fuel pipeline in 2021. The attack, orchestrated by cybercriminal group DarkSide, used ransomware against the Colonial Pipeline operator. The attack involved infiltrating the company's billing system through weaponizing old VPN account passwords [21a; Dra21a]. As part of the mitigation strategy, a subsection of systems was shut down to prevent extensive damage, and loss [Dra21a]. If higher levels of visibility into the OT-infrastructure had been in place, improved decisions could have been made [Dra21a].

The presented examples corroborate that critical infrastructures are attractive targets for cybercriminals. This reality highlights the importance of the industries staying updated on their threat landscape to best prepare for and mitigate attacks and consequences. IACSs have suffered from a 500% increase in ransomware attacks between 2018 and 2021 [Dra22], with new vulnerabilities and threats emerging daily [ZL21]. The increase in attacks result from the parallel increase in IACS vulnerabilities [Dra21a]. The manufacturing sector also accounts for 65% of ransomware attacks, which is worrisome considering they are the least mature sector where OT security is concerned [Dra21a]. Common issues contributing to the weak security include limited visibility into these systems [Dra21a], making detection, control, and overview hard. In contrast to safety, IACS security is not explicitly stated in the Norwegian regulations. This fact contradicts the rising issue of threats against them.

2.2 PSA Regulations - Barrier Management

This section introduces the concept of Barrier Management, defined by the PSA. Barrier Management is a framework developed in the industry to manage safety and address governmental regulatory requirements [Nor17].

The PSA regulations contain risk and performance requirements that the industry needs to enforce to ensure a safe work environment. The management regulation is one of five regulations to which the petroleum industry of Norway must oblige. Chapter two of this regulation covers risk management. The Management Regulation §5 Barriers states that stakeholders should establish barriers so that at all times, they can [Pet20]:

a) identify conditions that can lead to failures, hazards, and accident situations.
b) reduce the possibility of failures, hazard and accident situations occurring and developing.
c) limit possible harm and inconveniences.

This requirement has been a part of the regulation for some time. However, its implementation and scope delimitation has been a PSA project which in 2011 led to the publication of the Barrier memorandum. The memorandum is a document that describes the principles of Barrier Management. The memorandum has been updated twice, the most recent in 2017 [Nor17]. The developed memorandum encompasses §5 and related requirements by putting them into context. The concept of Barrier Management involves establishing and maintaining barriers and ensuring that they fulfill their functions. The provided definition of a *barrier* for safety is:

> *A measure intended to identify conditions that may lead to failure hazard, and accident situations, prevent an actual sequence of events from occurring or developing, influence a sequence of events in a deliberate way, or limit damage and loss* [Nor17].

With an ever-changing risk picture, threat landscape, and technological development, the management of barriers is iterative and continuous [Nor17]. Barrier Management involves a systematic approach that ensures the identification, establishment, and maintenance of necessary barriers to ensure safety [Nor17]. The industry can manage barriers through measures such as, e.g. accessing the barrier status and performing a risk analysis of the system. Figure 2.1 illustrates the key elements of the Barrier Management process as described in the Barrier Memorandum [Nor17]. In addition to risk analysis and identification of barriers, the process should identify performance requirements, map these to performance-influencing factors and continuously ensure and maintain the barrier's performance [Nor17].

The Barrier Management framework addresses safety. Visualization of the framework is possible through a barrier diagram. This diagram is shaped like the familiar bow-tie. The model's components include barrier functions, sub-functions, and elements of the barrier hierarchy, concepts elaborated on in Section 2.2.2.

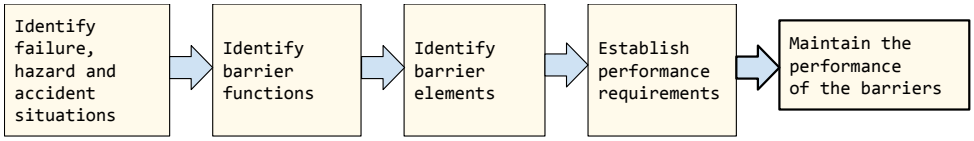

Figure 2.1: The key features of the Barrier Management process. Derived from [Nor17].

2.2.1 The Bow-Tie Model

A bow-tie model can be used to illustrate barriers and to analyze and communicate risk scenarios [Nor17; DNV16; BFM+18]. The model displays the architecture, elements, and phases of barrier management [BFM+18]. Focusing on the steps and actions after the system has left regular operation, the model highlights the position of barriers in a timeline. The four parts that make up the model are:

1. **Identification**: Identifying potentially hazardous and failure conditions
2. **Preventative measures**: Actions that focus on reducing the possibility of incidents
3. **Incident**: The undesirable event itself
4. **Reactive measures**: Limiting and preventing consequences

The list above makes up categories used to classify barriers, excluding the incident as this represents the hazard or failure state addressed by the barriers. Figure 2.2 presents the relationship between the categories and the respective positions of barriers, visualized by green lines, within each of them.

2.2.2 Barrier function, Elements and Hierarchy

The task or role of a barrier is its barrier function [Nor17]. In order to fulfill this function, the barrier may consist of several elements operating together, referred to as barrier elements. These elements fit into three specified categories: technical, organizational, or operational [Nor17]. Questions that clarify the distinction between the different categories are:

- What system or equipment is needed to realize the function (technical).
- What action should be executed (operational).

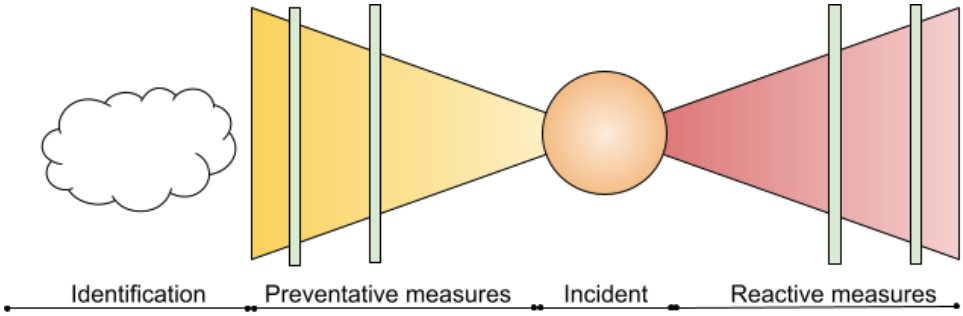

Figure 2.2: Bow-tie model - displaying the structure and elements of barriers in light of an incident. Derived from [Nor17].

– Who will be activating or executing the needed action (organizational).

The categories are all involved in identifying a barrier function and its sub-functions, making up the barrier hierarchy structure shown in Figure 2.3.

The performance requirements define what the barrier element must fulfill to be considered adequate. These requirements are measurable and verifiable, making it possible to assess the status of each element. Performance-influencing factors are mapped to performance requirements and barrier elements. They define factors that significantly impact the barrier function and elements' ability to operate and perform as intended [Nor17].

2.2.3 Cybersecurity Considerations - Securing Safety

Securing safety becomes more critical with the interconnectedness and external connections to safety-critical OT segments, and addressing vulnerabilities in the bridge between the domains should be prioritized [Dra21a]. Security incidents are, like safety incidents, examples of situations outside normal operations. Like safety barriers, security countermeasures are critical to mitigate and limit the security incidents' potential scope, and effect [Nor17], as well as its cascading effects on safety. In particular the final safety barrier SIS is critical to secure [ZL21]. SIS is the final control element or barrier in place that possess the functionality to take processes into a safe state when certain conditions are met [22b]. Other terms used in the context of SIS are: emergency shutdown system, safety shutdown system, and safety interlock system [22b]. As the digitization trend starts to influence critical assets, such as SIS, the need for a new approach and strategy towards barriers, management, and monitoring of them arise with the need to preserve the safety of the petroleum industry assets [ZL21].

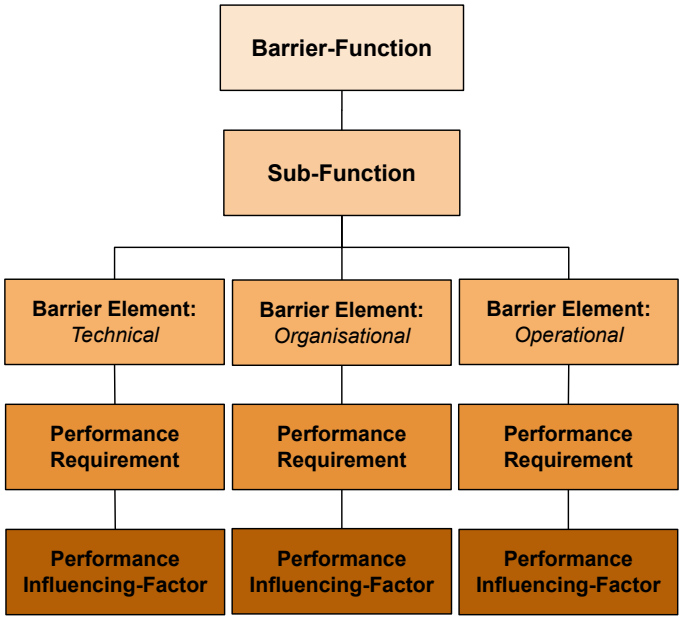

Figure 2.3: Barrier hierarchy structure. Adopted from [Nor17].

When addressing barriers as a concept, today's focus is on safety barriers to prevent failures, hazards, and accidents. Using barrier management principles in the security domain is an ongoing research area in the Norwegian petroleum industry. The overall objective of the research project initiated by SINTEF is to provide new knowledge and guidance for Cybersecurity Barrier Management (CBM) covering both technical and non-technical aspects as a continuous process during development and operation [21b]. The framework developed for safety can provide a documented, systematic way to perform identification, implementation, and maintenance of security barriers [Nor17]. When specifying a new framework for the establishment and management of cybersecurity barriers, it is useful to look to the existing National Institute of Standards and Technology (NIST) Cyber Security Framework for their definition of concepts and processes. To comply with the Safety Barrier Management framework, one must define performance requirements for the cybersecurity barriers to fulfill. IEC 62443 contains relevant documents to address requirements that must be addressed by all stakeholders to ensure the adequate performance of cybersecurity barriers. The next section will present some relevant documents that are currently used for cybersecurity in the Norwegian petroleum industry.

2.3 Cybersecurity Documents and Concepts

Available standards, guidelines, and frameworks used to address security issues are, in many cases, insufficient and lack updates to mirror the advancement of adversaries [HOG+21]. This section presents some of the cybersecurity concepts and relevant documents used by the Norwegian petroleum industry today.

2.3.1 Relevant Frameworks, Standards, Recommended Practices, and Guidelines

The industry is currently trying to implement the IEC 62443 series of standards regarding the security of IACS. The series proposes an extensive set of requirements, roles, and terminology. The Cybersecurity Barrier Management (CBM) project will incorporate this series. Current guidelines and frameworks used by the industry for cybersecurity involves NIST Cybersecurity Framework (CSF) and Norwegian Oil and Gas Association (NOG)104, both of which refer to IEC 62443 for some of their requirements. These documents, with some additional mentions, will next be elaborated on for clarification of content and relevance to the industry's approach to cybersecurity.

NIST Cybersecurity Framework

NIST CSF aims to provide critical infrastructures guidance to *identify, assess and manage cyber risk* in an iterative manner [oST18]. The framework includes information security measures and controls that can assist critical infrastructures in managing and reducing their cybersecurity risk [oST18]. NIST CSF can assist in developing security requirements, work as a basis for security programs and provide a shared understanding and overview of the organization's security risks. The five security functions of the framework are: Identify, protect, detect, respond and recover [oST18].

NIST CSF is not sufficient as a standalone element [HOG+21], indicating that organizations need additional documents, standards, and guidelines to realize a robust cybersecurity strategy. IEC 62443, referred to in NIST CSF, is pairable with the framework to address IACS security. Equinor is one company using this combination in their development of requirements [16b].

IEC 62443

IEC 62443 is a series of standards and technical reports that address the security of IACSs [oAut20]. The benefit of having standardized requirements and terminology is that all involved parties along the supply chain can obtain a shared understanding of cybersecurity and how it should be approached, leading to more robust security

[oAut20]. For the Norwegian petroleum industry, IEC 62443 has gained acknowledgment as a framework in their strategy and approach to implementing and managing cybersecurity [16b; DNV17].

While the IEC 62443 standard holds many benefits, stakeholders have found understanding and implementing it challenging [HOG+21; SS20; OBH+22]. In addition, some parts are incomplete, outdated, or not created [oAut20]. The scope and content are extensive, over 900 pages, requiring significant effort and time to understand and implement correctly. Additionally, the series only considers IACS [09a]. Like NIST CSF, it offers organizations a framework expressing cybersecurity requirements industries should include. However, it does not specify how to include these, leaving many organizations with considerable work needed to realize it.

DNVGL-RP-G108

DNVGL-RP-G108, *Cyber security in the oil&gas industry based on IEC 62443* [DNV17], is the result of an initiative to develop a globally Recommended Practice (RP) addressing the increasing cyber-threat within the petroleum industry by applying the IEC 62443 series. The RP proposes an implementation of the standards and clarifies the roles and responsibilities of stakeholders such as asset owner, system integrator, service provider, product supplier, and compliance authority. The incompleteness of the IEC 62443 series thus also affects the exhaustiveness of this guideline [DNV17].

NOG104

Norwegian Oil and Gas Association (NOG) has developed a guideline together with the industry that addresses information security of process control, safety and support (PCSS) Information and communication technology (ICT)-systems by describing how organisations can implement Information Security Baseline Requirements (ISBRs). The document is considered *"good practice"* when used in collaboration with the company's information security policies [16a].

According to the guideline, a holistic approach that considers the system's entire life cycle, including the development and the operational phases, is needed when addressing security measures and their management [16a]. NOG104 incorporates this by structuring the guidelines according to the five security functions defined in NIST CSF [oST18]. Using this structure, the organization may address the ISBRs in a bow-tie manner [16a]. The first three functions make up the right side of a bow-tie before the incident, and the remaining two belong to the left after the incident.

The industry is referencing NOG104 in their attempt to mitigate security challenges. They have acknowledged that it is outdated, but it is still the only cyberse-

curity guideline noted in the PSA regulations [HOG+21].

Other relevant standards and guidelines

The previous section provided an overview of central frameworks and guidelines used to address the security of IACS in the industry. This section will briefly introduce additional relevant documentation.

The ISO/IEC 27000 series of standards aim to provide an information security management system, a systematic approach to risk management, to secure information in organizations of all types and sizes [22d]. ISO 27002 provides a comprehensive overview of information security controls that organizations can choose to implement based on individual risk assessments [22d]. The document can be used as a reference to develop cybersecurity management guidelines. Petroleum companies, including Equinor, use ISO 27002 [SS20].

DNV-RP-A204, *qualification and assurance of Digital Twins* [DNV21], provides industries with requirements necessary to ensure the qualification and assurance of the Digital Twin technology. Digital Twins described in this RP comprise the asset, its virtual replica, and the connection between them. With this technology being adopted more widely across industries, a subsequent need to ensure an adequate level of trust in the output emerged. The document refers to requirements and the cybersecurity management plan specified in DNVGL-RP-G108 to ensure a cyber-secure Digital Twin.

Summary of Standards and Guidelines

Table 2.1 illustrates a summary of standards and guidelines presented in this section.

Table 2.1: Summary of standards and guidelines.

Institution	Short title	Last revision	Title	Description
IEC	62443-1-1	2007	Terminology, Concepts, and Models	Includes definitions of terms and concepts relevant within the standard-series [09a].
	62443-2-1	2009	Establishing an IACS security program	Describes the responsible parties for operation of industrial facilities [10].
	62443-2-3	2015	Patch management in the IACS environment	Technical report concerning patch management program requirements for asset owners and IACS suppliers [09b].
	62443-3-3	2013	System security requirements and security levels	Contains security requirements and the systems functional capabilities used as functional requirements, and describes security levels in this context [oAut20].
	27002	2022	Information security, cybersecurity and privacy protection - Information security controls	Describes controls for information security risk management sorted into four categories: organisational, people, physical and technical [22d].
NIST	CSF	2018	Framework for Improving Critical Infrastructure Cybersecurity	Provides a generalized taxonomy and mechanism for organisations to describe cybersecurity state and goals, identify, prioritize and assess improvement areas, and communicate risks between stakeholders [oST18].
NOG	104	2016	Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems	Describes how organizations can implement ISBRs, and is the only standard mentioned in the PSA regulations [16a].
DNV	DNV-RP-G108	2017	Cyber security in the oil&gas industry based on IEC 62443	Provides implementation practices for IEC 62443 in the Oil&Gas Sector [DNV17].
	DNV-RP-A204	2017	Qualification and assurance of Digital Twins	Provides requirements and recommendations to ensure quality and trustworthiness of Digital Twin implementation [DNV21].

2.3.2 Concepts

Relevant concepts and definitions from the described standards are aggregated and presented next. The aim is to clarify the scope and definition of concepts used throughout this work and provide a good foundation for the later discussion of Barrier Management in a cybersecurity context when assessing the Digital Twin technology.

Cybersecurity Barriers

Cybersecurity barrier is not standard terminology in the context of cybersecurity. The currently most relevant and updated standard, according to literature, are the IEC 62443 series [HOG+21; DNV17; OBH+22].

Security documentation uses different terms and definitions for concepts when referring to barriers. Examples are listed below.

- NIST CSF - **security control**: *The management, operational, and technical controls (e.g., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data* [oST18].
- NOG104 - **control**: *Measure that is modifying risk* [16a]. The standard also refers to NIST's definition above.
- IEC 62443 - **security control/countermeasure**: *action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken* [09a].
- IEC 27002 - **control**: *measure that maintains and/or modifies risk [22d]*

Det Norske Veritas (DNV) use the term barrier in the context of cybersecurity in their work [DNV16], using the exact wording as the definition for a *security countermeasure* in IEC 62443. This definition is therefore used in this work when addressing cybersecurity barriers.

Performance requirement

A central aspect of the barrier management process is maintaining the performance of barriers [Nor17]. This process involves predefining performance requirements and continuously measuring the barrier conformance. Standards and guidelines presented in 2.3 define different concepts for addressing the performance aspect of assets. IEC 62443-2-1 defines security levels and performance standards [10]. The

series highlights that cybersecurity levels of assets must be measured and managed throughout the asset life cycle to maintain sufficient performance [09a]. Addressing cybersecurity only at the start and end of a project results in declining security levels over time, motivating a collective, organization-wide management approach to asset cybersecurity [09a].

The concepts presented are applied in the later discussion of identified use areas and challenges for the Digital Twin technology for cybersecurity. The technology in light of I4.0, trends, and enabling technologies relevant to the scope of this work is introduced next.

2.4 Digital Twins in Industry 4.0

The term "*Digital Twin*" gained popularity when NASA's John Vickers introduced it in 2010 [DNV21]. However, its origin is traceable back to the 1960s, when NASA precisely replicated each voyaging spacecraft and used it for study and simulation purposes [IBM20]. Since this, the concept of Digital Twins has matured and developed, and the industry speculates that it to reach a market value of USD 35,8 billion by 2025 [ESBC19]. This section will present the Digital Twin in the light of Industry 4.0 (I4.0), give an overview of some of the essential enabling technologies and the state-of-the-art, and present previous works regarding the Digital Twin from a cybersecurity perspective. Section 4.2 presents a more extensive literature review on the Digital Twin based on the initial analysis of use areas.

2.4.1 The Digital Twin

Simulation of systems or assets is not a new concept. However, in the era of I4.0 the bridge between the physical and virtual environments has become more prevalent [HV20]. A Digital Twin is a digital representation of a process, object, or system facilitated by the advancements of ICT, communication technology, and Machine-to-Machine (M2M) communication [PHH22]. It provides the ability to generate a complete lightweight replica of a system, sub-system, or complex systems of systems, bridging the data, information, and knowledge collected from the physical component into the virtual replica in real-time [Gri15; HV20]. The concept of real-time analysis and control of a system as a whole in a connected real-and-virtual world provides opportunities in several use areas of the life cycle of industrial systems. DNV (2021) define a Digital Twin as:

> *a virtual representation of a system or asset that calculates system states and makes system information available, through integrated models and data, with the purpose of providing decision support over its life cycle [DNV21].*

Additionaly, Hartmann and Van der Auweraer (2020) defines that the Digital Twin:

> *...integrates all data (test, operation data,...), models (design drawings, engineering models, analyzes, ...), and other information (requirements, orders, inspections, ...) of a physical asset generated along its life cycle that leverage business opportunities.*

The roles and use areas of the Digital Twin are becoming more frequently discussed in the literature, as the numerous applications across the processes industry and life cycle of an asset become evident [WGE+17; PVU+19; FPPD22]. One enabling factor is more affordable and compact sensors, increasing the ability to communicate, process, and collect information [ASM+21]. The conference paper by Holmes *et al.* (2021) presents applications of the technology, along with some arising cybersecurity challenges [HPM+21]. Firstly, Digital Twins are a great source and generator of data that can be analyzed for optimization and planning purposes, allowing for more efficient business decisions and optimizing process performance [MT21]. Secondly, using Digital Twins as an emulator that presents real-time data and can act on the input data provides a virtual mirror-version of the physical system [IBM20]. Lastly, using Digital Twins in cybersecurity allows for the execution of security analysis, such as attacks and defenses, to assess security levels [HPM+21].

Maturity Level of the Digital Twin

The Digital Twin concept is evolving from the traditional use of simulation and emulation of systems and components into a virtual environment [IBM20]. The definition provided in Hartmann and Van der Auweraer (2020) states that the Digital Twin has the capability of collecting and integrating data through the life cycle of the asset to leverage business opportunities [HV20]. This definition does not incorporate performance requirements, communication capabilities between the physical and virtual twin, or level of autonomy [HV20]. Consequently, the Digital Twin concept implies diverse systems with different capabilities and challenges. In order to address the specter of available definitions, it is essential to differentiate between Digital Twins possessing different capabilities.

Maturity level is a tool for assessment of the effectiveness of a system and supports the identification of capabilities needed to improve performance [PB16]. Several sources propose a five-level maturity spectrum or model, with capabilities ranging from mirroring to autonomy [ESBC19; KYL+20]. The five-level model defined by Evans *et al.* (2019) form the basis of Figure 2.4, where the most promising capabilities are possessed by levels 3, 4, and 5 of Digital Twins.

Moving towards higher levels increases the level of autonomy, implying reduced human involvement. Further, this development through levels induces increased complexity, connectivity, and value [ESBC19].

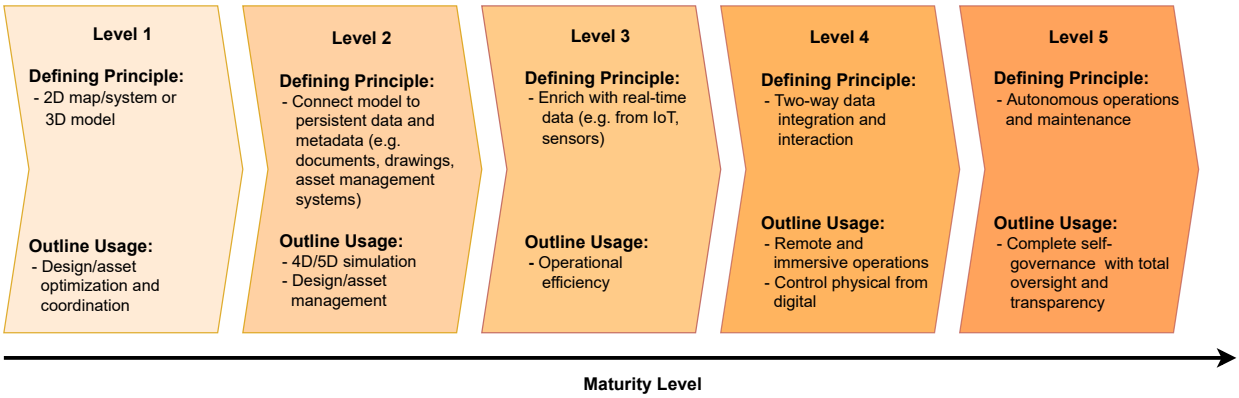

Figure 2.4: The five maturity levels of a Digital Twin/AAS defined in [ESBC19]

Echo Digital Twin

Equinor initiated a first-wave project in 2017 to make the plant more digital. One part of this project was the development of the Digital Twin, the Echo. Echo provides the oil rig operator with a 3D model that functions as a tool in "*planning, support, optimization follow-up of operations and maintenance*" by displaying life cycle information and data from sensors [LTS+20].

2.4.2 Trends and Enabling Technologies of I4.0 and the Digital Twin

In the petroleum- and manufacturing industry Industry 4.0 (I4.0) is characterized by inter-connectivity, automation of industrial processes, and manufacturing using smart technology, e.g., augmented reality, IIoT and CPSs [TTAA18]. I4.0 brings evolution to automation of processes, digitization, standardization, and openness. This evolution is facilitated, for instance, by the extensive amount of data available from implementing IIoT in industrial processes [WGE+17], giving traditionally unaware and isolated assets of production pipelines internet connection. Some benefits of this digitization are improved efficiency in production, reduced costs, and improved communication and self-monitoring enabled M2M communication [JGW21]. This section will present essential and predominant technologies in I4.0 for realizing the Digital Twin and the plant life cycle, presenting its benefits for the petroleum industry.

Several technologies lay the foundation for the evolution of the process industry, including cloud computing, the Internet of Things (IoT), Machine Learning, M2M communication protocols, and CPS. The following paragraphs will introduce some of these technologies to present the state-of-the-art security considerations and opportunities following the era of I4.0.

Cyber-Physical Systems (CPS)

The NIST Cybersecurity Framework (CSF) defines CPS as "*engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components*" [oST18]. CPSs provides an extended version of real-world, physical objects. The interconnection of objects and their digital descriptions enable this extension. Information stored in models and data objects that can be updated in real-time represents an additional, second identity of the object itself [SSH+18b].

In 2006 CPS was declared a national priority by the Council of Advisors on Science and Technology [RG22], and are considered an essential technology in I4.0 [KYL+20]. Current terminology and descriptions make it challenging to differentiate between a CPS and a Digital Twin, as they both present digital extensions of physical objects facilitated by interconnection and digital descriptions [KYL+20]. Some research papers apply the terms interchangeably [KYL+20].

Industrial Internet of Things

Gartner defines the IoT as "*the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment*" [22a]. The IoT comprises sensors, actuators, and other intelligent terminal equipment connected to a physical object and the Internet [NK19]. It relies on mobile intelligent terminal devices and wireless communication technology to help operators monitor equipment reliably in near real-time [NK19]. These capabilities can dramatically affect productivity and real-time decision-making [NK19].

In the context of the petroleum sector, the concept is taken one step further into the IIoT [SSH+18b]. The purpose of introducing the IoT into this domain is to understand the manufacturing processes better and enable efficient and sustainable production [SSH+18b]. The amount of available data is expanding together with the increasing number of internet-connected devices [ZPG12]. Unlike the conventional IoT networks, the IIoT networks take into consideration both the volume and characteristics of the data [ASM+21]. Many IIoT systems rely on cloud or edge computing due to the large amount of data that requires storage, processing, and analyzing [ASM+21].

When IoT paradigm is merged with the idea of the CPS, the I4.0 concept emerges [ASM+21]. This is visualized in Figure 2.5 where IIoT is a subset of IoT, and I4.0 is the intersection of all the above concepts. IIoT is one of the main enabling technologies for realizing the Digital Twin and vice versa. The Digital Twin can also be interpreted as a proxy, solving the challenge of seamless integration between IIoT and data analysis using edge and cloud computing [JGW21].

