Master's thesis

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

Andrea Neverdal Skytterholm
Guro Hotvedt

Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry

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

June 2021

NTNU
Norwegian University of Science and Technology

Andrea Neverdal Skytterholm
Guro Hotvedt

Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry

Master's thesis in Communication Technology and Digital Security
Supervisor: Maria Bartnes
Co-supervisor: Lars Bodsberg, Roy Thomas Selbæk Myhre
June 2021

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:	Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry
Students:	Andrea Neverdal Skytterholm Guro Hotvedt

Problem description:

The petroleum industry plays an important role in the Norwegian economy and welfare. The ongoing digitalization of the sector reduces costs and makes production more efficient. This makes petroleum competitive against other energy sources and ensures that the sector still is a major contributor to the Norwegian economy. Digitalization involves interconnecting systems of Operational Technology (OT), which traditionally operated in isolated networks, with Information Technology (IT) that is connected to the Internet. This interconnection enables remote control and maintenance of the oil platform from dedicated onshore control rooms. Consequences of an attack against IT can now propagate and lead to an OT-related incident where human lives, economy, and environment are at stake.

Regulations from the Petroleum Safety Authority Norway (PSA) require operators to train personnel and perform exercises. Training and exercises are crucial for the industry to be able to handle and limit the damage and harm of unwanted incidents. The industry has regularly performed exercises, but the focus of these has been safety and OT systems. Digitalization addresses a need for training and exercises on cyber security-related incidents. Today, there are few guidelines on how to perform exercises in this area, and standards and guidelines can be difficult to interpret. The industry has explicitly stated a need for more detailed guidelines.

Preparedness exercises can be developed either as discussion exercises or practical exercises. Independent of the type of exercise, a description of the event to be practiced on is needed. The event, or sequence of events, can be presented as a scenario and/or playbook. In this thesis, we will investigate what characteristics are present in well-designed exercises and how the description of such exercises should be constructed. Our goal is to contribute to preparedness exercises being conducted as efficiently as possible where a good learning outcome is provided.

Date approved:	08.02.2021
Supervisor:	Maria Bartnes, IIK and SINTEF

Abstract

In the petroleum industry, operations are monitored and controlled using Industrial Automation and Control Systems (IACS), also known as Operational Technology (OT). IACS are critical for the operation of the platform and for ensuring a safe operation. As in other industries, digitalization has now introduced Information Technology (IT) to OT components, leading to an increased attack surface. New challenges arise as IACS now are connected to the Internet. Previously, preparedness exercises in the industry have concerned safety-related incidents. Today, digitalization requires the industry to also exercise on security incidents, especially against IACS. There are few guidelines present for this area, and the industry explicitly states a need for more detailed guidelines.

We wanted to lessen this shortcoming by investigating descriptions of events to use in exercises, known as scenarios. This project investigated what characterizes a scenario to be realistic and expedient for tabletop exercises on cyber attacks against IACS in the petroleum industry. We have created two lists of criteria that characterize such scenarios. One list characterizes individual scenarios while the other characterizes scenario collections. We also developed a scenario collection with example scenarios for cyber attacks against IACS. When creating this collection, we used the lists of criteria to provide realistic and expedient scenarios.

During the project, we used design science as the method. For the different phases, we conducted various activities. Most of the activities used a qualitative approach. To collect data, we conducted interviews with the industry and a literature review. The criteria and the scenario collection were developed based on the collected data and revisited and improved by feedback from the industry. Both the lists and the scenario collection were validated and approved by respondents from two different operator companies.

The lists of criteria and the scenario collection can be used as guidelines for the industry on how best to develop and take usage of scenarios in tabletop exercises on cyber attacks against IACS. Using the criteria and example scenarios as guidelines could make it easier for the industry to develop exercises in this area and conduct the preparedness exercises efficiently where a valuable learning outcome is provided. From our results, we want to highlight the importance of basing the scenario on

today's threat landscape and making the scenarios plausible. In addition, we want to highlight the importance of exercising a scenario where a cyber attack causes events that appears to be caused by technical faults.

Sammendrag

I petroleumsindustrien monitoreres og kontrolleres operasjoner av industrielle automasjons- og kontrollsystemer (IACS), også kjent som operasjonell teknologi (OT). IACS er kritisk for operasjonen av plattformen og for å sørge for trygg drift. Som i andre industrier har digitaliseringen nå introdusert informasjonsteknologi (IT) til OT-komponenter som fører til en økt angrepsflate. Nye utfordringer oppstår når IACS nå er koblet til internett. Tidligere har beredskapsøvelser i industrien omhandlet safety-relaterte hendelser. I dag krever digitaliseringen at industrien også øver på security hendelser, spesielt rettet mot IACS. Det finnes få retningslinjer på dette området, og industrien adresserer eksplisitt et behov for mer detaljerte retningslinjer.

Vi ønsket å bidra på dette området ved å undersøke beskrivelser av hendelser å bruke i øvelser, kjent som scenarier. Dette prosjektet undersøkte hva som karakteriserer et scenario til å være realistisk og hensiktsmessig for tabletop øvelser som tar for seg cyberangrep rettet mot IACS i petroleumsindustrien. Vi har utviklet to lister med kriterier som karakteriserer slike scenarier. En liste karakteriserer individuelle scenerier, mens den andre karakteriserer en scenariosamling. Vi har også utviklet en scenariosamling med eksempelscenarier for cyberangrep mot IACS. Vi brukte listene med kriterier for å sikre realistiske og hensiktsmessig scenarier når vi lagde denne samlingen.

Metoden vi brukte gjennom prosjektet var teknologivitenskap. For de ulike fasene gjennomførte vi ulike aktiviteter, hvor de fleste av disse brukte en kvalitativ tilnærming. For å samle data brukte vi intervjuer med industrien og et litteraturstudie. Kriteriene og scenariosamlingen ble utviklet basert på den innsamlede dataen, og revidert og forbedret etter tilbakemeldinger fra industrien. Respondenter fra to ulike operatørselskaper validerte og godkjente både listene og scenariosamlingen.

Listene med kriterier og scenariosamlingen kan bli brukt som retningslinjer for industrien på hvordan man best kan utvikle og bruke scenariene i tabletop-øvelser for cyberangrep mot IACS. Å bruke kriteriene og eksempelscenariene som retningslinjer kan gjøre det lettere for industrien å utvikle øvelser i dette området, og gjennomføre beredskapsøvelser som gir et verdifullt læringsutbytte effektivt. Fra våre resultater vil vi trekke frem viktigheten av å basere scenariet på dagens trusselbilde og å gjøre scenariene plausible. I tillegg vil vi trekke frem viktigheten av å øve på

et scenario hvor cyberangrep fører til hendelser som ser ut til å være forårsaket av tekniske feil.

Preface

This master's thesis is submitted to the Norwegian University of Science and Technology (NTNU) as the final part of our Master of Science (MSc) in the Communication Technology and Digital Security degree.

To all participating organizations contributing in interviews and conversations for this thesis, we want to express our gratitude. You gave us valuable input to our project and helped us get invaluable insight into the industry. We hope our project will contribute to helping the industry conducting exercises in the researched area efficiently in the future.

We want to thank Maria Bartnes, Lars Bodsberg, and Roy Thomas Selbæk Myhre for the great support and guidance during these two semesters. You raised our work to a new level and kept us motivated during the project.

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

Guro Hotvedt & Andrea N. Skytterholm
Trondheim, 2021

Contents

List of Figures

List of Tables

List of Acronyms

APT Advanced Persistent Threat.

BPCS Basic Process Control System.

CRIOP Crisis Intervention and Operability analysis.

DigDir The Norwegian Digitalization Agency.

DMZ Demilitarized Zone.

DSB The Norwegian Directorate for Civil Protection.

FFI Norwegian Defence Research Establishment.

HMI Human Machine Interface.

IACS Industrial Automation and Control Systems.

ICS Industrial Control Systems.

IIoT Industrial Internet of Things.

IoT Internet of Things.

IT Information Technology.

NIST National Institute of Standards and Technology.

NSM Norwegian National Security Authority.

NTNU Norwegian University of Science and Technology.

NVE The Norwegian Water Resources and Energy Directorate.

OT Operational Technology.

PLC Programmable Logic Controller.

PSA Petroleum Safety Authority Norway.

PST The Norwegian Police Security Service.

RAT Remote Access Tool.

SIS Safety Instrumented System.

SOC Security Operations Center.

VPN Virtual Private Network.

Chapter 1
Introduction

Norway is a small country but is fortunate to be blessed with significant natural resources. Oil and gas are two of these resources and make the petroleum industry prominent in Norway [Nor20]. The industry stands for approximately 10 percent of the country's total income and helps secure the Norwegian economy [oF20].

Oil and gas are materials that could cause severe damage [oLA18]. For this reason, the petroleum industry has always focused on training and exercises to mitigate the probability and consequences of unwanted situations [Top12]. Consequences of such events may be loss of human lives, damage to equipment, environmental damage, and economic consequences [oLA18]. The industry faces incentives to do everything possible to avoid such outcomes.

As in other industries, digitalization has introduced Information Technology (IT) to Operational Technology (OT) components in the petroleum sector [SFS11]. OT, also known as Industrial Automation and Control Systems (IACS), are systems controlling industrial processes such as drilling [iS20]. Originally, these systems were designed to work in a closed environment [SFS11]. Connecting these systems to IT reduces the costs of operations, increases efficiency, and opens new possibilities, like remote access to offshore platforms [SFS11]. IT systems are systems that control digital information and are connected to the Internet [iS20]. By having OT systems exposed to the Internet as well, an increased attack surface with new risks and threats arises [Hål20]. Among these new threats are cyber attacks [Hål20] that attempt to gain unauthorized access to a computer, computing systems, or computer networks to cause damage [Pra21]. Today, an attacker can perform a cyber attack against a platform that may lead to physical consequences [Hål20].

When categorizing specific threats and risks, the terms safety and security emerge. Safety focuses on securing against unintentional events, such as faults in the systems, while security focuses on securing against intentional events. Previously, the focus of training and exercises in the petroleum sector has been safety. Because of the

digitalization of the sector, the industry needs to address security-related incidents in their training and exercise program as well. Threats compromising security and IACS components are relatively new in the industry. Hence, the industry needs guidelines on how to best develop and conduct exercises in this area. A report published in 2020 by DNV GL for the Petroleum Safety Authority Norway (PSA) states that the industry lacks clear and concise guidelines for this, which is our motivation for the project. Besides, they state that existing guidelines are not comprehensive enough, and there is a desire for new guidelines in the area of cyber attacks against IACS [Hål20].

1.1 Scope and Research Questions

To narrow the scope of the thesis, we will investigate descriptions of events to use in exercises, known as scenarios, through a literature review and interviews with the industry. The scenarios' area of utilization will be tabletop exercises, which are small-scale exercises based on discussions. Besides, other characteristics that are present for these descriptions to reach their full potential will be investigated. Our scope will thus exclude other areas of guidelines for training and exercises. Further, we have scoped the study to cyber-related attacks against IACS, which also includes attacks on the IT network where it is used as an entrance to IACS. Other types of attacks that are not related to the digital domain are excluded from the study.

Our focus is to investigate characteristics present for the scenarios to be valuable, realistic, and expedient. We will answer the following research question and sub-question throughout this thesis:

> *RQ 1: What are expedient and realistic scenarios for tabletop exercises related to cyber attacks against IACS in the petroleum industry?*

> *RQ 1.1: Which criteria must be evaluated in order to categorize a scenario as expedient and realistic?*

We will distinguish between the terms *expedient* and *realistic* in the research questions. By *expedient* scenarios, we mean scenarios that give a valuable learning outcome for the participants. The organization and participants should have new, useful knowledge and experiences after using the scenario in an exercise. *Realistic* scenarios revolve around using scenarios that could indeed happen and hence are important to prepare for.

Our goal is to provide guidelines for the industry on how best to develop and take usage of scenarios for tabletop exercises regarding cyber attacks against IACS, for the exercises to provide a satisfying learning outcome. Following an exercise plan, including tabletop exercises with expedient and realistic scenarios, may better prepare the industry for possible future incidents.

1.2 Limitations

The focus of the study is on the Norwegian petroleum industry. For the literature review, papers and reports from other sectors and countries will also be analyzed, along with literature from the Norwegian petroleum industry. For the interviews, we will only include companies present in Norwegian sea areas. The interviewees are either from the petroleum industry or related industries with insight into the petroleum industry, IACS, and cyber security. Only including companies present in Norwegian sea areas may be limiting, as interviews with companies outside Norway and other industries may have added extended input to our study.

1.3 Outline

This section establishes an overview of how the thesis is structured into chapters.

Chapter 2 gives background information that is necessary for the project's context as well as related work.

Chapter 3 describes the chosen research methodology used in the thesis along with its trustworthiness.

Chapter 4 first presents the results from the literature review along with findings from the interviews. We then give the developed criteria, along with the created scenario collection. At last, we present the feedback received from the industry on our first draft of the scenarios.

Chapter 5 discusses the results from the interviews and literature review with the developed criteria and scenarios. The content of the scenarios and criteria is justified in order to answer the research questions.

Chapter 6 draws a conclusion based on the findings along with presenting areas for future work related to the thesis.

Appendix A shows the interview guide used for semi-structured interviews in the validation phase of the scenarios and the criteria.

Appendix B presents an overview of the presence of 4G connections in the North Sea today.

Chapter 2
Background and Related Work

This chapter presents necessary background information for the project's context as well as related work. An overview of the petroleum industry and related aspects are presented in Sect.2.1, IACS are elaborated in Sect. 2.2, and the influence of IT to OT in the industry is presented in Sect. 2.3. Further, the current threat landscape for the petroleum industry is elaborated by previous incidents and threat assessments in Sect. 2.4, and the incident management process is presented in Sect. 2.5. Lastly, central concepts in training and exercise are defined in Sect. 2.6 while existing guidelines regarding training and exercise in other sectors are introduced in Sect. 2.7.

2.1 The Petroleum Industry

The petroleum industry has been important for the Norwegian economy for several years. Especially, it was important when the corona pandemic hit, and Norway could use years of saved funds from the industry to support the society where needed [oFN20]. The role of petroleum as the dominating energy source is now threatened by new energy sources and an increased focus on the environment [GMR+18]. Digitalization of platforms with sensor technology, data storage, and artificial intelligence opens new possibilities and solutions. This digitalization will be important for the industry to be able to compete with other energy sources [GMR+18]. The term petroleum is often used alternately with the term "oil and gas" and may be used interchangeably throughout this thesis.

Companies in the petroleum industry may operate on land (onshore), sea (offshore), or both. The sector consists of several companies, both large and smaller ones. In Norway, there were 24 operating companies at the turn of the year 2020 [Pet21]. Larger operator companies typically operate several platforms or other facilities. All platforms and other facilities, such as gas plants, have a control room. The control room has a central location where technicians and managers manage their everyday operations [Con21]. For technicians working in a control room at an oil

and gas installation, this involves maintaining the organization's everyday operations' integrity. This is done through the visibility of real-time data for optimal performance for management, supervisors, and operators [Con21]. The personnel working in the control room is titled control room operators [Job21]. The control room for a given installation will also work as a location where the organization can enact and maintain crisis operations if needed [Con21]. The systems used in the control rooms are called Industrial Automation and Control Systems, and we elaborate them in Sect. 2.2.

In addition to a central control room, there are several other rooms present on the plants. One of those is the telecommunication equipment room. This room accommodates most of the central telecommunication equipment like servers, Programmable Logic Controllers (PLCs), which is a part of IACS, and network switches [Nor03].

The petroleum industry separates between different roles and levels for emergency response. These roles are named first-line, second-line, and third-line. First-line emergency response corresponds to the tactical level and includes employees who are physically present at the installation. First-line personnel is handling the technical and executive aspects of the incident. Examples of first-line personnel are control room operators and maintenance personnel. Second-line emergency response corresponds to the operational level, which supports the affected installation from a remote position. This support may include resources, competence, or communication with other involved parties or public institutions. Besides, the second-line is responsible for verifying that the first-line handles the situation correctly. An emergency response team is usually a part of the second-line. Third-line emergency response corresponds to the strategic level and consists of the organization's top management. Their functions are to verify that the second line handles the incident according to the governments' requirements and internal procedures, protect the organization's and industry's reputation, and protect first-line and second-line from unnecessary and unwanted events [HNW+12].

2.2 Industrial Automation and Control Systems (IACS)

IACS refers to a collection of hardware, software, and personnel that can influence or affect the reliable operation of an industrial process, as well as the safety and security of the process [IEC10]. Most of these systems can be operated and monitored remotely [Too21], which now happens with the ongoing digitalization in the petroleum industry. Other terms like control systems, OT, and Industrial Control Systems (ICS) are often used interchangeably when talking about IACS. Throughout this project, we will use the terms IACS and OT.

IACS that are usually considered are Safety Instrumented System (SIS) and Basic Process Control System (BPCS). BPCS are systems that respond to input signals from sensors, programmable systems, and the process. Based on these signals, BPCS generates an output signal. The output signal then controls how the process and attached equipment will behave according to an approved design control strategy. Functions performed by BPCS should optimize the installation operations by attempting to keep all the process variables within its safety limits, provide input to a Human Machine Interface (HMI), provide alarms/event logging, and generate production data reports. SIS are systems responsible for ensuring the safety of an installation. The systems are programmed to perform specific control functions to maintain a safe operation when unacceptable or potentially dangerous conditions occur. In addition, the specific control function controls the events of fail-safe when necessary [Too21]. A fail-safe mechanism is a mechanism to ensure that if something fails in one part of the system, the whole system goes to a safe state to avoid dangerous situations [Dic21a].

2.3 Operational Technology (OT) Influenced by Information Technology (IT)

OT systems were initially designed to work in closed environments with no connection to other networks [SFS11]. Availability has been the main focus of OT, whereas the confidentiality and integrity of these systems have not been a priority. In the petroleum industry, OT systems control critical operations, and it is therefore important that these systems are available and without delays [Dra19]. Traditionally, the focus on confidentiality and integrity has dominated the IT systems, which differs from the focus of OT systems. Higher deployment costs, and costs related to maintenance and operation, have contributed to IT being integrated into OT systems to reduce cost and increase efficiency. The integration increases the need for confidentiality and integrity among the OT systems as well [Hål20]. Integrating IT in OT gives OT a connection to the Internet, and makes IT a potential attack vector into the OT systems [Dra19].