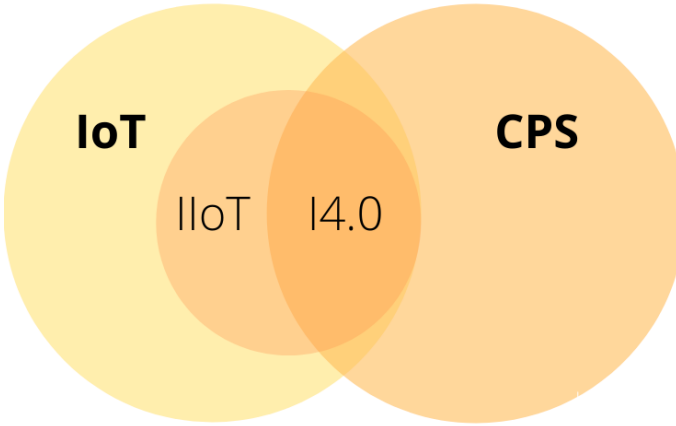

Figure 2.5: The connection between IoT, IIot, CPS, and I4.0. Inspired by [SSH+18b]

Machine-to-Machine Communication

Gartner defines that Machine-to-Machine (M2M) communications is used for "*automated data transmission and measurement between mechanical or electronic devices*" [22a]. It is a core concept in I4.0, allowing exchange of information between the CPS which constitute the I4.0 production environment [22c]. The M2M environment consists of the physical machine, the server, and the communication network [22c]. The physical part implements the protocols for communicating with the machine and sending information, and the server manages the sending and receiving of information. Some of the positive impacts of the technology are remote control enabled by applications, cost reductions, automation of processes due to Artificial Intelligence (AI), and better real-time monitoring [She19]. M2M systems face several security issues, ranging from device hacking to unauthorized access to wireless intrusion [She19]. One must address physical security, privacy, fraud, and the exposure of mission-critical applications to implement M2M communication securely [She19].

2.4.3 Asset Administration Shell

Simulation and emulation are just two of many benefits and capabilities of the Digital Twin in the planning and operation of the plant. To eliminate the need to differentiate

between a pure simulation model and the Digital Twin, Wagner *et al.* (2017) propose the Asset Administration Shell (AAS) as a synonym for the implementation of the fully enriched version of the Digital Twin. This work will use the terms *Digital Twin* and *AAS* interchangeably. However, the definition of the AAS is important to present the state-of-the-art Digital Twin.

The process industry uses the term AAS for the implementation of the Digital Twin [YHS+21]. The implementation aims to describe an asset electronically in a standardized manner [YHS+21]. The German Plattform Industrie 4.0 glossary defines AAS as a "*digital representation of an asset*" [21d], where *digital representation* is further defined as "*information in the digital information world that represents characteristics and behaviors of an entity*" [21d].

The definition of these concepts is hard to follow for non-experts, and Wagner *et al.* (2017) stress the need for a more precise vocabulary for the Digital Twin and the AAS [WGE+17]. An AAS holds the set of all available information of an asset, and also contains the specific asset's administration interface [4020]. The data object contains all data related to the asset it represents, which means it essentially makes up the virtual representation of the asset. This virtual data is accessible to other I4.0 components through the administrative interface [4020]. This 3-level model of a CPS enables the continuous, real-time updating and availability of asset data and status, usable, for, e.g., system optimization [MG19].

Figure 2.6 illustrates the AAS. A deployed AAS implements several sub-models, each representing the asset's functions, aspects, and information. This sub-model structure in software makes the AAS simpler to work with, easier to comprehend, and possible to share and update [WGE+17]. Displaying the overall platform model through an interconnected set of AASs allows for testing dependencies, events, additions, and other system changes in the virtual, information-updated, and enhanced Digital Twin [WGE+17]. It will provide the operators and engineers with the information and data of the assets throughout their respective life cycles, as the data is stored and preserved within the AAS [WGE+17].

Communication Capabilities

The three alternative types of information exchange via the AAS are the passive AAS, the re-active AAS, and the pro-active AAS (Figure 2.7). These can be seen as similar to the five maturity levels of the Digital Twin. The passive AAS is utilized for file exchange between value-chain partners where asset information is stored in the AAS in a unified data format [4020]. The re-active AASs have the capability of exchanging information between one another or other software applications through an API, ensuring seamless communication to the OT and IT networks [BETW21]. The third type of information exchange uses a I4.0 language and defines the pro-active

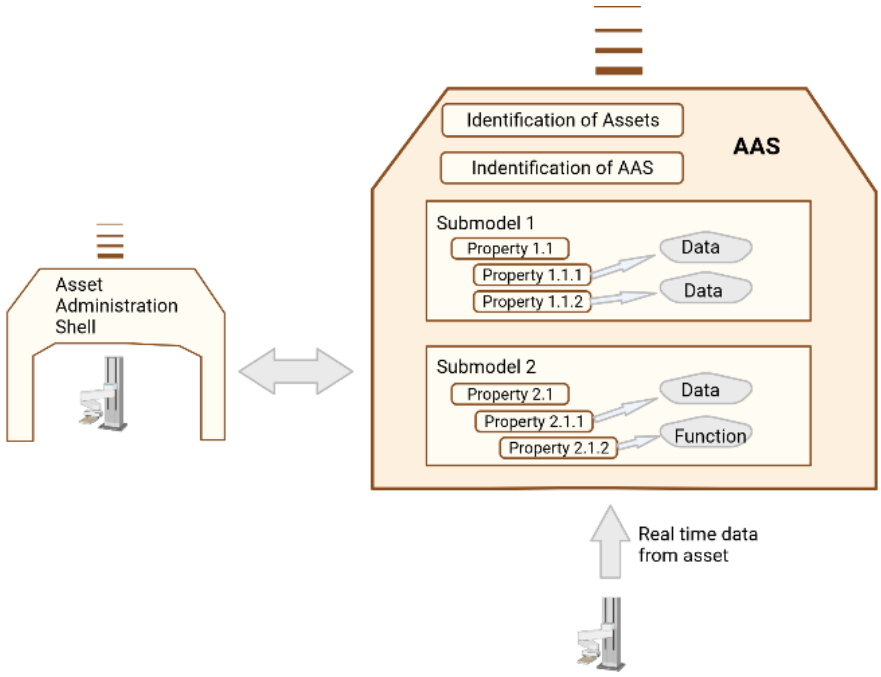

Figure 2.6: An overview of the parts of an Asset Administration Shell. Derived from [WGE+17]

AAS. This type of AAS has the capability to autonomously initiate active behaviour and communication with one another in a peer-to-peer environment. Plug-and-play scenarios assisted by AAS between I4.0 components is an example of a pro-active AAS use area [4021b]. Open Platform Communications United Architecture (OPC UA) (2.4.3) is chosen by the German Plattform I4.0 as the standard communication protocol between assets [BETW21].

RAMI 4.0

German standardization and industrial standardization organization developed Reference Architecture Model Industry 4.0 (RAMI 4.0) as a guide for the implementation of I4.0 technology and components [PFKK16]. Figure 2.8 illustrates the three-dimensional, layered RAMI 4.0 model to provide a common language and structured framework that describes the requirements of I4.0.

A challenge with adopting RAMI 4.0 is that it is currently more a concept and not a solution [MG19]. It does not specify which communication technologies, programming standards, or integration tools should support the functionalities of

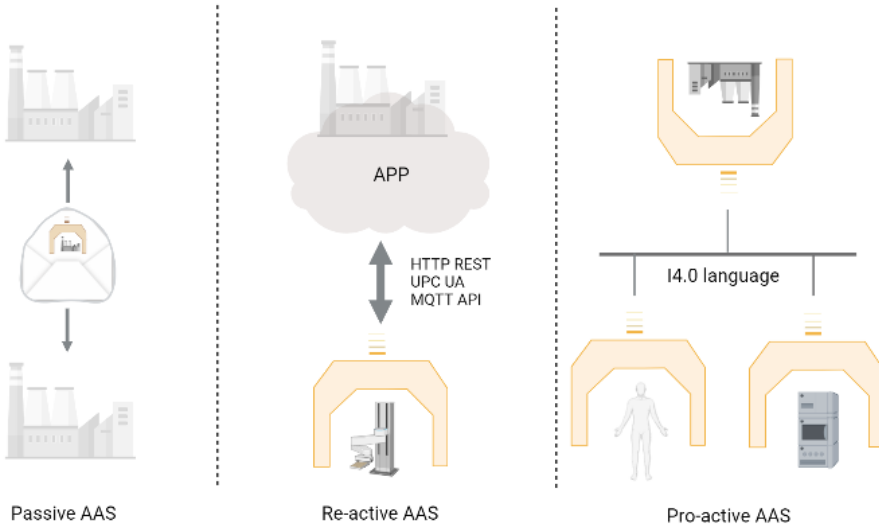

Figure 2.7: Three different types of information exchange via the AAS. Inspired by [4021a]

each layer [MG19]. The recent work focus on the development and standardization of these solutions [MG19].

OPC UA

OPC UA is a M2M protocol for industrial communication and information modeling, first published in 2008 [PVU+19; MG19]. It has gained popularity in the last couple of years, being selected by many leading companies in the German Plattform Industrie 4.0 as the most important M2M protocol [PVU+19]. The protocol aims to ensure secure communication across platforms between IT and OT. OPC UA contains an information model for enhancing data with semantics. This model can be used to describe all devices in a system, and the protocol is highly customizable [PVU+19].

NAMUR Open Architecture

The basis of the I4.0 is the availability of data within a network [TTAA18]. Both sender and receiver must reconcile the syntax and semantics of the exchanged data to facilitate M2M communication [PFKK16]. Figure 2.9 illustrates the simplified NAMUR Open Achitecture (NOA) architecture, consisting of the core process control

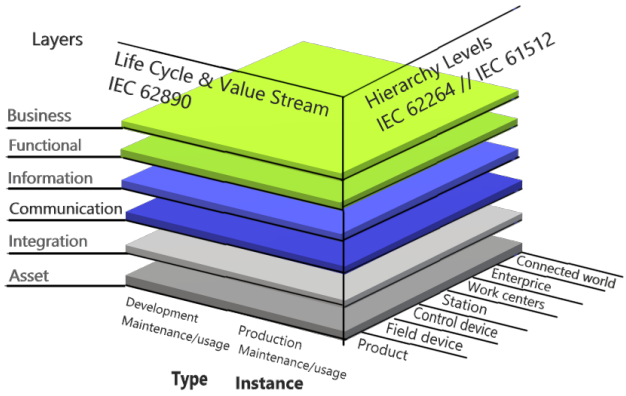

Figure 2.8: RAMI 4.0. Adapted from [PFKK16].

and Monitoring and Optimization (M+O) [NAM21]. NOA is a framework aiming to provide secure and easily usable data for monitoring plants and assets as well as optimization, and describes how this can be executed by the use of open interfaces and data diodes [NAM21]. NOA consists of five building blocks [NAM21]. Three of them are the *NOA information model*, providing the syntax and semantics of data exchange between the Core Process Control (CPC) and the M+O applications, *NOA Diode* enabling secure communication from the CPC to M+O applications, and *verification*, enabling a controlled data flow to the CPC domain [NAM21].

The information model ensures non-proprietary and flexible communication within the NOA architecture. This NOA Information Model will serve as an integrative information space for plant data. A standardized information model guarantees that all applications in the area of M+O, without individual configuration efforts, will know which parameters to expect and in which form [NAM21]. The basis of the unified interface to the parameters is OPC UA as a default [NAM21].

In the context of increased cybersecurity, improvement of security barriers to improving safety factors should be included. Onshus *et al.* (2022) specifically states that NOA do not account for secure communication between SIS and the Digital Twin.

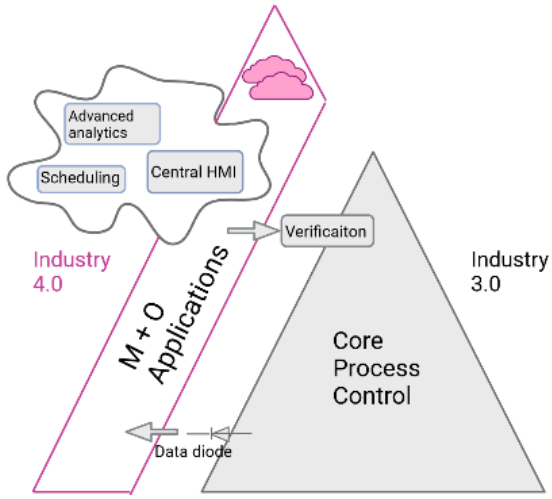

Figure 2.9: NAMUR architecture. Inspired by [NAM21].

2.4.4 The Plant Life Cycle

The realization of I4.0 can significantly benefit the life cycle of both product, machine, factory, and plant [WGE+17]. The plant life cycle is a continuous development process, including the plant's planning, operation, reconstruction, and termination. This holistic manufacturing approach can address two main concerns in cybersecurity; supply chain management; and security by design [EE19; ESBC19]. The following paragraphs will provide an overview of the product and plant life cycles of both Industry 3.0 (I3.0) and I4.0 to illustrate some of the possibilities induced by I4.0 components in the petroleum industry.

The plant life cycle of I3.0 consists of planning, requirement definition, configuration, implementation, and testing before delivering the system to the stakeholders [WGE+17]. Some of the challenges in I3.0 are related to updates and re-calibration of devices and systems [WGE+17]. Finalizing plans and documentation in the early stages of the life cycle, without updates about software and hardware changes during commissioning, results in a divergence between plans and reality [WGE+17]. Another challenge presented by Wagner *et al.* (2017) is the lack of a common database for all engineering tools used in the plant, together with inconsistencies and misunderstandings induced by the number of different vendors with different regulations and views. I4.0 aims to provide technologies and frameworks to mitigate these challenges and many more.

I3.0 devices such as sensors, pumps, and motors have no awareness of their surrounding components or systems [WGE+17]. In contrast, I4.0 devices and equipment can communicate over the Internet and explore their environment, allowing them to communicate their functionality, register themselves to the system, and identify themselves [WGE+17].

The result of the I4.0 plant life cycle is a comprehensive information model of the plant. This model contains all documentation from the planning phase, all implicit knowledge and assumptions made by the engineers, and all manufacturing catalogs. The object model is used to build, configure and test the plant before operating. Components can communicate with other components, and the automation solutions through a standardized I4.0 administration [WGE+17]. Figure 2.10 presents cybersecurity use cases for the Digital Twin in the plant's life cycle, based on the previous works of [EE19].

The modification of the life cycle from I3.0 to I4.0 results in a comprehensive digital instance model of both plant and assets, ensuring efficient accessibility of all relevant information. This instance model is updated continuously with real-time data from assets, sensors connected to assets, and IoT devices [WGE+17]. Gathering information from assets is one of the three main stages of the fourth industrial revolution. The other stages are analyzing and visualizing data through a cloud service and converting information into meaningful results [LLC18]. These stages represent potential cyber threats by relying on underlying Internet connections and communication between assets and the cloud [KHA+20]. Previous works have stressed considering this problem area before I4.0 can be implemented on a large scale [KHA+20]. Less research exists on how this implementation can improve cybersecurity by providing a complete overview of assets and potential vulnerabilities.

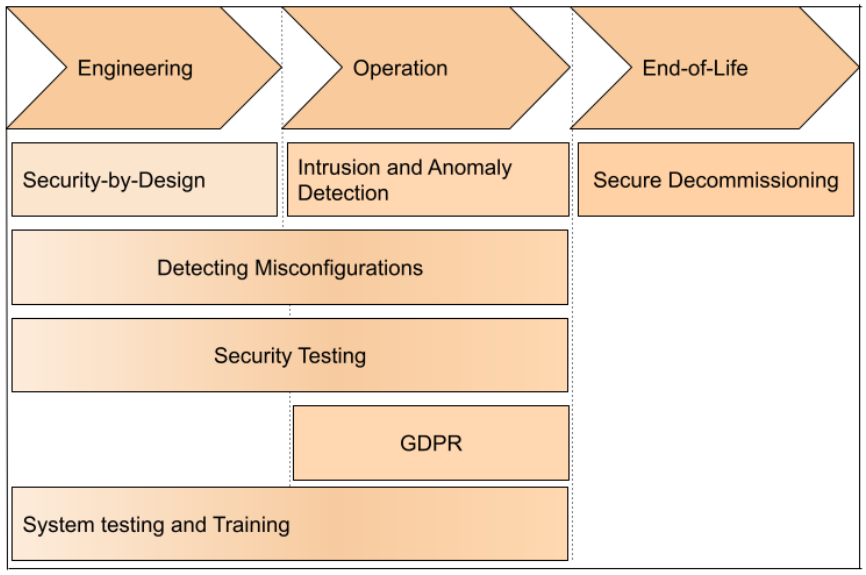

Figure 2.10: Previous works defining use areas for the AAS in the life cycle of a plant. Based on [EE19].

Chapter 3
Methodology

The following chapter presents the applied research methods and approaches used to derive the results of this thesis. Section 3.1 starts by presenting an overview of the chosen research design. Section 3.2 presents the data collection methods, which involved performing literature studies (3.2.1) and interviews (3.2.2). Next, Section 3.3 describes the method used for analyzing the data. Finally, Section 3.4 will address the trustworthiness of the conducted research evaluated through three concepts: Validity, generalizability, and reliability [RM16]. Figure 3.1 provides an overview of the methodology.

3.1 Qualitative research

This section will address and explain our use of qualitative methods as the research design for this thesis.

Digital Twins benefiting the different aspects of the plant life cycle is a developing field of interest and research in the Norwegian petroleum industry [WGE+17]. Following the increasing interest and implementation initiatives in the industry, the possible effect on cybersecurity in the industry becomes important to address [HPM+21]. In this thesis, we aim to create a deeper understanding of how the technology can be utilized to benefit cybersecurity and which considerations the industry must address to promote security and safety. The initial research suggests that the maturity of the selected problem area remains low. However, attributes of the technology and exploratory studies indicated that cybersecurity in the petroleum industry is an interesting use area for the Digital Twin.

The low maturity of the subject affected our access to interviewees with knowledge and understanding of cybersecurity in critical infrastructure and Digital Twin technology. As a consequence of the lack of maturity, we chose to conduct a qualitative study. Our observation of the limited amount of research and implementation of the Digital Twin and its implications and potential benefits for cybersecurity lay the

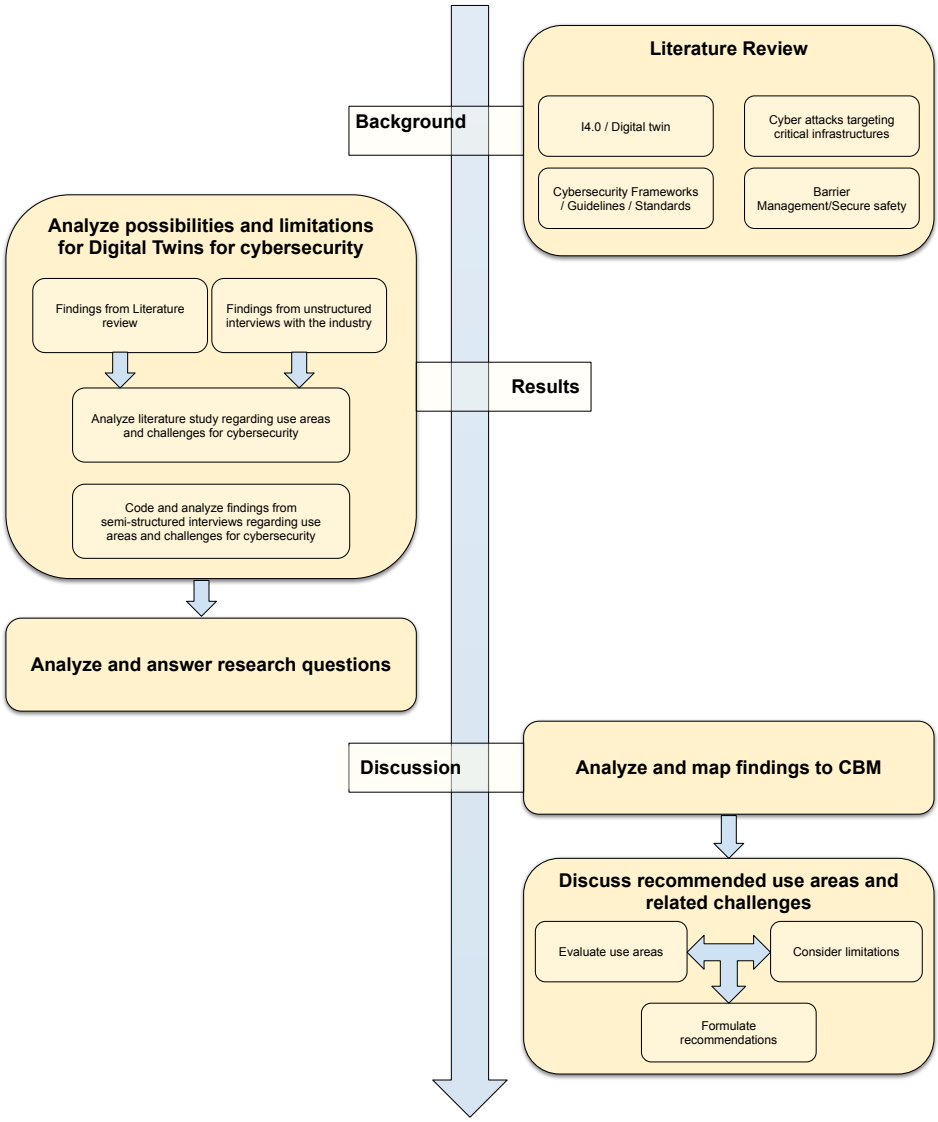

Figure 3.1: A complete picture of the methods used in the thesis.

basis for this thesis. This statement is compliant with qualitative research where the study is grounded in observations and not so much existing theory [BWG20]. The choice was made to facilitate in-depth insights on a subject and topic not previously clearly defined or investigated [BWG20]. The approach enabled us to understand how the Digital Twin technology can aid in the cybersecurity domain, what the relevant literature and the industry view as its most valuable aspect, and which limitations to consider. The literature studies and the interviews provided a holistic view of the context of study, in line with Miles and Huberman (1994) description of qualitative research.

We chose an inductive research approach to explore how the Digital Twin can affect the Norwegian petroleum industry's cybersecurity. The inductive approach allows the development of a theory based on observations and observation patterns [MH94]. This argument implies that we can develop a theory about the use areas of the Digital Twin within the cyber domain based on observations from literature and interviews. Opportunities and challenges make up the categories used for the empirical data. The former addressed the benefits and opportunities and highlighted motivational factors for implementation. The latter involved challenges and limitations to address when adopting Digital Twins.

3.2 Data Collection

A central activity when conducting research is data collection [JP21]. Johannesson and Perjons (2021) lists questionnaires, interviews, focus groups, observation studies, and document studies as the five most commonly used means of data collection. We based the research on two of these: interviews and document studies in the form of a literature review [JP21]. The methods were conducted as two separate data collections and analyses. However, their execution was parallel due to the time constraint.

3.2.1 Literature review

Literature studies aim to identify and combine as much relevant and updated research as possible regarding a defined research question [TDS03]. The results of a literature study provide a foundation for advancing knowledge by integrating several empirical findings [TDS03]. The reviews can have a systematic, semi-systematic, or integrative approach and should be verifiable and well-documented [Sny19; 22e]. Robson and McCartan (2016) describes this method of data collection as:

systematically identifying, locating, and analyzing documents containing information related to the research problem.

Furthermore, Machi and McEvoy (2021) defines the six steps of the literature review as:

1. Select and define a topic - *Recognize and define a problem.*
2. Develop tools of argumentation - *Create a process for solving the problem.*
3. Search the literature - *Collect and compile information.*
4. Survey the literature - *Discover the evidence and build the argument.*
5. Critique the literature - *Conclude.*
6. Write the review - *Communicate and evaluate the conclusions.*

One basis for choosing a literature study as an additional data source in our qualitative study was the difficulty of finding enough candidates with deep insight into the Digital Twin for cybersecurity. As the objective of this work was to provide valuable insight for implementing the technology, we spent much time investigating technical specifications, possibilities, and limitations. The following sections will describe the selection of review types, and the execution of the reviews throughout steps one, three, and six, defined by Machi and McEvoy (2021).

Selecting the Literature Review Type

The literature reviews in this study motivated the research, provided relevant background, and aided in answering the research questions. Due to the novelty of the research area and the limited time frame, a combination of the semi-structured and integrative literature review was chosen as our approach in the document study [WGW+13; Tor05].

A semi-systematic literature review is suited for topics like the Digital Twin, where groups of researchers have studied the subject across various disciplines [Sny19]. The various groups of researchers and the number of documents on the subject hinder a complete systematic review process [Sny19]. This part of the review aimed to identify and understand the attitude and opinions in the literature regarding Digital Twins and cybersecurity. The integrative and semi-systematic reviews are closely related [Sny19]. The integrative review creates preliminary concepts and insights, using a more creative collection of data [Sny19]. This part of the review aimed to find, review, and structure relevant literature and conceptualize the emerging topic of Digital Twins for cybersecurity.

Figure 3.2 provides an overview of our execution of the literature studies through some of the relevant steps defined by Machi and McEvoy (2021). As displayed in the figure, we conducted two iterations literature studies to define the topics and include literature. The first iteration aimed to identify five areas for further study. This step complies with the inductive research of the qualitative method, where we aimed to observe areas of interest to develop our theory about the technology's

potential [BWG20]. This iteration resulted in a set of technical reports, research papers, identifying five potential use areas. The areas identified in the analysis of the initial search and coding from the initial interviews (Sec. 3.2.2) lay the basis for the second iteration of the search. This search iteration aimed to derive the use areas and challenges for the Digital Twin in cybersecurity and contribute to the final answer to the research questions. The following sections will describe the method for deriving the topics for the literature study and the inclusion and exclusion of literature. Section 3.3.2 presents the methods used to analyze the literature studies.

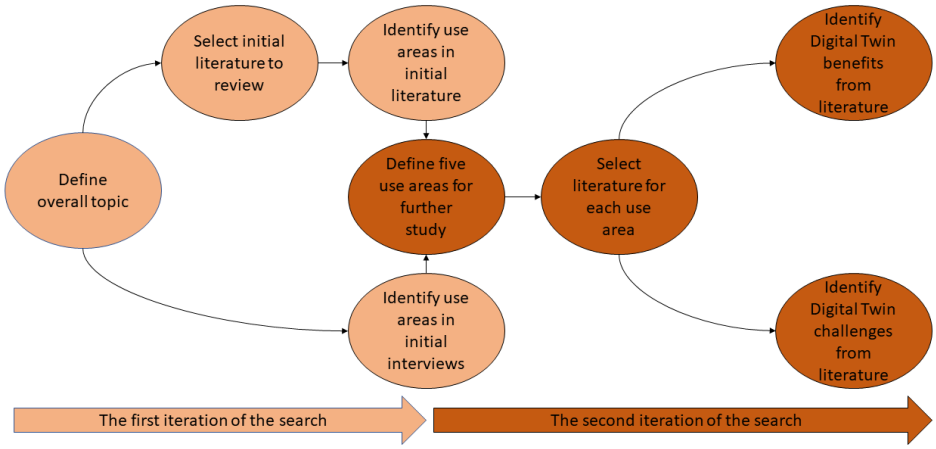

Figure 3.2: The two iterations of the literature search.

Step 1: Select and define a topic

The selection and definition of the overall research topic resulted from the pre-project [PH21] and represent the first oval in Figure 3.2. We initially decided to write our thesis about how the Digital Twin technology could affect cybersecurity in the Norwegian petroleum industry. We identified a knowledge gap based on relevant articles and industry conversations, which resulted in the research questions presented in Chapter 1. The five topics derived from the initial analysis defined the topics for the second iteration of the search. This is visualized by the first dark oval in Figure 3.2.

Step 3: Select the literature to review

In this step, we defined the inclusion and exclusion criteria for selecting the relevant literature. The research question set an initial boundary for the literature search and included two main survey areas: cybersecurity in Norwegian petroleum and Digital Twins in a cybersecurity context. The result from the first survey area is presented in Chapter 2 and is used to provide context for the discussion. The result from the second survey area is presented in Chapter 2 and Chapter 4. This section will focus mainly on the criteria defining the latter's scope, which lay the basis for the analysis. Both iterations of the search consisted of three main stages for selecting the literature: scanning, skimming, and mapping.