An illustration of the separation between IT and OT in typical networks in the petroleum industry can be seen in Fig. 2.1. Note that this is only an illustration and may vary with different organizations. The green zone, Level 4: Enterprise, represents IT and is connected to the Internet via a Demilitarized Zone (DMZ). A DMZ is a subnetwork that separates an internal network from an untrusted, external network, usually the Internet. The subnetwork is usually protected with firewalls to control the traffic going in and out to the network [Lut21]. The DMZ provides an additional layer of security to the internal network. IT is then connected to OT, illustrated in the red zone with Level 0, 1, 2, and 3, via a separate DMZ. The yellow

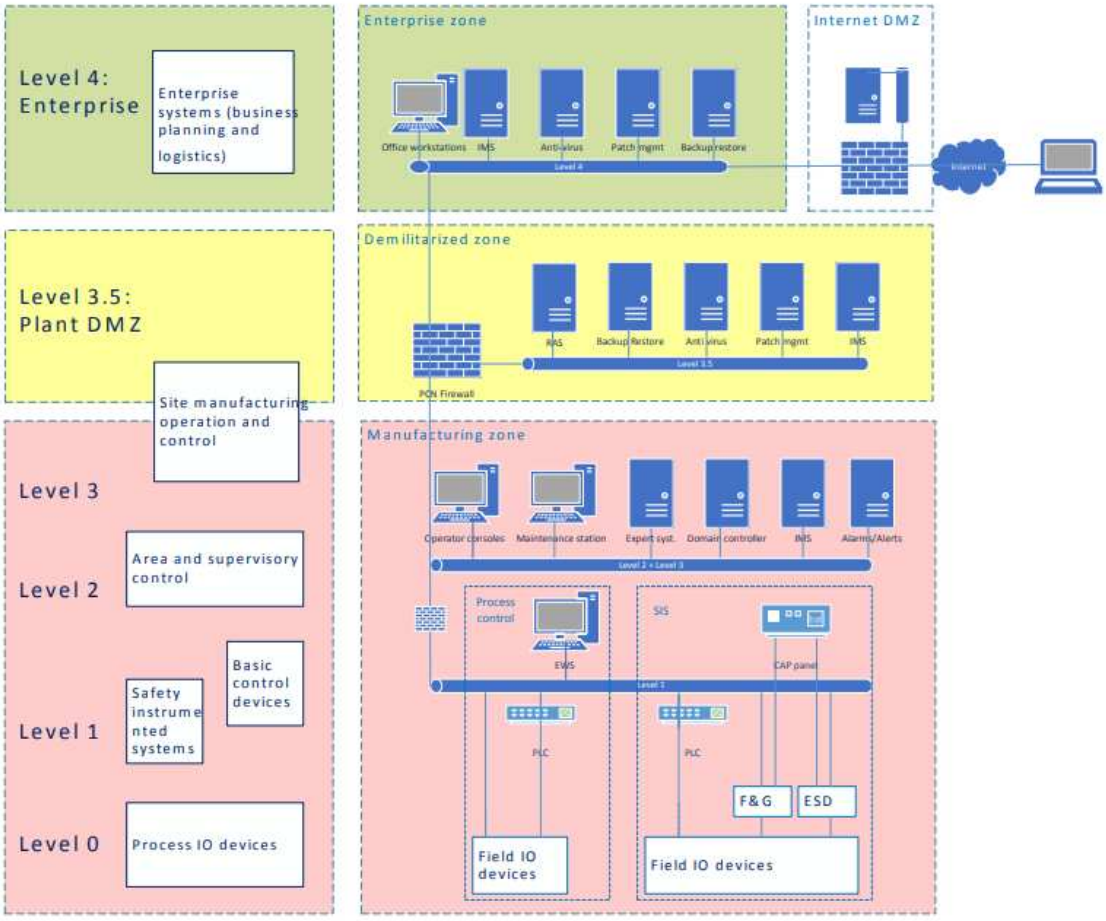

Figure 2.1: An illustration of the separation between IT and OT in networks used in the petroleum industry. Level 4 corresponds to IT, while the red area with Level 0, 1, 2, and 3 corresponds to OT. Taken from [GL17].

zone, Level 3.5: Plant DMZ, illustrates this DMZ. Also, this DMZ is set up for protection, respectively between IT and OT. Even though a DMZ is separating IT and OT in this illustration, the two systems are still connected. Hence, it will be possible to maneuver from IT to OT and vice versa [GL17].

Previously, attacks against the IT systems could not reach the OT systems. With the present connection between these systems, the administrative IT systems can now potentially be used as an entrance gate to the technical OT systems. The attack surface for OT systems is increased, opening up for new types of attacks directed towards the petroleum industry and these systems. Especially, cyber attacks targeting OT are made possible due to the increased attack surface. In addition to IT being used as a gateway, the influence of IT in OT opens for exploitation of other vulnerabilities. Attacks targeting mainly the IT systems in the administrative part

can now lead to complications in production, even if the attack does not directly hit the OT systems [Hål20].

2.4 Current Threat Landscape

Overall, the number of cyber attacks against IACS is increasing, and adversaries interested in oil and gas companies are evolving their behaviour [Dra19]. Therefore, the industry needs to stay updated on the current threat landscape to prepare for attacks. Investigating previous and predicted incidents and attacks might help the sector predict what kind of threats are relevant. If they know what threats are present, they can base the scenarios on this, and the companies may then be able to prepare themselves for such an attack through an exercise.

To understand today's threat landscape, we have analyzed previous incidents and threat assessments. They are presented in Subsect. 2.4.1 and Subsect. 2.4.2.

2.4.1 Previous Incidents

Cyber attacks targeting IACS are not new, and threat actors are working to find new ways to attack industries and critical infrastructures [Dra19]. In this section, we will present some of the most known and severe cyber attacks that have targeted industries using IACS independent of the sector where they occurred. Tab. 2.1 presents an overview of former attacks, and we will present the highlighted ones in more detail as those are the ones most relevant for our project. The table addresses the year, name, and type of the attack. In addition, we have presented the target(s) of the attack. Most of the attacks are taken from Hemsley's and Fisher's report named *History of Industrial Control System Cyber Incidents* [HF+18]. Petya, LockerGoga, Sunburst, and the Colonial Pipeline ransomware attack are added to the adapted table, as these are relevant to our study area.

Year	Name	Type of attack	Target
2010	Stuxnet	Malware	Iranian nuclear facilities
2010	Night Dragon	Malware	Global oil, energy and petrochemial companies
2011	Duqu/Flame	Malware	Specific organizations including IACS manufacturers
2012	Gas Pipeline Cyber Intrusion Campaign	Campaign	Natural gas pipeline sector

2012	Shamoon	Malware	Saudi Aramco (energy company) and RasGas (natural gas company)
2013	Target Stores	Attack	Target's financial systems
2013	New York Dam	Attack	Bowman Dam in Rye Brook, New York
2013	Havex	Malware	IACS used in the U.S. critical infrastructure
2014	German Steel Mill	Attack	German steel mill
2014	Black Energy	Malware	Human Machine Interface (HMI)s in IACS
2015	Ukraine Power Grid Attack No. 1	Attack	Ukraine power grid
2016	"Kemuri" water company	Attack	PLCs that control water treatment chemical processing
2016	Return of Shamoon	Malware	Saudi Arabia's civil aviation agency and other Gulf State organizations
2016	CRASHOVERRIDE (Ukraine Power Grid Attack No. 2)	Malware	Power Grids
2016	Petya	Ransomware	Microsoft Windows-based systems
2017	NotPetya	Destructive Malware	Microsoft Windows-based systems
2017	TRITON/Trisis/Hatman	Malware	Industrial safety systems in Middle East, oil and gas sector
2019	LockerGoga	Ransomware	Norsk Hydro
2020	Sunburst	Malware	US Government, SolarWinds
2021	Colonial Pipeline Attack	Ransomware	Colonial Pipeline (American oil pipeline company)

Table 2.1: Overview of previous incidents targeting industries using IACS. Adapted from [HF+18].

Stuxnet

In 2010, the Stuxnet-malware infected control system networks of the Iranian Nuclear facilities. Stuxnet is believed to be the first publicly known cyber attack targeting IACS and giving attackers control of specific systems, causing physical damage. The malware tampered, among other things, with data sent to the HMIs to make them look normal simultaneously as changing the values in the PLCs. This attack was a wake-up call to all critical infrastructure systems and showed that well-financed and patient attackers with could likely attack any system they wanted to [HF+18].

Petya & NotPetya

In 2017, a destructive malware camouflaging as the ransomware named "Petya" appeared in Ukraine [HF+18]. Ransomware is a type of malware that encrypts the victim's files and systems. In that way, the victim loses access to all of its data. The attacker then demands payment to decrypt the files and give the access back to the victim [Fru20]. The Petya ransomware attacked Windows-based systems, and once a system was infected, a message demanding payment in Bitcoin appeared. If the claim was paid, the system access was regained. However, the malware that occurred in Ukraine was different. It was designed to be fully destructive, and once hard drive data was encrypted, it was no way to decrypt it. This attack, similar to Petya, was named NotPetya. The U.S. Government has called the attack *"the most destructive and costly cyber-attack in history,"* and the U.K. and Australian governments claim that the Russian Government was responsible for the NotPetya malware. The Russians, on the other side, deny having anything to do with it [HF+18].

TRITON/Trisis/Hatman

The TRITON malware was used against a petrochemical plant in Saudi Arabia in 2017 to shut down SIS. It was the first malware of its kind and is also known as Trisis and Hatman [HF+18]. The attackers got a foothold in the IT network of the organization in 2014 and conducted reconnaissance activity, and advanced deeper into the network towards the OT network [Hig19].

The malware returned to its second victim in 2019 with much of the same code as in 2017 [Hig19]. This kind of attack shows that the digitalization of the oil and gas industry opens up for new attack vectors as the attackers now can use the IT network to advance towards the OT network. It also shows that if threat actors have enough resources and time, it is frightening how much damage they could perform. TRITON also shows that an adversary now can compromise SIS which leads to loss of safety [Dra19], and gives a new dimension to the consequences of a cyber attack.

Ransomware attack against Norsk Hydro

In March 2019, Norsk Hydro, a Norwegian industrial concern with businesses within energy and aluminum, was attacked by a ransomware named LockerGoga. The threat actors used e-mails to lure employees into downloading a malicious file or accessing a link to download the file automatically. The malware was designed to access and encrypt sensitive user data on the infected devices in the IT network [OMJA19, Bri19]. When opening the malicious file on a device, it encrypted files using the RSA-4096 and AES-256 encryption algorithms [OMJA19]. According to Norsk Hydro, or Hydro for short, they did not pay the ransom to regain access to the computers and servers and used backup systems to repair the data instead. The attack is estimated to have a cost of around 550-650 million Norwegian kroner (NOK) [Hyd20].

Sunburst attack against SolarWinds

SolarWinds is an American software company [Sol] and was used as an attack vector in the attack targeting users of SolarWinds Orion products [Wil20]. The attack was first discovered in December 2020. The company has over 300 000 customers, and among these are people working in the U.S. Government and actors in critical infrastructures [Age20, Wil20]. The threat actors gained network access by getting more than 18 000 private and government users to download a malicious software update. Once inside, they were able to monitor internal e-mails at some of the top agencies in the United States [Pau20].

This type of attack stands out from the attacks above as it is a supply-chain attack. SolarWinds were used as an attack vector as a supplier to get access to its customers. The attack against SolarWinds may potentially be one of the most damaging attacks seen in recent history, and the outcome is still not yet determined [Wil20].

Ransomware Attack Against Colonial Pipeline

On the 8th of May, 2021, the Colonial Pipeline company released a statement to confirm they were under a ransomware attack and had to close their pipelines [DG21]. Colonial Pipeline operates pipelines carrying 45% of the fuel used on the East Coast of the United States [DG21]. This responsibility makes them critical for society, and the incident represents one of the largest disruptions of the critical infrastructure in the United States by hackers in history [Gre21].

A control room operator discovered the ransomware in a note displayed on a control room computer [EV21]. Later, the company revealed that they had paid the ransom, which is a controversial decision as the official guidance recommends otherwise [SW21].

2.4.2 Threat Assessments

To get an overview of what kind of threats the industry faces today, we analyzed threat assessments. These assessments look at trends in the threat landscape based on previous incidents and common risks in different industries. Some of the analyzed assessments are from the oil and gas industry, while some are more general and relevant to all sectors. By analyzing these, we got an overview of today's threats seen from different actors. The assessments examined in this project were *The Threat of Intelligence Against the Norwegian Petroleum Sector* (In Norwegian: *Etteretningstrusselen mot norsk petroleumssektor*) from The Norwegian Police Security Service (PST), *Global Oil and Gas Cyber Threat Perspective* from Dragos, *National Threat Assessment 2020* (In Norwegian: *Nasjonal Trusselvurdering 2020*) from PST, *Digital Security 2020* (In Norwegian: *Digital Sikkerhet 2020*) from Telenor Norway, *Risk 2021* (In Norwegian: *Risko 2021*) from Norwegian National Security Authority (NSM), *Internet Organised Crime Threat Assessment* from Europol, *Security Report 2021* from mnemomic, and *The Top 20 Cyber Attacks On Industrial Control Systems* by Andrew Ginter in Waterfall Security Solutions.

Threat Actors

Threat actors are a subject of focus in the assessments. Telenor chooses to divide threat actors into five categories: states, counter actors, organized crime, politically motivated hackers and individual criminals, and fraudsters. States act to support their own political goals. Counter actors work project-based and are hired by states, industry, or organized criminals to fulfill their intentions. Their focus may vary along with the projects. Organized crime in cyberspace is performing fraud for their profit. The most advanced threat actors are called Advanced Persistent Threats (APTs). They have the capacity, resources, and will to perform operations over a long time period to fulfill their goals. According to Telenor, states, counter actors, and organized crime can all be APTs. Hackers are cyber criminals with a political intention, but they are less seen in the threat landscape recently. A politically motivated hacker may, for instance, fight for more environmentally friendly energy sources than oil and gas. The last category is individual criminals and fraudsters who focus on their profit or want to gain access to the other groups of criminals [Nor20].

Some of these threat actors are highlighted to a greater extent than others. Telenor, Dragos, PST, and NSM all highlight states as one of the largest threat actors [Nor20, Dra19, Ser20a, Aut21c]. Dragos and the threat of intelligence report from PST both predict that state-associated actors will target oil and gas increasingly to reach political, economic, and national security goals [Dra19, Ser20a]. Dragos also specifies that cyber attacks on critical infrastructure now are easier to conduct for states that invest in offensive cyber operations [Dra19]. In addition to states as threat actors, organized crime is emphasized by NSM [Aut21c].

Dark Web

The dark web is a part of the Internet where criminals can trade services and access to forbidden areas [mA21] as it is not indexed by search engines [Guc18]. In the security report for 2021, mnemonic describes an observed change in the dark web when looking back at the security year of 2020. They have observed specific cases where APTs sell access and a foothold on different targets to the highest bidder at the dark web. This new service, which they call breach-as-a-service, enables less sophisticated threat actors to compromise their targets by paying APTs offering this service [mA21]. Europol also presents a variant of breach-as-a-service in their assessment, named ransomware-as-a-service [Eur20]. We present this service in more detail in a section on ransomware presented later in this chapter.

Human as the Weakest Link

According to NSM's threat assessment for 2021, humans still constitute one of the most considerable vulnerabilities in the threat landscape for 2021. NSM also addresses that known vulnerabilities are still being exploited, and the lack of updating software is still a problem [Aut21c]. Both areas are related to the human as a vulnerability.

As it is known that humans can be the weakest link, the attackers focus on exploiting them. Social engineering attacks are still popular, and the use of e-mail as an entrance is still working [Aut21c]. Social engineering attacks mentioned in the threat assessments are various forms of phishing [Nor20, Eur20, Aut21c, mA21].

Phishing is an attack strategy that seeks personal and sensitive information through social manipulation. The most common platforms used are social media, e-mail, SMS, and phone calls [Nor20]. A simple example of phishing can be an e-mail that claims to be from your bank and requests you to enter your username and password. NSM states that this kind of attack still often succeeds [Aut21c]. However, mnemonic informs that the total number of phishing attacks has not increased in 2020 [mA21].

Even though technical security is increasing among companies, and the attackers are getting more sophisticated [Eur20], it is still essential to be aware of these "simple" types of attacks that exploit the human factor. Telenor considers the attacks mentioned above to be the methods that most often compromise private users and larger firms today [Nor20].

Intelligence

In their report on the threat of intelligence against the Norwegian petroleum sector, PST considers the industry exposed to intelligence from foreign states in today's threat landscape until May 2022 [Ser20a]. Telenor also addressed the threat of

intelligence, especially against political authorities, natural resources and industry, defense and preparedness, and research in Norway for 2020 [Nor20].

Both PST and Telenor state that the threat actors focusing on intelligence against Norway and the Norwegian petroleum sector mostly are Russia and China. However, they also address that other state's intelligence services are interested in information regarding Norwegian businesses, including businesses in the Norwegian petroleum sector [Ser20a, Nor20].

Dragos specifies that there is an ongoing reconnaissance activity targeting oil and gas companies in Europe, which also should be emphasized in today's threat landscape [Dra19]. PST elaborates that the gathered information could be used to customize network operations against the Norwegian petroleum sector. The network operations might further lead to sabotage actions, which might question the credibility of Norway as a secure and predictable petroleum supplier [Ser20a].

Insider Attack

PST highlights inside attacks as a likely threat in 2020 in their national threat assessment [Ser20b], and NSM and mnemonic follow up on this as a prediction for 2021 [Aut21c, mA21]. mnemonic states that the risk for insider threats is particularly high for companies and industries with critical assets [mA21]. Companies with critical assets include the petroleum industry.

Insiders can be intentional or unintentional, where the intentional threat has the higher focus in the threat assessments. An unintentional insider might reveal sensitive information without the intention of doing so, while an intentional insider seeks to threaten the company [mA21].

The motive of an insider might vary. It could be own interests or an external actor that influences the insider. The latter seeks to recruit or pressure employees of a company to perform expedient actions for that actor [mA21]. PST states in their national threat assessment that foreign intelligence is willing to recruit sources to get information on persons and businesses in Norway. Cultivation of these sources over a longer period seems to be prioritized from state actors and other APTs that seek an entry to Norwegian businesses [Ser20b]. In their report on the threat of intelligence for the Norwegian petroleum sector, PST addresses that persons working in the petroleum sector could be approached and tried recruited by foreign intelligence [Ser20a]. Telenor also states the APTs's focus on recruiting is increasing [Nor20].

Digitalization has resulted in an increased number of vulnerabilities related to key personnel and other intelligence-exposed personnel. Individuals with wide access

to information systems can change and extract a lot of information without being discovered. This vulnerability opens up for insider attacks [Aut21c]. Also, mnemonic highlights the difficulties of asking employees about potential issues covered through security clearance and authorization [mA21]. They further elaborate that these issues can be related to their background, economic status, dependencies, close relatives, and other questions.

Supply Chain Attack

According to NSM, attacks targeting supply chains are an increasing risk [Aut21c]. NSM, mnemonic, Dragos, Europol, and Telenor are all focusing on supply chain attacks in their threat assessments [Aut21c, mA21, Dra19, Eur20, Nor20]. A constantly growing and more complex chain, both inside and outside a company's country borders, challenges the security of a company. Weak security at a subcontractor, or even a subcontractor of a supplier, can be a risk for the whole chain of suppliers. Directed attacks against suppliers are also realistic as it may be easier than going directly after the intended target. Access control may be challenging when the number of actors grows as it is hard to keep track of who needs access and who does not. The growing complexity and the difficulty of maintaining an overview of all links in a chain are areas attackers may exploit [Nor20].

Dragos specifies that supply chain compromises targeting equipment manufacturers, third-party vendors, and telecommunications providers pose a threat to all entities using IACS [Dra19]. They also mention that the companies in oil and gas, among others, are especially at risk as there is a variety of security zones and trust relationships present for them [Dra19].

Europol has seen significant development in malware attacks on organizations that play a crucial role in the supply chains of major organizations. Both ransomware and other forms of malware are targeting suppliers and third-party companies, putting the supply chains at significant risk. Impacts of such attacks could involve data leaks or disruptions [Eur20].