Scanning In this stage we scanned the library materials for sources. In the first iteration of the search we selected the relevant sources to the subject of both Digital Twins and cybersecurity in the petroleum industry, using online libraries, such as NTNU Oria, Science Direct, and IEEE Xplore. Because of the limited availability of primary studies on Digital Twins concerning cybersecurity in the petroleum sector, we also choose to include secondary studies and web articles. Table 3.1 shows the keywords used to scan the library materials in the first iteration of the search. For specific keywords, synonyms such as *Oil&Gas* for *petroleum* were used to detect more relevant documents. We repeated this step in the second iteration of the search, with the keywords resulting from the five identified use areas.

Table 3.1: Keywords used in the first iteration of the search for the two survey areas of Cybersecurity in the petroleum industry and Digital Twins.

Category	**Search query**
Cybersecurity in Oil & Gas	Cybersecurity AND Petroleum
	Cybersecurity AND Countermeasure AND Petroleum
	Cybersecurity AND Barrier AND Petroleum
	(Standard OR Guideline OR Framework) AND Security AND Petroleum
Digital Twin	Digital Twin AND Petroleum
	Digital Twin AND Cybersecurity
	Digital Twin AND Challenge
	AAS AND Cybersecurity

Snowballing Systematically searching several databases do not guarantee to identify all relevant literature [Sny19]. Because of this, researchers recommend studying the reference list of the most central articles [Sny19]. When collecting the sources, we used both forward and backward snowballing. With backward snowballing, we scanned the reference list of relevant literature to identify other articles of interest.

With forward snowballing, we found other articles citing the literature of interest. These measures had the purpose of identifying further relevant research.

Skimming In this stage of selecting the literature, we skimmed the sources to determine the appropriateness of the study's inclusion and exclusion criteria. The abstract, conclusion, and table of contents provided the article's essence and made the basis for inclusion or exclusion [MM21]. Due to the research subject's originality, the publication date was not a strict exclusion criterion. However, the majority of the literature was published between 2020 and 2022. The main interest in the first iteration of the search was literature regarding cybersecurity and barriers, problem areas concerning the petroleum industry, Digital Twin development and enabling technologies, and Digital Twin for cybersecurity. Because of the size of the result set and limited time, we mainly skimmed the most cited publications and prioritized the ones including more of the search terms. This review stage resulted in a set of initial relevant articles, presented in Table 3.2, for further analysis and mapping to define the topics for the second iteration of the search. There is only a limited number of articles as its primary purpose was to derive use areas for further study.

Mapping After selecting the relevant articles by skimming their contents, we did a more extensive reading to define the main subjects addressed in each article. The objective of the first iteration of the search was to identify five interest areas of the Digital Twin for cybersecurity. Section 3.3.2 presents the methods used to map and analyze the result of the first iteration to derive these use areas. From Figure 3.2, these use areas mark the starting point for the second iteration of the search. We repeated this step in the second iteration of the search to map and code the article contents, identifying the use areas and challenges for the Digital Twin in cybersecurity.

Step 6: Write the review

In the last step of the process, we reviewed the materials gathered to write the review, refining the work by auditing, and editing until the completion of the project. The final review is presented in Chapter 4.2.

3.2.2 Interviews

The interviews represented a second data collection method in our qualitative study. Robson and McCartan (2016) describe three different types of interviews based on their level of structure. The three types are structured, semi-structured, and unstructured interviews. An extreme example of a structured interview is the survey interview. The questionnaire used in such interviews uses standardized wordings with fixed questions in a pre-decided order. Interviews are semi-structured if the questions

Table 3.2: Overview of the literature identified in the first iteration of the search.

Source	Title	Author	Type
[HV20]	Digital Twins	Hartmann and Van der Auweraer	Article
[PHH22]	Implementation of Digital Twins in the process industry: A systematic literature review of enablers and barriers	Perno, Hvam, and Haug	Article
[HPM+21]	Digital Twins and Cyber Security - solution or challenge?	Holmes *et al.*	Conference Paper
[BETW21]	Secure Usage of Asset Administration Shells - An Overview and Analysis of Best Practises	Bröring *et al.*	Article
[PKC20]	Digital Twin for Cybersecurity Incident Prediction: A Multivocal Literature Review	Pokhrel, Katta, and Colomo-Palacios	Conference Paper
[PVU+19]	The Industrie 4.0 Asset Administration Shell as Information Source for Security Analysis	Patzer *et al.*	Book
[BFP+18]	CyberFactory nr1 Securing the Industry 4.0 with cyber-ranges and Digital Twins	Becue *et al.*	Article
[FPPD22]	Digital Twin for Cybersecurity: Towards Enhancing Cyber Resilience	Faleiro *et al.*	Book
[WWP+20]	Digital Twin for the Oil and Gas Industry: Overview, Research Trends, Opportunities, and Challenges	Wanasinghe *et al.*	Article
[LaG19]	Developing a Digital Twin: The Roadmap for Oil and Gas Optimization	LaGrange	Article
[KYL+20]	Characterization of Digital Twin	Kim *et al.*	Article
[YHS+21]	An Industry 4.0 Asset Administration Shell-Enabled Digital Solution for Robot-Based Manufacturing Systems	Ye *et al.*	Article

act more as a guide, allowing adjustments on the order, wording, and inclusion or exclusion of questions. An unstructured interview usually only has predefined areas of interest. This interview type could be experienced more like a conversation as they usually are informal [RM16]. This work involved conducting unstructured and semi-structured interviews.

Unstructured interviews with professionals provided keywords and codes, which, together with the identified initial articles, provided a basis for deriving focus areas for the literature study (Sec. 4.1). The semi-structured interviews provided a parallel means for data collection that contributed insight into the motivations and limitations of Digital Twins for cybersecurity in a barrier management context from an industry professional's perspective. Digital Twins used for cybersecurity and barrier management are not widely documented, so the semi-structured interviews provided information about the industry's posture and opinions that was difficult to obtain and not covered in the literature.

Unstructured interviews

When defining our research questions and focus areas for the literature study, we used unstructured interviews. This interview type allowed the participants to discuss the topics of cybersecurity and Digital Twin technology within Oil&Gas to the extent that they deemed relevant. The conversations aimed to gain insight into the industry's interest areas within cybersecurity, barrier management, and Digital Twins. All areas were not relevant to all participants to the same extent. Hence the topics overlapping with the interviewees' expertise formed the base and focus of the conversation. Information on all areas was ensured by conversing with experts with different backgrounds.

Wildemuth (2016) uses the term *agenda* in the referral to a general interview guide consisting of topics or open-ended questions [Wil16]. As we did not have previous interview experience, utilizing an agenda ensured that the interest areas in the unstructured interviews were covered. The agenda mainly included neutral, open-ended questions and terms included in the research questions, such as Digital Twin, Cybersecurity barriers, and the Norwegian petroleum industry.

Semi-Structured Interviews

The semi-structured interviews provided industry experts' opinions on challenges and motivations regarding Digital Twins, cybersecurity, and barrier management. This approach was used in the four final interviews when the research questions and objective of the thesis were clearly defined. Semi-structured interviews are based around the interview guide [RM16]. The interview guide was generated based on the core topics of this work, initial literature reviews, and areas of interest highlighted

in the unstructured interviews. The semi-structured approach allowing adding, removing, and altering questions was necessary due to the novelty of the research area and combination of topics.

Interview Guide

An interview guide as a tool comprises an introduction followed by a list of topics. Each topic contains a set of key questions and associated prompts, ending with closing comments [RM16]. These elements formed the basis of our guide, where the prompts are follow-up questions. Wildemuth (2016) describes the development of an interview guide in the context of a semi-structured interview, comprising these three stages:

1. Outline main topics related to the objectives
2. For each topic, list relevant questions
3. Order the topics and subsequent questions into the preferred order

Our guide starts with introducing the researchers, presenting our background, and the context and goal for the interview and research. Next, the warm-up phase involved asking open questions and asking the subject to present themselves, including current work situations and relevant knowledge areas. The body of the guide involved topics, questions, and associated prompts. *Digital Twin*, *Barrier Management* and *cybersecurity* provided a frame for the questions, either alone or in combination. An outline of the guide used in the interviews is presented in Appendix A, where the wording, inclusion, and exclusion of questions varied between interviews based on their role in the industry.

Participants

With the goal of analyzing the potential that the Digital Twin technology could have on cybersecurity and barrier management in the petroleum industry, it was desirable to talk with experts from these domains. The roles involved, OT-expert, cybersecurity expert, Digital Twin experienced professionals, all of which had insight into the current cybersecurity strategies used within the petroleum industry. The final number of conducted interviews was six, which included two unstructured interviews and four semi-structured interviews.

The interviewees had expertise in different domains. Thus the opinions and insight they brought regarding their expert area were emphasized. The opening questions aimed to identify the participants' expert domain. This information made it possible to highlight the data mapping to their background and use this knowledge to discuss their respective statements. Table 3.3 presents the mapping between the semi-structured interviews and their focus areas. The second interview involved two

Table 3.3: Interviews mapped to their main areas of expertise.

Interviewee	Main expertise
Interview 1	Cybersecurity in OT
Interview 2	Digital Twins and cybersecurity in IACS
Interview 3	IACS security and safety
Interview 4	OT

participants, leading to a total of seven interviewees. The participant had similar expertise, and both will be referenced as "interviewee 2" in the result and discussion.

The recruitment of interviewees happened with assistance from supervisors and their connections. Before the interview, recruitment and communication took place through email involving the researchers, the supervisor, and the interviewee. The email exchange involved the research questions and a paragraph describing the thesis objective and goal. The researcher's theoretical background and knowledge provided additional context for the participants before the interview. The email exchange also included appointing a suitable time slot for all parties. Due to the ongoing COVID-19 pandemic, the interviews took place over Microsoft Teams.

Implementation

Regardless of the interview type, the interviewer's role is central. Specifically, the ability to generate responses through statements, clarifications, and questions, based on the interviewees' answers will significantly impact the results.

Robson and McCartan (2016) highlights the importance of obtaining a complete record of the interviews [RM16]. They state that record-taking can either be through later transcribed recordings or note-taking live during the conversation [RM16]. Neither interview phase required the documentation of personal information, only the expert opinions. Choosing note-taking as the documentation approach ensured informal and casual conversations. Both researchers took notes actively during the conversation to capture the essence of the interviewee's story. Robson and McCartan (2016) highlights that the action of taking a recorder is likely to remove the informal element [RM16].

By sending information about the research questions and areas before the conversation took place, the participant had the opportunity to think about elements they wanted to bring forward. The start of each interview included the participant's initial thoughts about the research area and questions. The researchers' interview experience grew throughout the work period. The low level of structure meant that large parts of the interview time involved the interviewee talking, where the

researchers listened, took notes, and provided follow-ups when relevant.

3.3 Data Analysis

Data analysis involves preparing, interpreting, analyzing, and presenting the data collected through one or more data collection methods [JP21]. Generally, qualitative data analysis is characterized as *iterative*, *inductive*, and *researcher-centered*. Analyzing qualitative data is often performed in parallel with the corresponding data collection [JP21]. We applied an inductive approach to analyze the collected data in this work. Inductive logic implies starting with a data set and use it to derive new ideas, and concepts [RM16]. With this work's novelty and exploratory nature, inductive data analysis proved suitable.

This section will present the methods we have used to analyze our findings from the interviews and the literature studies. We analyzed the two data sources separately before combining the results. Section 3.3.1 describes the extraction of thematic coding networks and the methods used to analyze the semi-structured interviews, and Section 4.3.3 presents the partial result derived from this analysis. Section 3.3.2 describes the derivation of initial use areas from the literature and the methods used to analyze the findings, and Section 4.2.3 presents the partial result derived from this analysis. Section 4.4 presents the results from the overall analysis of the two data sources.

3.3.1 Analysis of Interview Data

The data collected in one interview was processed, and the experience made adjustments in the following interview iteratively. Inductive analysis means going from specific to general. The specific data collected from conversations involve subjects' individual experiences and insight. This specific information can, to some degree, be generalized to a broader part of the industry through analysis. Lastly, the researcher-centered characteristic of qualitative data analysis indicates that the researcher's background, knowledge, and experiences influence the analytical results. As the researcher, in this case, will collect and analyze the data, the state of knowledge on the topics before the interview will affect the execution, and the post-interview analysis will logically be affected by the researchers' interpretation and apprehension of the conversation.

Coding is central in qualitative analysis. It involves the identification of text or data that exemplify the same idea and then grouping these into themes that capture something of interest [RM16]. The thematic coding approach was chosen for its high flexibility as it can work on all types of qualitative data. This coding approach is considered easy, requires limited experience, and is quick to apply [RM16]. These

factors motivated the choice as they suited the limited experience of the researchers and the small time frame of the study [RM16].

Robson and McCartan (2016) describes the thematic coding analysis as a generic approach to qualitative analysis, which involves five phases.

1. Familiarizing - *reading and re-reading the data and noting down ideas.*
2. Code generation - *Extract data and assign codes systematically through the dataset, assigning similar data the same codes.*
3. Identify themes - *Compare codes that address similar themes, generating potential groups of themes. Revise codes and themes if necessary.*
4. Construct thematic network - *Map the themes by "fitting them together" into maps.*
5. Integrate and interpret - *Compare the data, interpret patterns and communicate result.*

Step one involved reading and re-reading the notes taken from each interview. A conversation between the researchers followed each interview. Discussing each interview's essence and main contributions ensured a shared interpretation of the collected data. Reiterating and conversing post-interview allowed us to form an initial set of ideas about the data's essence, interest, and relevance to the research questions and objectives. Completing the second step resulted in extracted data and assigned phrases or code words that summarized the interpreted message. Words or sentences that stood out were highlighted if they addressed the scope of the research questions or presented an area the interviewee emphasized. During the previous stage, some potential themes were starting to show. The themes were visualized using tables to reveal relationships in this next step. Theme identification is the purpose of the third step. Techniques used during identification consisted of identifying repeating topics and words and identifying theory-related material that mapped to the research questions. Both techniques are acknowledged as methods to complete this step [RM16].

The codes from step two were revisited to verify and confirm interpretations and perceived coding correlations. These three steps of familiarizing, assigning code words, and grouping them into themes were iterated to confirm the interpretation. As Robson and McCartan (2016) states, the thematic coding approach is not sequential but iterative and overlapping [RM16]. Step four aims to construct one or more thematic networks [RM16]. This network were used in Section 4.3, where the headlines reveal the derived themes with respective sub-themes. The interpreted and analyzed data from each semi-structured interview are presented within each header. This network makes up the final step of generating meaning from the structured data and relating and using it to address the research questions. The network derived are roughly

visualized in Figure 3.3.

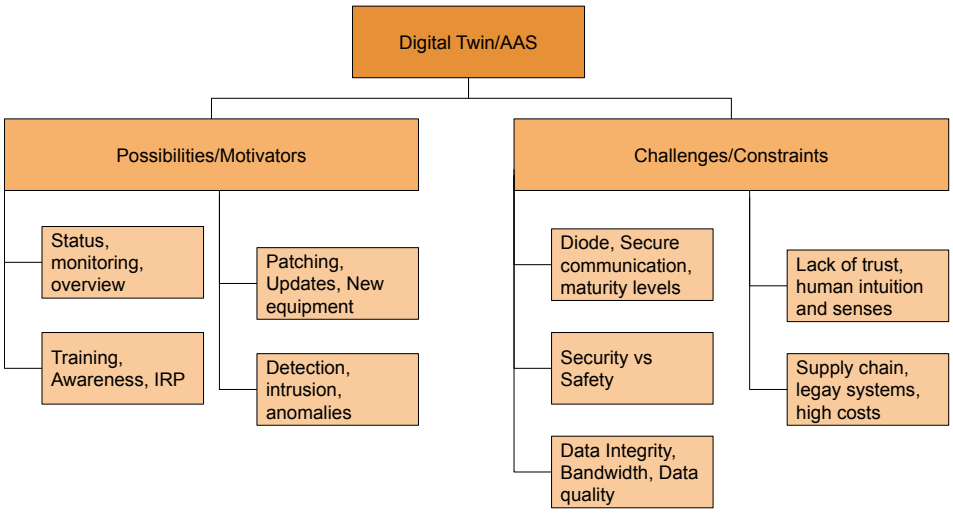

Figure 3.3: Thematic network derived through coding of semi-structured interviews.

3.3.2 Analysis of Literature and Final Results

As stated in Section 3.2.1, the literature study conducted in this work combines semi-systematic and integrative types of reviews. Several methods for analyzing and synthesizing the findings exist for both types. The analysis of the semi-systematic literature review is similar to the qualitative approach used for the unstructured and semi-structured interviews. This approach involves a thematic or content analysis for identifying, analyzing, and reporting patterns in the form of themes within the text. For emerging topics like the Digital Twin for cybersecurity, an integrative review is suitable to create preliminary concepts and insights. The analysis of this type of review is not developed according to a specific standard and is more creative in its execution. This data analysis examines the literature and the relationships of an issue's main ideas.

As visualized in Figure 3.2, two iterations of searches defined the literature study. The first iteration involved identifying five use areas for further study. Two initial analyses lay the basis for this identification: thematic coding of the initial articles in Table 3.2 and thematic coding of unstructured interviews. The use of unstructured interviews as an additional data source for the analysis complies with the experimental data collection defined by the integrative literature review. The coding of the unstructured interviews was similar to the semi-structured ones. The initial articles were coded inductively and grouped by the concept of cybersecurity

barriers to identifying use areas correlating with the scope of this definition. Section 4.1 presents the coded unstructured interviews and articles together with the result from the initial analysis. A mention in the interviews was weighted two points, and a mention in an article or seminar was weighted one point. This weighting strategy was chosen due to the limited number of interviews and to emphasize the industry needs and considerations. Using this simple scoring or frequency counting method, the use areas highlighted by these data sources formed the starting point for the second iteration of the search: the literature studies presented in Section 4.2. In this second iteration, we derived and analyzed the semi-systematic literature reviews deductively regarding the five identified use areas. The analysis divided the findings into thematic networks: use areas and challenges.

The Digital Twin for cybersecurity is an emerging topic with only a limited number of published articles. The purpose of the qualitative study in this work was to provide insight on the subject of Digital Twins for cybersecurity in the Norwegian petroleum industry; hence the integrative literature study and subsequent qualitative analysis combined the results from the different data sources. Table 4.6 presents the use areas and answers to research question RQ1. Table 4.7 presents the limitations, challenges, and answers to research question RQ2. These results were derived from the two separate analyses of the literature and the semi-structured interviews and are presented in Section 4.4.

3.4 Trustworthiness

When conducting an extensive study, such as a thesis, the trustworthiness of the research methods need evaluation to address the potential biases, limitations, and fallacies. Three aspects are generally involved in evaluating a study's trustworthiness [RM16]: reliability, validity, and generalizability.

Reliability

Reliability of the research indicates the level at which its processes and results can be replicated [RM16]. The reliability of the literature review and interviews lies in the study's potential to be reproduced. Interviews as a tool for data collection are hard to recreate completely, as other interviewers will not obtain the same data if the same people were interviewed [RM16]. The lower level of structure in the interviews and the use of non-fixed follow-ups made the data collected through this method challenging to recreate, stressing the need for continuous data comparison. As the literature selection and information extraction happened over a limited period, overlooking relevant available data may have affected this measure of trustworthiness.

The problem in flexible research approaches is that identical circumstances can not be replicated [RM16], making documentation of the activities conducted and the data collected critical elements to maintaining high reliability. Interview notes, data analysis, and additional data collected throughout the study were recorded in documents and kept for the duration of the study. Performing re-reading of the data and constant comparison contributed to increased consistency and accuracy, promoting reliability.

Validity

The validity of the research evaluates the "appropriateness" of the tools and methods used to answer the research questions [RM16]. The possible incompleteness of the data collected and researcher bias in data analysis are two threats against the validity of the research [RM16].

A challenge with unstructured interviews is when and how to intervene if the conversation moves beyond the predefined scope. Finding the right amount of control to guide the conversation is essential to ensure data quality. Analysis of the collected data from the interviews is a second challenge. The lack of a fixed structure, openness, and on-the-spot generation of some questions makes each conversation different, depending on where the interviewee chooses to direct their focus. Thus, post-interview analysis and conversation comparison were complex and might have been prone to researcher bias. The number of interviews and published literature on the research area were limited. This fact likely affected the level of completeness in the data.

Different measures can assist in increasing a study's validity. Relying on multiple data collection methods was one applied approach [RM16], referred to as *data triangulation*. This measure was applied by collecting data from attended seminars, interviews, and literature. Being two researchers also aided in the validity concern regarding researcher bias. Involving more than one observer is referred to as *observer triangulation*. The fact that two researchers were involved provided the opportunity for discussing the findings to confirm a shared interpretation and overall essence of the data. Debriefing after interviews promotes guarding against researcher bias [RM16].

Generalizability

Generalizability is a measure of the extent to which the research results apply outside the studied situation [RM16]. In other words, are the results applicable to areas outside the ones studied? This research focused on the Norwegian petroleum industry offshore. The interview data originated from this domain, whereas the collected literature stemmed from data on a more general level concerning the technology. A

challenge in the study was to achieve a high level of generalizability, making the results applicable outside the investigated domain.

The issue of generalizability also applied to the amount of conducted interviews. Due to the limited knowledge and experience with the combination of topics locating and obtaining a significant amount of subjects with the proper knowledge proved a difficult task.

The conducted research is an exploratory study on the possibilities and limitations of Digital Twins for cybersecurity. With this, we aim to contribute with knowledge and insights to a research area currently in its start phase of being established. This fact and the chosen research design limit the level of generalizability. However, the provided insights and knowledge can apply to other sectors to motivate exploring the Digital Twin for use cases related to cybersecurity.

Chapter 4
Results

This chapter presents the findings from the literature review and semi-structured interviews concerning Digital Twins for improved cybersecurity. Section 4.1 presents analyzed data from initial unstructured interviews and articles (Tab. 3.2), which narrowed down the selection of research areas in the literature study presented in Section 4.2. The results from the semi-structured interviews regarding opportunities and challenges the technology brings to the domain of cybersecurity are presented in Section 4.3. Lastly, the information from the two data collection methods is evaluated and used to answer the research questions:

RQ1 *How can the Digital Twin technology be used to improve cybersecurity in the Norwegian petroleum industry?*

RQ2 *What are the challenges that limit the industry from utilizing Digital Twins for cybersecurity?*

4.1 Implication of Focus Areas

Analyzing initial articles and interview data contributed to narrowing down the five focus areas. This process occurred in the research's early phases before initiating the two main data collection methods. The study's time constraint and broadness of the scope of Digital Twin possibilities and challenges motivated using initial articles combined with industry insight from unstructured interviews and seminars to derive a manageable sub-set of focus areas. Initial analysis of these two data sources together thus resulted in five use areas where the data correlated most, ensuring that the focus of the subsequent literature study encompassed insight of relevance to the Norwegian petroleum industry.

Unstructured interviews and Seminars

The unstructured interviews involved one professional with insight into security and safety in the Norwegian petroleum industry and one with Digital Twin experience. Data from industry forums covering security and safety further ensured applicability. The data were analyzed using the inductive approach described in Chapter 3, frequently mentioned words relevant to cybersecurity and barriers are emphasized in bold and visualized in Figure 4.1.

Initial Interview 1 The concept of **zones and conduits** provides a modeling tool relevant to the conversation addressing barrier management, cybersecurity, and Digital Twins. Predefined information flow, network **segmentation** and **firewall** were presented as benefits of the technology. This segmentation can aid in limiting information flow. Further, the current challenge regarding asset visibility and complete architectural overview was stressed. Obtaining a comprehensive overview of **asset status** and system processes would bring opportunities to routines concerning **patch management** and updating legacy assets. By aggregating and visualizing data in one location, **monitoring** and comparison advantages present additional benefits. One can measure if **requirements** are fulfilled and model the whole bow-tie. This overview will require choosing the correct sub-models for the AAS. The possibility of modeling no-technical barriers, such as humans, presents an interesting concept.

Initial Interview 2 **Anomaly detection** present one of the use areas of the Digital Twin beneficial in improving cybersecurity. Data accumulated over time provides the company with a solid foundation that allows for improved **reporting** and identification of abnormal activity by users and intruders. The technology can aid in improving preventative and reactive measures, where time is a specific critical factor. Another opportunity of the Digital Twin involves improved reporting of incidents and the possibility of using the Digital Twin for **prediction** and **attack simulation** for **training**, possibly improving decision making. **Incident reporting** today is poor. People need to gain an understanding of the criticality of incidents.

Seminars Topics of the seminars included cybersecurity and safety of IACS and SIS in the Norwegian petroleum industry. Each seminar presented current and future research projects and interests in these domains.

One concern raised in the first seminar involved **logging** and **reporting** as challenges that the industry is facing concerning ICT incidents. By having information readily available, better identification of **abnormal activity**, and **intrusion detection** is possible. One presentation stated that roughly 10,000 errors occurred before a successful cyber attack. With the high number of errors, it is difficult for an

operator to predict the potential impact of the exploit or vulnerability. In discussions involving simulation and Digital Twin technology, the benefits it would bring to **maintenance** and **patch management** became highlighted. Other use areas concerned Digital Twins and testbeds, emphasizing the possibility of **attack simulation** and **training**. System overview and asset status presented additional use areas for the technology. One organization is adopting a **barrier status panel** and acknowledges its advantages for keeping an overview of the countermeasures. However, this barrier panel did not display degrading barriers, which is hard due to the lack of system visibility. The bow-tie model was mentioned as a tool in barrier management and provided a well-known recognizable visualization of **defense-in-depth**. Finally, several presenters mentioned the IEC 62443 standard and the benefits of the **zones and conduits segmentation** approach.

The second seminar mentioned many of the same topics. During presentations involving the AAS concept, the presenter mentioned the benefits of **barrier status** visualization and how it addresses issues concerning system **overview** and legacy **asset status**. Again the bow-tie model was used in this context. One final mention was **intrusion detection** as a part of incident management, which in the context of control barriers involved the **detection** of abnormal activity.

Figure 4.1: Keywords from initial interviews.

Selection of research areas

Initial analysis of the articles collected in the first iteration of the literature review (Tab. 3.2) led to identifying potential use areas of the Digital Twin for cybersecurity. The literature addresses different potential benefits of the technology while addressing relevant challenges and implicit considerations with its adoption. These areas were derived by skimming the articles for relevant keywords with a strong relation to cybersecurity and barriers. Examples of such keywords are *firewall*, *segmentation*, *encryption*, *intrusion detection*, and *incident response training* [09a].

Table 4.1: Initially identified use areas of the Digital Twin.

Use area	**Literature**	**Interviews and Seminars**
Firewall	[BETW21]	Initial Interview 1
Intrusion and Anomaly Detection Systems	[HPM+21], [BETW21], [FPPD22], [LaG19], [PKC20]	Seminars, Initial Interview 2
Network Segmentation	[KYL+20], [YHS+21], [BETW21]	Initial Interview 1, Seminars
Monitoring and Status Assessment	[PVU+19], [WWP+20], [KYL+20], [PKC20], [HV20], [PHH22], [FPPD22], [BETW21], [LaG19], [YHS+21]	Initial Interview 1, Seminars
Patch and Update management	[HPM+21], [LaG19], [BETW21], [WWP+20]	Initial Interview 1, Seminars
Defence-in-depth	[HPM+21], [FPPD22]	Seminars
Response training and Awareness	[PHH22], [HPM+21], [BFP+18], [LaG19], [KYL+20], [FPPD22], [WWP+20]	Initial Interview 2, Seminars
Attack simulation	[BFP+18], [HPM+21], [PHH22]	Initial Interview 2
Impact prediction	[BFP+18], [HPM+21], [PKC20]	Initial Interview 2

The time constraint of the thesis limited the literature study to cover five use areas. Each of the potential use areas received a score based on mentions as described in Section 3.3.2. The result of the scoring and selection steps is presented in Figure 4.2, derived from the sorting displayed in Table 4.1. The top five highest scores are in bold with highlighted column colors.

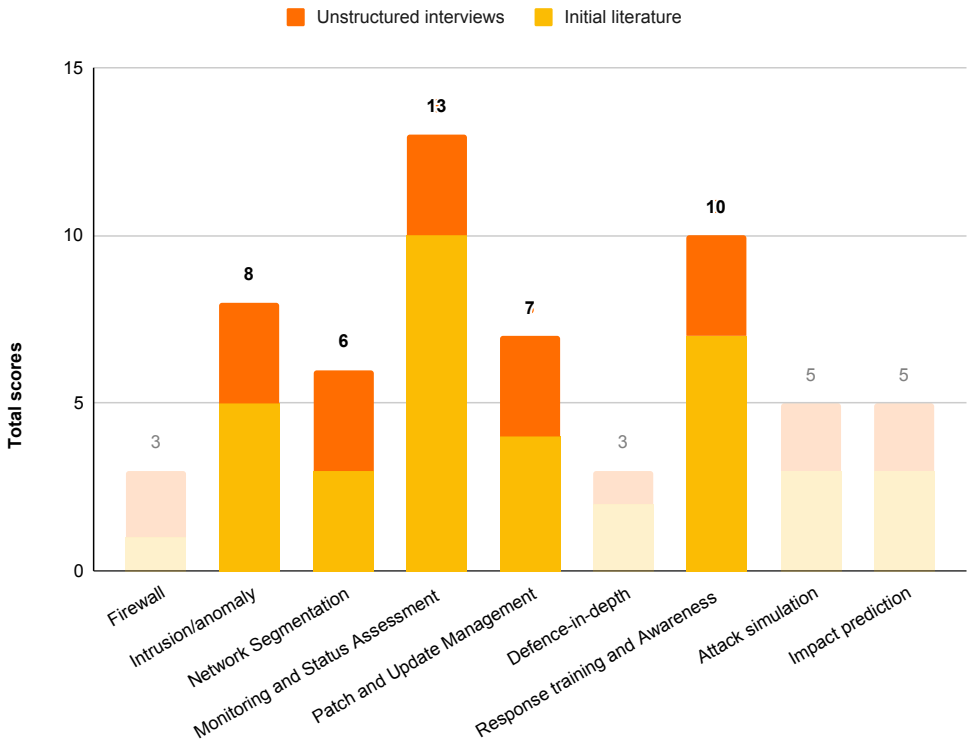

Figure 4.2: Use Areas with Scores.

4.2 Literature study - Digital Twins for cybersecurity

This section presents the semi-systematic literature study addressing the possibilities and limitations of the Digital Twin for cybersecurity. The result of the analyzed literature studies is presented in Section 4.2.3. Before presenting these findings, the literature that is used to derive the result are replicated fully in the next sections, each of which is introduced by addressing its relevance in light of the identified set of articles. The replication and granularity of the presented data is intended to facilitate the discussion in Chapter 5. The five use areas resulting from the initial analysis are studied closer to understand better if and how the Digital Twin contributes. This is presented in Section 4.2.1. In Section 4.2.2, the literature derives the industry's limitations for the technology to securely and safely implement the Digital Twin.

4.2.1 Opportunities and Use Areas

Use areas for Digital Twin to improve cybersecurity, contributing to increased resilience, awareness, and hygiene within the industry, is presented next.

Response Training and Awareness

Seven of the twelve initial articles mentioned response training and awareness as one of the potential benefits of the Digital Twin for cybersecurity. In addition to the initial articles, seven supplementary sources provided insight for the analysis of this use area.

Wanasinghe *et al.* (2020) concludes with the training of employees, for emergency response, operation, and maintenance, as being one of the most valuable use areas of the Digital Twin. Improved training can influence and limit the impact and damage of undesired events and is a requirement stated in PSA regulations [Pet19]. Training personnel and operators are thus a crucial part of incident response [Pet19]. Becue *et al.* (2018) establishes that Digital Twins may be the strongest ally in improving cybersecurity training and testing to enable accurate impact prediction and risk anticipation [BFP+18].

Hotvedt and Skytterholm (2021) stresses in their work the importance of realistic scenarios for developing successful training material. As previous exercises have focused on safety-related incidents, cyber incidents that compromise the IACS and other IT-systems call for new exercises, and training practices [HS21]. The Digital Twin can be an asset for enhancing training and developing new scenarios for cyber-related incidents [HPM+21]. Virtual Reality (VR) and Augmented Reality (AR) has been considered as enabling technologies for the Digital Twin [PHH22]. These technologies allow the operator to use the Digital Twin more interactively and enable the development of training systems for new operators [PHH22]. Realistic scenario testing with a Digital Twin can train responsible personnel to optimize response time and decision making by analyzing an incident more effectively [KYL+20; ED15; EE19]. A Digital Twin allows employees to practice security preparedness exercises, procedures, and maintenance virtually and onshore through emulations using testbeds [MRB+22]. This possibility further eliminates the safety risks of traveling offshore performing these activities [MRB+22]. An analysis reproduced in LaGrange (2019) proved that the project cycle time could be reduced by 4-12 weeks in a project where elements of the Digital Twin were delivered.

The strict availability and business continuity requirements of IACS make it challenging to perform penetration testing in a training scenario [EE19]. One of the possibilities the Digital Twin brings is to use the virtual environment to perform penetration testing, facilitating awareness training in the systems directly involved

in the Incident response plan (IRP) [HPM+21]. Penetration tests on the virtual environment could also reveal vulnerabilities in the system configuration [EE19]. Testing with the Digital Twin is possible in all development phases of the plant, not limited to operation alone, but also in the engineering phase [FPPD22]. IEC 62443-1-1 includes *timely response to event* as a fundamental requirement, stating the importance of fast appropriate actions in safety-critical situations [09a]. Replicating real-world previous cyber incidents with a Digital Twin is beneficial to optimize the operators response to attacks [ED15].

Attack simulation as a strategy for testing and training is thus one of the central use areas for the Digital Twin in a security context [WWP+20; FPPD22]. However, the authenticity of the attack simulation depends on the correctness of the predictions of the machine learning algorithm [Alp20]. This dependence stresses the need for accurate and clean input data and a sufficient amount of datasets [Alp20]. Cybersecurity competence and perception of cyber threats are a concern in the context of training and timely response to events [21c]. This issue partly results from bad cyber hygiene and a lack of understanding of the potential consequences of cyber incidents [PS21; 21c]. The literature addresses skepticism towards the correctness of the Digital Twin as a predominant obstacle in examining the technology in the context of personnel training, IRP, and organizational awareness [ALK+18]. Alharthi *et al.* (2018) address the challenge of a virtual model accurately representing the physical system. This difficulty is partly a result of the lack of system visibility, making it challenging to capture the whole picture of the system [ALK+18]. For example, a security incident scenario's stressful, physical, and social complexity is not necessarily adequately replicated [ALK+18]. Operational and technical countermeasures will not matter without the right organizational culture, knowledge, and skill to support the new technology adoption [Lam18]. In order to be adequate for extensive training, the Digital Twin needs to provide a comprehensive, realistic picture of an immense system, which is expensive [EE19]. Such an implementation must be cost-effective and, at the same time, complex enough to be worth the investment [EE19].

Monitoring and Status Assessment

Of the twelve initial articles, ten mentioned monitoring and status assessment as a potential beneficial use area for the Digital Twin in cybersecurity. Additional six sources provided insight for the analysis of this use area.

IEC 62443 stresses that a successful cybersecurity defense must include status monitoring of the established barriers to ensure that they conform with requirements [10]. Due to the lack of visibility across OT networks, real-time monitoring and status assessment are current challenges faced by the petroleum industry [Dra21a]. The implementation of the Digital Twin uses sensors to monitor the system in

real-time, and several exploratory articles mention this as one of the key benefits of the technology [EE19; PKC20; WWP+20]. Improved insight into the complex architecture of the plant and the digital system conducted based on Digital Twins can identify unnecessary, excess, or unprotected services [FPPD22]. The network's complexity and attack surface can then be minimized and optimized when removing these services or devices [EE19].

Reduced system visibility and knowledge make it difficult to collect and analyze data in an accurate virtual model [EE19]. Over 40% of offshore facilities have been in operation for half a decade, resulting in a low number of incorporated sophisticated monitoring tools [MSZ17]. Furthermore, newer generation systems also have outdated operating systems, no longer receiving updates [RSR+21]. Lamb (2018) lists Digital Twin as one solution to the aging infrastructure problem, using NAMUR solutions to standardize the communication between physical assets and monitoring applications [NAM21].

A characteristic of the Digital Twin is the visualization of real-time data through a centralized and synchronized interface [KYL+20]. The processing logic receives the data for monitoring, and one can implement reactive controls for management and operation [KYL+20]. The ability of the virtual system to communicate information in real-time across industry domains to all involved stakeholders in a clear and commonly understandable format can reduce delays and issues that arise from miscommunication [WWP+20]. The overview and interoperability that the technology provides can assist in optimization throughout the whole plant life cycle [EE19]. Once the virtual replica can collect and analyze the data, the operator can act on the insights from the Digital Twin instead of conducting repetitive and routine data processing [WWP+20]. In the context of life cycle management, the real-time visualization of the system provides opportunities for semantic interoperability through OPC UA [EE19]. Ensuring real-time data exchange between the physical and digital twins is a big challenge [PHH22]. Security must be a high priority when allowing data aggregation and centralized control because of the criticality of the data [BETW21].

Lantz, Heller, and McKeown (2018) highlights the use of Digital Twins to monitor the CPS throughout the whole plant and asset life cycle as a benefit. The authors further propose that this could be beneficial in documenting that operators of CPSs encounter an increasing number of regulatory requirements for safety and security [LHM18]. Another benefit of this is the ability to compare status measures of assets, and cybersecurity barriers against security standards, e.g., IEC 62443, to provide evidence for compliance or deviation from requirements [LHM18]. A strength of using the Digital Twin as an information source for security analysis is that one can analyze the system's security status in situations where it traditionally would endanger the system [PVU+19]. Another benefit is that the Digital Twin monitors

deviations from the security requirements and sub-optimal operations, enabling the system to replace a barrier before it fails [LaG19].

Another implication of real-time and extensive system monitoring and operating condition assessment with a Digital Twin is remote control and reactive response to incidents [HV20; YHS+21]. This ability would require a mature Digital Twin with bidirectional communication between the digital and physical assets [YHS+21]. Despite its advantages, this also contributes to a dynamic attack surface for cybercriminals [21c; FPPD22]. Real-time control and monitoring systems used today are a critical asset to secure as the consequences of compromise could lead to loss of life [Lam18]. A more mature Digital Twin can introduce the vulnerability of single-point-of-failure if implemented as a re-active or pro-active AAS [EE19]. A less mature Digital Twin still needs to hold a vast amount of data where compromise can lead to data disclosure or alterations, resulting in financial loss and damage to reputation [EE19]. The organization can mitigate these risks by placing the Digital Twin in an isolated operational environment with a clear distinction between zones and conduits [EE19]. However, the interconnections between assets present an obstacle in isolating critical systems.

Intrusion and Anomaly Detection Systems

Out of the twelve initial articles, five of them mentioned intrusion and anomaly detection as a key use area of the Digital Twin. Seven additional articles were identified during the second iteration of the search to supplement the findings.

Investigating new approaches for accurate intrusion detection is a prominent area of interest within CPS security [OBH+22]. The Intrusion Detection System (IDS) improves the system's resilience and reliability by detecting and reacting to incidents, violations, and threats to the security policies or practices of an organization that endangers the system [FPPD22]. A shared characteristic between these malicious activities is that they are deviations from the regular operation and network traffic [NFDS20]. It is a recommendation that the system uses AI to self-learn communication patterns between assets to detect abnormal activity [LaG19]. A Digital Twin collects an asset's historical and real-time data [DNV21]. By comparing historical and simulated signals with the measured data with AI, the Digital Twin can detect anomalies and failures before they occur [KRM+19]. The IDS can benefit from a real-time comparison between the Digital Twin's specification-based signals and real device signals [PKC20]. Additional security rules can be specified in the Digital Twin to facilitate continuous security, and safety [PKC20]. Holmes *et al.* (2021) explores the use of a Kalman filter to estimate the integrity of the input and output signals.

Bröring *et al.* (2021) points to the potential of the Digital Twin to add an extra layer of protection to the CPS, replacing direct connections between the asset and

remote access providers, the Internet, or smartphones. Where there is a constraint on the IDS of the physical asset because of limited bandwidth and computational capabilities, the Digital Twin is often cloud-based and would not have the same issue [PKC20]. The Digital Twin could work as an IDS, or a firewall [BETW21]. Additionally, Faleiro *et al.* (2022) propose that the Digital Twin could build an operator's profile to establish a normal baseline. This way, the Digital Twin could detect events where the operator's behavior deviates from the baseline, isolating anomalies from a security and safety point of view [FPPD22].

An Intrusion Prevention System (IPS) is an IDS with the additional capability of reacting to the detected incident, and attempting to mitigate it directly [SM10]. However, Eckhart and Ekelhart (2019) indicates IPS for CPS is a challenging task because of false positives, indicating a malicious event even during normal operation. This issue is also relevant for Digital Twins as IPS since data flow from the virtual to the physical counterpart can serve as a response mechanism [KKT+18]. A prerequisite for the Digital Twin to successfully detect anomalies by comparing input and output signals is that malicious actors cannot tamper with the specification or historical data [EE19].

One challenge faced when implementing IDS and IPS in critical infrastructures is the high availability requirements of systems and components [HPM+21]. Anomaly detection systems aim to recognize abnormal behavioral patterns, making their performance depend on the quality of the extracted network traffic features used to train the detector [NFDS20]. This requirement makes the quality and timeliness of transmitted data a bottleneck for using Digital Twins as a resource for intrusion detection. Inaccurate data can result in a high number of false positives and negatives [KA21].

The reviewed works indicate that Digital Twins can be used as a measure for intrusion detection in IIoT environments, both by introducing an additional layer of protection and by assisting in anomaly-based intrusion detection [KKT+18; KRM+19; KA21]. Naseer *et al.*, (2020) brings attention to the need for specialized tools for simulating IIoT environments and for conducting deep learning methods on resource-constrained devices. Significant work is still required to implement Digital Twins providing an adequate level of data quality and detail [MRB+22]. Further research should focus on the potential of Digital Twins for realizing IPSs in CPSs to detect and respond to Advanced Persistent Threats (APTs) [DP20].

Network Segmentation and Access Control - Zones and Conduits

Three of the twelve initial articles mentioned network segmentation as motivational use area for the Digital Twin in cybersecurity. Nine supplementary sources provided additional insight for the analysis of this use area.

Attacks targeting IACS are challenging to counter. These attacks are often executed indirectly or directly through a device or a person located inside the private network [LCHL21]. By applying network segmentation and segregation to the system architecture, access to sensitive information and control systems can be minimized [ED15]. The measure also enables an additional level of protection segmenting safety-related systems from other systems [19]. Kim *et al.* (2020) suggest that *"multi-persona twins"* can be specified with specific sub-roles in different space-granularity planes.

Increased visibility inside the OT system enabled by the Digital twin can indicate that the technology can improve network segmentation [PVU+19]. One study suggests allocating critical assets in different segments, requiring a definition of assets criticality [AKP20]. The Digital Twin analyses the asset's criticality and weak parts and measure it against the real-time data to predict the asset's exposure to other systems [PKC20].

An advantage of a more precise definition of zones and conduits through a Digital Twin is improved access control [10]. Access control is an essential factor in the security of a system. The Digital Twin supports Attribute-Based Access Control (ABAC) [YHS+21], where an attribute may be one role and can be used with Role-Based Access Control (RBAC) [4020]. This authentication scheme makes it possible to grant access to different zones based on the role of the user [YHS+21]. A compromised device may cause significant damage within a manufacturing environment, leading to economic and safety-related harm [FPPD22]. A Digital Twin can become a zone between the outside network and the physical assets, introducing an additional barrier to implementing security measures like firewalls and access control [BETW21].

Because of the overview and extensive data within the Digital Twin, one can view it as a blueprint of the industrial plant, identifying components, interfaces, and behaviors [FPPD22]. If compromised, it can aid adversaries in blackmail and reveal company secrets [FPPD22]. It could additionally be used for penetration testing of the physical system, allowing the attacker to fine-tune their attack mechanisms [EE19]. Strong authentication and access control must be in place to mitigate the consequences of an attack targeting the Digital Twin [FPPD22]. Without these capabilities, a targeted attack could have the same impact or consequences as attacking the physical asset [EE19]. Literature suggests that good network segmentation can limit the consequence of malware introduced via a Digital Twin [BETW21]. The OPC UA protocol, the standardized communication protocol for the German Plattform Industrie 4.0, aims to ensure secure data communication in Digital Twin applications by addressing authentication, integrity, and confidentiality [YHS+21].

Patch and Update Management

Out of the twelve initial articles, four mentioned patch management as a potential motivational use area of the Digital Twin. Nine additional articles were identified during the second iteration of the search to supplement the findings.

One of the main activities for ensuring cybersecurity during the operation of a plant is patch management of CPSs [09b; DNV17]. Patch management ensures that all network devices and computers are up to date with the newest software updates to be capable of resisting low-level cyber attacks [DNV17]. A patch can take weeks or years for a mission-critical system without the option to be switched off. DNV urges the industry to have a patch management policy [DNV17]. This policy will define which risk-mitigating actions to implement if applying the patches is causing greater risk than running the system un-patched [DNV17]. With a Digital Twin, one can explore the impact of a patch without affecting the deployed infrastructure [HPM+21]. Another significant advantage concerning safety-critical applications is that there is no longer a need to maintain an expensive secondary system solely for testing [HPM+21].

Baiardi and Tonelli (2021) describes a solution for continuous patch management by implementing two Digital Twins. The first has attributes for the infrastructure modules and their vulnerabilities. The other imitates the threat actor with attributes for the attack surface, goals, and handling of attack failures [BT21]. The article points out that multiple emulations can discover an actuator's paths by covering stochastic factors such as attack success or failure [BT21]. Knowing these paths enables the remediation policy to minimize the patches to deploy [BT21]. The AAS interface can collect data from assets and provide this to the external endpoints [BETW21]. Thus, as the AAS is easier to patch than the industrial asset, this can support cybersecurity barriers with more secure connections to external endpoints compared to the IACS interface that is worse patched [BETW21].

One of the most valuable aspects of the Digital Twin is the ability to provide an overview of the system state [PKC20]. This system overview enables the running of machine learning algorithms for predicting future states and simulation of "*what-if*" scenarios [ESBC19]. According to Becue *et al.* (2018), several companies, e.g., Siemens and ABB, listed predictive maintenance as one of their primary use areas for Digital Twin technology [BFP+18]. The predictive maintenance strategy aims to optimize the maintenance cycle by balancing a correcting maintenance approach, fixing equipment as it fails, and a preventative approach, fixing equipment before it fails [BFP+18]. The Digital Twin uses extensive data with machine learning models to predict component failure and optimize component lifetime, reducing unscheduled maintenance [DP20; WWP+20]. One of the challenges with patch management in critical infrastructures is its interconnectedness and complexity [LaG19]. This

correlation makes it difficult to foresee how updates affect the surrounding architecture [EE19]. The Digital Twin enables penetration testing virtually on the digital counterpart instead on the actual system [EE19]. This way, one can predict the effects of a security patch in a way that does not negatively affect the operation of the system [EE19].

Many vendors and stakeholders are involved in the production life cycle, contributing to the ecosystem complexity, making the petroleum industry vulnerable to cyber attacks [MSZ17]. When assets rely on different vendor-specific security guidelines and patching strategies, irregular and retrofitted patching of legacy assets contributes to bad cyber hygiene and vulnerable systems [MSZ17]. Eckhart and Ekelhart (2019) stresses the challenge of balancing the fidelity of Digital Twins and the expenses involved in creating them for the use of testbeds for testing the system's reaction to updates.

4.2.2 Challenges and Limitations

This subsection presents and summarizes the challenges and limitations of the Digital Twin in the context of cybersecurity. The identified limitations are *data quality* to assure an accurate representation of the physical asset in real or near real-time and *authentication and access control* to assure no malicious actor can gain access to the Digital Twin. These limitations must be addressed before realizing the maturity levels 4 and 5 of Digital Twin in critical infrastructure security and safety systems, which requires the development of a shared understanding and *standardization* of the technology across domains.

Quality of Data

Six of the identified sources mentioned data quality as one of the main challenges and limitations of the implementation of the Digital Twin for cybersecurity in the petroleum industry.

One of the main challenges the industry has to address to implement a reliable Digital Twin is the adequate collection and distribution of data through IIoT sensors [FFS+18]. Sensors may require retrofitting to ensure adequate data exchange [FFDB20]. Generally, IIoT devices are deployed in environments for supporting safety- and mission-critical applications, such as Oil&Gas production. These environments have stringent requirements for timely delivery of control decisions and data collection [FFS+18].

One of the main prospects of the Digital Twin is the accurate representation of the state of the asset enabled through real-time and historical data. This fact makes the fidelity of the digital representation directly dependable on the quality

of the transmitted data [FFDB20]. As Digital Twins utilizes AI for predictions and decision support, the data fed to the algorithms must be noise-free with a constant, uninterrupted data stream to ensure a reliable result [FFDB20]. This reliability of the data produced in the Digital Twin is of great importance when used for security analysis and cyber resilience [FPPD22]. These use areas require the industry to address the limitations of their systems, such as the CPS. These systems are often limited to passive means for data collection, where volatile memory in combination with availability requirements is an obstacle that requires attention to preserve operation while collecting the data [EEW19]. There is a need to analyze the devices and assets to ensure sufficient data is collected and transmitted to the Digital Twin without disrupting business continuity.

Another industry characteristic is significant reliability- and availability- requirements. This requirement represents a problem when considered in conjunction with the Digital Twin's essential need for significant amounts of real-time data. A large number of sensors and sensor data used to support the digital representation within one process poses a significant challenge to the system's reliability when connecting them simultaneously [FFDB20]. These conflicting requirements stress the need for balanced data collection. There needs to be enough data collected so that the virtual copy presents a realistic picture of the system in question but not too much, as too much data will present a bottleneck where transmission is concerned [WWP+20]. The data amount requires storing, processing, and transformation to provide the desired value. Here data mining is one way to identify patterns in data [SSH+18a]. However, this strategy is uncommon in manufacturing [SSH+18a]. The chosen data storage strategy will require high security levels while enabling fast, and reliable data extraction [WWP+20]. Thus, the large and complex data amounts require proper and secure data management and utilization approaches to ensure data integrity, availability, and confidentiality.

Authentication

In the analysis of authentication as a limiting factor for the technology four sources formed the basis for this finding.

When information is accessed and unauthorized changes can be made, the data loses its integrity. Data integrity is maintained by collecting correct information and having authentication and security measures that prevent unwanted modifications [Tho].

The Digital Twin includes a large amount of IIoT sensors to provide the needed data and a collective interface representing the assets [4020]. Attacks targeting IACS are commonly executed by highly motivated adversaries with a significant number of resources, named APT [LCHL21]. These attacks are difficult to defend against and

are often executed indirectly or directly through a device or a person located inside the private network [LCHL21]. The increasing number of connected devices within the Digital Twin, as well as the threat picture, calls for a well-defined access control policy to reduce the attack surface, following the principle of least privilege [oAut20; LCHL21].

The literature mentions the lack of sufficient access control as a barrier to implementing a level 4 or 5 Digital Twin in the petroleum industry [Tho]. Two-way communication between the physical and virtual assets for real-time optimization of processes characterizes Digital Twins of this maturity level. If the Digital Twin has this capability, attacking the virtual system could have similar consequences and impact as attacking the physical asset. An advisory with access could obtain insight and unauthorized control of physical assets, resulting in uncontrollable behaviors [Tho]. There is a need for further research in this field to investigate how much control a malicious actor would have of the system if such an attack were to happen.

Maturity Level 4 and 5

The challenge area of the upper maturity levels were based on eleven articles.

The terms Digital Twin and AAS define systems with various technical capabilities. Figure 2.4 presents the five different maturity levels, ranging from simple monitoring and 3D modeling to autonomy. Not all levels are new concepts but went through a rebranding after the term *Digital Twin* gained its popularity [IBM20].

The Digital Twin of maturity levels 4 and 5 adds the ability to co-operate with other Digital Twins and interact in their cross-dependent operations [KYL+20]. This level of maturity enables the digital to control the physical [ESBC19]. Two-way communication between the physical and digital assets will contribute to remote control capabilities, making it possible to mitigate the safety risks of on-site operational workers to a minimum [WWP+20; ESBC19]. If implemented as a part of the safety or security systems, pro-active Digital Twins could allow operators to immediately send the system into the fail-safe mode or isolate the affected assets [DP20].

The potential impact and consequence of a cyber attack targeting the Digital Twin increase with the level of interconnectivity between the physical and digital counterparts [EE19]. Countermeasures include authentication and encrypting the connection between the Digital Twin and the physical asset it replicates [Tho]. There is a need for a standardized lightweight encryption scheme to support the availability requirements of the assets represented by the Digital Twins. Although extensive work is needed to ensure the confidentiality of the transferred data, protocols such as OPC UA show promising results [PHH22]. OPC UA address both the authentication and the integrity and confidentiality of the information exchange [KHA+20]. As

an integral part of the platform's cybersecurity system, a successful attack on the Digital Twin could tamper with the implemented cyber barriers, deactivating IDS and firewalls without operators' awareness. Such control would have catastrophic consequences, and it motivates the separation of SIS, and the Digital Twin [OBH+22].

Even though Digital Twins' transformative potential lies in connecting them, there is a need for further research and risk assessments on the re-active and pro-active Digital Twins before secure implementation can be guaranteed [ESBC19]. However, the level 3 Digital Twin has the advantage of better performance, and higher quality as the technical features of the previous lower levels supports it [KYL+20]. Achieving the fifth level of maturity is aspirational at present, with only a small number of discrete situations possible to represent [ESBC19]. Keeping the discussion on a lower level of maturity is important, as unrealistic expectations and futuristic goals contribute to slowing down industry adoption and development [FFDB20].

Standardization and Trust

Three sources listed standardization as a challenge that must be addressed for the successful implementation of the Digital Twin.

Engineering challenges limiting the Digital Twin involve the complex infrastructure it tries to represent [SSH+18a]. Without a sound and well connected IT infrastructure its effectiveness is limited [FFDB20]. As the Digital Twin aims to connect and facilitate IoT interoperability, compatibility between the Twin and IoT is required [FFDB20]. The "*alphabet soup*" that make up the current IoT standardization's is a challenge [SSH+18a]. The vast number of vendors and suppliers involved in the industry infrastructure is hard to visualize but remains critical to realizing the benefits of the Digital Twin [SSH+18a].

No standard data format and vendors using different methods to present and structure their data make aggregation and integration in real-time difficult [WWP+20]. This fact adds to the already present issue regarding the lack of a standardized way of modeling the technology, which limits user and organizational understanding [FFDB20]. Coordinated information sharing and data consistency are fundamental requirements for enabling and realizing the Digital Twin [SSH+18a], underpinning the need for a unified model and standardized way of building it [FFDB20]. With data originating from internal and external sources and across domains, aggregation and combining these will require considerable financial investments to achieve a truthful and standardized model [SSH+18a; FFDB20].

Increased automation and reliance on AI predictions face skepticism from users [FFDB20]. The shift in control from humans to machines is something many find daunting, stressing the importance of introduction using familiar formats and focusing

on operator struggles and difficult tasks [FFDB20]. A contradicting perspective arises from the operator's point of view. Only seeing the benefits and trending aspects of the technology, assuming and expecting it to solve all problems, can have the opposite effect [FFDB20]. If operators do not see or experience apparent benefits, resistance and unappreciative attitude are likely [WWP+20]. Ensuring adoption and implementation for the right reasons and in the right operations is important for the technology's success. Communication and understanding of the positives and negatives require discussion involving the organization and the user to ensure a proper and sufficient level of trust [FFDB20].