Ransomware

Ransomware is a dominant threat that is being emphasized by NSM, Europol and Telenor [Aut21c, Eur20, Nor20]. Europol states that it might be the most dominant threat for public and private organizations within, as well as outside, Europe [Eur20]. Statistics used by Telenor show that the average downtime for companies exposed to ransomware in 2019 was 16 days. The average payment was 84 116 dollars in each case [Nor20]. For the petroleum sector, a downtime of 16 days could cause serious economic consequences if it affected or stopped production.

Ransomware is constantly evolving, and it is becoming more targeted [Eur20]. In addition to encrypting files and systems, attackers are now performing a "double ransomware attack" [Nor20]. Double ransomware attack means that the attackers may threaten to leak stolen, sensitive data, shutting down critical services, disclose business-critical information or information on customers and, in addition, encrypt systems [mA21]. Shutting down critical services would be especially harmful to companies in the petroleum industry. The development of ransomware attacks makes them more complex, and it is no longer sufficient only to have backups and restore processes in place if you get exposed [Nor20].

Previously, ransomware attacks have been used directly against their target. Europol now states that ransomware also poses a significant indirect threat to companies where the attackers target supply chains and third-party service providers as a new entrance to the initial target [Eur20]. Previously, attackers needed to compromise systems to encrypt them, whereas now, this threshold is mitigated. Ransomware-as-a-service is available for criminals who may buy this service on the dark web to access different systems to encrypt them. It enables less sophisticated attackers to perform ransomware attacks, which may increase the number of these attacks [Eur20].

Malware

In their threat assessment, Dragos presents five scenarios they see as threats to the global oil and gas industry [Dra19]. The content of one of them is malware using IT as an entrance to OT. They specify that the IT environment is a potential gateway into the OT environment caused by the expanded connectivity. Commodity malware can now propagate to operations and affect a variety of operational elements like disruptions to a potential plant shutdown.

Internet of Things (IoT)

Today, sensors and other smart systems, called Internet of Things (IoT), are being used to a greater extent. These devices ease monitoring and enable quick access to the data, helping companies save time and resources. Despite the advantages of using IoT devices, the usage of sensors is to a small extent regulated. When seen from a security perspective, there will be a risk that large amounts of information will be accessible for a threat actor [Aut21c].

Report Presenting Top Cyber Attacks Against IACS

In December 2020, Waterfall Security Solutions published a list with the top 20 cyber attacks on IACS they considered most relevant today [Gin20]. We wanted to present the findings from this report in a separate section, as it presents 20 attacks

that are highly relevant to the topic of this thesis and should be presented in their entirety. The attacks presented include most of the topics covered from the threat assessments above, which confirms that they are relevant areas for industries using IACS, including the petroleum industry.

The report presents the attacks and a detailed explanation of each of them and how they could be conducted. The provided explanation is considered an example of an implementation of the attack. The attack is not limited to follow this explanation [Gin20].

We will present the list of attacks along with explanations of some of them. We have chosen to provide the examples of implementation for the attacks we find most relevant for our thesis. The list of possible attacks is organized from least sophisticated to most sophisticated and the attacks presented are [Gin20]:

1. IACS Insider
2. IT Insider
3. Common Ransomware
4. Targeted Ransomware
5. Zero-day Ransomware
6. Ukrainian Attack
7. Sophisticated Ukrainian Attack
8. Market Manipulation
9. Sophisticated Market Manipulation
10. Cell-phone Wi-Fi
11. Hijacked Two-Factor
12. IIoT Pivot
13. Malicious Outsourcing
14. Compromised Vendor Website
15. Compromised Remote Site
16. Vendor Back Door
17. Stuxnet
18. Hardware Supply Chain
19. Nation-State Crypto Compromise
20. Sophisticated Credentialed Insider

IACS insider revolves around a dissatisfied employee stealing other technicians' passwords by looking over their shoulder. The insider can then log on to the equipment controlling the physical processes, and make desired changes. The *IT insider* attack is based on the same principle. However, the insider is now stealing a IACS support technician's remote access credentials that visits a remote office [Gin20].

Common ransomware involves an engineer accidentally downloading ransomware on an IACS-connected workstation. The ransomware encrypts all the connected systems, which leads to a shutdown of IACS. This attack may also be varied by first infecting an IT workstation and then spread [Gin20].

Targeted ransomware is a more sophisticated attack where the attacker gains a foothold on the IT network. The foothold is gained via phishing attacks against IT employees. From there, the attacker uses Remote Access Tool (RAT) malware to steal credentials to get remote access to an industrial control system. When the access is granted, ransomware is sent to IACS to encrypt the systems and demand a ransom [Gin20].

The last type of ransomware attack mentioned is *zero-day ransomware*. It utilizes a mistakenly released list of zero-day vulnerabilities on the web. From this list, specialized ransomware is developed and sent to companies using this technology [Gin20].

The *hijacked two-factor attack* starts with phishing attacks including custom RAT malware towards support technicians of the target. The attackers wait until the technician logs on the industrial site remotely by a Virtual Private Network (VPN) connection using two-factor authentication. Once the technician is logged in, the malware moves the remote desktop window to an invisible extension. In addition, it shows an error message asking the technician to log in again. This way, the attackers can use the invisible extension to browse the IACS network if the technician has an open VPN connection [Gin20].

Industrial Internet of Things (IIoT) are making their entry into IACS and are opening up for new types of attacks [Koo20, Ram21]. An *IIoT pivot attack* uses these devices to get an entry to IT and IACS networks of the target. Through media, the attackers learn what types of devices and vendors the target uses. Through phishing attacks, they attack systems of vendors using the same IIoT devices, but that is less defended. Further, the attackers target the cloud database of the IIoT devices. By controlling the cloud database, they may now have the possibility to send commands to the IIoT end devices of the heavily-defended main target [Gin20].

Stuxnet, also mentioned in Sect. 2.4.1, is a sophisticated attack. Firstly, it compromised a less-defended service supplier of the target to extract details of how the target's systems were designed and protected. Then, autonomous, custom-made malware that exploits zero-day vulnerabilities was developed and carried to the site on removable media [Gin20].

An attack in the category of *hardware supply chain* requires a sophisticated attacker. Firstly, the attacker compromises the IT network of the target. The method to do so is not specified. Information about which vendors deliver servers and workstations to the site is then obtained. A relationship with the vendor's delivery drivers is established in order to pay them to take longer lunch breaks than usual when asked. When new equipment is delivered to the target, the drivers take a longer lunch break, and the attackers break into the delivery van. Once inside the van,

wireless-accessible single-board computers are inserted into the new equipment and repacked. After a while, the attackers may access their embedded computers wireless to manipulate the physical processes of the target [Gin20].

The most sophisticated attack presented by Waterfall Security Solutions is *sophisticated credentialed IACS insider*. This attack requires an IACS insider. The attacker bribes or blackmails the IACS insider into leaking information systematically. Information of interest could be the design of the target's physical processes, control systems, and security mechanisms. The attacker is then able to develop customized malware. The insider receives the malware from the attacker and releases this malware with its credentials on the system [Gin20]. The malware could be anything the attacker prefers. In a worst-case scenario, this malware can infect the safety systems leading to severe consequences.

2.5 Incident Management

To handle and manage threats and challenges, the companies need to follow a comprehensive incident management process. NSM has published four phases with associated principles on how to prevent from and handle unwanted incidents [Aut21a]. These phases are general and may contribute to holistic thinking for the companies regarding security. They are meant as an introduction to other more specific security branches, such as cyber security [Aut21a]. We have chosen to include the general phases in our project as they address training and exercise, and they also present incident management in a more general manner. We will also introduce the incident management phases specified in the international standard, ISO 27035, that are specific for information security [NEK16], and show how these phases correspond to the phases of NSM.

2.5.1 General Recommendations for Incident Management

The phases introduced by NSM are: identify and mapping, protect and maintain, discover, and handle and restore. The phases with additional principles are illustrated in Fig. 2.2, and we will elaborate the phases and the most relevant principles further in the following paragraphs.

In the category of *identifying and mapping,* NSM has presented seven principles on how the company should evaluate risks and create a plan for risk management [Aut21a]. It is essential to be aware that a risk assessment reflected the situation when it was created, and the threat landscape changes over time. The companies should, therefore, regularly check if a new risk assessment is needed. The seven principles presented are: mapping of internal and external requirements, identify

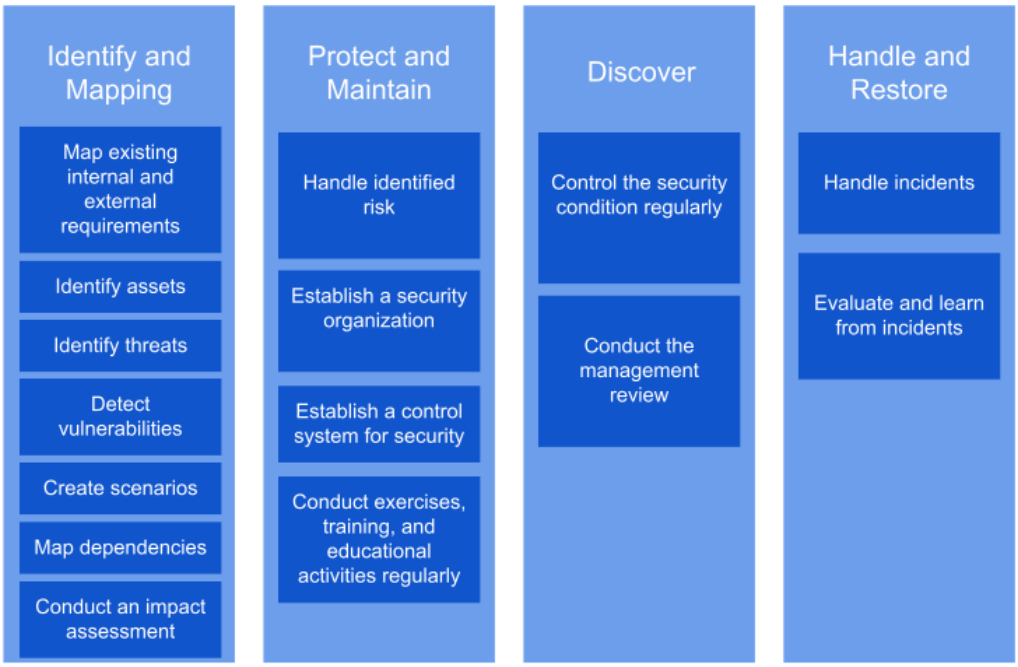

Figure 2.2: Fundamental principles on incident management. Adapted from NSMs fundamental principals for security management [Aut21a].

assets, identify threats, detect vulnerabilities, create scenarios, map dependencies, and carry out an impact assessment [Aut21a].

When the company has mapped internal and external requirements, identified assets and threats, and detected vulnerabilities, they should evaluate how a threat actor could affect their values. The threat and value assessments are the foundation for creating scenarios of unwanted incidents. Creating scenarios can help the companies in detecting vulnerabilities that may be exploited by a threat actor [Aut21a].

The phase of *protect and maintain* describes four principles on adjusting the companies security organization and control system for security. Also, how to implement security measures to reduce the identified risk and keep it at an acceptable level are described. The principles are: handle identified risk, establish security organization, establish control system of security, and conduct exercises, training, and educational activities regularly [Aut21a].

When the identified risks are managed and reduced to an acceptable level, the

security organization is established, and areas of responsibility are assigned. A control system for security is also established, and the company should conduct training, exercises, and other educational activities. Lack of these activities may lead to the desired level of security not being achieved [Aut21a].

In the *detect* phase, NSM has presented two principles [Aut21a]. This phase is about controlling the security condition to detect or discover vulnerabilities that threaten the security. The two principles are: regularly control of the security condition and conduct the management review. When controlling the security condition regularly, the company can detect whether the security condition is justifiable concerning the company's values. Controlling the security condition can give the company's leaders an indication of whether the preventive work works as intended. The management's review is an essential part of the preventative security work, as it detects whether the security managing system works as intended and if changes are needed [Aut21a].

Handle and restore is about handling incidents or deviations from the company's control system for security. This phase presents two principles: handling incidents and evaluate and learn from incidents. It is vital to handle unwanted incidents to mitigate the damage, restore the systems, and prevent the incident from happening again. How the unwanted incident was handled should be evaluated regarding the company's preventive security work. This may also prevent the company from making the same mistakes later on [Aut21a]. Preparedness exercises are usually focusing on events that require work in the *handle and restore* phase or the *detect* phase.

2.5.2 Incident Management for Information Security

The phases presented in ISO 27035 [NEK16] are quite similar to the phases of NSM but have an increased focus on information security. The standard describes five different phases: plan and prepare, detection and reporting, assessment and decision, responses, and lessons learnt. Figure 2.3 shows the phases and provides a brief description of them.

The first phase of information security incident management is *plan and prepare*. This phase corresponds to the two first phases presented by NSM, *identify and mapping* and *protect and maintain.* In this phase, the ISO 27035 standard presents eight activities to create an efficient and effective information security incident management plan. Among these activities is developing an awareness and training program for information security incidents. The company should also establish an incident response team and test the use of the information security incident management plan. Preparedness exercises will, among others, be used to test the incident management plan. Hence, these exercises will be conducted in this phase.

Fulfilling this phase will give the organization a foundation to properly manage information security incidents [NEK16].

The following phases, *detection and reporting* and *assessment and decision,* correlates with the *discover* phase described by NSM. *Detection and reporting* is about detecting and collecting information of occurrences of information security events and further report these occurrences. The ISO 27035 standard presents eight key activities the company should conduct during this phase. These activities can be used as input to assessments, decisions, and actions to be taken [NEK16]. The *assessment and decision* phase describes activities to evaluate information associated with the occurrences of information security events and then deciding whether the events should be classified as information security incidents. The standard separates between information security events and information security incidents. An event is described as a possible breach of information security or failure of controls, while an incident is considered an event that could harm the organization's assets or compromise its operations [NEK16].

Figure 2.3: Phases of incident management described by ISO/IEC 27035 [NEK16].

The company must, in the *responses* phase, respond to information security incidents based on the actions determined in the *assessment and decision* phase. Also, here, the standard lists multiple activities to be taken during this phase. The following phase, *lessons learnt*, is about learning from the incident and how it was handled. Key activities listed in this phase describe how the company should document the lessons learnt and improve current procedures and other relevant

aspects. Incident management is an iterative process, and a company should make improvements to information security regularly. The two phases *responses* and *lessons learnt* correspond to the *handle and restore* phase described by NSM.

2.6 Training and Exercise

Training and exercise are activities performed in the first phase of the ISO 27035 standard, plan and prepare, and we will elaborate on them further in this section. Sequentially, we present concepts related to training and exercise, different types of exercises, and a recent report from DNV GL on training and exercises in the petroleum sector. The concepts are presented in Sect. 2.6.1, the types of exercises in Sect. 2.6.2, and the exercise forms used in the petroleum industry today regarding IACS in Sect. 2.6.3. Lastly, the report from DNV GL is presented in Sect. 2.6.4.

2.6.1 Concepts

Training and exercise are terms often used interchangeably or as a collective term. To differentiate them and define the meanings used throughout this paper, we have presented the definitions below. In addition, the terms scenario and playbook are introduced and elaborated.

The definitions used are also used by DNV GL [Hål20] and are based on The Norwegian Directorate for Civil Protection's (DSB's) [fCP16] and The Norwegian Digitalization Agency's (DigDir's) [Age15] guides for exercises. The definitions are as follows:

> **Training:** Increasing individuals' knowledge, competence, and skills which are necessary to fill their given roles in the organization, and for handling an incident/event.

> **Exercise:** Developing an organization's ability to handle an incident/event and to reveal whether the current procedures and plans are suitable for the given purpose.

In other words, training focuses on the individuals and their capacities, whereas an exercise enhances a group of individuals' (an organization's) ability to respond to an event in a preferred way.

A scenario must be present to conduct any exercise. The scenario is presented to the participants at the beginning of the exercise, and is a model or description of a simulated event or sequence of events. It will be used throughout an exercise as a

backdrop that drives the participant discussion [DoEM21]. In the scope of security, a scenario is further defined as a description of an imaginary situation where a threat actor tries to influence the company's assets [Aut21b]. By practicing a given scenario during an exercise, the practicing organization can test their current procedures and plans for that specific situation.

During larger exercises, a playbook may be used as a supplement to the scenario. A playbook is the script of the exercise. It consists of different inputs meant to convey a message leading to a wanted effect among the participants. The playbook should only be available for the leaders of the exercise, not the participants. The exercise management uses the playbook to lead the participants through the exercise. A scenario, however, only describes the incident that has happened and the starting situation [fCP16]. Facilitators are another term for members of the exercise management [Gov21], and we will use this term throughout this thesis.

2.6.2 Types of Exercises

Exercises can be divided into four different types: functional, tabletop, game, and full-scale exercises [fCP16]. The different types have different approaches that must be considered when an exercise is planned and developed.

Functional Exercises

A functional exercise is an exercise where practically testing one or more functions within a company (or a group of practitioners). The exercise lasts for a couple of hours or a maximum of one day. The goal of this type of exercise can be to test alert plans and systems, decision processes within and between organizations, function technique or checklists, and parts of a plan. These exercises require little resources to plan, implement, and evaluate and are hence a supplement to full-scale or game exercises [fCP16].

Tabletop Exercises

Tabletop exercises are exercises where the participants meet in the same room (physically or virtually) and discuss how they will handle different situations. The situations to discuss are based on a pre-made scenario. In contrast to functional exercises, this exercise does not require any practical implementation. The exercise only revolves around the discussion of the scenario. The duration of a tabletop exercise goes from a couple of hours to a maximum of one day [fCP16]. This type of exercise is also called a discussion exercise by some actors, but we will use the term tabletop exercise throughout this paper.

Game Exercises

A game exercise is a type of exercise where the actions take place inside an exercise environment. The exercise group is separated from the outside world. All of the communication must take place in the exercise environment [fCP16]. As for tabletop exercises, no practical actions are taken during the exercise. The exceptions may be communication and notifications among the different participants as they may be present in different locations [Lar15].

Game exercises have two types of participants. There are the ones that are practicing on a scenario and the counter-players. The counter-players simulate the outside world and are supposed to provide input leading the exercise in a given direction [fCP16]. As an example, a group of firefighters may be discussing how best to let out a fire. A counter-player can then simulate the police that takes a phone call to inform the firefighters that there are explosives inside the burning building and hence change the direction of the exercise. The practitioners must now discuss how they will approach the changed situation.

Planning and conducting a game exercise requires more resources than tabletop and functional exercises. The duration may also be longer, which may increase the cost and resources needed [fCP16].

Full-scale Exercises

A full-scale exercise involves all elements from the game exercise in addition to practical work. The exercise involves parties that would be involved in a real incident similar to the scenario. The scope of a full-scale exercise is wider than a game exercise, and the goal is to have the exercise as close to an actual incident as possible. This type of exercise always plays out in real-time, and the participants use clothing, methods, and equipment that are used in real situations [fCP16].

Full-scale exercises are especially educational as the situation is perceived as genuine, and the participants see how they react and behave in a pressured and realistic situation. Even though this type of exercise can be especial educational, it also demands many resources and expenses [fCP16]. For companies in the petroleum sector, a full-scale exercise would often require a stop in the production.