4.2.3 Summary and Analysis of the Literature Review

The literature study indicates that the industry and research community take great interest in the use areas of the Digital Twin for increased cybersecurity. However, to our knowledge, it has not been implemented for security use cases. This section will summarize the key findings from the analysis.

Table 4.2: Summary of use areas identified in the literature.

Use areas	**Description**
Response training and Awareness	Awareness of the effects of a cyber incident through training and simulation of realistic scenarios with a Digital Twin. Impact prediction in near real-time can assist operators in responding to and classifying cyber incidents.
Monitoring and Status Assessment	The Digital Twin can be assisted by smart sensors to gain a comprehensive view of the system status. This overview can help reduce the complexity and the attack surface by removing redundant components. Another outcome is assessing the asset status to assure compliance with security requirements.
Intrusion and Anomaly Detection Systems	Intrusion and anomaly detection can be enhanced by the system status and overview gained by implementing a Digital Twin. Digital Twins provides additional data, making the deep learning algorithms for detecting attacks more robust.
Network Segmentation and Access Control	A Digital Twin can improve segmentation as an additional zone between the outside network and the physical assets. Monitoring and system overview facilitates dependability analysis to ensure critical assets are separate from other zones.
Patch and Update management	Patch management processes can improve by simulating the patch on the Digital Twin, predicting the impact on the system. Attack simulation can support the patch management policy by defining attack vectors and realizing mitigation strategies in scenarios where the system cannot be patched.
Maturity levels 4 and 5	Increased interconnectedness, remote control, and autonomy of assets endorse human safety by removing them from safety-critical situations.

Table 4.3: Summary of challenges and limitations identified in the literature.

Challenges	Summary
Quality of Data	The digital representation strictly depends on high-quality data at a sufficient frequency. Extracting, aggregating, and visualizing enough data at sufficient quality to ensure a realistic representation in real-time without creating a data bottleneck must be achieved.
Authentication	Lack of sufficient access control prevents advancement to high maturity levels. Strict access control and policies are required to prevent the Twin from becoming a vulnerability and attack scope enhancer.
Maturity levels 4 and 5	Increased interconnectedness at this level requires extensive risk assessment and testing before implementation. Confidentiality, authentication, and integrity at a high level need to be ensured. Transmission protocols such as OPC UA show promising results in theory in addressing some of these issues.
Standardization and Trust	Infrastructure complexity with its many standards, formats, and methods for data management makes complete visualization and modeling of the plant and supply chain challenging. Ensuring organizational understanding, operator usability, and trust in the Digital Twin is critical for its success.

4.3 Interviews - Insight from professionals

This section presents and analyzes the information collected during the semi-structured interviews. Notes taken during each interview were analyzed as presented in Section 3.3. The following three sections present the findings. The first two sections contribute to the derived thematic network concerning the Digital Twin (Figure 3.3). Four coding groups representing potential use areas resulted from the analysis. Section 4.3.1 presents and analyzes the use areas brought forward by the interviewees, and Section 4.3.2 describes the problems, issues, and concerns regarding the technology in the context of cybersecurity. Additionally, information regarding status today, are presented in Section 4.3.2.

4.3.1 Identified Use Areas

The interview data led to four sub-themes which make up the identified use areas from the point of view of industry professionals. Notes from each interview were analyzed. The essence of the subjects' opinions and insight is presented in the paragraphs under each sub-theme.

Virtual Security Training and Testing

With low acceptance for downtime, there are limited options for testing different scenarios, training guidelines, and the impact of system changes [HS21]. Testing the system security is challenging as such tests would require taking the system in question offline or risking harming the involved assets [EE19]. Another testing issue involves the IRP, which is also challenging to test in practice for the same reasons [Dra21a]. Training offshore personnel involves high risk, and safety concerns [WWP+20].

Interview 1 IRPs on large facilities today from an IT perspective involves "*chasing*" the incident in their attempt to contain the consequences after detection. With the heavy safety focus, ensuring that the final barrier is intact in these situations is critical. A fire presents an illustrative example of the mindset that should be present, "*forget about the fire; check that the final barrier is intact.*" Ensuring the final barrier makes consequence reduction of the worst-case scenario possible. Attack and threat modeling with safety consequences present the first identified use area. By simulating threat and attack scenarios virtually, employee response is possible to test. Including safety consequences in the simulation can aid in the cultural issues and generally poor attitude towards the involvement cybersecurity and IT compromise has on safety. This kind of testing also gives companies a possible advantage in keeping up with attackers in the ongoing cyber arms race.

Interview 2 The potential of using the Digital Twin as a tool for awareness training and risk assessment are interesting areas for the technology. The Digital Twin can help see data in a shared context and assist in awareness training. As a defense-in-depth strategy with a sequence of barriers, the bow-tie model with a proposed barrier for awareness training could indicate whether or not personnel has completed a sufficient amount of training, but measuring other aspects of training and awareness is hard. However, operator and control personnel training do present a motivating Digital Twin use area. The management can produce a scenario where a ransomware message pops up in the operator panel using a facility simulation. Indicating testing of how well the response procedures are if they exist. The IRP is the most critical barrier but also the least developed one. Many companies do not have a plan, and it is never exercised if they do. Tests of this today would, with a high probability, show that most operators do not know what to do. Training on how one should act to limit and reduce the scope and consequences of attacks is an example of how the technology could aid in improving the IRP. Scenarios like these can also aid in improving the poor culture surrounding cyber incidents as a source of safety issues by showing how ransomware can easily lead to safety issues. It is currently a yearly practice to train on how to disconnect from the system. This

testing and training could be done more frequently with the proposed solution with the Digital Twin.

Interview 3 The industry must add the new threat of cyber to existing strategies and scenario development. A challenge is integrating this into the existing security and safety systems. "*Should one ask how cyber affects existing security barriers or create cyber as its control system?*". Today's industry focuses on developing these scenarios to identify barriers needed to address the vulnerabilities and threats. Having a Digital Twin at their disposal can improve current methods and allow visualization of effects and sequences of events, insert roles and responsibilities, and thus, aid in increasing overall cyber awareness.

Interview 4 The industry shows an increased need for improved preparedness. Personnel must acquire a better understanding of the challenges of the new technologies they adopt.

Intrusion and Anomaly Detection

Visibility issues make it hard for operators to detect intrusion, thus increasing the overall time an advisory has at their disposal to inflict damage [Dra21a]. Understanding the available data is also a barrier that affects the time to detection. Thus, companies can improve their detection rates and response time by grasping and analyzing the available data.

Interview 1 Detection within companies has a low level of maturity, and internal control possesses vulnerabilities and weaknesses. Many of these companies can assume that a compromise has occurred with a high probability. In this context, the topic of Consequence-driven Cyber-informed Engeneering (CCE) presents a model based on the perceived fact that if a malicious actor has targeted you, system compromise is 100% successful. This mindset supports a proposed shift in resources toward the right side of the bow-tie and in ensuring solid, final barriers.

Interview 2 Use areas for the Digital Twin involve measuring end-point protection, access control, and detection systems. As long as the proper controls are in place, the company can achieve a reasonable level and quality monitoring that should detect anomalies in and intrusion of systems. By aggregating and visualizing alerts, they can try to produce an overall picture that would allow them to see the status of different parts and assets of the system. The industry sits on a vast amount of data that is possible to collect, and the production of the overall picture would require a set of rules that reduce the data to a manageable amount. In an IACS facility, the chances of being able to map the entire facility are not high, as there are parts not possible to detect online. Scanning the visualized parts to say what is on the network

can detect anomalies. If the level of visualization discussed is obtained, it would be possible to realize things like network status. This could indicate denials of access, changes in firewall rules, suspicious authentication attempts, and other anomalies.

Interview 4 One use area for Digital Twins is detection. Training personnel to understand the data, alerts, and indicators become important if the industry utilizes the technology. Further, data from previous incidents or potential scenarios are required to adopt the technology for detection to allow the system to learn the patterns it should react to. The definition of what values and activities categorize as anomalies are required. A challenge is obtaining enough data to base the detection on to create good predictions.

Barrier Status and Monitoring

A general issue revealed through the conducted research was that an overview is difficult to obtain due to the high complexity of the systems. Monitoring and status validation of assets and security controls is one of the five recommendations provided by Dragos in their report from 2021 [Dra21a]. The same report lists network visibility as one of the four critical issues listed in their findings [Dra21a]. Limited visibility seems to be a problem stemming from legacy systems lacking in design to provide insight and the increasing system complexity and supply chain.

Interview 1 The technology shows potential for better showing the status of assets. The assessment of status is currently a difficult task. The Digital Twin concept has shown potential when addressing this as it can provide an easy interface to see if the system meets a specific set of requirements.

Interview 2 Using a barrier model or a bow-tie for visualization and overview is a valuable area for the Digital Twin technology. Aggregating data automatically and visualizing the status is one way the industry can benefit from seeing different elements together in a larger context. Understandably visualizing status could motivate stakeholders to initiate actions that make the status good. Compiling work orders, process information, cameras, and other aspects can provide workers with a much-needed overview. Examples of status that could be visualized are patch status of equipment, IDS status, firewall status and rules, alerts and locations in an orderly fashion, log access attempts and security policy compliance. It allows for system insight in operation and the project phase, which can support these phases through its features. Additionally, such visualization of barriers can aid in obtaining the attention at the right organizational level.

Interview 3 Currently, companies are attempting to find ways to catch barrier status at all times. Current strategies involve manual tables and text. There is no

digital connection between documentation and operation. Moving these tables and text elements into a Digital Twin presented an interesting research area. Seamless communication between management and other systems and elements presents an interesting topic for further investigation.

Interview 4 An essential requirement and need is a system overview. In the context of analysis requirements, the management regulation states that operators must have a collected overview of the performed analyses, and sufficient conformance between dependent ones must be secured. When adopting a Digital Twin for status and overview purposes, displaying the status of an asset may not be a challenging task. The challenge lies in obtaining dynamic real-time values, where OT systems are more difficult due to the legacy system, data integrity, and bottleneck issues.

Patch Management and New Equipment

When considering a new patching update, one general concern is how the OT systems will react. This reaction is not easy to predict in advance and may be costly if they inflict damage or downtime. If patches and their consequence is possible to test in advance, some of these costs could be reduced or avoided.

Interview 1 In addition to simulated attacks, the Digital Twin provides an environment for testing updates and patches before implementing them in the physical system. Such testing allows the operator to assess how the virtual system reacts to the changes. Patch and update visualization is a beneficial use area. However, involving humans and not viewing the virtual test as 100% accurate remains essential as the digital space cannot include all possible aspects of the analog reality.

Interview 2 Some companies focus on one aspect of barrier management in the cyber context. Examples of tasks involved are system update monitoring. Some companies could argue that they have a Digital Twin in realizing this task. However, the way this research investigates the Digital Twin as a tool for cybersecurity is not present today. Applying the technology using a swiss-cheese format in real-time, then the industry would have the ability to visualize outstanding patches, indicating the patch status of their equipment. Patch status of equipment is basic cyber hygiene practice that could benefit the organization if visualized.

Interview 3 The technology presents an opportunity to provide seamless communication as a part of maintenance.

4.3.2 Identified Challenges

During the interviews, professionals mentioned the following problem areas concerning barrier management, cybersecurity, and Digital Twins.

Security for Safety

Safety is given high priority within the Norwegian petroleum industry. The processes and operations, especially offshore, require personnel to operate in a high safety risk environment, making safety systems and procedures critical. The discussed interconnectedness and IT/OT overlap emphasizes the need for a more unified approach to safety and security.

Interview 1 By simulating actions on the digital asset, potential incidents or hazards become limited to the digital copy, thus reducing risks against the physical version and, consequently, safety. This benefit also presents a challenge as the solution provides a way into the physical system. Safety risks this might create must be addressed and require additional barriers that secure the communication between the digital and physical copy. The added two-way communication between the Digital Twin and the physical asset requires extensive security barriers. NOA presents a possibility of providing a secure gateway back and forth.

Interview 2 Digital Twins on the next maturity level include new safety and security challenges. The two-way communication widens the attack surface, making it so that compromise of the Digital Twin could provide the attacker with a clear path into critical physical control and safety systems. Implementation must involve a heavy security focus to maintain safety. The industry attitude of IT as its domain, where some issues and risks are "*left for IT to sort out*," contributes to an increased risk. In most companies, discussions about cybersecurity concerns and questions are present in the IT department and their teams. These topics are not common to address in OT. Making security barriers a more integrated part of safety barriers could improve the currently weak cybersecurity culture and hygiene present in the industry. The industry needs to change the culture, aiming for an attitude where people acknowledge that a cyber incident implies safety incidents and consequences.

Interview 3 Where the industry previously was concerned about protecting physical assets against physical threats using physical barriers, the cyber domain adds additional concerns regarding the cyber threats against digital systems using cyber barriers. This change stresses the need to develop a holistic approach to security.

The Human Contribution

Actions like the insertion of portable, removable media, phishing links, and remote control with inadequate security are attack vectors that exploit the human asset. One misconception in industries today is that the cyber threat is the responsibility of the IT operator and department. As more devices go online, employees across apartments become dependent on computers to complete their work, generating more potential vulnerabilities. Despite the positivism towards digitization, one can not remove humans from the equation, and they will have an essential role for years to come.

Interview 1 A future area of interest is to include the human element as an asset in the virtual representation of the AAS, suggesting a reduction in human-machine interaction. The main argument is that humans are among the primary sources of incidents and reduced safety concerns revolving around offshore activities. Despite this futuristic potential, human operators are still essential. Even with today's vast amount of advanced sensors, human characteristics like "gut-feeling" and experiences have yet to be digitized.

Interview 2 Poor basic cyber hygiene within the Oil&Gas industry is a general issue, as they tend to focus on higher levels of control but neglect the basics of cybersecurity. When considering the high-profile incidents that have impacted the industry, the root cause often involves "someone clicked on a link" or "the system had bad inadequate remote access controls," which are issues that sufficient training and policies would address. Keeping information in a known, familiar format is essential when introducing changes. New technologies are often met with skepticism and the "if I do not understand it, I will not use it" attitude. The focus when implementing such technologies should focus on how to help people do what is difficult to do, not force them to change things that work well.

Legacy Systems

Oil&Gas production has been around for decades. From a Norwegian point of view, the production and organization of national oil and gas companies date back to the 1960s. As a result, it comprises several legacy systems. A large part of the physical infrastructure involves OT and IACS. These systems involve analog data and are not initially designed for integration towards IT.

Interview 1 Existing Safety and Automation Systems (SAS) and SIS lack isolation and security. Safety is exposed if an incident develops in a company's SAS. Therefore, it is important to isolate these, in particular SIS, due to the importance of keeping the final barrier, the red fail-safe button, unhackable at Safety integrity level (SIL)

level 4. CCE presents a model where the focus is solemnly on the right-side of the bow-tie, assuming a 100% probability for system compromise if targeted. This model shows an example that supports focus on the right side of the bow-tie. When incidents occur IT "runs after the accidents" this emphasizes the need to secure the final barrier that might provide access to systems and compromise human safety.

Interview 2 Implementing the Digital Twin depends on the industry and the company's ability to collect data. The data must be filtered down to a manageable amount and presented understandably.

Interview 4 OT generates analog data not originally designed to transmit with a high frequency. AAS require real-time data to present a sufficient model. The bandwidth and transmission capacity of the physical legacy systems is a limitation. The amount of data that these systems possess is grand and extensive. Collecting it is challenging; subsequently, structuring and filtering it presents another. Not all the data is necessary or needed in the AAS. As aggregating and transmitting data in large quantities were not a part of the original design, the CPU may not be able to complete these tasks at the frequency required to obtain a real-time, high-resolution result. Implementation of the technology depends on where the data extracted is from. The fact is that all protocols have a send and receive, which presents a limitation.

Data Integrity

IT and OT convergence has caused several new challenges; data integrity presents one highlighted challenge as the Digital Twin is dependent on data from both domains. The technology's reliability depends on the transmission speed and quality of the data it receives.

Interview 1 The integrity and confidentiality of data present a concern when considering the Digital Twin. The analog format from the physical domain indicates the need for data transformation to accommodate for and fit into the digital format of the Digital Twin. During such a transformation, some value will ineluctably become lost. Intuition and human senses such as smell and sound will also be absent, limiting the completeness of the virtual replica. Current limitations include artificial intelligence and price that hinder recreation of some analog aspects to digital. Suppose the Digital Twin is used to implement patching of updates. In that case, the analog elements missing from the Twin can lead to consequences one was unprepared for.

Interview 2 Data integrity, quality, and reliability are concerns that must be addressed when considering the next maturity level of Digital Twins. When building

the Twin, data quality and integrity must be high to produce a reliable model. If this is not the case, a compromise of data integrity can lead to Denial of Service (DoS). So when acting on the data visualized in the Digital Twin, the data must be intact, high-quality, and reliable.

Interview 4 The analog format of the data from OT systems becomes degraded during the transit and adjustments towards digital, evidently affecting the data resolution. Obtaining data with adequate resolution and at sufficient speed is difficult. The distance the data must travel may be too long, so transmission at the desired frequency is complex. Additionally, the data available for collection in OT systems is extensive. A lot of it will probably not be necessary.

Supply Chain

When discussing cybersecurity in the industry today, one mentioned issue is the long, complex supply chain. When many vendors contribute to the overall system and its architecture, security issue arises when many follow different requirements and guidelines.

Interview 1 The data passes through many system levels, each with different checks and tests. An increasing supply chain leads to a reduced overview and control. When each level addresses security differently, it is very challenging to analyze the final security level of the overall system. The technology would be very prevailing if the Norwegian petroleum sector possessed its own cloud. Locating a critical solution such as the Twin in a third-party cloud may not be justifiable and imply poor security protection. Having it located locally could limit some security threats with the implementation.

Interview 2 The supply chain issues introduce a domino effect of security vulnerabilities. All vendors must understand the cybersecurity risk they pose to the end solution. Sadly a lot of them do not understand this today. They all contribute and pose a risk that the industry should face with a zero-trust approach where the company validates all levels. The vendor's cybersecurity awareness is a primary concern when adopting Digital Twins for cybersecurity and managing barriers. Vendors often have access to the system, allowing them to manage their products post-implementation. Neglecting to train these workers on cybersecurity culture and hygiene increases the system vulnerability. Many parts of the solution live in the vendor environment, which is unacceptable from a risk point of view. Having solutions locally and defining its boundaries must be a key priority. When considering a Twin of this complexity, its location is critical to ensure security, safety, and data integrity.

Interview 3 The vast number of vendors involved in realizing the industry architecture is one reason for its high complexity. Thus, one highlighted need was joining assets from different vendors in a common language to aid the process. A barrier management approach to cybersecurity using acknowledged shared documentation and a shared framework is promising.

Interview 4 A challenge the Digital Twin can address is the issues arising from the vast number of components from different vendors. The opportunity for reducing the current complexity through Digital Twins depends on the implementation and how it becomes incorporated with the IT and OT systems. Possible benefits depend on what data it involves and its location. Moving the control domain to the cloud implies making the cloud a part of the OT system, which threatens the independence requirements.

Maturity Level 4 and 5

A problem the industry must address if implementing the technology at the maturity level of Digital Twin is the potential single-point-of-failure and new way into critical assets it may imply. Adding new technologies without proper security measures and concerns will lead to new vulnerabilities.

Interview 1 The main opposing argument towards the higher level Twins is the single-point-of-failure two-way communication can bring. Sufficiently securing the solution is critical to maintaining adequate security and safety levels. Compromise of the virtual copy, with its many connections to the physical system, provides attackers with new entryways. Data diodes as a tool for unidirectional communication from the assets to the Digital Twin contribute to high security. As one opens up the flow to more prosperous and more data, a barrier that secures the path between the control system and Digital Twin is crucial for blocking the possible entryway. This solution must be hardware and not software, as the programmable side of software makes it hackable. The potential pathway must maintain high security, stressing the importance of using unhackable hardware. As long as life and health are involved, one cannot trust software.

Interview 2 Organizations becoming too reliant on the Digital Twin would become a vulnerability. The users must not become too dependent on the Digital Twin for operation. High availability may not be the main concern for Digital as it is a solution weighing more towards the IT domain. So, if a Twin of maturity level 4 or 5 becomes utilized, operators must still know what to do without it. The implementation must maintain a high-security level to limit its potential as a new vulnerability, which must involve a secure connection to access the Twin.

Interview 4 The final barrier is the emergency shutdown system, referred to as "*the big red button*" that disconnects all. This barrier must be isolated and independent from the programmable systems to maintain a high level of security and safety. OT systems today have high independence requirements. These requirements become threatened when considering solutions like the Digital Twin in this manner, as the pathways become open. Opening up the system and allowing the Twin to collect data and affect the system threatens the independence aspect. In collecting data, a data diode is a hardware tool and potential solution that addresses the issues regarding secure data transmission to and from the Digital Twin. However, adopting this tool will require it to work at a sufficient speed.

Different Perceptions of Current Maturity Levels

The conversations included questions regarding the industry's current maturity level of simulation, emulation, and virtualization. There is no standard measuring tool or framework when assessing the level of the technology. However, the subjects agreed that many companies had utilized level 1, involving 2D/3D modeling without metadata. The highest experienced level of the simulation was level 3, where one-way communication from the systems to the simulation was achieved, enriched with data from IoT and sensors. Interviewee 2 stated that many believe the simulation to be on level 3 when they, in reality, are on level 2. Whereas interviewee 1 shared their opinion of levels 4 or 5 being the levels that would be considered new.

When discussing the upper levels of maturity, interviewees stated that the term AAS is more suitable for the Digital Twin with two-way communication. Interviewee 2 implied that the technology to accomplish this next level is available, but culture holds the industry back. Interviewee 1 and 3 mentions the technology's potential to reduce the number of people sent offshore as a key motivator and driver that will promote further research and discussion. When asked about the future of the technology, interviewees considered the higher maturity levels an inevitable step that will require extensive research and testing to ensure requirement conformance.

4.3.3 Summary and Findings from the Interviews

This section summarizes the presented findings from interviews regarding the motivating use areas of the Digital Twin and concerns relevant to their realization. The summary reveals that the Digital Twin has high potential in some areas but also considerations that the industry must address. Findings concerning Digital Twin today were also presented. Current maturity levels are identified as somewhere between levels 2 and 3, depending on the interview subject.

Table 4.4: Motivational use areas of the Digital Twin for cybersecurity identified in interviews.

Use areas	Description
Awareness and Incident Response Training	Employee attitude, perception, and awareness concerning cybersecurity can improve by visualizing training exercises, scenario simulation, and incident response plans. Improved cybersecurity culture is an implicit safety-enhancing factor, a central focus area within offshore petroleum.
Intrusion and Anomaly Detection	Increased overview and insight into the system of systems can improve the understanding of the overall complexity and provide faster detection. Training the AAS on anomalies and patterns can allow it to provide alerts and indicators on which the operator can respond earlier, faster and better.
Barrier Status and Monitoring	The vast amount of vendors that contribute to increased system complexity can be aggregated and structured in an understandable format with the AAS technology. Today information about barriers appears spread between digital text and manually accessed and updated tables. Assessment of assets throughout the different phases of the plant life cycle presents an opportunity for testing system reaction to changes early in production and operation phases.
Patch Management and New Equipment	The high-availability requirements on OT-systems make it challenging to deploy patches to discovered vulnerabilities as it would require unpredictable amounts of downtime dependent on how the system reacts to the change. This also applies to the introduction of new equipment. Testing a patch or new assets beforehand in a Digital Twin presents a beneficial to visualize the system's reaction and thus limiting the damage and cost it may inflict on the physical system.
Cybersecurity strategies and Compliance	Seamless verification of requirement conformance at higher frequency through near real-time visualisation presents an opportunity not yet realised. Linking manual and digital data sources can allow for more frequent and continuous assessments.

Table 4.5: Challenges and concerns of the Digital Twin for cybersecurity identified in interviews.

Challenges	Summary
Security for safety	Making security a part of safety is essential when the industry aims to prepare and arm itself for the cyber threat. Getting employees to acknowledge and address the cyber risks can aid in improving the culture in this area. The long multi-vendor supply chain where all address cybersecurity differently contributes to the poor cyber hygiene, which must be addressed.
Maturity Levels	A shared perception of where the industry is currently at regarding these levels are not present. A shared perception of what categorizes the different levels will support future and current assessments of the technology. The two-way communication of the AAS is crucial to secure at the highest level. If one fails to consider carefully, the solution adds a new single-point-of-failure. NOA and data diodes are tools mentioned when attempting to address these issues.
Human Contribution	Humans are skeptical of new technologies and changes. Basing new implementations on familiar concepts can accommodate this. Even on the higher maturity levels, human intuition and instinct present aspects not captured by the AAS, stressing the need to keep human operators with the correct knowledge.
Quality of Data	Legacy systems appear as the main barrier to high data integrity and quality in a Digital Twin. Getting data with adequate quality and speed is required to ensure high reliability and trust in the technology.

4.4 Overall Findings and Results

This chapter identified potentials for the Digital Twin and analyzed literature to understand how its implementation in different use areas could affect cybersecurity and barriers in the Norwegian petroleum industry. The analysis also identified limitations of the technology and challenges related to its adoption. Figure 4.3 provides a visualization of the overlapping identified use areas and challenges presented in the previous sections.

Securing safety With the industry's heavy safety focus, securing safety is a critical and important task. With the increasing interconnectivity IT incidents often lead to cascading consequences into the OT domain. When analyzing a new technology

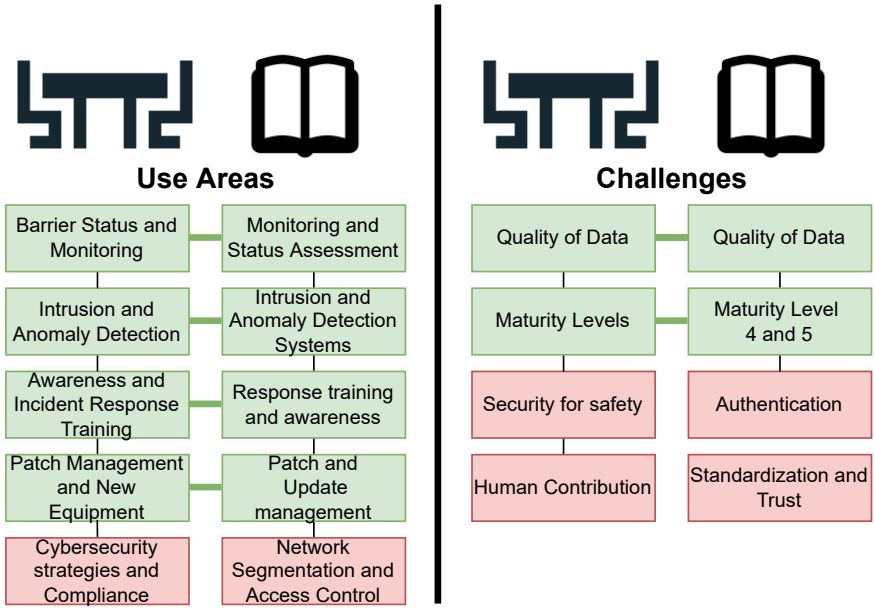

Figure 4.3: Visualization of overlap between literature and interview data.

for cybersecurity, the data presented emphasized the importance of protecting the safety barriers, such as the final barrier SIS to secure safety. When adopting new technologies, strict security considerations are critical to ensure security and safety [21b].

Cyber hygiene The different priorities of IT and OT present a conflicting aspect when interconnectivity between the domain increase. Interview data stated that the attitude towards cybersecurity today lacks cross-domain understanding, as cyber risks "*are left for IT to sort out*". Further, threats and risks changing from physical to digital motivate a holistic cybersecurity approach. As Chapter 2 stated, new technologies are introduced fast due to the digitization of the industry. One interviewee stated that, to some degree, the industry perceives itself as having good conformance with basic security strategies when these are often insufficient.