2.6.3 Exercises in the Petroleum Industry: Cyber Attacks Targeting IACS

Findings from the interviews conducted by DNV GL in the report *Training and exercise* (in Norwegian: *Trening og øvelse)* show that there are considerable differences between various operators regarding how mature their work with preparedness

strategies are [Hål20]. These differences also apply to planning, conducting, and evaluating preparedness exercises for IACS. The exercises considered also include using IT as en entrance. Some of the operators interviewed were in the planning phase, while others had conducted one or two such exercises the last years [Hål20].

All of the operators interviewed in the study had introduced measures to increase the awareness of cyber security through e-learning courses and phishing campaigns. These measures were general and mainly directed towards the IT systems, and little focus has been given cyber security for IACS [Hål20].

The exercises in the area of cyber security for IACS have compassed functional exercises testing the proactive security functions where penetration testing and red-team exercises have been used [Hål20]. Hence, less focus has been given to tabletop exercises in this area. Penetration testing attempts to exploit known and unknown security vulnerabilities by using different tools and techniques [Des18]. Red-team exercises are a type of exercise where the red-team attacks the systems while a blue-team tries to defend and work as a cyber security defense team [BBJ20]. Some operators have also established a Security Operations Center (SOC) which acts as a blue-team in a red-team exercise [Hål20]. These types of exercises are often resource-demanding in the form of costs and time [BBJ20].

2.6.4 Lack of Guidelines Regarding Exercise on Cyber Attacks Against IACS

Further, in their report on training and exercise, DNV GL recommends PSA to give out, or refer to, detailed guides for the industry regarding cyber security and IACS [Hål20]. This recommendation addresses that the industry lacks clear guidelines of what is expected of them when it comes to training and exercise, especially for cyber attacks against IACS [Hål20]. We have based our research in this project on this finding.

Today, PSA holds different rules that are to be followed to ensure that the Norwegian petroleum companies keep an acceptable level of safety and security. PSA divides the rules into multiple regulations with associated guidelines. The guidelines explain in more detail how the regulations could be met and may, for instance, consist of a reference to a standard or examples of best practices. By following the suggested guidelines from PSA, a company fulfils the associated regulation and hence the requirement for safety and/or security in that specific area.

Only one of the regulations PSA holds, explicitly addresses requirements for training and exercises. *The activities regulations § 23 - Training and drills* require conduction of necessary training and exercises [Nor16]. The guidelines, on the other hand, is lacking references to standards and other documents to follow when planning

and conducting exercises towards IACS. It is this lack that is addressed in the report from DNV GL.

2.7 Existing Guidelines for Exercises

As seen in the previous section, there are no specific guidelines on how to best develop and conduct exercises within the scope of cyber attacks against IACS in the petroleum sector. However, there is related work that addresses guidelines for exercises in other contexts and sectors. This section will introduce the related work relevant to this project regarding existing guidelines for exercises.

In October 2016, DSB published a guide on how to plan, conduct, and evaluate exercises [fCP16]. This guide is written to be used by every actor that needs to perform exercises. The actors include public, private, and volunteer organizations. DigDir (formerly called Difi) and The Norwegian Water Resources and Energy Directorate (NVE) are two organizations that have used this paper to develop guidelines for exercises regarding information security and the energy sector [Age15, Lar15]. The guide from DSB introduces words and expressions. The guide first defines what exercises are and then explains all steps included in an exercise [fCP16]. It is often indicated that an exercise only exists of the performance of working through a given scenario, but that is not the case [Hål20]. Working with exercises includes planning, evaluation, and follow-up of the exercise in the time after the completion of the exercise [fCP16].

2.7.1 Phases of Conducting Exercises

DSB, NVE, and DigDir all separates the work on exercises into three phases. These are the planning phase, the exercise itself, and an evaluation phase. We have presented the different parts and their belonging activities in Fig. 2.4.

Planning Phase

Before the organization starts planning an exercise, they need to clarify a framework for all exercise parts. This framework should include the purpose, goal, structure, and scenario theme of the exercise. It will also be necessary to clarify the economic limits in advance. Some companies have an exercise plan to follow, and for them, it will be helpful to use this in the planning phase [fCP16].

The work on the scenario should start early in the planning process and once the scenario theme is set. During the planning phase of the exercise, the scenario is extended and improved to fit the goals of the exercise [fCP16]. Details on how to develop a scenario are elaborated in Subsect. 2.7.2.

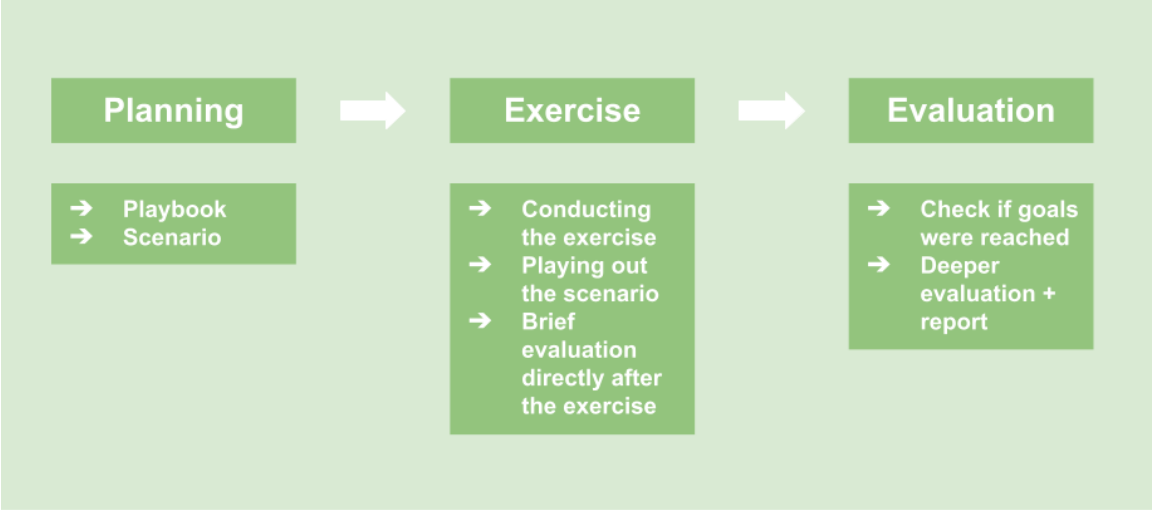

Figure 2.4: Steps in planning, executing, and evaluating exercises. The figure is adapted from [fCP16].

DigDir suggests using a playbook when conducting the exercise. The playbook may be relatively short for a tabletop exercise, but it is a helpful tool for ensuring that the exercise achieves the desired outcome and goals. The playbook must be designed during the planning phase [Age15].

Exercise

A few days ahead of carrying out the exercise, it may be beneficial to test parts of it once or several times to ensure that the exercise works as intended. How detailed this is done may vary depending on the different exercise types and the exercise's scope. The scenario is played out during the exercise. After the exercise is completed, it is important to gather the participants' first impressions. These impressions, and also feedback from the participants, will later be used in the evaluation of the exercise [fCP16].

Evaluation Phase and Follow-Up

When the exercise is completed, the work of evaluating the exercise starts. The evaluation process begins in the planning phase by defining concise goals, but the most time-consuming part starts in the evaluation and follow-up phase. In this phase, the evaluators evaluate if the goal of the exercise was met. An evaluation should also be made of the entire process, including the scenario, related to the exercise to see if changes are needed. An evaluation report should include the findings made [fCP16].

2.7.2 Scenario

As presented in the previous subsection, we see that the scenario is a central part of all types of exercises. Developing a solid scenario is fundamental for conducting an exercise that gives value to its participants [Lar15].

When selecting the scenario theme, companies may use several sources as inspiration and a base. NSM has published a guide with fundamental principles on security management and recommends basing the scenarios on the organization's threat and value assessments [Aut21b]. NVE suggests that risk- and vulnerability analyses from the companies should be used as a starting point [Lar15], whereas DSB suggests using evaluation reports from previous incidents for inspiration [fCP16]. DSB also states that sometimes it is expedient to exercise on a predefined scenario [fCP16].

The scenario must be developed in a way that triggers the exercised systems. Using the scenario theme as a base, one could identify which systems could be affected, what tasks the system has, and in which context the system operates. Then, one could investigate what consequences (direct and indirect) the event could have and what levels are affected. If the scenario triggers systems intended to be tested, and is adjusted to the purpose and goal, the exercise goals are met when executing the scenario in an exercise. A correlation between the scenario, the goal of the exercise, and the evaluation criteria is essential for the exercise to be successful. Often, the purpose and goal of the exercise, hence the purpose and goal of the scenario, should be predetermined. The purpose should answer why the exercise is conducted, while the goal states what is to be achieved.

For the content of the scenario, both NSM and DSB present parts they recommend to include [Aut21b, fCP16]. NSM suggests to include the following parts in their fundamental principles for security management [Aut21b]:

- The sequence of events: What, when, where, and how does it happen?
- The threat actor's intention and capacity.
- How the assets are affected (E.g., corrupt data, or unavailability of data).
- Other assets which are affected indirectly (e.g., environment, economy, or reputation).
- Possible notification of the event(s) in advance (e.g., from intelligence, the police, or extortioners).
- Time the threat occurs (e.g., time of the day or year, or during a gathering)
- The duration of the event(s).

DSB presents their recommended parts as follows [fCP16]:

- Prehistory/Backdrop.
- Framework conditions and facts.
- Causes and consequences.
- Events and input (from the playbook).

When developing scenarios, it could be valuable to include relevant aspects from these lists.

To help companies develop scenarios, NVE has included a collection of scenarios for companies in the energy sector in their guide [Lar15]. These scenarios should be used as a basis for the companies' own scenarios. By using this collection of scenarios, the companies have a foundation for adapting their scenarios. Even though the scenarios already give well-defined descriptions of various incidents, they should be adapted to each exercise and company to make them as appropriate as possible based on the key points mentioned in the paragraphs above [Lar15]. DigDir addresses the need to evaluate if the scenario picked from a ready-made collection is relevant for the planned exercise and that it is adjusted to fit the purpose, goal, form, and scope of the planned exercise [Age15].

Chapter 3
Methodology

In this chapter, we present the methodology used in this project. The design science method was chosen for the thesis, as we wanted to expand the reality with new artifacts. This method consists of three phases which were used iteratively. In each of these phases, we conducted various activities. All activities used for data collection go under the category of qualitative research. The activities conducted for developing and improving the artifacts are not specified as qualitative research but rather a part of the design science method where artifacts are developed. The chosen methodology was carried out in the project preceding this thesis and further maintained [HS20].

As all data collection methods used within the phases of design science are qualitative research, we first present the concept of qualitative research in Sect. 3.1. Further, the design science method with the belonging phases is elaborated in Sect. 3.2. In this section, the methods used within the phases are also presented. Sect. 3.3 gives an overview of the participants interviewed, and in Sect. 3.4 and 3.5 we elaborate on the trustworthiness and ethical aspects of the chosen research methodology.

3.1 Qualitative Research

According to Robson in *Real World Research*, there are three different research design strategies: fixed, flexible, and multi-strategy. In a fixed research design strategy, the design should be pre-specified. The data are likely in the form of numbers, and the strategy is referred to as a quantitative strategy [Rob11, p. 74]. In the flexible research design strategy, the design of the research can change slightly over time. The data are usually not numerical but in the form of words. The design strategy is also referred to as a qualitative strategy. The multi-strategy combines elements from both the fixed and flexible design and often consists of a flexible phase followed by a fixed phase [Rob11, p. 75]. We chose to use the flexible strategy for the data collection methods used in different phases of the design science method. Our research data was based on interviews and a literature review, and it was non-numerical, thus

qualitative data. By choosing this research design strategy, we had the opportunity to slightly change our approach throughout the study if we needed to.

Robson elaborates qualitative social research as a strategy where the researcher understands phenomena in their settings. The research is small-scale, meaning that few people or situations are studied [Rob11, p. 19-24]. We used interviews to gather data, making it possible to study different perspectives. This strategy made it possible to include the different perspectives and collect the knowledge from various sources and experts in our results. Using a qualitative approach, rather than a quantitative, gave us the opportunity of studying a real-life context and consider the human aspect [Rob11]. We wanted these elements in our study, and they amplified our choice towards using the qualitative social research strategy for parts of the phases in the design science method.

3.2 Design Science

Stølen defines design science in *Design Science - Research method for scientists* (In Norwegian: *Teknologivitenskap - Forskningsmetode for teknologer*) as *"science where you focus on expanding the reality with new or significantly better artifacts"* [Stø19, p. 15]. To answer our research question and sub-question, we created a collection of example scenarios, and two lists of criteria. The criteria identify an expedient and relevant scenario and an expedient scenario collection. These were based on input and feedback from relevant actors and literature. This strategy helped us understand what characteristics are present for expedient and realistic scenarios and helped us answer our research question.

The design science method consists of three phases. Fig. 3.1 shows a modified model of the method adapted to our project. It illustrates the three phases and the order in which the phases can be visited and revisited, finally leading to the result. The first phase of the design science method is to analyze the need for a new artifact [Stø19]. For our project, we found the artifact by analyzing the needs of the industry. In particular, we were looking at the needs of the petroleum industry in the area of training and exercises for cyber attacks against IACS. As a part of that artifact, we also analyzed the need for scenarios. The second phase involves innovation and creating something new [Stø19]. In our project, this involved developing a collection of example scenarios plus two lists with criteria for scenarios targeting cyber attacks against IACS in the petroleum industry. The third phase of the design science method consists of an evaluation concerning the needs of the industry [Stø19]. For us, this phase involved evaluating the artifacts we created in phase two, seen in the context of the industry's need found in phase one. The design science process is iterative, and we needed to go through the phases multiple times

to get the results that we aimed for and results that fulfilled the need identified in phase one.

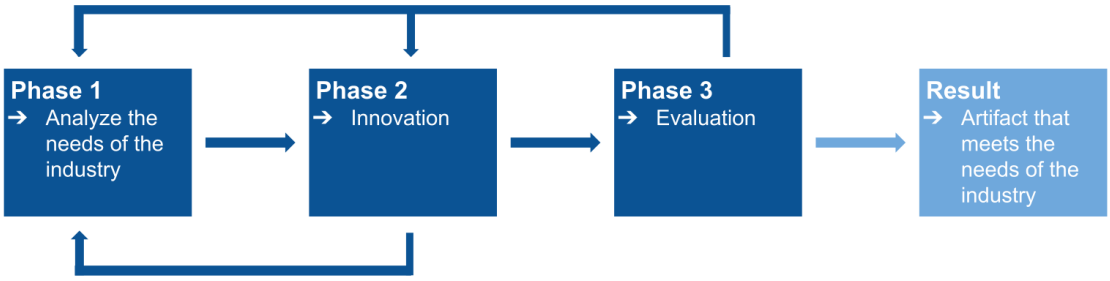

Figure 3.1: Research approach based on the design science methodology. The methodology consists of three phases that may be revisited if needed during the project work. Adapted from [Stø19, p. 20].

In each phase, we conducted several activities. Fig. 3.2 presents the different activities and the order in which they were performed. This figure illustrates how we visited phases two and three twice before we were satisfied with our results. In phase one, we conducted both a literature review and unstructured interviews with the industry. Moving to phase two, qualitative data analysis of the data gathered from phase one was conducted. Based on the analysis, we created two lists of criteria and a scenario collection. We then entered phase three, where we evaluated the scenarios in a new round of unstructured interviews with respondents from the industry. After the evaluation, we revisited phase two to improve the criteria and scenarios. In a new round in phase three, we validated our scenarios and criteria. The validation was done through semi-structured interviews with operators and a test of the scenarios with two fellow students. After the second round of phase three, we obtained our results. The results were strived to be scenarios that meet the needs of the industry in the form of lists that characterize expedient and realistic scenarios and a scenario collection with realistic and expedient scenarios.

We explain the three phases and their activities in detail in the following subsections.

3.2.1 Phase One - Analyze the Needs of the Industry

To analyze the needs of the industry regarding training and exercise, we conducted a literature review and unstructured interviews. Both of these methods are qualitative research as they collect non-numerical data. We started the literature review in the pre-project preceding this project. In the pre-project, we addressed the need

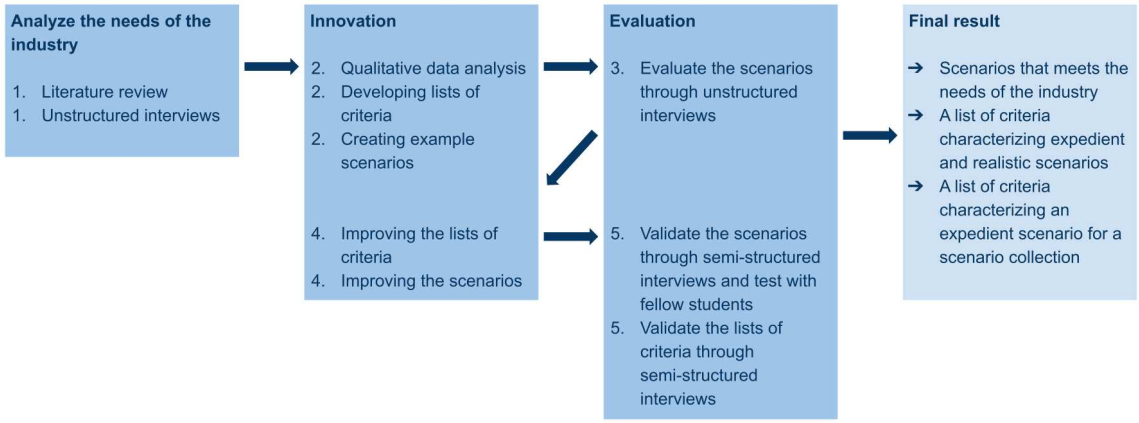

Figure 3.2: Detailed presentation of our iterations in the methodology. The figure presents the different activities in each phase of the design science method. Adapted from [Stø19, p. 20].

for scenarios related to cyber security incidents involving IACS for tabletop exercises [HS20]. Phase one continued throughout the thesis with a further literature review followed by unstructured interviews with the industry.

Literature Review

According to Robson, a traditional literature review involves systematically identifying, locating, and analyzing documents containing information related to the research problem [Rob11, p. 51]. In the pre-project, we first decided to write a thesis on a topic related to security and safety in the petroleum sector. We started phase one by searching for relevant literature and looking for deficiencies in that area. We found a lack of guidelines for training and exercises related to cyber attacks against IACS in the petroleum industry [HS20], which we decided to examine further. As this project had a time limit of 21 weeks, we narrowed the scope even further. We did not have time to make guidelines in their entirety. We decided to focus on scenarios for tabletop exercises on cyber attacks against IACS in the petroleum sector. We scoped the literature review and only included literature on this specific area.

The literature review consisted of two parts: searching for literature that verified that our research area was an area that needed contribution and searching for literature that could give us input to our research question. When searching for literature verifying our research area, we used a systematic approach. The other part, searching for input to our research question, was partly conducted using a systematic approach. In addition to using a systematic approach for this part, we also searched for literature from known sources and studied sources our supervisors recommended.

Verify the research area	Input to research question
Identify existing scenarios regarding cyber attacks against IACS.	Identify relevant literature on how to develop well-designed scenarios for tabletop exercises in general.
Identify existing criteria on how to best develop scenarios for cyber attacks against IACS.	

Table 3.1: Overview of areas for the literature review. The table show the two parts of the literature review as well as the three defined searches and how they correlate to the parts of the review.

Based on what we wanted to find, we conducted three different searches. The overview of the searches and how they correlate to the two parts introduced in the previous paragraph is presented in Tab. 3.1. The first search analyzed if there already existed scenarios for the petroleum industry (or other similar industries using IACS) regarding cyber attacks against IACS. The second search identified if criteria existed on how best to develop scenarios in the area of cyber attacks against IACS. The third search of the literature review sought to identify relevant literature on developing well-designed scenarios for tabletop exercises in general.

When searching for literature throughout systematic searches, we used the databases NTNU Oria and Google Scholar. When searching these databases, keywords and search strings were specified and used. The keywords are the terms we wanted to find papers on, while the search string combines these terms and is used when searching the databases. We have also provided inclusion and exclusion criteria for each search. These criteria focus on the content of the papers in addition to availability and language.

Search strings and keywords for the search targeting existing scenarios in the area of cyber attacks against IACS are presented in Tab. 3.2. We decided to use the identical search string for both NTNU Oria and Google Scholar. In addition, we defined one more search for Google Scholar to extract more results.

After searching the databases with these specific search strings, we obtained 42, 266, and 41 results. The searching process continued by manually filtering papers based on the inclusion and exclusion criteria shown in Tab. 3.3. When analyzing the different papers, we first examined headlines and abstracts to decide if we should study the paper more deeply. After manually filtering the papers, we were left with the result of no relevant papers. Some of the papers presented scenarios, but none specified cyber attacks against IACS.

Keywords	Search string
scenario, tabletop exercise, table top exercise, discussion exercise, IACS, ICS, control systems, industrial control systems, cyber security, cyber attack	**For Oria and Google Scholar:** scenario AND ("tabletop exercise" OR "table top exercise" OR "discussion exercise") AND (IACS OR ICS OR "control systems" OR "industrial control systems") AND ("cyber security" OR "cyber attack")
scenarios for, tabletop exercise, table top exercise, discussion exercise, preparedness exercise, IACS, ICS, control systems, cyber security, indust*	**For Google Scholar:** "scenarios for" AND (("tabletop exercise" OR "table top exercise") OR "discussion exercise" OR "preparedness exercise") AND (IACS OR ICS OR "control systems") AND "cyber security" AND indust*

Table 3.2: Key words and search strings used when searching for existing scenarios on cyber attacks against IACS. Two search strings are specified.

Inclusion Criteria	Exclusion Criteria
1. Papers containing scenarios for cyber attacks against IACS 2. Papers written in English	1. Papers are relevant to scenarios but not to cyber security and IACS 2. Papers are relevant to IACS and cyber security but not to scenarios 3. Papers that lack the full text 4. Books that are not available online

Table 3.3: Inclusion and exclusion criteria when searching for existing scenarios for cyber attacks against IACS. The criteria are focused on the content of the papers. In addition, criteria regarding availability and language are specified.

Keywords	Search string
scenario, criteria, characteristics, discussion exercise, tabletop exercise, table top exercise, cyber security, cybersecurity, cyber attacks, IACS, ICS, control systems, industrial control systems	**For Oria and Google Scholar:** scenario AND (criteria OR characteristics) AND ("tabletop exercise" OR "table top exercise" OR "discussion exercise") AND ("cyber security" OR "cybersecurity" OR "cyber attacks") AND (IACS OR ICS OR "control systems" OR "industrial control systems")

Table 3.4: Keywords and search string used when searching for existing criteria of well-designed scenarios for cyber attacks against IACS. One search string was defined and used for both NTNU Oria and Google Scholar.

Inclusion Criteria	Exclusion Criteria
1. Papers containing criteria of well-designed scenarios for cyber attacks against IACS	1. Papers are relevant to scenarios for cyber attacks against IACS but do not include any criteria
2. Papers written in English	2. Papers are relevant for criteria for scenarios but not for IACS and cyber security
	3. Papers that lack the full text
	4. Books that are not available online

Table 3.5: Inclusion and exclusion criteria for the search targeting existing criteria and characteristics of well-designed scenarios for cyber attacks against IACS. The criteria are focused towards the correct content of the papers in addition to availability and language.

When searching for existing criteria on how best to develop scenarios in the area of cyber attacks against IACS, we used the keywords and search string presented in Tab. 3.4. One search string was defined and used for the search in both NTNU Oria and Google Scholar.

From this search, we obtained 28 and 238 results from respectively NTNU Oria and Google Scholar. The procedure continued in the same way as with the first search by manually filtering out papers based on the inclusion and exclusion criteria presented in Tab. 3.5. After filtering, we were left with the result of no relevant papers here as well. None of the papers from the search focused on presenting criteria for well-designed scenarios on cyber attacks against IACS to be used in tabletop exercises.

Keywords	Search string
scenario, criteria, characteristics, discussion exercise, tabletop exercise, table top exercise, incident response, health, nurse, medical	**For Google Scholar:** "scenario" AND (criteria OR characteristics) AND ("discussion exercise" OR "tabletop exercise" OR "table top exercise") AND ("incident response") -health -nurse -medical **For Oria:** scenario AND (criteria OR characteristics) AND ("discussion exercise" OR "tabletop exercise" OR "table top exercise") AND ("incident response") NOT health

Table 3.6: Keywords and search string when searching for existing criteria of well-designed scenarios. One search string is used for both NTNU Oria and Google Scholar with some deviations in syntax.

In the last search, we sought to find criteria for scenarios to be well-designed and give a successful exercise. We also accepted results regarding characteristics for a successful tabletop exercise. For this search, we conducted both a systematic search and one less systematic. The latter, not using a systematic approach, was targeting other sources than scientific databases.

The systematic search is presented in Tab. 3.6. We defined one search string for this search as well, but the syntax was somewhat divergent to adjust correctly to the databases. We needed to be even more specific than in the previous searches as we obtained many results. We observed that some of the results were papers addressing health, medical issues, and crises. As these results were not of interest to our project, we chose to exclude papers containing the words *health*, *nurse* and *medical*.

The NTNU Oria search resulted in 24 search results, whereas in the Google Scholar search, we obtained 54 results. After manually filtering based on the criteria in Tab. 3.7, we were left with three relevant papers presented in the results (Chapt. 4).

For the second part of this search, not using a systematic approach, we investigated other sources of information to answer our research question. We sought to find input on criteria for scenarios regarding cyber attacks against IACS. Throughout the project, we received relevant literature from our supervisors that we used as a starting point. Further, we investigated the sources of this literature to find material relevant to our research question. Besides, we also searched for literature from various instances working with training and exercises, which regularly give out reports in

Inclusion Criteria	Exclusion Criteria
1. Papers containing criteria of well-designed scenarios for tabletop exercises	1. Papers are relevant to scenarios for tabletop exercises but do not include any criteria for scenarios or tabletop exercises
2. Papers containing criteria for a successful tabletop exercise	2. Papers that lack the full text
3. Papers written in English	3. Books that are not available online

Table 3.7: Inclusion and exclusion criteria for search targeting existing criteria of well-designed scenarios to be used in tabletop exercises. The criteria are focused on the content of the papers. In addition, criteria such as availability and language are specified.

this area. These instances were primarily Norwegian. The literature examined were current regulations, standards, research papers, recommended guidelines, and other relevant documents and reports.

Unstructured Interviews

In addition to the literature review, we conducted unstructured interviews to collect data and information regarding content to our example scenarios and criteria determining a well-designed scenario. Further in this project, we will refer to these interviews as data collection interviews. The interviews were conducted with actors from the petroleum industry or with insight into the industry. The participants are described in detail in Sect. 3.3.

We chose to conduct interviews over surveys as we were able to get a more in-depth understanding. Also, it allowed us to ask follow-up questions to the interviewees. We could also be more flexible in the question wording with different interviewees than we would have been with surveys.

Robson mentions three different types of interviews that can be used for data collection. These types are fully structured interviews, semi-structured interviews, and unstructured interviews. They are separated based on the degree of structure or standardization [Rob11, p. 279]. In fully structured interviews, the questions are predefined, and the wording is fixed. In the semi-structured interviews, the interviewer uses an interview guide with a checklist of topics to cover. This interview guide also includes a default wording and order for the questions. The wording and order of questions can be modified during the interview, allowing the interviewer to follow the interview flow. This type of interview allows the interviewer to ask unplanned questions to follow up on statements from the interviewee. Unstructured

interviews can be informal, and here the wording and order of questions do not have the same focus as in structured and semi-structured interviews. This informality allows the interviews to develop more freely and in different directions as long as it stays within the topic area set by the interviewer before the interview. Both semi-structured and unstructured interviews are widely used in flexible designs, and they are also known as qualitative interviews [Rob11, p. 280].

Unstructured interviews were chosen over semi-structured interviews in this phase as we wanted to get as much input on the selected topic as possible. To get this, we did not want to impact the interviewee's answers by having a particular order and wording of questions. As the interview was informal, the conversation allowed the interviewees to speak freely without worrying about following a specific script. We believe their interests and experiences may have emerged clearer from this type of interview.

It is essential to take a complete record of the interview to preserve the full potential. According to Robson, it can either be from notes taken during the interview or from a recording of the interview [Rob11, p. 282]. Rutakumwa et al. state that when comparing the data quality, these two methods are comparable in details captured [RMB+20]. As we were conducting interviews to get input on relevant content for the scenarios and how to develop them, we chose to write a summary from notes made during the interview. We were not to analyze the wording and appearance of the interviewees, and notes were therefore sufficient. Since we decided to take notes instead of recording, both of us had to take notes during the interviews to ensure that we captured as much information as possible. By choosing not to record the interviews, we believe that the interviewees could speak more freely without concern about being recorded. Besides, we believe more people were willing to participate and share their thoughts with us when not using video or audio recording.

We found it challenging to know in advance how many interviewees were needed. Robson states that qualitative research is usually small-scale in terms of numbers of persons or situations researched [Rob11, p. 19]. To determine how many interviewees we needed for our study, we used data saturation. Data saturation is the concept of collecting data until the researcher reaches a point where no new information is retrieved. However, Moser recommends continuing with the data collection by, e.g., interviewing two or three more participants to confirm that data saturation has been reached [MK18]. Throughout our study, we used data saturation as a measure of when enough interviews were conducted. Once the interviews no longer gave us new information, we carried out a small number of interviews before ending the interview process to ensure we had reached data saturation.

3.2.2 Phase Two - Innovation

Phase two of the design science method started with qualitative data analysis of the data collected from the interviews and the literature review. We used the analyzed data to create new scenarios plus two lists of criteria that characterize an expedient and realistic scenario, and an expedient scenario collection. They thus contributed to answering our research question. Phase two was visited two times, as presented in Fig. 3.2. The first iteration focused on creating the scenarios and criteria, while the second iteration focused on improving them.

Qualitative Data Analysis

In *Real World Research*, Robson stresses the need for a systematic analysis of qualitative data [Rob11, p. 465]. In our research, we used the thematic coding approach, which is a generic approach [Rob11, p. 474]. Thematic coding is flexible and can be used for all types of qualitative data [Rob11, p. 476]. It is also a simple method and requires little effort to understand and use [Rob11, p. 476], which was beneficial as the thesis was constrained to 21 weeks. We used the approach for both the literature review and data collection interviews in the first iteration and the interviews collecting feedback on the scenarios in the second iteration of phase two.

Before we could start the thematic coding of the data, we had to reduce the data. Robson recommends using summaries to perform this type of reduction. Deciding on what and how to summarize are analytic choices. They are thus a part of the data analysis [Rob11, p.473]. Right after the interviews, we had a brief discussion of the content of the interview to confirm that we had interpreted the information the same way. A summary was written shortly after each interview to reduce the lost data to a minimum. Also, when going through the literature, we wrote a summary shortly after reading to get the relevant aspects from each source written down. Writing summaries for both interviews and literature clarifies the context and significance of the data source and reduces the amount of data, which is an essential part of the analysis process [Rob11, p. 474].

The thematic coding approach consists of five phases: Familiarizing with the data, generating initial codes, identifying themes, constructing thematic networks, and integration and interpretation. The phases seem to be following each other sequentially, but Robson states that the process is not linear. Not having a linear process means that the different phases may be revisited several times, and they might also blend into each other [Rob11, p. 476].

Familiarizing with the data was done through reading and re-reading the summaries from interviews and the literature review. This way, we could see patterns. In phase two of the thematic coding approach, similar data extractions were labeled

with the same code to categorize the data. When moving to phase three, we grouped these codes into bigger groups, called themes. All three phases were visited and revisited several times and could be hard to separate as they blended into each other. In phase four, we developed a thematic network to clarify connections between the different themes. We began to see how themes and codes were related to each other and tried to systematize these connections to a sufficient extent. The last phase was the actual analysis of the data. In this phase, we searched to understand what the structured data told us and how it related to our research question and sub-question.

First Iteration: Developing Lists of Criteria

After conducting the data analysis, we were able to start developing a list of criteria. These criteria characterize how scenarios best could be developed, leading to tabletop exercises that achieve the desired learning outcome in the area of cyber attacks against IACS. In addition, we developed a list of criteria for an expedient scenario collection. The lists were developed based on relevant findings from the data analysis of the literature review and the interviews with the industry.

First Iteration: Creating Example Scenarios

After conducting the data analysis and creating the criteria, we started creating scenarios for our scenario collection. The developed scenarios were based on the analyzed data, and previous incidents and threat assessments from our background study. We used the lists of criteria when developing the scenarios. The scenario themes were chosen from various topics presented in the interviews and typical incidents and threats of earlier incidents and threat assessments. Typically, former attacks or incidents against IACS in critical infrastructures were used as a starting point when developing the scenarios.

When creating the scenarios, we aimed to make them understandable, easy to adapt, and relevant for the industry. To answer our research question based on these scenarios, we tried to make them both expedient and realistic for the industry as well. The scenarios presented in the report *Exercises - A guidance on how to plan and conduct exercises in the energy sector* (In Norwegian: *Øvelser - En veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen*) from NVE were used as an inspiration for the format of our scenarios.

Second Iteration: Improving the Scenarios and Criteria

After conducting unstructured interviews for feedback on the scenarios in phase three, we returned to phase two to improve the scenarios in the collection and the lists of criteria. Qualitative data analysis was used to code and categorize the findings from

the interviews. The findings were further used to improve the scenarios and lists of criteria before moving to phase three to validate our scenarios and criteria.

3.2.3 Phase Three - Evaluation

Phase three was visited two times during the project. In the first iteration, we received feedback on our first draft of the scenario collection. In the second iteration, we aimed to validate the criteria and scenarios against the needs of the industry.

First Iteration: Evaluate the Scenarios

In the first iteration of phase three, we contacted people from the industry that we previously interviewed to get feedback on the first draft of the scenarios. Seven of the respondents contributed to a new round of qualitative data collection through unstructured interviews. In these interviews, we received feedback that the scenarios needed adjustments to be expedient and realistic. We also used notes for these interviews to take a complete record of the interview. We then went back to phase two to make changes to ensure that they fitted the industry's needs and interests. The interviews conducted in this phase will be referred to as feedback interviews hereafter.

Second Iteration: Validate the Scenarios and List of Criteria

In the second and last iteration of phase three, we sought to validate our scenarios and criteria. To do this, we conducted semi-structured interviews and tested our scenarios on two fellow students. Both these activities go into the category of qualitative research.

The semi-structured interviews were conducted with two previously interviewed representatives from two operators to validate the scenarios and criteria. Since the interviews were semi-structured, we developed an interview guide to follow during the interviews. This guide is presented in App. A. With this guide, we first went through the scenarios one by one, asking the interviewees if they found the scenarios expedient and realistic. When validating the criteria list, we asked the interviewees if they considered the criteria important to meet for a scenario they would use in a tabletop exercise. Also, for these interviews, we used notes instead of audio recordings to preserve our data. This part of the validation was the most important for us, as the interviewees are the ones to use the criteria and scenario collection for their exercises. The interviews conducted in this iteration of phase three will hereafter be referred to as validation interviews.

As mentioned as a limitation of this study, we were not able to validate our scenarios by conducting exercises with the industry. We sought to solve this challenge

by testing our scenarios on two fellow students. We presented the different parts of the scenario to them as would have been done in an exercise. We then verified if the scenario description was understandable and included all the relevant information needed. We have to consider that the students only know the area of cyber security and do not have any technical knowledge from the petroleum sector, which may have impacted our results.

3.3 Participants

Our focus for this thesis was to gather information about training and exercises in the petroleum sector. To give the industry valuable contributions, we wanted to collect information about previous experiences, thoughts, and needs from suppliers, operators, and the government. We interviewed a total of eight different actors for our first round of unstructured interviews in phase one of the design science method. The participants included people from one supplier, two operators, two external parties working with incident responses for IACS, two external resources from the petroleum industry, and one person with work experience from both supplier and operator companies in the petroleum industry. A description of the companies and interviewees is given in Tab. 3.8. The table presents both a description and role of the company, and the interviewees. For the feedback interviews and the validation interviews, we interviewed selected interviewees from the participants in the data collection interviews.

3.4 Trustworthiness

To evaluate the trustworthiness of our study, we considered three different aspects: validity, reliability, and generalizability. We present them in more detail in the following subsections.

When using a flexible design with interviews as one of the data collection methods, Robson states that it is not possible to re-create identical circumstances and replicate the research later on [Rob11, p. 155]. According to Stølen, ensuring validity and reliability is in practice almost impossible, and one should therefore instead seek to estimate the degree of validity and the degree of reliability [Stø19, p. 122]. Based on this, we will seek to evaluate the degree of validity and reliability instead of arguing whether or not we have achieved it.

3.4.1 Validity

> *Validity is concerned with whether the findings are 'really' about what they appear to be about [Rob11, p. 77].*

Table 3.8: Description of companies and interviewees.

Role	Company Description	Interviewees
Supplier	Large global supplier that delivers control systems to several industries all over the world	Two interviewees: One IT expert and one expert on control systems
Operator	Large international company. Among the largest operators on the Norwegian continental shelf	IT security expert
Operator	Another large international company. Also among the largest operators on the Norwegian continental shelf	Expert in engineering and control systems, works with barrier management
External party	This company is an international company with expertise in risk assessment and quality assurance	Expert in risk assessment for safety
External party	National IT-security company	Expert on control systems and cyber security
Authority	State-owned. Responsible for requirements and follow-ups for safety, work-environment, and readiness in the petroleum sector	Chief engineer responsible for cyber security
Computer emergency response team for the industry	Organization that work as a support for the entire power industry both in preventive work and in handling incidents	Two interviewees: Head of the organization and an expert on prognosis and analysis, with exercise experience from other settings
Supplier/Operator	The interviewee previously worked for a global supplier company that delivers control systems to several industries all over the world. The operator company, that the interviewee now works for, is a large international company, which is among the largest operators on the Norwegian continental shelf	Expert in system integration, HMI and PLCs. The interviewee has also experience with maintenance of IACS systems, and is now responsible for barriers for cyber security.

One of the methods used to ensure a higher degree of validity for our project was member checking. This method protects the research against researcher bias. Member checking involves returning and presenting material such as notes from the interviews and interpretations made by the researchers to the respondents [Rob11, p. 158]. The interpretation of the summaries we wrote after the interviews was written

down in our results in the thesis. These results were sent back to the interviewees to show what we obtained and interpreted from the interviews and confirm that our interpretations were correct. This way, we ensured that we did not include any misunderstandings or misinterpretations in our results.