Holistic overview and monitoring All interviewees mention that assessing asset status and activity patterns in real-time is challenging, and a lack of visibility enables security compromises. Interviewee 3 mentioned the importance of addressing the lack of overview and status assessment when increasing the cybersecurity levels, further motivating this as a cybersecurity barrier for improved security. The literature and interviews indicated that using a Digital Twin to improve the poor overview, insight,

and monitoring presented a motivational use area. As the industry is trying to assess how assets conform to the requirement of standards such as IEC 62443 and government regulations, from the analyzed data, it is clear that the Digital Twin, with its real-time, or near real-time, visualization capabilities, shows promising prospects. Aggregating and storing large amounts of data in one location presents a valuable target for attackers. A compromise of the Digital Twin will provide the adversary with the same complete overview of the system if targeted, which data indicates is highly probable. Literature and interviews stress the need for high security focus in such implementations. Technologies such as NOA and data diodes are potential tools that can assist in securing the data transmission from barriers to the Digital Twin.

Testing the System Reaction to Change The reviewed literature shows that security patching is a challenge in the petroleum industry. A challenge, according to interviews, is that system complexity makes it difficult to correctly predict the effect of a patch in the overall system. Additionally, some legacy assets can no longer receive updates, removing the ability to fix them. With the zero-tolerance for downtime, patching and policies surrounding their management are areas deemed motivational as a use area for the Digital Twin. According to Interviewee 2, the industry needs to improve and ensure a high level of basic cybersecurity strategies before exploring higher-level barriers. Building barriers on top of a weak, poor foundation could reduce or limit the realized benefits. A Digital Twin, with its system and asset state overview, shows the potential to predict and simulate future states relevant when assessing the "what-if" scenario of patches and updates according to literature. The interview data support this use case. However, the industry appears skeptical about trusting this as 100% reliable.

Improved Emergency and Incident Response When operators are shown malware alerts as an exercise, the lack of confident response supports Dragos's claim that such plans rarely are in place at all [Dra21a]. Interviewee 2 mentioned relevant attack scenarios in training as a key development area of a company related to their work. The statement that "*IT is chasing the incident*" shows that there are limited strategies or guidelines in place to secure more optimal responses. The interviews indicate improved cybersecurity awareness training as a tool for the industry to address the poor cyber culture and motivate further improvements in basic cyber hygiene. Despite its clear potential, this use area is difficult to realize if the whole picture of the system involved is not capturable. As the results show, elements like the situational complexity and some human senses are challenging to replicate virtually. Even if the technology available could realize the use case to some degree, culture and skepticism limit the extent of adoption.

Faster Identification and Detection One of the most predominant cybersecurity barriers used by the industry for ensuring cybersecurity is intrusion- and anomaly detection systems [NFDS20]. Due to the complexity and availability requirements of the petroleum infrastructure, detecting anomalies and intruders is difficult [KA21]. According to the interview data, the level of maturity of IDS as a security barrier is currently low. As the number of vulnerabilities increases, where a substantial number of them resides within the IACS, this motivates identifying ways to increase visibility levels.

Network segmentation and Access Control This use area did not make it to the derived set from the interview data, which presents a deviation between the literature and interviews. However, these concepts should be considered when implementing a Digital Twin to ensure that the system does not affect the SIS. The criticality of high security of these systems became stressed in interviews. So, the action of separating the most critical assets presents a motivational application of the technology.

Maturity levels The maturity levels are included in the final results table to clarify the scope of the motivation and constraints for each use area. The data showed the various perception of where the industry currently is regarding the different maturity levels of Digital Twins. One stated that many believe to be on level 3 but are actually on level 2, while another specified that introducing level 4 would indicate something new to the industry. A standardized general definition of where the industry is currently and what classifies as a Digital Twin on the specific levels did not come forward in literature or interviews.

The main opportunities that motivate the industry in the adoption of Digital Twin technology lie in the use area of asset status overview and monitoring, training and awareness, and patch management. The previous sections have identified potential areas for the technology to improve overall cyber hygiene and other current struggles. The challenges and concerns that limit the implementation of cybersecurity involve several factors, including security culture, skepticism towards the next maturity level, data quality and extraction bottleneck, and authentication concerns. Table 4.6 presents aggregated use areas from an industry perspective supported by literature findings. The table includes identified challenges and limitations relevant to the respective use areas for the specific maturity levels. The maturity levels used are based on the definitions presented in Figure 2.4 in Chapter 2.

The challenges that limit the industry from adopting the Digital Twin for cybersecurity identified in interviews and literature are aggregated and presented in Table 4.7. Two of the identified challenges involved maturity levels. The remaining ones covered the areas of data quality and bottleneck, authentication, human contribution,

and standardization and trust. Due to limited overlap, the table includes all identified challenges from both data sources to provide a more extensive and valuable output.

Table 4.6: Recommended use areas and respective concerns regarding Digital Twin for improved cybersecurity.

Use Areas	Motivation	Considerations	Maturity Level
Awareness and Incident Response Training	Low-understanding of cybersecurity and its effects on safety is possible to visualize and aid in training employee awareness. The IRP can become developed and tested in the virtual space.	Enough data at sufficient quality and frequency is required. The technology should be introduced in a familiar format to ensure acceptance. It is important to focus the fix on challenging areas and not areas that work well today.	Level 3
Visualization and Monitoring of Barrier Status	Improved insight and overview of complex architecture. There is a positive attitude toward aggregating distributed data sources in an easy, commonly understood format. Asset life cycle assessment. Ensure compliance with relevant documentation and regulations, such as IEC 62443 and barrier performance requirements, can become more seamless.	High data quality, timeliness, and amounts are required to realize an overview. A complete overview is near impossible. It will require capturing of human senses, instincts, and offline assets.	Level 3
	Additional ability for the digital to act on the physical using its derived analysis and recommendations. Autonomous operation with the possibility to reduce human interaction and thus human-imposed errors and safety risks.	Same as lower levels. Additional security concerns regarding access control and authentication are needed to secure the control pathway into the physical.	Level 4/5
Patch Management and New Equipment	Simulation of cascading effects of a change can aid in deployment decisions. Visualizing the system's reaction can aid in limiting potential downtime, damage, and cost that might occur when applying changes to the physical system.	High data quality is required to create realistic simulations. Not all assets and aspects of the physical domain can be replicated, implying that not all potential effects will be accounted for.	Level 3
Intrusion and Anomaly detection	System overview can enhance intrusion detection strategies by providing aggregated data that aid in more robust algorithms. Historical and real-time data can improve detection patterns, implying faster and more accurate detection.	Complete system overview is difficult to realize until all assets and aspects of the plant are possible to capture online. False positives and negatives must be limited to ensure reliability in the presented data.	Level 3

Table 4.7: Challenges that limit the industry from utilizing Digital Twins for cybersecurity.

Challenges	**Impact**
Maturity levels	**Level 4-5:** Two-way communication capabilities contributes to increased asset and system interconnectedness, adding to the already existing complexity issues. Strict confidentiality, integrity and availability requirements are needed at high levels to prevent it becoming a new single-point-of -failure. NOA and data diodes are suggested technologies, but explicit safety considerations must be taken to secure SIS.
	Shared perception: The perceived level of the technology currently present in the industry differs among interviewed experts. A clear definition of what each level encompass is needed.
Data quality	Quality and trustworthiness of the digital representation require high data quality and timeliness. Legacy systems and some OT assets present bottlenecks in data extraction, aggregation, and visualization. This bottleneck must present a limitation the industry must consider and address to obtain adequate data integrity and quality fast enough.
Authentication	Strict access control and authentication are required to realize the upper maturity levels while still conforming with security requirements and prevent it from expanding the attack surface.
Standardization and Trust	Standardization issues limits the technology's potential realization. Modelling the complex plant and supply chain with its varying data formats, methods and standards is needed. Limitations regarding operator trust and acceptance of the technology is critical for its success.
Human contribution	Lack of trust in the Twin due to the absence of certain human aspects in the digital representation and skepticism towards new technologies present challenges to consider when assessing adoption.
Security for safety	A holistic cybersecurity approach is needed to ensure shared perception and understanding of cyber risks and threats within the organization across its domains and along the multi-vendor supply chain. There is a need for improved cyber culture and hygiene.

Chapter 5
Discussion

In this chapter, we will discuss the results of the qualitative research related to the Norwegian petroleum industry utilizing Digital Twins for cybersecurity. Table 4.6 and Table 4.7 presents the results derived from the qualitative analysis with findings from the two data sources: the semi-structured interviews and the literature study. For the industry to realize the benefits of the Digital Twin, one must address the limitations and potential challenges to assure a safe and secure implementation. The research questions addressed by this thesis are the following:

RQ1: *How can the Digital Twin technology be used to improve cybersecurity in the Norwegian petroleum industry?*

RQ2: *What are the challenges that limit the industry from utilizing Digital Twins for cybersecurity?*

The analysis showed a lack of a shared understanding of the concept *Digital Twin* and the capabilities of the technology. Section 5.1 discusses this finding and its implications for the derived use areas. As specified in the introduction, we will use terminology familiar in the safety domain when presenting our findings to facilitate and emphasize the concept of securing safety. The result of the qualitative research regarding research question RQ1 is discussed in Section 5.2. The derived use areas of the Digital Twin will be presented in the light of cybersecurity barriers and the bow-tie to see how its implementation can influence cybersecurity in the Norwegian petroleum industry. Section 5.3, revolves around RQ2 and discusses the identified limitations and challenges of the technology before Section 5.4 place attention on the limitations of the overall study, results, and discussion. The main objective of this chapter is to answer the presented research questions and contribute valuable insights on how the technology can aid in increasing both safety and security.

5.1 Definition of the Digital Twin and its Capabilities

There is a need for a common understanding of the Digital Twin concept and abilities to discuss its potential to improve cybersecurity in the petroleum industry. It became evident in the early phases of this work that there does not exist a common understanding and standardization of the term Digital Twin. One finding from the reviewed articles in Section 4.2 is that related works and literature often fail to address the capabilities and abilities of the Digital Twin. Since the Digital Twin can be everything from a 2D model to an autonomous system, one should address this issue since such a definition has an important implication for the research result.

Chapter 2 presents the different maturity levels of the Digital Twin. Related works and literature on the subject reveal the existence of several definitions and maturity specters. The literature study and interviews have revolved around maturity levels 3, 4, and 5. Figure 5.1 reiterates their capabilities for clarification. In this work, these form the basis for the definitions and capabilities associated with the Digital Twin. The two upper levels describe a Digital Twin with the ability to control the physical system.

This thesis's research questions are not directly related to defining the current maturity levels in the industry or providing a standard definition of the Digital Twin. However, the analysis presented in Chapter 4 indicates that this is a critical issue to address. The objective of this thesis is to provide valuable insights into the technology for cybersecurity. Defining the technology and its capabilities is essential in the following discussion since the Digital Twin of different maturity levels has different use areas and limitations. The following section will thus discuss our findings revolving around the current state-of-the-art of the Digital Twin and its related implications for the possibilities and limitations of the technology.

5.1.1 Today's Status from Literature and Interviews

The interviews enhanced the preliminary impression that a clear and standard definition of the technology would be beneficial in addressing today's status and cybersecurity use areas. This fact became evident when the interviewees answered questions regarding the status and potential of the technology today and what they deemed most valuable in the future. During these questions, the characteristics of the different maturity levels were presented. This clarification aimed to ensure a common understanding of the capabilities of the Digital Twin and which type of Digital Twin they had in mind when answering the subsequent questions.

When asked about the technology, one interviewee answered that for the Digital Twin to introduce something "*new*", it had to have two-way communication capabilities and thus reach maturity level 4 or 5. However, another interviewee stated

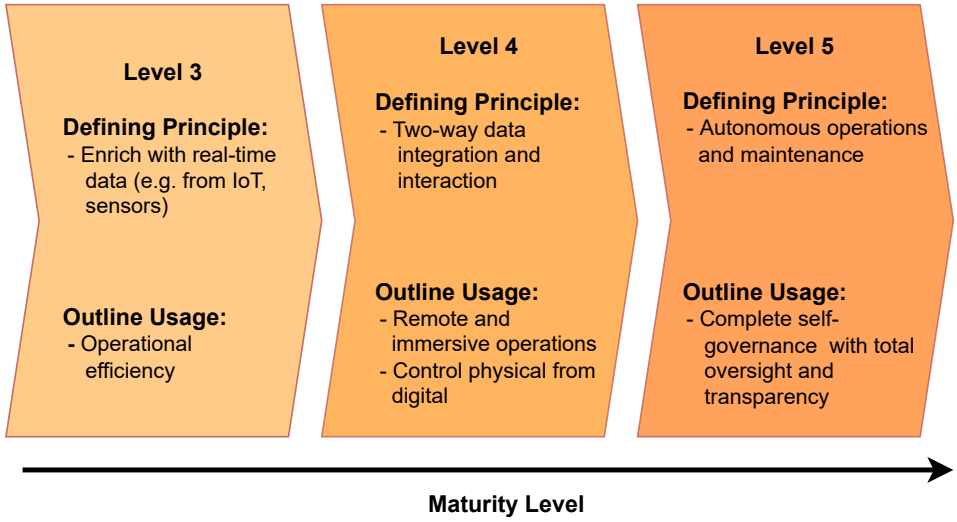

Figure 5.1: Maturity levels 3, 4 and 5. Excerpt from Figure 2.4, adopted from [ESBC19].

that *"some companies believe they have a level 3 Digital Twin when in reality it is level two"*. This inconsistency further motivates the need for a clear definition of the technology and a comprehensive understanding of today's status (Fig. 5.2).

In this study, the focus has been on security-related use areas for the Digital Twin in the Norwegian petroleum industry. Due to this scope, most of the articles and literature analyzed in Chapter 2 and Chapter 4 have revolved around this subject and not other use areas. This fact makes it challenging to address the correct and current maturity level of the Digital Twin in the industry, as most of the literature is only on a theoretical level. However, we find the statement indicating that current Digital Twins are, in reality, of lower capability levels than what the industry believes to be most reliable. The basis of this decision is on the interviewee's knowledge and experience with Digital Twins and pointers from the literature.

5.1.2 Use Areas and their Related Maturity Levels

In order to discuss the technology's use cases and limitations, we must address which maturity level is related to each use case and how this choice of capabilities affects the security and limitations of the implementations.

As presented in Chapter 2, the industry is working with adoptions and ways to benefit from the Digital Twin. From our discoveries, the industry remains to

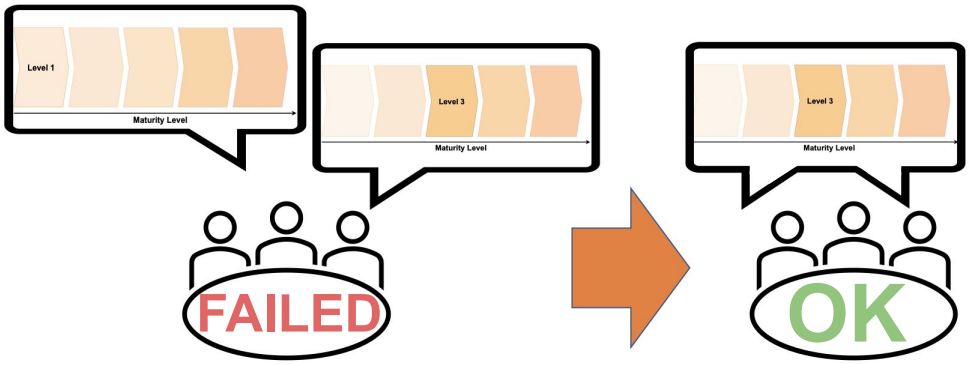

Figure 5.2: Communication failure and success. Adopted from [KYL+20].

realize the upper maturity levels of the technology. The step towards level four would present further opportunities for the Digital Twin to act back onto its physical counterpart. However, taking this step would require an increased security focus. The safety and security risks of opening up for the digital to act back stress the need for strict requirements and considerations. Our data shows that the industry seems optimistic toward the concept of data diodes as a secure gateway from the IACS to the Digital Twin supported by, e.g., NOA.

Based on our data, we regard the implemented state-of-the-art Digital Twins as less impactful than the maturity level 3 Digital Twins. As a result, we reflect on the benefits of realizing cybersecurity use cases of this maturity level. To answer RQ1 regarding how the Digital Twin can be used to improve cybersecurity in the Norwegian petroleum industry, we developed Table 4.6. The table presents the use areas for cybersecurity that we found most valuable based on the analyzed data to implement with the current maturity of the technology and its potential impact on existing cybersecurity barriers and measures. In the first step of realizing the Digital Twin, we recommend relating the use areas to a maturity level 3 Digital Twin. This way, we think the industry can benefit from extensive monitoring, predictions- and analysis of future and current states and visualization without making the Digital Twin too great a source of vulnerabilities.

5.1.3 The Next Maturity Levels

The data analysis showed that if a Digital Twin with two-way communication capabilities became realized, this would make it possible to reduce human involvement further in a transition towards new levels of remote control, automation, and autonomy. As humans are often the reason for security breaches, this could benefit the

industry by limiting the potential threat humans pose to the systems while reducing the safety risks involved with the offshore operation and maintenance tasks.

When realizing the next level of maturity, proper security measures must be in place to preserve the isolation and independence of safety-critical assets, such as the final shut down barrier and the Safety Instrumented System (SIS). If the industry advances in this direction, considerable security focus is crucial if opening up for two-way communication. From the interview insight, this maturity level appears possible with available technology. Based on the received feedback, we derive that the cybersecurity advantages do not appear beneficial enough to compensate for the extensive security risks this advancement would bring.

5.1.4 Summary and Insights

The above discussion shows that an essential step towards realizing the benefits and potentials of the Digital Twin is to provide a standard definition of its abilities and its current status. Before discussing it further, one must ensure a common understanding of the Digital Twin concept. The industry does not agree on what level Digital Twins are today. We think that most implementations are still level 2 and that it would be valuable for the industry to start implementing security use areas at lower levels. Therefore, Table 4.6 connects the use areas to a level 3 Digital Twin. We think the limitations are too forthcoming to implement the highest levels securely. However, many opportunities will come with the following maturity levels. The industry mentions physical data diodes to support this level. Examples of possibilities related to the next generations of Digital Twins are faster incident response and segmentation of the networks autonomously in the case of cyber attack.

5.2 Motivating the Digital Twin for Cybersecurity

To answer RQ1: *"How can the Digital Twin technology be used to improve cybersecurity in the Norwegian petroleum industry?"*, we will discuss the identified use areas of the Digital Twin together with the relevance and trustworthiness of our findings. It is not in the scope of this thesis to provide a comprehensive definition of the Cybersecurity Barrier Management (CBM) framework or concepts, as this is an ongoing project [21b]. However, as expressed in Chapter 1, we find it valuable to discuss the findings in the bigger picture of cybersecurity, using terminology from the safety domain. Therefore, the discussion includes concepts with close relation to the safety barrier memorandum, such as cybersecurity barriers, CBM, and performing influencing factors (Sec. 2.2 and Sec. 2.3). We included these concepts in the interview conversations to ensure the context of the findings.

The data analysis revealed that one of the ongoing projects involving Digital Twins for cybersecurity for an offshore plant uses the bow-tie or the swiss cheese model. This model is used in the barrier memorandum to visualize all barriers included in an incident, promoting a holistic view of safety. We will investigate and discuss how cybersecurity and safety within the industry can benefit from a Digital Twin improving and maintaining cybersecurity barriers visualized in a bow-tie diagram.

5.2.1 Bow-Tie

Figure 5.3 is an example of a bow-tie visualizing a set of cybersecurity barriers to prevent and mitigate a malware attack, adopted from [DNV16]. This specific bow-tie is not a verified result in our thesis and is not considered a complete representation of cybersecurity barriers included in a malware attack. It is solely an instrument to discuss our findings. The cybersecurity barriers in the diagram include the resulting use areas of the Digital Twin presented in Table 4.6. The bow-tie diagram includes network monitoring, security patching, and network segmentation as preventative cybersecurity barriers and IDS and IRP as reactive cybersecurity barriers. The following discussion involves the motivation for these choices. Interviewees highlighted these barriers as challenging with today's approach to cybersecurity while also presenting the motivation of using the Digital Twin to improve them. The following sections will discuss the identified use areas in light of the bow-tie.

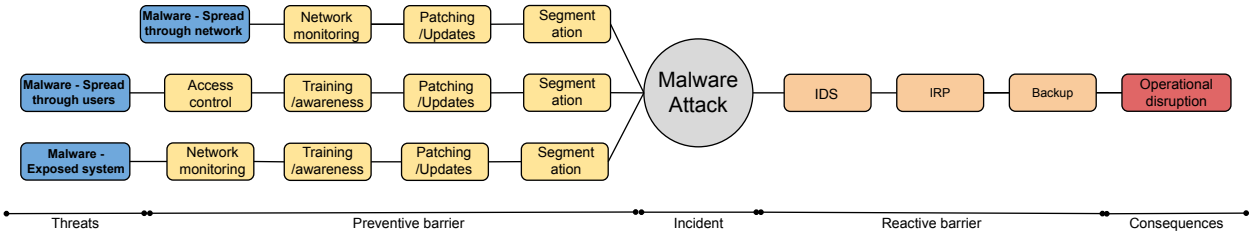

Figure 5.3: Bow-tie model example. Adopted from [DNV16].

5.2.2 Cybersecurity Barriers and Influencing-factors

Chapter 4 identified a set of cybersecurity use areas that could benefit from Digital Twin implementation in the Norwegian petroleum industry. The following discussion revolves around the findings presented in Section 4.4. First, the discussion considers the four use areas which fall within the presented definition of a cybersecurity barrier (Sec. 2.3). These comprise *IRP*, *system patching and testing*, *IDS*, and *segmentation and access control*. Each cybersecurity barrier enhanced by the Digital Twin is

discussed in light of the bow-tie model. This visualization aims to promote a holistic overview of the effect the technology can bring to the overall cybersecurity of the industry.

Next, the discussion revolves around the two remaining use areas that do not conform with the cybersecurity barrier definition. These involve *awareness and incident response training* and *visualization and monitoring of barrier status*. We consider both to comply with the performance-influencing factor definition provided in Chapter 2.2. Hence when addressing how Digital Twins can improve cybersecurity, the influencing factors align with this objective. The section closes by discussing our findings concerning the poor *cyber hygiene* and the technology's potential to address this issue. It also discusses the importance of keeping humans involved and using the technology as a tool in improved *decision-making* despite its potential to facilitate complete automation.

Security Patching, Testing and Updates

Security patching is present on the left side of the bow-tie diagram in Figure 5.3 as a preventative cybersecurity barrier. Modeling security patching as part of the bow-tie is intended to highlight the importance of this measure to ensure the safety and security of the IACS during a cyber incident. Interviews mentioned management and status of outstanding patches as basic cybersecurity practices. The Digital Twin can store historical and real-time information and run continuous predictions [BT21]. We think that information about all outstanding patches and their impacts could be beneficial to visualize in a bow-tie to discover when the status of the patches is degrading the barrier performance.

The literature implies that improved continuous patching is one of the primary motivators for the Digital Twin for cybersecurity [BT21]. The interviewees mostly agreed but stressed the importance of knowing the technology's limitations. Predictions are just as good as the underlying data, making it essential to involve the human in the decision-making process for patching [FFDB20]. However, from the analysis, we find this to be one of the main motivations for implementing a Digital Twin for cybersecurity, removing personnel workloads and thus facilitating better decision making [WWP+20]. A Digital Twin of maturity level three would be sufficient to implement this feature. However, the analyzed data indicate that it would be valuable in the future if the technology could automatically install patches in a manner that optimized timing motivated by the availability and downtime constraints.

Testing the system's reaction to change is challenging to practice today with the high availability requirements and the potential negative impact such actions may pose. It is a challenge in the OT domain as systems are complex, making it difficult to predict an action's impact on surrounding components and effect on safety,

operation, or reliability if performed incorrectly [09b]. If sufficient data amount and quality are captured, using the Digital Twin to simulate system updates and introduce new equipment can provide operators with valuable knowledge in their decision-making and risk assessments. IEC 62443-2-3 confirms that patching is a big task as it comprises analyzing patch information, testing, ensuring backups, testing again, and logging all documentation of the changes [09b]. If the cost of applying patches is higher than the risk of running the system un-patched, other cybersecurity barriers must ensure that the vulnerability is not exploitable [DNV17]. Interviews emphasize that keeping the patch status of equipment is a basic cyber hygiene activity. Visualizing this in an orderly and real-time manner can benefit the organization by contributing to more seamless communication as a part of maintenance work.

Faster Identification and Detection of Threats

One central cybersecurity barrier the industry uses for ensuring cybersecurity is an intrusion- and anomaly detection systems [NFDS20]. Figure 5.3 models this as a mitigating cybersecurity barrier in a malware attack. It falls under our definition of a cybersecurity barrier as it is a direct action in a sequence of events, detecting and alerting possible incidents, violations, or threats. Literature highlights the poor cyber incident detection rates resulting from the increasing complexity. One interviewee supports this claim as they stressed the low maturity of current IDS as a security barrier in the industry. Due to the complexity and availability requirements of the Oil&Gas infrastructure, detecting anomalies and intruders is difficult [KA21]. As the number of vulnerabilities increases, where a substantial number of them resides within the IACS, this motivates identifying ways to increase visibility levels. The seminars we attended mentioned that an average of 10,000 errors occur without acknowledging them as a potential attack. This fact shows a lack of understanding and awareness of the persistent cyber threat. Available data from previous attempts, attacks, and incidents could aid the Digital Twin in learning to detect malicious or dangerous patterns and activities not acknowledged with today's strategies [NFDS20]. We derive from the interviews and literature study the opinion that improved prediction and detection are possible by aggregating alerts and historical data, indicating the incentive for this as a motivational use area for the industry.

The industry highlights the difficulty of realizing Digital Twins on a larger scale, where the older assets present a challenge. Using a Digital Twin for anomaly and intrusion detection will require defining and specifying the scope of what categorizes as anomalies and intruders. Having the Digital Twin make these decisions after providing the required definitions still has the potential of providing false positives and negatives if the data is not complete [EE19]. So, the data foundation the Digital Twin builds upon becomes a critical element in its success as a tool for improved resilience.

Network Segmentation and Access Control

The reviewed literature indicated that improved network segmentation and access control would be one of the main motivating factors for implementing the Digital Twin for cybersecurity. However, interview data did not reflect this. One of the interviewees mentioned the importance and problem of assuring that there does not exist dependabilities between cybersecurity barriers. From the literature review, exploring dependabilities through status monitoring and predictions is a feature of the Digital Twin, possibly addressing this challenge (Sec. 4.2.1). One possible explanation of the difference between the industry conversations and the literature is that this use area could require a maturity level 4 or 5 Digital Twin. The interviews indicate that the status of the technology today is not secure enough to implement a Digital Twin with bi-directional communication capabilities.

Strict and strategic segmentation and access policies can aid in "*eliminating or minimizing the harm of an incident or attack*", conforming with the definition of cybersecurity barriers. As stated in Chapter 2, zones and conduits are a central concept in this series, providing a means for improved access control. A simplistic example of zones and respective conduits are shown in Figure 5.4 derived from the Recommended Practice (RP) proposing implementation of the IEC 62443 series of standards. Despite the concept not being mentioned specifically during the semi-structured interviews, one interviewee indicated that the Digital Twin bow-tie could reflect the firewall status, rule change, alerts, and locations in an orderly fashion. Thus, using the technology for network and user account status implies motivational use areas contributing to improved cyber hygiene.

Improved Incident Response Plan, Training and Awareness

Incident response plan (IRP) is included in the bow-tie in Figure 5.3 as a reactive cybersecurity barrier as the plan represents an action that directly impacts the chain of events that unfold in a cyber attack. The plan has the intention to aid in identifying incidents earlier and ensure the execution of appropriate actions to limit consequences [10]. One aspect of the barrier management process is measuring and validating the barriers' performance. One of the interviewees mentioned assessing non-technical barriers, e.g., incident response plans, as challenging. However, modeling it as a cybersecurity barrier emphasize its importance for overall cybersecurity.