Data triangulation was another method used in our study as it helps counter threats to the validity of the research. Data triangulation is when the researcher uses more than one method of data collection [Rob11, p. 158]. For our thesis, we used both interviews and literature for our data collection.

As recommended by Robson to ensure a higher degree of validity, we provided a trace of the route back to how we got our interpretations [Rob11, p. 157]. A walk-through of the chosen research method is presented in Sect. 3.2 to give the credibility of our results. We carefully selected this method and the chosen activities for the different phases to answer the research question and sub-question. By providing a step-by-step explanation of the method used in this project, it may be easier for the reader to follow how we obtained our results and further how we came to our conclusion.

In *Real World Research*, Robson mentions several deficiencies of the human as an analyst [Rob11, p. 468]. These deficiencies could affect the validity of our study. Neither of us had former interview experience, and this may have influenced the interview sessions. As we conducted several interviews, we learned what worked and what we needed to improve for the following interviews. We learned better ways to formulate our questions to avoid leading and yes or no questions.

It was also beneficial for the thesis that we were two researchers working together. After the interviews, we could discuss and see if we had made the same interpretations when writing down the results from the interviews. Debriefing after periods in the research setting may contribute against researcher bias, hence ensure a higher degree of validity [Rob11, p.158].

3.4.2 Reliability

> *Reliability is the consistency or stability of a measure; for example, if it were to be repeated would the same result be obtained [Rob11, p. 77].*

Robson suggests using an audit trail to show others that you have been thorough, careful, and honest when carrying out the research [Rob11, p. 159]. During the research, we kept a record of all our activities. The activities include summaries from the interviews and notes from the literature we read. Details of our data analysis were also kept. These records provide a higher degree of reliability for our study.

Other researchers in a later study can obtain our results based on literature, but this might be challenging for the interviews. It is unlikely that another researcher replicating our study receives the same answers and information as we gathered through our interviews. Even though it is unlikely to get the same results, a description of the participants and their organizations is provided in Tab. 3.8 to show what type of interviewees we had. Other researchers may strive after the same types of interviewees to get similar results. This table contributes to making our study reach a higher degree of reliability, even though reliability is hard to obtain for research using interviews as data collection.

3.4.3 Generalizability

When planning our interviews, we sought to find interviewees from different parts of the oil and gas industry to give us valuable insight on training and exercise within the sector. We interviewed both operators and suppliers to get both perspectives for the research. Out of 24 operating companies on the Norwegian continental shelf [Pet21], we interviewed three representatives from two different operators. We also interviewed some relevant actors not directly involved in the industry but still had insight into how the industry's structure and systems worked. Since we only interviewed a fraction of the industry, the study does not reach generalizability.

Although the study does not reach generalizability, we believe our study will be useful for the Norwegian oil and gas industry. We received much of the same information from the different interviewees, which indicates that our findings apply to a larger sample.

3.5 Ethics

When carrying out a real world research involving people there is a potential for harm, stress and anxiety, as well as other negative consequences for the research participants [Rob11, p. 194]. The primary ethical concern regarding this study was the potential disclosure of confidential information. Wrong adversaries may misuse details regarding what types of events the organizations more or less are prepared for and should be kept confidential. Thus, the interviewees and their organizations had to be kept anonymous. In this thesis, we have only described their role and organization, and identifying information was removed. This anonymization protects the participating interviewee and their organization from being recognized. In addition, code words were used when mentioning the interviewees in other documents or talking about them during the project.

To ensure that we did not include any confidential information in the thesis, the interviewees' description was sent back to them for approval and quality check. We

also sent the results obtained from the interviews to the interviewees to verify that the results did not include any confidential information, and get their approval of the content. If they disagreed with the results, they had the option of modifying the information they had given us such that it fitted better and did not disclose any confidential information.

Chapter 4
Results

This chapter presents the results obtained from the literature review and the data collection interviews, the two lists of criteria, and the developed scenarios. In addition, results from the validation of the scenario collection and the criteria are presented. Along with the developed scenarios, we present feedback received on the first draft of the scenarios to show what kind of characteristics were lacking for the scenarios to be expedient and results from the validation interviews.

We present the results from the literature review in Sect. 4.1, results from the data collection interviews in Sect. 4.2, and the lists of criteria in Sect. 4.3. Further, we present the design of the scenarios in Sect. 4.4, along with the developed scenario collection and feedback of the first draft. At the end of the chapter, in Sect. 4.5, we present the validation.

4.1 Literature Review: Existing Criteria and Scenarios

For the literature review, we conducted three different searches as presented in Sect. 3.2.1. In this section, we present the results from these three searches. We have searched for literature concerning the petroleum industry, but other sectors are also analyzed to find valuable input to the research question and sub-question.

During the first search, seeking to find existing scenarios for tabletop exercises on cyber attacks targeting IACS, we found no relevant literature. As we did not find any relevant literature, we believe that it indicates a lack of publicly available example scenarios the industries can use today in the scope of cyber attacks against IACS. When performing this search, we looked for results in both the petroleum industry and other relevant industries. We obtained search results containing scenarios, but none of them were related to both cyber attacks and IACS and hence not what we aimed to find.

The second search, targeting existing criteria for scenarios regarding cyber attacks

against IACS to be used in tabletop exercises, did not result in relevant findings either. We could not find criteria targeting these types of scenarios, which indicates that there may not be any publicly available sources within this scope today. The criteria we found were more general and not as specific as we aimed for with this search. The results of these two searches verify that our research area indeed is an area that needs contribution.

The third and last search we defined in Sect. 3.2.1 revolved around finding literature with criteria for scenarios to be used in tabletop exercises in general. This search would give us valuable input to our research question and sub-question. For this search, we obtained more results both from a search through two databases as well as literature from other relevant sources, explained in more detail in Sect. 3.2.1. We present the results from this search in the following subsections that are sorted by themes. In addition, we give an overview of the literature analyzed in Tab. 4.1. The overview presents the titles, author(s), type, and focus of the literature relevant to our study for each of the analyzed elements. The themes of the literature are slightly different from our research area. However, we find the criteria and information presented to have value for our research.

Title	**Author(s)**	**Type**	**Focus relevant for our study**
CRIOP: A scenario method for Crisis Intervention and Operability analysis	Johnsen et al. for SINTEF	Report	Scenarios for safety in the petroleum industry
Fundamental principles for security management	NSM	Guide	Security scenarios to identify threats
Exercises - A guide in how to plan and conduct exercises in the energy sector	NVE	Guide	Safety and security scenarios for the energy sector
Guide in planning and conducting ICT-exercises	DigDir	Guide	Scenarios for ICT-exercises
Guide in planning, conducting and evaluating exercises	DSB	Guide	Scenarios for all types of exercises
Method for developing scenarios to plays and exercises	FFI	Report	Scenarios for civil protection
Scenario-Based Strategy in Practice: A Framework	Louis van der Merwe	Article	Scenarios for resource development professionals

Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	NIST	Guide	Scenarios for tabletop exercises regarding IT
Mapping the best practices for designing multilevel cyber security exercises in Estonia	Katrin Kukk	Master thesis	Scenarios for national cyber security
Getting Big Results by Going Small - The Importance of Tabletop Exercises	Joseph J. Gleason	Article	Tabletop exercises
Tabletop Exercises - Preparing Through Play	Laura Patrick and Cliff Barber	Article	Tabletop exercises

Table 4.1: Overview of the analyzed literature for the literature review. The overview shows the title, author(s), type, and focus relevant to our study for each of the elements.

4.1.1 Development

Kukk writes in her master thesis that the scenario should reflect reality [OL17], and NVE emphasizes in their guide on training and exercise the importance of making the scenario realistic [Lar15]. The literature has several suggestions on developing the scenarios to make them reflect reality and be realistic. We will, in this section, present these suggestions and recommendations.

NVE, Kukk, and DigDir recommend including other parties in the scenario creation to make the scenario relevant and realistic. Kukk recommends including delegates from cooperating entities or companies [OL17], while NVE suggests involving representatives for the participants of the exercise [Lar15]. DigDir suggest basing the scenarios on interviews of key personnel and also asking a varied selection of both internal and external sources to get even more input for the scenario theme [Age15].

In 2011, SINTEF wrote a report on a methodology, named Crisis Intervention and Operability analysis (CRIOP), to verify and validate the ability of a control center to handle all modes of operating safely and efficiently. The industry of concern in this methodology is the petroleum industry. One part of this methodology was a

scenario analysis. For this scenario analysis, they presented several criteria, including one regarding what the scenario should be based on. In their report, they suggest that the scenario should be based on real situations. In particular, they suggest basing it on previous situations on installations in the North Sea as far as possible. According to the authors, it will make the scenario realistic [JBS+11].

NVE, DSB and DigDir also address some recommendations on what to base the scenarios on [Lar15, fCP16, Age15]. NVE and DSB suggests basing the scenario on previous situations [Lar15, fCP16]. DSB elaborates that previous situations can be used as valuable sources of inspiration [fCP16]. According to NVE, scenarios may be based on risk assessments, the threat landscape, and experiences (both internal and external) [Lar15]. The experiences can be from previous exercises, accidents, incidents, or other unwanted situations. DigDir also highlights risk assessments [Age15]. In addition, other companies' exercises or actual incidents are addressed as areas to base the scenarios on. However, DigDir specifies that the content does not need to be based on something that previously has happened, as this challenges the participants' ability to improvise.

DSB addresses in their guide on training and exercise some aspects related to the development of a scenario. For the scenario to be realistic, a fundamental understanding of tasks to conduct for the system to work is needed. It is also essential to focus on triggering the intended systems when developing the scenario [fCP16].

In 2013, the Norwegian Defence Research Establishment (FFI) published a method for the development of scenarios to games and exercises. The focus of the report is to describe a method for structured scenario development. In this report, FFI addresses that it often is expedient to split a larger scenario into smaller, time-limited phases or episodes, called vignettes. In this way, the participants of an exercise can focus on particular tasks or threats [MF13].

In addition, DigDir, DSB, and NVE suggest that the scenario must be designed so that the participants get to exercise on what they intend to. DSB addresses that the roles and functions of the actors and their interaction are essential to identify to create a scenario that suits them [fCP16]. NVE highlights that the companies must adapt the scenario and exercise to fit with the objective, purpose, and goals of the scenario [Lar15]. DSB presents the importance of adapting the scenario to the actors' desires and goals. The actors' desires and goals will affect the scenario, and the scenario's adaptation should be in focus from the beginning. DSB also specifies striving for consistency between the scenario, goals of the exercise, and criteria for evaluation [fCP16]. DigDir addresses that the scope and length of the scenario should reflect the goal of the exercise and the resource usage [Age15].

4.1.2 Elements

For the actual content of the scenario, the literature addresses two different elements: failures in barriers and human errors. The authors of CRIOP suggest involving failures in several safety barriers, in addition to including human errors in a scenario. Human errors should be vital for the scenario's outcome as this will lead to a focus for the participants on always making improvements. The scenario should provoke the participants, and this could be done with human errors as they would not feel comfortable with the selected solutions. Hence, when not being comfortable with the selected solutions, the participants would focus on making improvements [JBS+11].

4.1.3 Characteristics

The literature presents several characteristics which should be present for the scenario to be well-designed. We will, in this section, give the characteristics addressed by only one source before we present the characteristics addressed by several sources.

The authors of CRIOP present a list of criteria that should be taken into consideration when selecting scenarios for their scenario analysis. This list addresses, among others, five characteristics we want to highlight as they are relevant for our research. These characteristics are feasibility, acceptance, hazard potential, specificity, and complexity [JBS+11].

By feasibility, the authors elaborate that the scenario must be physically possible to conduct. Acceptance involves the scenario being accepted as possible among the participants, while the hazard potential characteristic specifies that the scenario has the potential to cause major accidents or installation damage. The characteristic of specificity requires that the scenario is specific for the installation that will practice the scenario. Complexity, the last characteristic CRIOP presents, says that the scenario should be made complex enough to stress the participants. Some keywords they further present are simultaneous operations/incidents, extensive communication, and the fallacy of multiple safety barriers [JBS+11].

NSM has in their fundamental principles for security management presented three characteristics they find to be central for a satisfying security scenario. Consistent is one of these characteristics. By consistent, NSM elaborates that something that happens one place in the scenario does not exclude something happening in another place in the scenario [Aut21b]. The other characteristics NSM presents will be introduced later in this section.

Relevant

Relevant is a characteristic that is highlighted by NSM, NVE, DigDir, FFI, and in an article by Louis van der Merwe [Aut21b, Lar15, Age15, MF13, VdM08].

NSM addresses that the scenario should contain sufficient information to be valuable and relevant [Aut21b]. As mentioned in the section of the development, NVE suggests involving representatives for the participants to make the scenario relevant [Lar15].

In their report, FFI addresses that for a scenario to be considered relevant, it must have usability and contain the necessary information for the users of the scenario [MF13]. By usability, they specify that the organizations must adjust the scenario to the problems and challenges it is supposed to cover. Lastly, in his article on scenario planning, van de Merwe elaborates that the scenario should be relevant to the concerns of the decision-makers [VdM08].

Plausible

Another characteristic highlighted for scenarios is plausible. NSM, FFI, and van der Merwe all include this characteristic in their literature [Aut21b, MF13, VdM08].

According to NSM in their fundamental principles, plausible means that the scenario is realistic and what the scenario describes can become a reality [Aut21b]. This definition is supported by FFI, which elaborates that it must be possible for the scenario to happen [MF13]. FFI also specifies that the scenario must not necessarily be the most probable event to be plausible. The future is unpredictable, and history shows that major unforeseen changes may occur [MF13]. Van der Merwe suggests to base the scenarios on deep analysis and research and keep them internally consistent for them to be plausible [VdM08].

Short and Concise

According to the literature, the scenario should also be short and concise to be well-designed. This characteristic is supported by both DigDir and in a publication on training and exercise for IT plans, and capabilities by National Institute of Standards and Technology (NIST) [Age15, GNB+06].

DigDir presents the relevance of having a short and concise scenario that gives the participants sufficient information to understand the input from the playbook. It is not problematic if the scenario is too informative in an early draft. The removed parts at a later stage could be a valuable input to the playbook to be used during the exercise [Age15].

NIST presents in their guide that having a short and concise scenarios for tabletop exercises regarding IT is valuable. NIST addresses that there is a *"common misconception that scenarios must be very detailed to be effective."* They state that it often is more effective with a short and concise scenario. If a tabletop exercise has

too long and detailed scenarios, participants may use more time to interpret and discuss the meaning of the scenario rather than discussing the intended topics. NIST also specifies that if the exercising company desires a long, detailed scenario, an actor with thorough knowledge of all procedures and plans within the company should be participating in the development of the scenario to ensure accuracy. If the details are not correct, the participants will put their focus there instead of the objectives of the exercise [GNB+06].

Credible

Both DigDir and FFI address that the scenarios should be credible [Age15, MF13]. FFI further specifies that a credible scenario is achieved through the involvement of and anchoring with stakeholders, among other things [MF13]. In addition, they specify that the scenario could achieve credibility through a transparent process. The transparent process connects the goals and guidelines of working with the scenario to the actual content in a concise, coherent, and traceable manner.

4.1.4 Scenario Collection

We also found some criteria and recommendations in the literature for a scenario collection. We will present recommendations for the content of the collection and how to adjust the scenarios from the collection in this section.

The authors of CRIOP highlight three criteria relevant for a scenario collection: width and depth, different scenarios, and emergency preparedness. They suggest that the collection should include at least one wide and one deep scenario. Wide scenarios mean the involvement of several participants where multiple conditions are analyzed over time to an emergency. Deep scenarios mean to cover special functions isolated. Emergency teams and external groups should not be involved in a deep scenario. The authors also address that the collection should include different scenarios. Not too similar scenarios should be present, but the scenarios could, for example, address various aspects of the control room. The last criteria presented involves having at least one scenario that results in emergency preparedness. In such a scenario, the crisis team and the emergency organization should take control of the situation [JBS+11].

In their guide, NVE suggests that some of the developed scenarios should be complex and some less complex. When using a scenario in an exercise, the organization should adjust the complexity to the intended participants. Based on this, a variety in complexity should be strived to reach. For short exercises, it will be expedient to present the scenario in one part, hence less complex. In contrast, larger exercises would require several parts and inputs, which again will require the scenario to be more complex [Lar15].

DigDir highlights some aspects for developing a scenario collection. The scenario collection does not need to be large and comprehensive to be valuable. A company could develop its own collection or use external ones. If a company chooses a scenario from an external collection, they need to adjust it to the exercise's purpose, goal, form, and scope. Areas to consider when using an external scenario are the relevance, scope, and purpose of the scenario and compare the findings with the intended exercise [Age15].

4.1.5 Tabletop Exercises

As we are focusing on scenarios for tabletop exercises, we also found it relevant to analyze current criteria and recommendations for these exercises. In addition to the previous literature introduced, we have analyzed two more articles specifically on tabletop exercises for this topic. The articles analyzed are *Getting Big Results by Going Small - The Importance of Tabletop Exercises* by Joseph J. Gleason and *Tabletop Exercises - Preparing Through Play* by Laura Patrick and Cliff Barber [Gle14, PB01]. We will present the relevant aspects from these articles in this section in addition to relevant content from the previously introduced literature.

For tabletop exercises, DSB states that it may be an advantage to inform the participants about the scenario ahead of the exercise and the main issue so that they can make the necessary preparations. DSB also says that the concrete dilemmas and problem descriptions that are to be presented to the participants can be held secret until the exercise starts [fCP16].

Kukk specifies that there should be a possibility to insert injects during the exercises. These injects can be made in situations where the exercise goes through a deflection and needs to get back on the planned track [OL17]. Kukk's thesis is not explicitly directed against tabletop exercises, but we choose to include this information as we find this information relevant for tabletop exercises as well.

The article by Patrick and Barber on using tabletop exercises to reduce the severity and frequency of specific safety incidents presents a list with characteristics. This list gives characteristics of a successful tabletop exercise, and we will provide the list in its entirety as most characteristics are only addressed by these authors. The characteristics are as follows [PB01]:

- Cost-effective and affordable.
- Can be completed in 1.5 hours, with an additional 0.5 hour site visit or demonstration for interested exercise participants.
- Focuses on one key objective and one of two supplementary objectives.

- Has a simple design consistent with the exercise objectives.
- Allows for meaningful participation by all invited individuals and organizations.
- Is a positive experience, providing a solid learning and training value to the individuals and organizations involved.
- Results in a tangible, measurable improvement in the tenants' awareness and overall levels of hazardous material response capability.
- Focuses on managing the response rather than completing tasks and procedures.

Gleason's article outlines the benefits of tabletop exercises compared to larger, practical exercises and how significant the change can be by using such exercises instead. In his article, Gleason presents two different lists. One of them presents objectives the tabletop exercise should meet, while the other presents steps to ensure a successful tabletop exercise [Gle14]. Also, for this article, we will present the lists in its entirety. The only common aspect with these lists and the list from Patrick and Barber is related to the participant's exercise experience. We will highlight these common characteristics in the next section.