Training as a Barrier Modeling training and awareness as a barrier is not standard practice as it is not a specific action taken during an incident. However, one interviewee mentioned that it could be beneficial for the overall understanding of the cybersecurity status of the company if training became a part of the cybersecurity barrier definition. This way, the bow-tie could indicate when and if personnel should perform new training sessions.

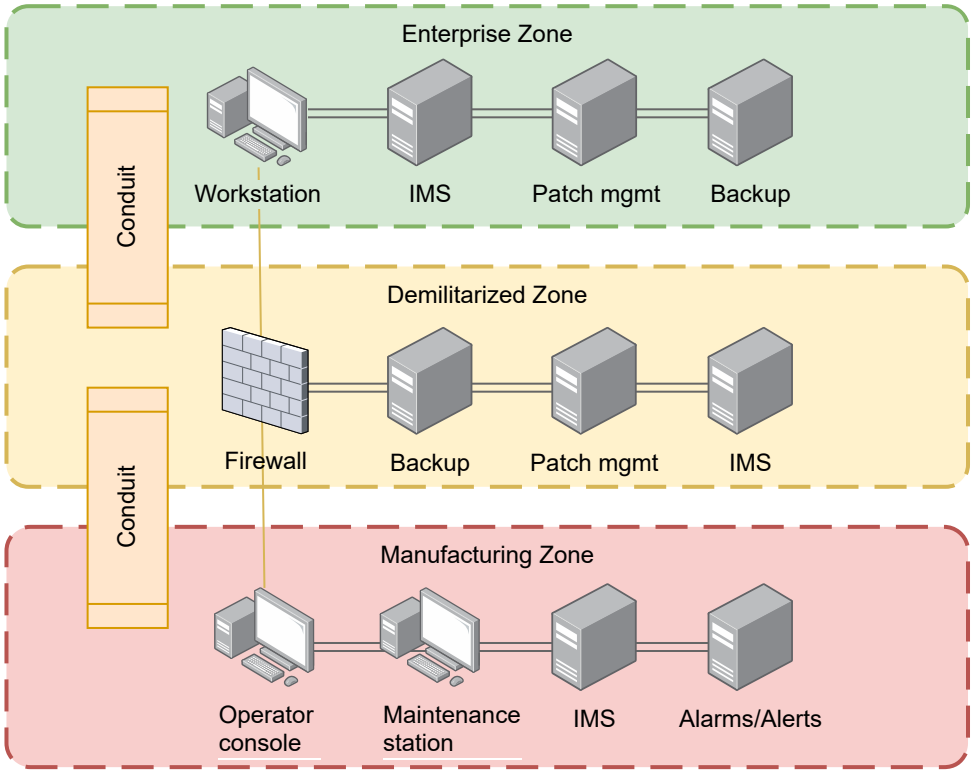

Figure 5.4: Simple zones and conduits example. Adopted from [DNV17].

The literature state that organizations often lack sufficient IRPs and respective testing of them to ensure high-quality response actions [Dra21a]. The interviewee's experience confirms this issue. One experience stated that when an operator was shown a malware alert unexpectedly during work, no one knew what to do. The characteristics available from Digital Twins at level 3 can thus provide a domain and ability to develop, update, test, and train operators and other relevant personnel on the IRP and additional awareness exercises. Additional ability to perform impact predictions and involvement of both IT and OT consequences can improve overall response actions. Based on the analyzed data, both industry and literature agree that developing robust plans that can subsequently become tested in practice could improve and optimize cyber attack response and awareness.

Regularity of Training Regularly training all personnel on cybersecurity scenarios is a way of increasing cybersecurity hygiene [Ire22]. IEC 62443-2-1 mentions emergency response plans and awareness training as required countermeasures for

cyber attacks [10]. However, it does not indicate how often one should perform new training exercises or how one should measure and validate the performance [10]. One of the Interviewees mentioned this as a challenge when assessing non-technical barriers.

> *"...we will have an annual exercise practicing to disconnect from the system. ...this exercise could be done more frequently."*

We derive from the analyzed data that making the training software more accessible during the whole plant life cycle would facilitate more frequent exercise execution. Since the Digital Twin includes all life cycle documentation and data, we think that using this technology would improve measuring and validating the performance of this countermeasure by keeping records of personnel training. Allowing for the visualization of status regarding who had performed what exercise and when tests were conducted last in a more orderly manner, which became highlighted as a motivational use area in interviews.

Realistic Scenario Training The interviews pointed out that the potentially harmful effect of testing IRPs on the physical systems presents a challenge. The data indicates that the organization can more clearly define guidelines for who is responsible for responding and what they should do by using the Digital Twin to test different response strategies to critical scenarios. Awareness of the imminent cyber threat against the industry can increase by incorporating IT/OT simulation exercises that show both security and safety consequences of attacks [SS20]. We derive from the findings that incorporating consequences from both domains can emphasize why addressing security to preserve safety is critical to operators and stakeholders. From this, we derive that improved training with increased frequency would be one of the central motivators for implementing the Digital Twin for cybersecurity.

Monitoring and Visualization of Cybersecurity Status

One of the most challenging cybersecurity aspects in the industry is legacy components with a long life cycle [EE19]. Another is that vulnerabilities can be latent in the system for several months or years before they are recognized [Dra21b]. The literature study indicates that the Digital Twin can be an asset in confronting these challenges through extensive monitoring with I4.0 components (Sec. 4.2.1).

> *"It is not just about collecting data and knowing the status but forcing people to visualize this and do the things that make the status good. Make operators think about cybersecurity as they think about safety. "*

One of the interviewees made this statement when asked how a Digital Twin could improve cybersecurity in the context of barrier management. The Digital Twin can extensively monitor a system or assets and compose this near real-time data with historical and semantic data [EE19]. For this reason, the data analysis concluded with *holistic status overview* and *monitoring* as important use areas and motivation for the industry to implement Digital Twins for cybersecurity (Table 4.6). Based on this, we think visualization and monitoring of barrier and system status through a Digital Twin could improve cybersecurity hygiene of personnel by *"forcing people to visualize"* the effect of degrading cybersecurity barriers.

To our knowledge, there have not been any actuators in the petroleum industry implementing Digital Twins to monitor cybersecurity barriers. However, one of the central use areas for the technology across industries is predictive maintenance [BFP+18]. This activity requires monitoring and analysis through the life cycle of an asset, making it plausible to expect this to be a useful area in cybersecurity as well. For the industry to realize the potential of this use area, high data quality, reliability, integrity, and fast transmission are required. If realized, the interview data indicates that this will endorse their current strive to map conformance to the developing IEC 62443 standard and ensure barrier performance requirements. According to interview data, assessing this conformance is a current struggle with today's operation. Figure 5.5 provides a visualization of this issue.

Figure 5.5: Interviewees stated the challenge of assessing the system compliance with security standards.

A bow-tie model is a familiar tool used by these stakeholders for handling safety.

One of the interviewees mentioned that visualizing the status of cybersecurity barriers with this model could increase awareness and understanding of cybersecurity incidents at all levels of the organization:

> *"Suppose cybersecurity is embedded in the bow-tie and its roles up to a single barrier. In that case, operation management can look at all overall barriers and see one of which is cybersecurity, making this a concern at the right level in the organization."*

Figure 5.6 shows *monitoring* as a degrading preventative cybersecurity barrier. It is normally not considered a barrier as it is not a specific action in a sequence of events. However, in the figure, it is visualized as a cybersecurity barrier as it facilitates the discovery of threats, vulnerabilities, and attacks (Section 4.2.1).

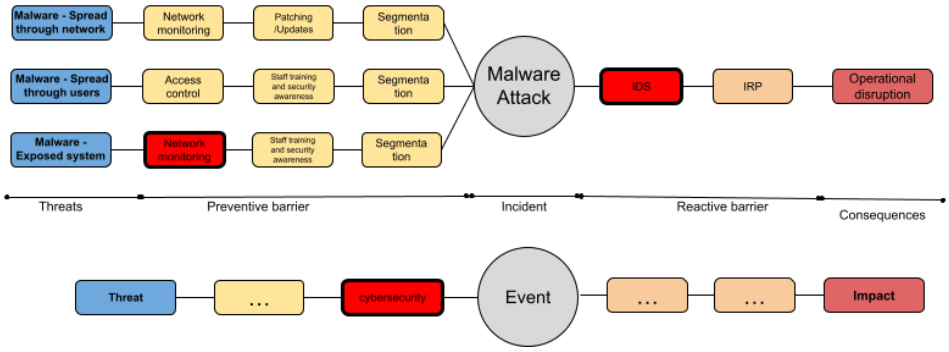

Figure 5.6: Visualization of degrading cybersecurity barriers and its effect on the overall bow-tie.

Cybersecurity Hygiene

One concern relevant for organizations and the stakeholders, as well as operators, is cybersecurity hygiene [Ire22]. Cybersecurity hygiene is a set of practices organizations and individuals regularly perform to maintain the health and security of users, assets, networks, and data [Ire22]. Enhancing the human contribution to adverse cybersecurity situations involves improving cybersecurity hygiene, awareness, and cybersecurity understanding among all personnel [21c]. A finding from one interview is that:

> *"In most companies, even large oil&gas companies, the concern about cybersecurity gets discussed in IT-teams and often not on the operational side."*

Irei (2022) expresses the importance of not limiting cyber hygiene to IT personnel and security managers and emphasizes that it is a shared responsibility that all departments and users must prioritize. The results presented in Section 4.4 imply that the Digital Twin could aid in improving overall cybersecurity hygiene through awareness, training, and visualization, not only for operators but for multiple levels throughout the organization.

Support Decision-making

The analysis in Chapter 4 resulted in four recommended use areas for the Digital Twin and related prerequisites promoting secure safety. The data identify that implementing a Digital Twin could remove humans from decision-making processes and potentially hazardous situations in offshore plants with a higher level of automation and remote control [WWP+20]. Conversely, one of the interviewees mentioned that removing the human element from the process would lose valuable insights from intuition and senses not yet possible to model in a Digital Twin. All interviewees indicated that extensively replacing on-site personnel would not be beneficial, even if the technology could facilitate this. Industry initiatives regarding human-in-the-loop reaffirm this statement [DCu22]. The PSA has established an initiative to increase operational cyber resilience by clearer priorities on human performance through work culture and the promotion of human-centered technology development [Saf21]. From these insights, we derive that the industry's focus when implementing the Digital Twin for cybersecurity should be not to replace but to assist and facilitate human decision-making and cybersecurity awareness.

5.2.3 Summary and Insights

To summarize, this section has discussed six use areas for the Digital Twin in cybersecurity in light of the barrier management concepts: bow-tie, barrier, and performance influencing factor. In the final table (Fig. 4.6) IRP and awareness training are presented together. Network segmentation and access control were not included in the table as this did not become highlighted throughout the interviews. Including this use area in the discussion was motivated by its importance and relevance to conforming with IEC 62443. Patch management, IDS, and IRP conformed with the definition of a cybersecurity barrier, positioned to both sides of the bow-tie. Awareness training and monitoring and status visualization present the last two use areas identified as performance influencing factors, both of which support the motivation for improved cyber hygiene.

When discussing the two data sources, a clear overlap between identified use areas is visible. As unstructured interviews and seminars influenced the scope of the literature study to ensure the highlighting of areas of value to the Norwegian petroleum industry, this overlap, with network segmentation as the only exception, was not

surprising. Network segmentation not being mentioned during semi-structured interviews was unexpected. The deviation may indicate that this use area would require higher maturity levels or extensive operational changes, which the industry may not necessarily prioritize or be ready for. Hence this is not included among the main motivational use areas for the Digital Twin for improved offshore cybersecurity.

The highlighted use areas included in Figure 5.6 indicate that one side of the bow-tie did not gain prioritization over the other. We consider this a surprising result, as one of the interviewees states that ongoing research indicates a shift towards Consequence-driven Cyber-informed Engeneering (CCE). In CCE one assumes that an attacker can infiltrate the system, thus prioritizing the reactive cybersecurity barriers. The interviewee with expertise in cybersecurity in OT supported a focus on the right side, increasing the statement's reliability. Even if the use areas did not imply a specific focus area within the bow-tie, several interviews stressed the importance of securing safety by focusing on securing the final barrier and Safety Instrumented System (SIS), further supporting a focus towards the right side.

Another finding was the heavy focus on improving overall cyber hygiene and awareness, implying that the current level of cybersecurity understanding is insufficient. As training and awareness do not fall within the definition of a barrier, all interviewees highlighting this as a central motivator stress the current need for improvement in this area. From this, we find that implementations of Digital Twins for cybersecurity in the Norwegian petroleum industry should include a heavy focus on adapting the solution to suit the use areas of training, testing, and other awareness-enhancing activities that will inevitably contribute to improved cyber hygiene. The statement from the interviewee with expertise on Digital Twins and IACS cybersecurity stating that basic cybersecurity hygiene in many cases is lacking supports this.

Overall the discussion motivates the choice of the identified use areas presented in Table 4.6, including those where the two data sources comply. Based on the discussed findings, current industry cybersecurity issues are possible to enhance through implementing Digital Twins on level 3, aiding in cyber awareness and still addressing the importance of keeping human-in-the-loop. We believe the identified use areas to be a reliable set of motivating factors as these are areas that characterize and address current challenges. Next, section 5.3 presents the limitations and challenges related to realizing the identified use area.

5.3 Challenges and Limitations of the Digital Twins

The introduction of this thesis stresses the PSA requirement implying that implementing new technology should not compromise safety and security [18a]. The following section discusses research question RQ2: *What challenges limit the industry from*

utilizing Digital Twins for cybersecurity?, addressing the PSA requirement. The results presented in Table 4.6 and Table 4.7 forms the basis of this discussion.

A Digital Twin consists of numerous fundamental technologies for, e.g., processing, analysis, communication, and data storage. Each one should be assessed in a cybersecurity context to gain a complete overview of the potential limitations and challenges of the Digital Twin. The reviewed articles in this thesis focused on implementations that complied with the AAS defined by the German Plattform Industrie 4.0. This specification implies a correlation between the identified challenges and their choice of technologies, for example, OPC UA and NOA. The lack of a clear and standardized definition of the Digital Twin concepts and capabilities makes it challenging to present common limitations for all Digital Twin applications. This discussion does not include data storage and processing limitations due to time constraints. It does not claim to be a comprehensive risk analysis of the technology and industry but enlightens the most prominent challenges identified through the qualitative research approach.

Standardization

To our knowledge, there is no current standardized approach to how the Norwegian petroleum industry implements technologies like AAS to ensure security and safety conformance. Section 2.4 presented RAMI 4.0, as an in-development framework for Digital Twin implementation. RAMI 4.0 was not brought forward during interviews, possibly due to its novelty and conceptual nature. However, the interviews mentioned NOA with data diode as a suggestion for secure communication. Literature, however, stated that the concept of NOA does not sufficiently address security and ensuring of SIS performance, which is highly critical to secure within the petroleum industry [OBH+22].

DNV recently published RP-A204, which addresses all phases of Digital Twin adoption on how organizations can assure the quality and trustworthiness of the technology [DNV21]. With its scope stretching from concept to operation, it presents a sound starting point for further assessment and shows that this area is of rising interest. Section 2.3 highlighted that the industry already struggles with outdated or in-development standards. With the increasing supply chain and multi-vendor involvement, ensuring security level conformance is challenging when stakeholders address security differently. Several benefits brought forward by the Digital Twin result from improved visibility and compliance during the plant's life cycle across the supply chain [WGE+17]. Interviews emphasize standardization of implementation and information models as prerequisites for realizing these benefits.

Human involvement and trust in the system

DNV-RP-204 *Qualification and assurance of Digital Twins* mention valid and accurate data and confidence that the Digital Twin mirrors the physical asset over time as prerequisites for an end-user to have confidence in the technology [DNV21]. The interviews imply the importance of communicating the limitations of the technology to operators to assure they do not falsely trust the system.

The reviewed literature did not bring forward humans as a big limitation for Digital Twin implementation. However, interview data highlighted that utilizing Digital Twins still requires involvement from human operators. The main arguments were the lack of sensors and actuators capturing human characteristics like the sense of smell, intuition, and instincts. These are all essential factors for sensing hazardous situations. With some assets not being detectable online, capturing a complete picture of the entire plant is near-impossible. This statement was made by an interviewee when discussing the limitations of the technology. Without a complete digital image of the plant, the trust in the Digital Twin remains limited. Despite this, another interviewee emphasized the future possibility of modeling the human as an asset as a motivation, as this reduces the possibility of human errors and the expensive and dangerous process of shipping personnel offshore for operation and maintenance.

Reaching Higher Maturity Levels

A clear understanding of the maturity levels of Digital Twins already present in the industry is needed. With data quality limitations and the current lack of technology standardization, we find it most valuable to implement a maturity level 3 Digital Twin without bi-directional communication and automation capabilities. If not executed securely, the realization of these capabilities could expose the system to a single point of failure [EE19]. Interview data shows that the industry is realizing the benefits of the technology at lower levels. As its benefits gain more acknowledgment analyzing and realizing higher maturity levels is an inevitable outcome. It will, however, require extensive research to address the security and safety considerations and requirements that come with bi-directional communication and autonomy.

5.3.1 IT/OT non-alignment of Data Requirements

The Digital Twin is in the subsection between the physical and the digital world, and in this work, we explore the Digital Twin in the cut between IT and OT. One fundamental challenge, visualized in Figure 5.7, is the difference in prioritization of data requirements between the two domains, affecting security and safety. We find it valuable to address these inconsistencies to understand the challenges faced by the industry in implementing Digital Twins for improved cybersecurity. A prerequisite

for the Digital Twin is extensive use of sensors to collect data [WSJ17]. The virtual Twin aims to become a replica of its physical counterpart and is consequently highly dependent on datasets with high integrity, reliability, availability, and quality [ASM+21]. In one of the interview's, it was stated that implementing the Digital Twin to its full potential could never happen before addressing the data collection bottleneck and integrity limitations.

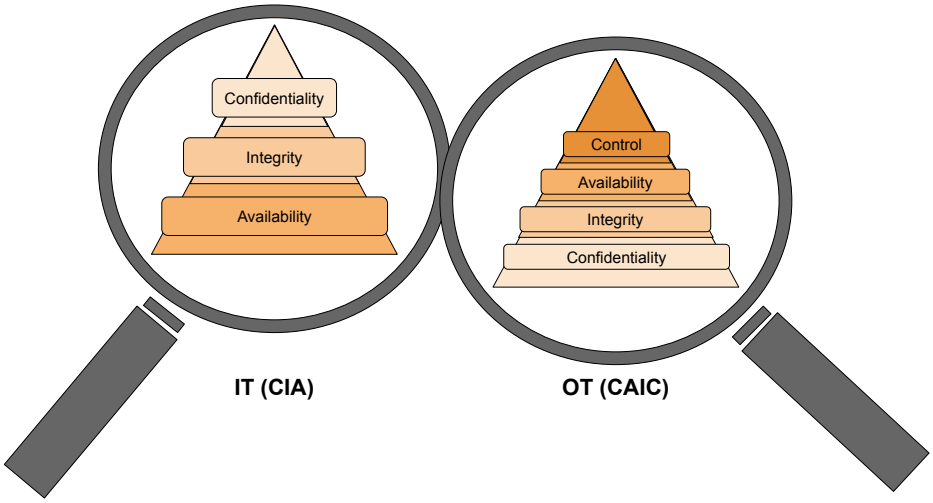

Figure 5.7: IT- vs OT-system priorities, IT prioritise confidentiality while the primary focus in OT is on control. Derived from [HOG+21].

Control

IEC 62443 states that security incidents in the control system should not affect SIS or other safety-related functions [10]. Maintaining the control of all assets and systems to ensure the safe operation is the primary objective of OT cybersecurity but is not mentioned as a requirement in the IT domain [HOG+21]. There is a clear principle that no systems at the OT level should be affected by new digital solutions, but this is challenged by the advantages of new technology like the Digital Twin [HOG+21]. Several interviewees mentioned the separation of the SIS and SAS systems and the Digital Twin as a priority to ensure that the safety and security of the system are intact. One statement made in the interview 1 involved several implications concerning this:

> *"Existing SAS and SIS lack isolation and security. Safety is exposed if an incident develops in a company's Safety and Automation Systems. Therefore, it*

is important to isolate these, in particular SIS, due to the importance of keeping the final barrier, the red fail-safe button, unhackable at SIL 4".

The statement implies that the separation of the SIS is not sufficiently ensured today. It also implies that the Digital Twin should be separate from the SIS to prevent negative effects on the last barrier. The reviews literature did not addressed how one should ensure that the Digital Twin is not affecting the SIS. This separation is thus a problem area that requires research and standardization before securely implementing the technology. Onshus *et al.* (2022) state that the zone concept from IEC 62443 present one opportunity for isolation of these systems by locating them in their own zone as a means to separate them and endorse access control [OBH+22]. Despite the technology showing promising complexity-reducing aspects, one of the interviewees stressed that this opportunity relies on how it becomes incorporated with IT and OT systems. Moving the control domain to solutions such as the cloud will threaten the domain's independence requirements, an issue already present due to the digitization trend.

Availability

The second topmost requirement for critical infrastructure cybersecurity is availability [Gil21]. This fact contrasts with the IT domain, where availability degradation is generally accepted to some degree [Mis]. The Digital Twin requires a large amount of semantic data to be considered a replica of the physical system. This thesis did not include experimental studies of the current or required bandwidth. However, Interviewee 4 highlighted that this data needs to be sent through the existing infrastructure, possibly compromising the availability of other services. We do not have sufficient amounts of analyzed data to say precisely how impactful this problem is. However, we find it plausible to consider the trade-off between quality real-time data in the Digital Twin and impacts on the system's availability. Insufficient amounts of data will affect the services the Twin can provide [ASM+21], while too much data can affect communication to and from control systems. One example from the interviews is incident response capabilities. The fundamental data must be sufficient and reliable for the system to support personnel in decision-making.

IEC 62443-3-3 motivates that one should ensure the availability of components against the degradation or denial of essential services [oAut20]. The extensive use of smart sensors to support the Digital Twin increases the system's attack surface and can affect system availability [FFDB20]. The literature study revealed that this could also concern lower maturity levels of Digital Twins. Today, the communication channel from the digital system to the physical asset is considered secure, but in reality, systems requesting data can be vulnerable to attacks. Two interviews indicated this weakness, emphasizing the need for a solution before securely implementing

the Digital Twin. Both interviews and literature refer to data diodes as a possible mitigating factor. Data diodes are a concept in NOA which is a technology and standard present in the specification of the AAS. One of the interviewees specifies that software data diodes are insufficient to secure the last barrier, the SIS. The industry should use hardware-based data diodes to secure and separate the Digital Twin from this barrier. The argument from interview 1 for choosing hardware over software is that programmable software is possible to hack. We find prioritizing the system's availability important when implementing the Digital Twin. The system must be secured to resist failure during DoS attack to ensure consistency with the related requirements.

Integrity

Integrity is the property that data remains unchanged, destroyed, or lost, and it is essential to ensure the safety and availability of assets [HOG+21]. The IT domain considers this attribute the second most important, contrasting to priority in OT systems. The literature mentions integrity and data quality as an essential foundation of the Digital Twin. This foundation would require secure communication between the physical asset and its digital replica, challenging current technology deployments, especially those in real-time [HPM+21]. Hanssen *et al.* (2021) list data quality and integrity as one of the six recommended focus areas for digitalization in the petroleum industry. The article states that the quality of digital services such as a Digital Twin directly depends on the data quality. This attribute will be just as crucial for safety as for security [HOG+21]. Significant work is still required to implement Digital Twins, providing adequate data quality and detail. Several interviewees highlighted the challenge of converting data from analog to digital without significant compromise of integrity and quality. This issue adds to the already identified threat to the technology's trustworthiness concerning the absence of certain physical characteristics. Testing these transmission limitations is necessary when considering the higher maturity levels as a tool for cybersecurity.

Confidentiality

Confidentiality is the property that information is not made available or disclosed to any unauthorized system entity, including unauthorized individuals, entities, or processes. The literature analysis revealed that ensuring authorized access constraints to system facilities and data is essential in protecting confidentiality [HPM+21]. One example from the literature is the scenario where an attacker compromises confidentiality and gains access to the Digital Twin. The attacker then has a digital replica of the physical system and has much more knowledge about the system than otherwise [HPM+21]. The arms race between attacker and organization was stressed as a possible vulnerability of complete virtual system overview during an

interview. Thus, a priority when securing the Digital Twin should be to ensure a high level of confidentiality to preserve security and safety levels. There is a need for a standardized lightweight encryption scheme to support the confidentiality and availability requirements of the assets represented by the Digital Twins. Although extensive work is needed to ensure the confidentiality of the transferred data, protocols such as OPC UA, standardized by the German Plattform Industrie 4.0, MQTT, and MTConnect, show promising results for the communication from the physical to the digital. The problem with confidentiality in OT systems is that it can sometimes compromise availability requirements, which underlines the need for a lightweight solution to address this.

5.3.2 Summary and Insight

Table 4.7 presented the discussed challenges in light of information presented in Chapter 2. Improved cyber culture and a shared perception of where the industry is currently at regarding cybersecurity present a preliminary step before adding to the increasing complexity. Interview data and literature agree that levels 4 and 5 of Digital Twin maturity are only aspirational and in the concept development phase. Thus, aiming to realize the level 3 Twin on a larger scale and including cybersecurity enhancing use areas presents an unrealized potential.

Further, the results suggest that *data quality* is one of the primary technical considerations for securing safety. The DNV quality assurance recommended practice shows that the industry is motivated and focused on addressing this. High data quality and frequency are prerequisites to realize the possibilities of the Digital Twin as a tool to visualize the complex and intricate supply chain and legacy systems. Despite current efforts to adopt the technology, our insight from professionals indicates a difficulty with making all assets available online, indicating a low probability of achieving a complete virtual replica. Therefore, these constraints and limitations restrict the level of completion of the presented use areas. Despite advances in sensors and actuators, some human characteristics are not yet possible to capture virtually. These arguments emphasized the need to keep humans involved. The optimism toward increased autonomy is still present.

Overall the discussion of priorities in light of OT and IT highlight the challenges and limitations the industry must consider and address to realize and meet the requirements for Digital Twins in the identified use areas at the considered maturity levels. As the arguments presented are derived from parallel analysis of industry interviews and literature data, the reliability and usability of the provided insight are limited to the petroleum industry. If the Norwegian petroleum industry allocates resources to the identified challenges, they can arguably obtain the ability to realize some of the benefits from the Digital Twin use areas at a higher maturity level and

scale than currently present.

5.4 Limitations

The conducted thesis work was subject to a time constraint of 21 weeks. A large part of answering the thesis statement was based on academic research on Digital Twins and cybersecurity, including articles, reports, guidelines, standards, and regulations. A trend regarding academic research is that articles with a positive result are published more frequently then articles with less impacting results. This may have impacted the ratio between sources answering research question RQ1 and research question RQ2.

Because of the mentioned time constraints, conducting a systematic literature review encompassing all available research from these areas was not feasible, limiting the scope of the literature search to a subset of areas based on indications from the industry to preserve applicability. Narrowing down the scope may have resulted in an incomplete understanding of the technology's limitations and possibilities within the area of cybersecurity.

The research topic of Digital Twins in the context of cybersecurity and Barrier Management is a novel research area yet to be documented at the time of writing. Analyzing these concepts together presents a new perspective and relevant insight for the ongoing research and development of the concepts. The lack of previous knowledge on Digital Twins and AAS resulted in a significant amount of time required to comprehend the technology. Continuous learning about the subject may have affected the quality of questions in the earlier interviews. Additionally, the industry and professionals with knowledge of more than one of these topics proved hard to identify. As a result, the interview data stemmed from a small set of interviews. We would have liked to have interviewed more professionals to secure and obtain a stronger research foundation. Thus, data restrictions have limited the study's generalizability and reliability.