The list of objectives tabletop exercises should be designed to meet are the following [Gle14]:

- Provide feedback.
- Clarify responsibilities.
- Identify roles.
- Enhance skills.
- Assess capabilities.
- Evaluate performance.
- Measure and deploy resources.
- Motivate employees.

To summarize, the exercise should meet these objectives when conducted. The goal of tabletop exercises is to strive to reach these objectives.

The steps Gleason presents to ensure a successful tabletop exercise are as follows [Gle14]:

- Don't shortcut the planning process.
- Define your objectives first.
- Use a trained facilitator.
- Involve each major participant.
- Document lessons learned.
- Improvement planning.

4.1.6 Participants' Exercise Experience

For the participants' experience during an exercise, Gleason, Patrick and Barber, the authors of CRIOP, NVE, DigDir, DSB, van der Merwe, and Kukk all addresses some related aspects [JBS+11, Lar15, Age15, fCP16, VdM08, OL17]. The scenarios should be developed such that they are sufficient for these aspects. Gleason, and Patrick and Barber focus on tabletop exercises, while the other literature focuses on all exercise forms. Despite the focus on all exercise forms, we find them relevant for tabletop exercises as well.

Both Gleason, and Patrick and Barber state in their literature that all participants should be involved in the exercise [PB01, Gle14]. Patrick and Barber specifies that the tabletop exercise should allow for meaningful participation by all participants and the exercising organization [PB01], while Gleason highlights the importance of involving each major participant [Gle14].

Gleason mentions in his article that tabletop exercises should motivate the employees present in the exercise [Gle14]. This aspect is supported by Patrick and Barber, and NVE. Patrick and Barber address that the exercise should be a positive experience and provide a solid learning and training value to the individuals and organizations involved in the exercise [PB01]. NVE does also address that the participants need to experience mastery during the exercise in their guide [Lar15].

NVE also emphasizes that the scenario should lead to an exercise that is challenging for the participants [Lar15]. DSB and van der Merwe support this recommendation [fCP16, VdM08]. Further, NVE elaborates that making the exercise challenging contributes to giving intensity to the exercise. It may be expedient to follow an intensity curve during the scenario. The scenario can start with a backdrop telling a short background for the scenario before proceeding to the first phase with low intensity. The intensity can then increase during the scenario and exercise. The intensity should reach its top at the end of the exercise before it decreases and the exercise is declared finished [Lar15].

The authors of CRIOP specify that the scenario should give an exercise that causes operator involvement and stress. Situations where one central employee is missing are suggested as this will create stress among the participants and challenge them further [JBS+11].

In her master thesis, Kukk presents that the scenario should lead to an exercise that allows resilience and various reactions by the participants. People often tend to behave differently than expected, which should be allowed in an exercise [OL17].

4.2 Data Collection Interviews: Needs in Industry

To obtain insight from the industry, we conducted unstructured interviews with eight different actors. A description of the participating companies and interviewees was given in Sect. 3.3, Tab. 3.8. We conducted these interviews to gain insight into previous incidents, the industry's focus and concerns regarding attacks against IACS, how to best design scenarios, and other aspects the interviewees found relevant.

In the following subsections, we present the results from the data collection interviews. Each subsection corresponds to a theme prominent in the results from the interviews.

4.2.1 The Use of Scenarios Among the Operators Today

When performing exercises today, the industry uses scenarios to build their exercises on. There are some variations in how the operators develop these scenarios. One operator has their own personnel to create different scenarios, while another operator uses a third-party training vendor to facilitate exercises for them. The third party knows the operator well and has employees who previously worked in the oil and gas sector. The training vendor is known in the industry, and other operators use them for the same cause. The benefit resulting from this is that they can create scenarios based on lessons learned from the industry. This way, the training vendor can develop scenarios for relevant exercises for the operator to maximize the learning outcome.

4.2.2 Threat Actors

Results from the interviews show that the industry may consider several actors as a threat. The actors mentioned are nation-states, environmental organizations and activists, insiders, individual criminals, and politically motivated actors. Actors like script kiddies with minimal resources and competence are generally not considered a real threat. It often requires dedication and a strong motive to attack the petroleum industry according to the interviewees. Several of the mentioned threat actors can

go under the category of APTs, as they are willing to use a lot of resources and time to succeed with the attack.

Insiders are a threat that is highlighted by several of the interviewees. Insiders working on an offshore platform usually have easy access to systems. There is often a lack of physical security on the platform, where the interviewees used unlocked doors as an example. Employees in difficult financial situations (e.g., high gambling debt) can be willing to take inside missions for outsiders who want to sabotage an organization or retrieve some information. The outsiders may force or trick employees into doing simple jobs for them, such as inserting a USB stick into a computer. The interviewees also mentioned that the insider has a low risk of being caught and that this kind of attack is difficult to discover. Specific personnel mentioned to have easy access to critical systems were maintenance personnel. The interviewees advised us to focus a scenario around this type of personnel.

The interviewees linked other individual criminals of concern to financial motives. An example given was a criminal who invests in oil price development and then sabotages an oil company. The sabotage leads to an increase in the oil price as there is less oil in the market and the existing oil increases in value.

4.2.3 Threats and Content to Scenarios

During the interviews, the interviewees mentioned several threats as realistic. Among these, malware, such as ransomware, is one of the threats the industry seems most concerned about. This concern may be natural as the attack against Hydro in 2019 was namely a ransomware attack [Hyd20]. The industry has seen that this type of attack may happen to similar companies and then acknowledges the threat as realistic. Other highlighted threats are inside attacks (both intentional and unintentional), phishing, sabotage in the forms of jamming, attacks via IIoT, attacks against the cloud, attacks using 4G connection on offshore platforms, and attacks via a supplier. One interviewee stated that phishing and ransomware already have well-defined scenario descriptions, so our focus should be to enhance them according to an incident involving IACS. One interviewee also specified that a lot of incidents nowadays start in the IT network and spreads towards IACS and the OT network. Having scenarios using this approach could therefore be favourable and realistic.

The interviewees also highlighted other types of malware. An interviewee from one of the operators pointed out that they have experiences with malware infiltrating the IACS systems. One specific example was malware using their computers as bots in a botnet. Their computers were infected with a piece of malware that allowed remote control from a remote attacker. A botnet is a network of several computers under the control of the same attacker, which may command every computer in the botnet to perform an attack simultaneously [Net21]. The interviewee's perception is

that no targeted attack was discovered up to this day for the operator. They have only discovered opportunistic malware attacks where the attack is distributed in large numbers. The operator points out that these attacks are most likely to occur to all companies periodically and should therefore be in focus.

In addition to malware, several interviewees highlight attacks via suppliers as a relevant threat. They state that suppliers can be used as an attack vector by outside threat actors. Suppliers used as attack vectors have also been seen in previous attacks such as Stuxnet and SolarWinds. The suppliers may, for instance, bring a compromised laptop or USB stick. According to the findings, it is less probable to have an intended insider attack where the suppliers are the responsible attackers. The suppliers must follow strict policies to make changes in an operator's system, and it is less likely that they can bypass these policies and rules. Therefore, an unintentional insider attack from one of the suppliers is more probable.

During one interview, an interviewee suggested that we created a scenario where it was uncertain whether the company was under a cyber attack or not. This scenario could, for instance, be played out in a control room. In this control room, the control room operators may lose their connection to parts of critical SIS systems like the fire and gas systems. For instance, if only the gas detectors are disconnected or disrupted, there may be uncertainty among the control room personnel if a technical fault causes it or they are under attack. The explanation of these types of incidents is most often technical faults, and the personnel may therefore easier assume that a technical error causes the disconnection. As such an incident may not initially be considered a cyber attack, it is vital to raise awareness that a cyber attack could also cause an incident that looks like a technical fault. The interviewee told us about a similar self-experienced incident where a range of gas-detectors was disconnected when the interviewee first was contacted. The control room operators assumed that a technical fault caused the disconnection and did not consider a cyber attack as the reason. The detectors had been disconnected for 17 hours when the interviewee got there. If this was a cyber attack, the attacker would have had a long time performing other actions in the infiltrated network. It seems like these types of exercises could be valuable for the control room personnel. Increasing awareness around the fact that situations that seem to be caused by technical faults also can be caused by cyber attacks could make a difference.

Because of digitalization, the threat landscape has changed drastically in only a few years. This change may have made the employees the easiest way to get malicious access to the systems. The interviewee from one of the operators presented that safety is always their number one priority and focus, and it is a prerequisite when assessing new systems and processes in the digitalization segment. Digitalizing can add benefits and value, and it is essential to stay updated on emerging technologies,

but safety always comes first. The interviewee from the operator highlights that their systems are well equipped with security mechanisms. Hence, with the increasing degree of sophistication and robustness of the systems regarding cyber security, the easiest way to gain malicious access to a system becomes through the weakest links - the users (employees) themselves. This finding correlates with the threats of phishing and insider attacks highlighted through several interviews.

One of the operators explained to us the architecture and structure of the systems, including both IT systems and OT systems. There are many barriers between and inside the different systems, and the systems are segmented. Under the implementation of the systems, the sector has used a "fire cell"-structure as inspiration for the IT systems. The "fire cell"-structure is a reference to the fire cells in buildings. If a fire starts in one fire cell, it is prevented from spreading to other fire cells. By using the same structure for the IT systems, one will be able to limit the damage when under an attack, and the systems are more protected against the situation where an attacker gets access to larger parts of the systems. Because of the "fire cell"-structure, we were encouraged not to include scenarios that could cause the entire platform to shut down, as this is an difficult and complex task that requires the attacker to break multiple barriers.

4.2.4 Input to the Design of Scenarios and Exercises

When conducting the interviews, we asked the respondents if they had any general input to scenarios and exercises and how to best design them. The results are presented in the sections below.

Hands-on Experience

Several of the respondents mentioned "hands-on experience" from exercises. A general tip was to develop scenarios that could be used to receive this kind of experience. Even though the scenarios should enable hands-on actions, the scenarios should not require a full-scale exercise as the industry seldom stops its production or risks stopping it. A suggested approach was to conduct the exercise in a control room where the participants verbally tell the rest of the participants which actions they want to take and explain how to perform them.

Technical and Procedure Exercises

It is seen during the interviews that the interviewees focus on the distinction between technical and procedure scenarios and exercises. The term procedure may also be alternated with the term process-oriented, but we use the term procedure throughout this project. Technical scenarios focus on the local and low-level technical solutions, hence require a more detailed scenario. In contrast, procedure scenarios often focus

on the interaction between different participants and management decisions. A combination of these types is also possible. Both types could be used in tabletop exercises or more practical exercises like functional or full-scale exercises.

The interviewees informed us that a pitfall with too technical exercises may be that the participants handle the incident locally. Hence, little interaction with other participants is needed. The exercise may then go in the direction of the training aspect rather than the exercise aspect. Technical exercises may also be valuable, but some interviewees recommended not having pure technical scenarios. Pure OT-related scenarios were especially discouraged. The argumentation was that it was easy for the participants to "solve" the scenario by outsourcing the incident to a supplier or other external party. They recommended to have a scenario where technical aspects were relevant in correspondence with procedures. In addition, they recommended pure procedure scenarios. Other interviewees also specified that they wanted technical aspects in their scenarios that they could use in tabletop exercises and more practical exercises. Examples of practical elements included checking logs and testing the restore mechanism for different systems. When deciding upon a technical or procedure scenario, one should first affirm the learning outcome. When the learning outcome is established, the scenario can be formed as either a technical or procedure scenario.

The interviewees also stated that the intention of the scenario should be clear and unambiguous from the beginning. It must be clear whether the scenario is technical or procedure. Some respondents had experiences where exercises meant to be procedure became technical, hence were not as valuable for the chosen participants as wanted.

Exercises with Suppliers

According to findings from the interviews, the exercises should include both operators and suppliers where it is suitable. Some interviewees meant that the operators should be in focus, while others wanted to include the suppliers more. It was a general perception that the focus of this thesis should not include specific scenarios for the suppliers only.

It was consensus among the respondents that the suppliers are not involved in exercises to a sufficient extent today. Our scenarios should focus on including the suppliers where it is applicable. By including suppliers, the operators can verify whether the suppliers can fulfill the response times stated in regulations and contracts when incidents occur. Another benefit is that the operator can verify whether they are clear on who has the different responsibilities and whether the supplier sends the right person.

When interviewing the suppliers, they stated that they often are involved when an incident occurs and believed that performing exercises together with the operators could be valuable. They further elaborated if suppliers are engaged in exercises today, it is often only the management and not the first-line personnel that participates. With more technical scenarios, the first-line personnel for the suppliers will be natural participants of the exercise.

Complexity

The interviewees recommended us to vary the complexity of the scenarios. There should be several straightforward scenarios in addition to a solid number of more complex ones in our collection. Some of the interviewees asked for not too complex ones whereas others wanted them to be more complex. The interviewees also say that more complex scenarios make more extensive exercises, which could be demanding for some companies. The exercise's intention should be seen in the context of the scenario's complexity. Too complex scenarios may result in the exercise not achieving its purpose and goal.

Presentation of the Scenarios

We also received input on how we should present and organize our scenarios. One interviewee suggested that we looked into the network architecture companies in the petroleum sector uses, see Fig. 2.1. We could use this to develop different scenarios of attacks in the different areas of the architecture. For instance, we could have one ransomware attack targeting (or being discovered in) the process control network and one targeting the IT systems. Another approach presented was to have one main scenario that can lead to new, more detailed scenarios. One main scenario could be ransomware, and a more detailed one could be attackers threatening to leak their data if they do not pay the ransom.

When it comes to how the scenario should start, it is not trivial that the attack already has been discovered. We could also begin our scenarios with the Security Operations Center (SOC) or other actors observing something abnormal. The abnormal element could, for instance, be a slow update, strange values, or something that says that a stranger is inside the system. The scenario does not always have to focus on something that is wrong, it may only be something abnormal. The exercise should often focus on normalizing the situation.

4.2.5 Exercise Plan

Some interviewees mentioned during the interviews that the scenarios themselves are not enough to accomplish a successful exercise. They pointed to the difficulties of adapting the scenario into an exercise and then use the depth of a scenario expediently.

Adding a note to the developed scenarios with input to an exercise plan was suggested by one interviewee as a solution on how to lessen these difficulties. The note may include the purpose of the exercise, recommended participants, samples of important areas to ask questions, and some examples of relevant questions to ask during the exercise. In other words, the attached note is supposed to be an input to the playbook used during the exercise. Another interviewee pointed out that playbooks, in general, could be helpful and give valuable input to the exercise. To some extent, we should focus on it in our project.

The result of an exercise may depend on the purpose of the scenario and exercise, and it is essential to clarify such areas when working with the scenario. The interviewees recommended having a narrow purpose for the exercise. Another suggestion was to have several narrow purposes in the note so that the companies could find and develop a purpose that fitted their needs best. We were also encouraged to make a guide in the project report on how to adapt the scenario and exercise to different purposes. For example, a recommendation in the guide could be: "If you want to practice procedures, we recommend that you stick to the scenario and do not go into deeper technical details." For the content of the purpose, some suggestions were also made. These suggestions were: crisis management, business continuity, test an agreement with a supplier, identify missing agreements, and preparing for something unknown.

Another highlighted area of the additional note with input to the exercise plan was the participants. By having the right competence among the participants, the exercise could be more valuable and expedient for all of them. Findings from the interviews show that the normal exercise program does not always include personnel working with IACS. One interviewee had seen examples of this kind of personnel being played by counter-players in game exercises. When personnel working with IACS is not included in exercises they do not get the relevant experience from exercises on particular incidents. All relevant personnel must be included in exercises using scenarios that involve them. In addition, the findings show that the interviewees think that the first-line personnel is the ones that should be in focus in exercises directed towards IACS and cyber attacks. Cyber attacks often require a quick response, and the first-line should know how to respond to future incidents precisely and quickly. One interviewee also highlighted that the emergency organization already has continuous exercises and should not be focused on for IACS exercises. Other interviewees think that the emergency organization should be included in the exercises in addition to the first-line personnel.

Interviewees from both operators specified that they involve control system operators when conducting exercises. If the scenarios were to have a technical focus, it would be a natural step to include this kind of personnel as they most likely will

be the ones that observe something abnormal.

4.2.6 Suggestions to Criteria for Scenarios

Regarding input to our research question directly, several interviewees had input and feedback. One feedback that repeated itself was to scope down the scenario to gain better exercises that are realistic and expedient.

When conducting this study, few incidents of attacks against IACS had happened. This applies to the petroleum industry as well as other sectors where IACS play a central role. According to the interviewees, the lack of incidents results in the industry not taking attacks against IACS that seriously since they do not feel they are realistic enough. Scenarios containing attacks against IACS are usually scenarios considered to have a low probability but significant consequences. Still, they need to be properly exercised since the consequences are large. Developing scenarios that feel realistic for the participants seems to be a challenge but basing them on previous incidents increases the degree of realism according to findings from the interviews.

One operator respondent stated that it is better for the scenarios to be "boring" rather than fancy and innovative. A "boring" scenario may be more realistic and describe an incident that the involved parties find credible. It can be challenging to develop a new and fancy scenario that the involved parties see as realistic, and the interviewee recommended avoiding such scenarios.

Other feedback from the interviews was that the description of the scenario must be unambiguous, simple, and precise. There cannot be any room for different interpretations among the participants. The description should also be well explained and justified to make the scenario more realistic. Having a realistic and well-justified scenario, will make it easier for the participants to adapt the scenario and perform a solid exercise.

4.3 Lists of Criteria

Based on the interviews and the literature review findings, we have created a list of criteria for realistic and expedient scenarios for tabletop exercises and a list of criteria for an expedient scenario collection. These lists are a part of our delivery to answer our sub-question, RQ 1.1, and our research question, RQ 1. We chose to develop two different lists as we observed that a scenario collection needed additional criteria to ensure that all the scenarios in the collection are expedient. The lists are focused towards IACS and the petroleum industry, but most elements are general and will fit scenarios in other industries with other focuses as well. In this section, we will present both lists and explain the different points.

4.3.1 Individual Scenarios

The list of criteria for scenarios targeting cyber attacks against IACS in the petroleum industry to be used in tabletop exercises is presented in Tab. 4.2. In the table, we have presented each criterion along with an explanation. The justification of each criterion is given in Sect. 5.1.1 to answer our research questions.

Criterion	Explanation
Plausible	Should be realizable such that the described incident could become a reality.
Credible	The participants believe in the scenario.
Based on today's threat landscape	This could be done by basing the scenario on threat assessments, previous incidents, risk analyzes, or the operator's experiences. The experiences can either be of earlier exercises, accidents, or other unwanted incidents.
Adapted to the operator's systems and have correct technical details	Should only contain details that are correct and relevant to the company.
No potential to shut down the platform	Shutting down an entire platform is a highly complex and challenging task and should be avoided.
Fit the participants' knowledge level	E.g., control room operators are typically skilled workers and do not have the expertise in cyber security. Hence, the scenarios for cyber attacks against IACS should not require such competence.
Unambiguous	All participants should have the same understanding and interpretation of the scenario.
Concise	Should be precise and not give too much information. However, it should provide enough information for the participants to understand the input given during the exercise.
Consistent	Something happening in one place in the scenario must not exclude something happening in another place in the scenario.
Hazard potential	Should have potential to cause larger accidents or installation damage.