A limitation of the study was the interviews as a means of data collection. Limited experience with conducting interviews will have affected the execution and the subsequent data analysis. Conducting interviews in parallel with a litterateur review further impacted the direction of the conversation and wording of questions to some extent. However, with each conducted interview, experiences were obtained. With added experience, better follow-up questions and improved wording aimed to limit leading questions and improve the overall quality of the data collection. Lastly, the conducted interviews involved both Norwegian and English speakers. The thesis being written in English means that the data collected in Norwegian needed translation. Misinterpretation may have occurred in this process which would have

affected the results and analysis.

The discussion surrounding maturity levels, where the industry is today, and what lies ahead brings a futuristic element into the equation, as this is the next step if the industry is going to advance and take advantage of the possibilities the technology brings. We chose to limit the research and analysis to highlighted areas of cybersecurity in the context of the upper levels as these encompass the new next step for the industry regarding the technology in this context. These areas were chosen based on feedback from the industry and maturity in the literature to ensure that the result conformed with the industry's needs and current focus.

Chapter 6
Conclusion and Future Work

This thesis has investigated Digital Twins as an emerging technology and its effects on cybersecurity and safety. A qualitative study has been performed comprising the semi-structured interviews and the literature review, analyzed in the context of barrier management and the Norwegian petroleum industry.

RQ1: *How can the Digital Twin technology be used to improve cybersecurity in the Norwegian petroleum industry?*

We concluded with four use areas (Table 4.6) that we find most valuable for the industry in an initial implementation of the Digital Twin. These are improved cybersecurity patching, training and awareness, anomaly detection systems, and extensive monitoring and visualization of barrier status. From the current state of the technology, we derived that implementing these use areas on a larger scale in a level 3 Digital Twin can aid in improving cybersecurity awareness and address current struggles.

SINTEF's ongoing research project on cybersecurity barrier management motivated discussing the identified use areas in the context of cybersecurity barriers and performance influencing factors. We found that the industry would benefit from using the Digital Twin to visualize cybersecurity barriers in bow-tie diagrams to address cybersecurity similarly to safety at all levels of the organization. The discussion concluded that a Digital Twin could benefit both in detection and reaction to cyber incidents and that visualization and monitoring could continuously indicate the status of the barriers.

We identified operators' and stakeholders' awareness and preparedness for cybersecurity incidents as factors with the potential to influence the performance of cybersecurity barriers. We concluded that the Digital Twin could improve cybersecurity in the Norwegian petroleum industry by facilitating improved awareness and response with more consistent training and development and testing of the

IRP, influencing the human contribution. In addition, we found that a Digital Twin can assist in human decision-making by running predictions and optimizations and proposing the correct action to be taken.

RQ2: *What are the challenges that limit the industry from utilizing Digital Twins for cybersecurity?*

We have concluded that the Digital Twin can become a valuable asset for cybersecurity in the Norwegian petroleum industry. However, one must address considerations regarding limitations and challenges of the technology to facilitate secure implementation and securing safety. The most significant consideration is ensuring that the Digital Twin is not affecting the Safety Instrumented System (SIS). This consideration includes ensuring that the amount of data needed in the Twin does not affect the performance of SIS. In this context, issues of unclarity regarding the current status and characteristics of maturity levels of Digital Twins became identified during interviews. Analyzing the data in light of maturity levels 4 and 5 revealed that the imminent threat this has on the SIS does not justify the benefits. The increased interconnectedness that comes with the upper levels of maturity adds to the already present issue regarding the isolation of safety-critical assets.

A Digital Twin's performance and usability are only as good as the data it relies on. Data quality is a limitation that affects the accuracy of simulations and predictions made by the Digital Twin. Operators must be aware of these possible implications and not put false trust in the system. The quality of the data is dependent on sensors, communication technology, and security requirements. These security requirements differ between the IT and OT domains, making it important to address the effect the prioritization of the requirements has on the system security and safety. We conclude that the Digital Twin should still prioritize *control* and *availability* of the physical resources while researching lightweight cryptographic schemes to ensure the integrity of the data transmitted to the digital counterpart. In addition, standardization is needed to enable the benefits of the Digital Twin across the whole life cycle of the plant. From the presented opportunities and limitations the technology presents, strict security considerations and quality assurance is required to realize the benefits of the higher maturity levels. Thus, the presented insight highlights areas for future prioritization of resources as the industry strives for optimization.

6.1 Future Work

Due to the comprehensiveness of the topics analyzed in the context of each other, the scope and derived results are on a high level, indicating the need for further in-depth assessments of the identified use areas and challenges. Future work includes testing the technology in the discussed use areas and identifying implementation

approaches that address the limitations, particularly the lack of common standards across vendors, suppliers, and assets.

Economic aspects were not a part of this scope but are a known limitation in digitalization processes. Assessment of the use areas and the technological alterations needed to realize them requires analysis in search of an economically sustainable solution where the identified potential benefits outweigh the costs. Cloud and edge technology aspects in the context of practical realizations were not within the scope of this work but present central factors in future realization when assessing the location and storing factors required by the technology. Thus, also these aspects require further analysis in light of the presented results.

From the presented data, future work includes defining the use cases for NOA sub-model architecture with its relation to AAS as the implementation of Digital Twins and describing assets systematically in an electronic format. In the context of modeling the use cases, data transmission speed and quality require an assessment to ensure sufficient data amounts at high quality are obtainable within speed requirements without compromising the operation of involved assets.

References

[09a] «Industrial communication networks - network and system security - part 1-1: Terminology, concepts and models», International Electrotechnical Commission (IEC), Standard, Jul. 2009.

[09b] «Security for industrial automation and control systems - part 2-3: Patch management in the iacs environment», International Electrotechnical Commission (IEC), Standard, Jul. 2009.

[10] «Industrial communication networks – network and system security – part 2-1: Establishing an industrial automation and control system security program», International Electrotechnical Commission (IEC), Standard, Nov. 2010.

[16a] «104 – norwegian oil and gas recommended guidelines on information security baseline requirements for process control, safety and support ict systems», Norwegian Oil and Gas Association, Standard, Nov. 2016.

[16b] «Statoil sin håndering av hendelser knyttet til ikt og informasjonssikkerhet, og tilhørende barrierestyring», Oct. 2016. [Online]. Available: https://www.ptil.no/contentassets/04039a6b73234018a2e08698f7ac5c79/vedlegg-1---tilsynsrapport_statoil.pdf.

[18a] «Health, safety and environment in the petroleum industry», Norwegian Ministry of Labour and Social Affairs, Tech. Rep., 2018.

[18b] *Olje og gass*, Jun. 2018. [Online]. Available: https://www.regjeringen.no/en/topics/energy/oil-and-gas/id1003/.

[19] «Security for industrial automation and control systems - part 4-2: Technical security requirements for iacs components», International Electrotechnical Commission (IEC), Standard, Apr. 2019.

[21a] *Colonial pipeline co. attack: What really happened...* Jun. 2021. [Online]. Available: https://www.cybertalk.org/2021/06/09/colonial-pipeline-co-attack-what-really-happened/.

[21b] *Cybersecurity barrier management*, Sep. 2021. [Online]. Available: https://www.sintef.no/en/projects/2021/cybersecurity-barrier-management/.

[21c] «Perspectives on cyber security for offshore oil and gas assets», English, *Journal of Marine Science and Engineering*, vol. 9, no. 2, p. 112, 2021.

[21d] *Plattform i40 glossary*, 2021. [Online]. Available: https://www.plattform-i40.de/IP/Navigation/EN/Industrie40/Glossary/glossary.html.

[22a] *Gartner information technology glossary 2022*, 2022. [Online]. Available: https://www.gartner.com/en/information-technology/glossary.

[22b] *Glossary*, 2022. [Online]. Available: https://csrc.nist.gov/glossary.

[22c] *I4.0 technologies in labs – machine to machine (m2m)*, 2022. [Online]. Available: https://examhub.eu/i4-0-technologies-in-labs-machine-to-machine-m2m/.

[22d] «Information security, cybersecurity and privacy protection - information security controls», Norsk Elektroteknisk Komite, Standard, Mar. 2022.

[22e] *Søke etter litteratur*, Apr. 2022. [Online]. Available: https://www.fhi.no/nettpub/metodeboka/litteratursok/soke-etter-litteratur/.

[4020] P. I. 4.0, Ed., *Details of the Asset Administration Shell Part 1*, Federal Ministry for Economic Affairs and Energy (BMWi), Nov. 2020.

[4021a] P. I. 4.0, Ed., *Details of the Asset Administration Shell Part 2*, vol. 1.0RC02, Federal Ministry for Economic Affairs and Energy (BMWi), Nov. 2021.

[4021b] P. I. 4.0, Ed., *Functional View of the Asset Administration Shell in an Industrie 4.0 System Environment*, 10119 Berlin: Federal Ministry for Economic Affairs and Energy (BMWi), Apr. 2021.

[AKP20] R. Arief, N. Khakzad, and W. Pieters, «Mitigating cyberattack related domino effects in process plants via ics segmentation», eng, *Journal of information security and applications*, vol. 51, p. 102 450, 2020.

[ALK+18] S. A. Alharthi, N. LaLone, *et al.*, «Practical insights into the design of future disaster response training simulations», in *ISCRAM*, 2018.

[Alp20] E. Alpaydin, *Introduction to machine learning*. MIT press, 2020.

[ASM+21] R. Amin Khalil, N. Saeed, *et al.*, *Deep learning in the industrial internet of things: Potentials, challenges, and emerging applications*, Jul. 2021. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9321458.

[BETW21] A. Bröring, M. Ehrlich, *et al.*, «Secure usage of asset administration shells - an overview and analysis of best practises», Nov. 2021. [Online]. Available: http://dx.doi.org/10.25673/39569.

[BFM+18] K. Bernsmed, C. Frøystad, *et al.*, «Visualizing cyber security risks with bow-tie diagrams», *Lecture Notes in Computer Science*, vol. 10744, 2018. [Online]. Available: http://hdl.handle.net/11250/2489600.

[BFP+18] A. Becue, Y. Fourastier, *et al.*, «Cyberfactory nr1 — securing the industry 4.0 with cyber-ranges and digital twins», Jun. 2018, pp. 1–4.

[BT21] F. Baiardi and F. Tonelli, «Twin based continuous patching to minimize cyber risk», *European Journal for Security Research*, 2021. [Online]. Available: https://doi.org/10.1007/s41125-022-00079-7.

[BWG20] L. Busetto, W. Wick, and C. Gumbinger, *How to use and assess qualitative research methods*. May 2020. [Online]. Available: https://doi.org/10.1186/s42466-020-00059-z.

[DCu22] S. D. DCunha, *Is ai shifting the human-in-the-loop model in cybersecurity?*, Jun. 2022. [Online]. Available: https://datatechvibe.com/ai/is-ai-shifting-the-human-in-the-loop-model-in-cybersecurity/.

[DNV16] DNV, «Cyber security resilience management for ships and mobile offshore units in operation», Tech. Rep. Recommended practice — DNVGL-RP-0496, Sep. 2016.

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

[DNV21] ——, «Qualification and assurance of digital twins», Tech. Rep. Recommended practice — DNVGL-RP-A204, Sep. 2021.

[DP20] M. Dietz and G. Pernul, «Unleashing the digital twin's potential for ics security», *IEEE Security Privacy*, vol. 18, no. 4, pp. 20–27, 2020.

[Dra21a] Dragos, «Ics/ot cybersecurity year in review 2021», Dragos, Tech. Rep., 2021.

[Dra21b] ——, «Understanding the challenges of ot vulnerability management and how to tackle them», Dragos, Tech. Rep., 2021.

[Dra22] ——, «Oil & natural gas cyber threat perspective», Dragos, Tech. Rep., 2022.

[ED15] *ICS and IT: Managing Cyber Security Across the Enterprise*, vol. Day 2 Wed, September 16, 2015, SPE Middle East Intelligent Oil and Gas Symposium, Sep. 2015. [Online]. Available: https://doi.org/10.2118/176779-MS.

[EE19] M. Eckhart and A. Ekelhart, «Digital twins for cyber-physical systems security: State of the art and outlook», in Nov. 2019, pp. 383–412.

[EEW19] M. Eckhart, A. Ekelhart, and E. Weippl, «Enhancing cyber situational awareness for cyber-physical systems through digital twins», in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2019, pp. 1222–1225.

[ENI21] ENISA, «Enisa year in review 2021», European Union Agency For Network and Information Security (ENISA), Tech. Rep., 2021.

[ESBC19] S. Evans, C. Savian, *et al.*, «Digital twins for the built environment», The Institution of Engineering and Technology, Tech. Rep., Oct. 2019.

[FFDB20] A. Fuller, Z. Fan, *et al.*, «Digital twin: Enabling technologies, challenges and open research», *IEEE Access*, vol. 8, pp. 108 952–108 971, 2020.

[FFS+18] P. Ferrari, A. Flammini, *et al.*, «Delay estimation of industrial iot applications based on messaging protocols», *IEEE Transactions on Instrumentation and Measurement*, vol. 67, pp. 2188–2199, 2018.

[FPPD22] R. Faleiro, L. Pan, *et al.*, «Digital twin for cybersecurity: Towards enhancing cyber resilience», in *Broadband Communications, Networks, and Systems*, W. Xiang, F. Han, and T. K. Phan, Eds., Springer International Publishing, 2022, pp. 57–76.

[Gil19] M. Giles, *Triton is the world's most murderous malware, and it's spreading*, Mar. 2019. [Online]. Available: https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/.

[Gil21] Gilje Jaatun, Martin and Wille, Egil and Bernsmed, Karin and Skaufel Kilskar, Stine, «Grunnprinsipper for ikt-sikkerhet i industrielle ikt-systemer», Tech. Rep., 2021. [Online]. Available: https://hdl.handle.net/11250/2835081.

[Gre18] A. Greenburg, *The untold story of notpetya, the most devastating cyberattack in history*, Aug. 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[Gri15] M. Grieves, «Digital twin: Manufacturing excellence through virtual factory replication», white paper, Mar. 2015.

[HOG+21] G. Hanssen, T. Onshus, *et al.*, «Premisser for digitalisering og integrasjon it-ot», Tech. Rep., 2021.

[HPM+21] D. Holmes, M. Papathanasaki, *et al.*, «Digital twins and cyber security -solution or challenge?», Aug. 2021.

[HS21] G. Hotvedt and A. N. Skytterholm, «Preparedness exercises for cyber attacks against industrial control systems in the petroleum industry», M.S. thesis, NTNU, 2021.

[HV20] D. Hartmann and H. Van der Auweraer, «Digital twins», in Dec. 2020, pp. 3–17.

[IBM20] I. B. M. C. (IBM), *What is a digital twin?*, 2020. [Online]. Available: https://www.ibm.com/topics/what-is-a-digital-twin.

[Ire22] A. Irei, *What is cyber hygiene and why is it important?*, Jan. 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/cyber-hygiene.

[JGW21] Z. Jiang, Y. Guo, and Z. Wang, «Digital twin to improve the virtual-real integration of industrial iot», *Journal of Industrial Information Integration*, vol. 22, p. 100 196, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2452414X20300716.

[JP21] P. Johannesson and E. Perjons, *An Introduction to Design Science*, eng, 2nd ed. 2021. Cham: Springer International Publishing AG, 2021.

[KA21] A. Khraisat and A. Alazab, «A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges», *Cybersecurity*, Mar. 2021. [Online]. Available: https://doi.org/10.1186/s42400-021-00077-7.

[KHA+20] H. Khalid, S. Hashim, *et al.*, «Cybersecurity in industry 4.0 context: Background, issues, and future directions», in Nov. 2020, pp. 263–307.

[KKT+18] W. Kritzinger, M. Karner, *et al.*, «Digital twin in manufacturing: A categorical literature review and classification», *IFAC-PapersOnLine*, vol. 51, no. 11, pp. 1016–1022, 2018, 16th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2018.

[KRM+19] A. Kummerow, D. Rösch, *et al.*, «Challenges and opportunities for phasor data based event detection in transmission control centers under cyber security constraints», in *2019 IEEE Milan PowerTech*, 2019, pp. 1–6.

[KYL+20] Y.-W. Kim, S. Yoo, *et al.*, «Characterization of digital twin», Sep. 2020.

[LaG19] *Developing a Digital Twin: The Roadmap for Oil and Gas Optimization*, vol. Day 1 Tue, September 03, 2019, SPE Offshore Europe Conference and Exhibition, Sep. 2019. [Online]. Available: https://doi.org/10.2118/195790-MS.

[Lam18] K. Lamb, «Challenges of digitalisation in the offshore oil and gas sector acknowledgements», 2018. [Online]. Available: https://www.repository.cam.ac.uk/bitstream/handle/1810/277734/CDBB_REP_1%5C%20Lambv2.pdf?sequence=8.

[LCHL21] B. Leander, A. Causevic, *et al.*, «Toward an ideal access control strategy for industry 4.0 manufacturing systems», *IEEE Access*, Aug. 2021.

[LHM18] B. Lantz, B. Heller, and N. McKeown, «Enabling security and safety evaluation in industry 4.0 use cases with digital twins», 2018.

[LLC18] M. Lezzi, M. Lazoi, and A. Corallo, «Cybersecurity for industry 4.0 in the current literature: A reference framework», *Computers in Industry*, vol. 103, pp. 97–110, Dec. 2018.

[LTS+20] *Johan Sverdrup: The Digital Flagship*, vol. Day 4 Thu, May 07, 2020, OTC Offshore Technology Conference, May 2020. [Online]. Available: https://doi.org/10.4043/30477-MS.

[MG19] P. Melo and E. Godoy, «Controller interface for industry 4.0 based on rami 4.0 and opc ua», Jun. 2019, pp. 229–234.

[MH94] M. B. Miles and A. M. Huberman, *Qualitative data analysis an expanded sourcebook*. SAGE Publ, 1994.

[Mis] Mission Secure, «A comprehensive guide to operational technology (ot) cybersecurity», Tech. Rep. [Online]. Available: https://www.missionsecure.com/ot-cybersecurity.

[MM21] L. Machi and B. McEvoy, *The Literature Review: Six Steps to Success*. SAGE Publications, 2021. [Online]. Available: https://books.google.no/books?id=PHpXEAAAQBAJ.

[MRB+22] A. S. Mohammed, P. Reinecke, *et al.*, *Cybersecurity challenges in the offshore oil and gas industry: An industrial cyber-physical systems (icps) perspective*, 2022. [Online]. Available: https://arxiv.org/abs/2202.12179.

[MSZ17] A. Mittal, A. Slaughter, and P. Zonneveld, «Protecting the connected barrels - cybersecurity for upstream oil and gas», Deloitte Center for Energy Solutions, Tech. Rep., 2017.

[MT21] M. C. Magnanini and T. A. Tolio, «A model-based digital twin to support responsive manufacturing systems», *CIRP Annals*, vol. 70, no. 1, pp. 353–356, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0007850621000676.

[NAM21] NAMUR, «Namur open architecture noa information model», Tech. Rep. NAMUR Recommendation — NE 176, Jun. 2021.

[NFDS20] S. Naseer, R. Faizan Ali, *et al.*, «Learning representations of network traffic using deep neural networks for network anomaly detection: A perspective towards oil and gas it infrastructures», *Symmetry*, Nov. 2020. [Online]. Available: https://www.mdpi.com/2073-8994/12/11/1882.

[NK19] *Challenges in Implementing the Digital Oil Field a Real-World Look at Data Retrieval, Storage and Efficient Utilization*, Offshore Mediterranean Conference and Exhibition, OMC-2019-1221, Mar. 2019.

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

[oAut20] T. I. S. of Automation, «Quick start guide: An overview of isa/iec 62443 standards security of industrial automation and control systems», Tech. Rep., 2020. [Online]. Available: https://gca.isa.org/isagca-quick-start-guide-62443-standards.

[OBH+22] T. Onshus, L. Bodsberg, *et al.*, «Security and independence of process safety and control systems in the petroleum industry», *Journal of Cybersecurity and Privacy*, vol. 2, pp. 20–41, Feb. 2022.

[oST18] N. I. of Standards and Technology, «Framework for improving critical infrastructure cybersecurity, version 1.1», *Framework for Improving Critical Infrastructure Cybersecurity*, vol. 1.1, Apr. 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[PB16] D. Proença and J. Borbinha, «Maturity models for information systems - a state of the art», *Procedia Computer Science*, vol. 100, pp. 1042–1049, 2016.

[Pet19] Petroleumstilsynet, «Forskrift om utføring av aktiviteter i petroleumsvirksomheten (aktivitetsforskriften)», Jan. 2019. [Online]. Available: https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/aktivitetsforskriften_n.pdf.

[Pet20] ——, «Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften)», Dec. 2020. [Online]. Available: https://www.ptil.no/globalassets/regelverk/gjeldende-regelverk-2022/styringsforskriften_n.pdf.

[PFKK16] F. Pauker, T. Frühwirth, *et al.*, «A systematic approach to opc ua information model design», *Procedia CIRP*, vol. 57, pp. 321–326, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212827116312100.

[PH21] R. K. Pauslen and I. A. B. Huus, «Digital twins. recommendations for cyber-attack consequence mitigation for the norwegian petroleum industry», Project report in TTM4502, Department of Information Security and Communication Technology, NTNU, Dec. 2021.

[PHH22] M. Perno, L. Hvam, and A. Haug, «Implementation of digital twins in the process industry: A systematic literature review of enablers and barriers», *Computers in Industry*, vol. 134, p. 103 558, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361521001652.

[PKC20] A. Pokhrel, V. Katta, and R. Colomo-Palacios, «Digital twin for cybersecurity incident prediction: A multivocal literature review», Jun. 2020, pp. 671–678. [Online]. Available: https://doi.org/10.1145/3387940.3392199.

[PS21] R. Perdomo and N. I. Serdyuk, «Cybersecurity in complex operations: A post-drilling approach foroil and gas wells», 2021.

[PVU+19] F. Patzer, F. Volz, *et al.*, «The industrie 4.0 asset administration shell as information source for security analysis», in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2019, pp. 420–427.

[RG22] Recaptcha and T. C. I. W. Group, «Winning the future with science and technology for 21st century smart systems», white papaer, 2022. [Online]. Available: https://www.nitrd.gov/pubs/CPS-OSTP-Response-Winning-The-Future.pdf.

[RM16] C. Robson and K. McCartan, *Real World Research*. 2016. [Online]. Available: https://uwe-repository.worktribe.com/output/915824.

[RSR+21] *Cyberdefence of Offshore Deepwater Drilling Rigs*, vol. Day 2 Tue, August 17, 2021, OTC Offshore Technology Conference, Aug. 2021.

[Saf21] I. R. F. .-. G. O. Safety, *Digitilization*, Jun. 2021. [Online]. Available: https://irfoffshoresafety.com/wp-content/uploads/2021/10/Problem-Statement-Digitilization.pdf.

[She19] S. Shea, *What is machine-to-machine (m2m)?*, 2019. [Online]. Available: https://www.techtarget.com/iotagenda/definition/machine-to-machine-M2M.

[SM10] K. Scarfone and P. Mell, «Intrusion detection and prevention systems», in *Handbook of Information and Communication Security*, P. Stavroulakis and M. Stamp, Eds. Springer Berlin Heidelberg, 2010, pp. 177–192. [Online]. Available: https://doi.org/10.1007/978-3-642-04117-4_9.

[Sny19] H. Snyder, «Literature review as a research methodology: An overview and guidelines», *Journal of Business Research*, vol. 104, pp. 333–339, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0148296319304564.

[SS20] T. Svenkerud Rydjord and I. Sørdal Volden, «Cybersecurity incident management process in industrial ict systems», M.S. thesis, NTNU, 2020.

[SSH+18a] S. Singh, E. Shehab, *et al.*, «Challenges of digital twin in high value manufacturing», Oct. 2018.

[SSH+18b] E. Sisinni, A. Saifullah, *et al.*, «Industrial internet of things: Challenges, opportunities, and directions», *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[TDS03] D. Tranfield, D. Denyer, and P. Smart, «Towards a methodology for developing evidence-informed management knowledge by means of systematic review», *British Journal of Management*, vol. 14, no. 3, pp. 207–222, 2003. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/1467-8551.00375.

[Tho] B. L. Thorpe, *Risk mitigation in digital twins*. [Online]. Available: https://global.royalhaskoningdhv.com/digital/resources/blogs/risk-mitigation-in-digital-twins.

[Tor05] R. J. Torraco, «Writing integrative literature reviews: Guidelines and examples», *Human Resource Development Review*, vol. 4, no. 3, pp. 356–367, 2005. [Online]. Available: https://doi.org/10.1177/1534484305278283.

[TTAA18] S. Tay, L. Te Chuan, *et al.*, «An overview of industry 4.0: Definition, components, and government initiatives», *Journal of Advanced Research in Dynamical and Control Systems*, vol. 10, p. 14, Dec. 2018.

[WGE+17] C. Wagner, J. Grothoff, *et al.*, «The role of the industry 4.0 asset administration shell and the digital twin during the life cycle of a plant», Sep. 2017, pp. 1–8.

[WGW+13] G. Wong, T. Greenhalgh, *et al.*, «Rameses publication standards: Meta-narrative reviews», *BMC medicine*, vol. 11, p. 20, May 2013.

[Wil16] B. Wildemuth, *Applications of Social Research Methods to Questions in Information and Library Science, 2nd Edition*. ABC-CLIO, 2016.

[WSJ17] M. Wollschlaeger, T. Sauter, and J. Jasperneite, «The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0», *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, 2017.

[WWP+20] T. R. Wanasinghe, L. Wroblewski, *et al.*, «Digital twin for the oil and gas industry: Overview, research trends, opportunities, and challenges», *IEEE Access*, vol. 8, pp. 104 175–104 197, 2020.

[YHS+21] X. Ye, S. H. Hong, *et al.*, «An industry 4.0 asset administration shell-enabled digital solution for robot-based manufacturing systems», *IEEE Access*, vol. 9, 2021.

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

[ZPG12] A. Zaslavsky, C. Perera, and D. Georgakopoulos, «Sensing as a service and big data», Jul. 2012.

Appendix A
Interview-guide

Introduction

Thank you so much for choosing to participate in this interview.

About us: We are two master's students in our 5th year studying communication technology and cybersecurity. The study has given us insights into IT, cybersecurity, communication technology, and digitization.

We are currently writing our thesis about cybersecurity in critical infrastructures, or more specifically the Norwegian petroleum industry. With our thesis, we want to look into digital twins and the asset administration shell to explore how the implementation of the technologies can contribute to the cybersecurity of the O&G industry. Because of the limited time frame, we have decided to direct our focus on the digital twin as a tool in cybersecurity to identify use areas and opportunities, as well as challenges and limitations of the different maturity levels.

Note: As the interviews were semi-structured the order, wording and amount of questions that were included varied between interviews. Those of relevance to the interviewee and their area of expertise were included, as well as additional follow-up questions.

Questions

General

1. Could you tell us about your work and role?
2. Do you have any initial thoughts regarding the research questions sent to you in advance?

Cybersecurity and Barrier management

1. What should be in focus when considering cybersecurity and barrier management?
2. Where in the bow-tie model (for reference) should the focus lie?
3. What issues do you see with the way the industry address cybersecurity today?

Digital twin

1. What use-cases do you see for Digital Twins for cybersecurity and barrier management?
   a) What motivates such implementations?
2. What are challenges/limitations with the implementation of Digital Twins for cybersecurity and barrier management?
3. What can you tell us about the use of such technology today?
4. Where do you see the industry in the future (within the discussed areas)?

Final notes

1. Is there anything you would like to add?

Ending

Thank you so much for taking the time to talk with us, we really appreciate the input and insight you have provided us on the discussed topics. We thank you for contributing to our master thesis research.

Andrea Huus and Rikke Paulsen

Securing Safety in the Norwegian Petroleum Industry with Digital Twins

NTNU
Norwegian University of
Science and Technology