Define targeted assets	One should determine which assets the attack affects, both directly and indirectly. For instance, when under a ransomware attack, the IT systems may be assets directly affected, while a company's reputation may be indirectly affected.
Presented in multiple parts where appropriate	At the beginning of an incident, things may be chaotic and confusing, but you get more and more available information as time passes. The scenario should also reflect this chaotic start and the availability of information.
Includes the source of the attack and how it was detected	E.g., the malware got into the systems by phishing and was discovered by the SOC.
No defined end	When discussing the scenario, the decisions made during the exercise define the outcome of the incident. Hence, the end should not be predefined.
All participants can contribute	The scope and theme for the scenario should enable all present participants to have the opportunity to contribute.
Trigger discussion and cooperation	Should be complex enough, so the scenario needs to be discussed among different participants, which leads to cooperation.
Challenging	Should challenge the participants in the same way that an actual incident would.
Creates a sense of empowerment	All participants should feel a sense of empowerment during an exercise using the scenario.
Not known to the participants in advance	The scenario description should not be known to the participants in advance. However, the participants should be given the theme of the scenario in advance so they can make the necessary preparations.
Fulfills the exercise's purpose, goals, form, and scope	The scenario should be adjusted to fit the purpose, goal, and form of the exercise without expanding the scope.

Relevant plans are available	Relevant plans, such as preparedness plans and response plans, should be made available ahead of the exercise. By having these plans available, the participants may use them as a reference or guide during the exercise.

Table 4.2: Criteria for a realistic and expedient scenario. Explanations of the criteria are given in the second column.

4.3.2 Scenario Collection

In addition to the list of criteria for individual scenarios, we also created a similar list for a scenario collection. The criteria in this list should help ensure that the scenarios in the scenario collection can be adjusted to many users and meet many different needs. The criteria for an expedient scenario collection are presented in Tab. 4.3.

4.4 Scenario Collection

In this section, we present our scenario collection and how to use it. The scenarios in the collection are created for tabletop exercises, but they can be adapted to other types of exercises. Subsection 4.4.1 provides an explanation of the method used to develop the scenarios, Subsect. 4.4.2 presents the template used for the scenarios, and Subsect. 4.4.3 provides an explanation on how to adapt the scenarios. The created scenario collection is presented in Subsect. 4.4.4, and the feedback received on the scenarios after finishing the first draft is presented in Subsect. 4.4.5.

The scenario collection is developed primarily for organizations in the petroleum industry, and the focus of the scenarios is cyber attacks against IACS. As other industries are using the same type of systems, the collection may be relevant for organizations in those industries. We focused on varying the themes of the scenarios in the collection for the organizations to exercise on different attack vectors. This variation may give the organizations a better foundation to prepare for today's threat landscape regarding cyber security.

4.4.1 Development Method

We developed the scenarios after a method that reduces the possible explanations of an attack in line with acquiring more information. The beginning of the scenario does

Criterion	Explanation
Scalable	The company using the scenarios should have the chance to expand or narrow the scenario as they want to.
Adaptable	It should be possible to adjust the scenario to the intended goal of the exercise. The scenarios in the scenario collection should be easy to adapt for the different actors using them.
Both width and depth	A scenario collection should consist of scenarios that cover both wide and deep scopes. A wide scenario will cover a broader and slightly more superficial perspective, while a scenario with depth will go deeper into the area in focus and focus on specific details.
Variation in content	The scenarios in the collection should have a variation in content.
Variation in complexity	There should be a variation in complexity among the different scenarios. Less complex scenarios includes few aspects whereas complex scenarios address several problems to be solved.
Enables procedure and technical exercises	The scenario collection should include scenarios for procedure, technical, or combined exercises.
At least one scenario involving emergency preparedness	At least one scenario should involve emergency preparedness where the crisis team and the emergency situation should take control over the situation.

Table 4.3: Criteria for an expedient scenario collection. Explanations of the criteria is given in the second column.

not include too much information about what has happened. This lack of information leads to the possibility of many explanations and sources to the presented event. As the scenario plays out, the participants get more information which shrinks the number of possible sources and explanations. This approach correlates with reality as the information and observations will happen over time and not all at once.

4.4.2 Template for the Scenarios

As we decided to include more information than only the scenario description, we have provided a scenario template. The scenario template describes the structure of each scenario and consists of the purpose, backdrop, description, justification, and exercise plan of a given scenario. Note that we only add the backdrop in scenarios where it is expedient.

Purpose

The purpose section suggests several possible purposes an exercise with the given scenario may have. The intention is to select one or more purposes that fit with the organization's needs and not include all of the listed ones. We have divided this section further into "Procedure" and "Technical," which respectively presents purposes relevant for exercises focusing on procedures and exercises focusing on more technical aspects.

Backdrop

Some of the scenarios have a backdrop that should be presented to the participants ahead of the scenario. The backdrop is used to guide the participants in the scenario's desired direction and hint at the reason for the incident or problem that occurs later in the scenario description. The backdrop could be information about the latest updates of the systems, personnel that has been present offshore, or other relevant observations.

Scenario Description

We divided most of the scenarios into different parts, which should be presented to the participants sequentially. The participants should have time to discuss a presented part before given a new part of the scenario.

Justification of the Scenario

To show the participants that the scenarios are realistic, we chose to include a section that justifies why the industry should exercise such a scenario. This section may refer to previous, similar attacks or situations we were made aware of during our interviews for this project. Note that this section is not the same as our justification of the

scenario in Chapt. 5, as it is meant to be presented to the exercising organization. Hence, this justification will be less extensive than our justification in Chapt.5, but will include some of the same elements.

Exercise Plan

The exercise plan is meant to be a supplement for organizations when planning exercises. A template of the exercise plan is provided in Tab. 4.4. The template consists of time duration, prerequisites, suggested participants, example questions, suggestions on variations for the scenario, and suggestions to the playbook.

Time duration	
Prerequisites	
Participants	
Example questions	Technical Procedure
Variations	
Suggestions to playbook	

Table 4.4: Template for the exercise plan attached to a scenario.

The time duration reflects the time we believe is natural to use for an exercise based on the current scenario. The duration may vary according to the exercise's purpose and scope. Prerequisites state if the scenario assumes something is present for the scenario to be relevant. These prerequisites may, for example, be training or equipment. The list of participants is a suggestion with participants we find appropriate for the given scenario, but the exercising organization may adjust it. Note that all included participants should be able to contribute to the given exercise.

Example questions include several questions we find relevant. The questions are sorted based on the different parts of the scenario. These parts are further separated into technical and procedure-related questions to help the participants find their relevant questions. In addition, we have added a "Discussion and reflection"-part at the end, which sums up the scenario in its entirety. "Discussion and reflection" is meant to be more of a reflective element. It provides an opportunity for the participants to evaluate different decisions made during the exercise, preventive measures for events similar to the scenario, and evaluate the existing procedures.

The variations section suggests other variants of the same scenario if it is desirable for an organization to change the scenario slightly. For instance, this may be to change the given entrance of malware into the corporate network. The last point in the exercise plan is suggestions to the playbook going to be used throughout the exercise. The information included in this section may be a more technical

description of the attack or further input to the scenario that the facilitator may use in the exercise.

4.4.3 How to Adjust the Scenario to the Applicable Exercise

This scenario collection should be used as a starting point and inspiration for organizations in the oil and gas industry. The scenarios are not complete in the sense that adjustments are needed to fit the specific organizations' needs and purpose of conducting the exercise. This section will point out different areas that need adjustment for the scenarios to reach their full potential.

The scenarios are based on today's threat landscape, and as the threats and threat actors change, the scenarios need to be changed. Being updated on the threat landscape is an essential part of scenario development. Developing scenarios that address today's security-threatening events could help the organization reveal vulnerabilities that a threat actor may exploit in their current architecture [Aut21b].

The organization conducting the exercise must determine the purpose of the exercise and perform changes to fit this purpose. If the exercise is a combined procedure and technical exercise, it is natural to have purposes for both technical and procedural aspects. Our contribution and suggestions for a time duration, participants, example questions, and purpose must all be adjusted to match the organization's needs. For instance, the participant list may deviate from the proposed one, as will the example questions presented in the scenario collection.

We have divided most scenarios into different parts, which may give various aspects to exercise. It is up to the organizations to include all parts based on their purpose with the exercise. All scenarios originate with a cyber attack, and the following parts are a natural continuation of a given scenario. Suppose the organization only wants to exercise on the parts that include the cyber attack. In that case, they are free to drop the parts they find irrelevant, for example, parts concerning personnel responsibility.

We have chosen to extract technical details that may deviate between operators for the scenarios to be easy to adapt for several actors. The exercising company may add these details if it is suitable. If such technical details are added or specified in the scenarios, it is essential to make sure that they are correct. If they are perceived as obscured, this may weaken the outcome of the exercise as the technical details may become areas to argue.

If the scenarios are to be used in more practical exercises, the company must prepare rooms, equipment, and other relevant material needed. In a practical technical exercise, technical equipment and other appropriate systems must be available. It may

also be necessary to inject false and non-harming malware to trigger antivirus systems or changing the logs. Phishing e-mails can also be sent out to the participants ahead of the exercise for the participants to find traces in logs and antivirus systems. In a practical procedure exercise, where setting emergency response team or evacuating to the lifeboats, the company must also prepare appropriate equipment and rooms.

4.4.4 Presentation of the Scenarios

Our scenario collection consists of eight different scenarios, which we will present sequentially in this subsection. The given scenarios show the final version of the scenarios and are a part of our delivery to answer the research question, RQ 1. In Chap. 5, we will justify the different themes and design of the scenarios.

An overview of the scenarios is presented in Tab. 4.5. This overview is included to help organizations find scenarios that are relevant for them. The overview contains the name of the scenario, the incident management phase it is targeting, the threat actor present in the scenario, motivation for the event in the scenario, and a column with additional notes. For incident management, we are using the phases by NSM: identify and mapping, protect and maintain, discover, and handle and restore. The threat actor is not defined in all scenarios, but it is specified in the overview for where there is a defined threat actor. The motivation column presents a suggested motivation for the incident in the scenario, but it may deviate if the scenarios are adjusted. Other aspects worth noticing are mentioned in the last note column.

Scenario	Incident Management Phase	Threat Actor	Motivation	Note
Scenario 1: Ransomware	Handle & Restore	Organized crime	Economical profit and economical loss/stop in production	
Scenario 2: Attack with USB stick enabling 4G	Handle & Restore	Undefined	Economical loss/ stop in production	
Scenario 3: Supply chain attack with information gathering	Handle & Restore	APTs like Nation-states & Organized crime	Information gathering	
Scenario 4: Disconnection of detectors	Discover	Undefined	Physical harm, stop in production	
Scenario 5: IACS insider attack	Handle & Restore	Undefined	Information gathering	Part 3 and 4 are only expedient in pure procedure exercises
Scenario 6: Industrial Internet of Things	Discover	Undefined	Financial loss	This scenario is directed towards a technical group of people
Scenario 7: Access to IACS via remote support	Handle & Restore	Undefined	Economical loss/stop in production	
Scenario 8: Disruption of safety systems	Handle & Restore	Nation states, Organized crime	Economical damage/stop in production. Physical harm to installation and people	Should not be used in combined procedure and technical exercises

Table 4.5: Overview of the content in the example scenarios. Theme, incident management phase, suggested threat actor, motivation for the attack, and additional notes are presented.

Scenario 1 - Ransomware

Purpose:

Technical:	• Verify that the procedures for restore are in place ◦ Employees know how to switch to backup systems • Raise awareness on how to identify malicious content in relevant logs • Verify that employees know how to isolate machines
Procedure:	• Cram on the responsibility areas around notification processes (police, media, the press, and others) • Cram on the responsibility areas for handling the situation of a ransomware attack

Backdrop:
An employee receives an e-mail from what seems like one of the coworkers, with an attachment containing relevant information. The employee has high privilege access to important parts of the system. The attachment is opened and looks legit.

Description of scenario:
Part 1: A control room operator is working a night shift in the offshore control room. Suddenly, the operator discovers a message in one of the text fields in the alarm lists. The message demands a ransom of 20 million Norwegian kroner. The ransom should be paid to a given Bitcoin address. When the employees in the control room take a closer look at their systems, they observe that everything is encrypted.

Part 2: After three days, the attackers reach out with a new message. This message tells that they are in control of the main generator of the platform. If the ransom is not paid, they will stop this generator and stop the production until they receive the payment.

Justification of the scenario:
Hydro experienced a ransomware attack in 2019, making this type of attack relevant for the petroleum industry. In addition, other large-scale ransomware attacks have

been targeting different sectors over the last few years. Petya (2016) and the attack against Colonial Pipeline (2021) are examples of such ransomware attacks. The economic benefits of performing a ransomware attack can be large if the ransom is paid, and this makes it attractive for potential attackers. If the operators choose not to pay the ransom, the economic consequences for the company might still be large, as the attack most likely causes a stop in production.

A stop in the main generator may also stop the production on other platforms nearby. According to information received by an interviewee, this stop can lead to costs up to 100 million Norwegian kroner a day which is critical for the platforms. This makes such a scenario relevant, and it needs to be included in the exercise program.

Exercise Plan:

Time duration	Total of 3 hours, including introduction and first evaluation.
Prerequisites	• Training of employees on system restoration • Training of employees on checking logs
Participants	• Control room operators • Platform management • The emergency response team (both offshore and onshore) • IT experts • Government authorities • Liaisons from PSA • Employees from SOC

Example questions	*Part 1:* *Technical:* • How can we restore our systems most effectively? • Should components be isolated? ◦ Which components? And why? *Procedure:* • Should emergency preparedness be set? • Who should be involved in this process? ◦ Should external parties be involved? • Should the media be notified? • How can we restore our systems most effectively?
	Part 2: *Technical:* • How to confirm if the attackers have control over the main generator? • If they control the main generator, how can we manage the situation and take back the control?

	Procedure: • If they control the main generator, how can we manage the situation and take back the control? • As the ransom is 20 million Norwegian kroner and is a relatively small amount compared to the potential loss of this attack, it is expedient to discuss the options around paying the ransom ◦ Consequences where a ransom is paid, or not • Who should be contacted? • Should additional parties be involved and notified? ◦ Who and why? • How to communicate with and inform nearby platforms? *Discussion and reflection:* • How can you distinguish the phishing e-mail from a legit e-mail? • What are the routines when suspecting a phishing e-mail? ◦ What are the routines if you open content and then get the suspicion? • What kind of security barriers may have been compromised? • What are the benefits of being open about the incident vs. not being open? • Are there any mechanisms for automatically detecting phishing e-mails? ◦ What is the reason this e-mail got through the filter?

Variations	• If the ransom is paid: the threat of shutting down the main generator continues, and the attackers request a higher ransom. • The ransomware may be used as a distraction to cover up their initial attack. For example, to delete tracks of other attacks. • The ransomware can find its way into the system via a USB stick, a service laptop, being downloaded from the Internet on an IACS-connected engineering workstation, or by a zero-day attack. • An attacker can access the data center onshore and install the ransomware on the backup-servers they have there.
Suggestions to playbook	None

Scenario 2 - Attack with USB Stick Enabling 4G

Purpose:

Technical:	• Raise awareness on how to categorize events as technical faults or cyber attacks • Raise awareness on how to identify malicious content in relevant logs • Verify that employees know how to isolate machines • Raise awareness around technical procedures of handling a USB stick, such that no evidence is potentially damaged or removed

Procedure:	• Practice procedures around categorizing events as technical faults or cyber attacks • Raise awareness around how 4G connections may open up for cyber attacks • Practice procedures on stopping physical malicious devices from being inserted and procedures where they have been inserted

Description of scenario:
Part 1: A control room operator discovers a drastic change in the pressure measurement on one of the HMIs.

Part 2: After six hours, a technician working in the telecommunication equipment room discovers an unfamiliar 4G dongle USB stick attached to one of the switches. Several pressure measurements are now showing a drastic change.

Part 3: A technician working on the specific switch had performed a control of the switch one week earlier, and then everything looked normal with no USB attached. There have not been any outside technicians or suppliers on the platform during the last month. It is therefore suspected that the USB dongle was plugged in during the previous week.

Justification of the scenario:
This is an important scenario because it does not require a very sophisticated attacker to place a USB stick into a switch or other components connected to the control systems. On a platform, most USB ports are normally disabled on computers and other devices connected to IACS. However, findings from the interviews show that some interviewees think that this attack is still possible. The attack can also cause costly material damage and have financial consequences.

4G connection is also getting more common in the North Sea. According to the coverage map of Tampnet presented in App. B, most of the offshore installations on the south Norwegian coast have 4G connections.

Exercise Plan:

Time duration	Total of 3 hours, including introduction and first evaluation.
Prerequisites	• 4G or 5G present on offshore platforms • Training of employees on checking logs • Training of employees on isolating machines
Participants	• Control room operators • Platform management • IT experts • Other relevant technicians
Example questions	*Part 1:* *Technical:* • How can we distinguish if this is a technical fault or the beginning of a cyber attack? • How should the change in pressure measurement be handled? *Procedure:* • Should emergency preparedness be set? • Should the control room operators involve anyone else? • What procedures should be conducted in response to this event?

	Part 2: *Technical:* • Is there a reason to believe that there is a correspondence between the two events? • How should the USB stick be handled? ◦ What are the procedures? • What types of consequences may these events cause? • Shall we isolate the machine? Why?/Why not? • When was the USB stick attached? ◦ How long has it been attached? *Procedure:* • Is there a reason to believe that there is a correspondence between the two events? • How should the USB stick be handled? ◦ What are the procedures? • Should the technicians involve other parties? • What types of consequences may these events cause? • Shall we isolate the machine? Why?/Why not? • When was the USB stick attached? ◦ How long has it been attached? *Part 3:* *Technical:* • Which logs can be checked to find out who had access to the switch? *Procedure:* • How can we determine who attached the USB? • If we find out who attached the USB, how do we approach the person?

	Discussion and reflection: • How is it possible that the USB stick was attached without anyone noticing? • Are there any pros/cons of having doors/cabinets unlocked? What are the drawbacks? Should the routines for this be more strict? • How can we prevent unwanted USB sticks from being attached? ◦ How do we do this today? Is it sufficient?
Variations	• A phone with 4G enabled is connected to the switch with a USB cable instead of a USB stick. • A USB stick with malware is used instead of the USB stick that enables 4G connection. • USB ports may not often be available, but keyboards and a computer mouse can be connected with a USB cable which then can be replaced with a USB stick.
Suggestions to playbook	*Possible explanation of the attack:* • An employee working offshore was contacted by an attacker asking to bring a USB stick to the platform. This USB stick enables the switch to connect to the Internet via 4G. The employee was promised an extensive amount of money and was ensured that no one could trace the attack back to him/her. The attacker had sensitive information about the employee and threatened to leak this information if the employee did not agree to bring the USB stick and connect it to a switch. The employee agreed to do as the attacker asked. When arriving at the platform on the next work trip, the employee connected the USB stick to a switch. The attacker could then log into the internal network via 4G and start an attack.

Scenario 3 - Supply Chain Attack with Information Gathering

Purpose:

Technical:	• Raise awareness on how to identify malicious content in relevant logs • Practice technical details on how to shut an attacker out from the systems • Practice how to investigate an ongoing incident without destroying evidence
Procedure:	• Practice procedures of investigating an ongoing incident without destroying evidence • Raise awareness around situations where advanced attackers are involved and how to deal with them • Raise awareness on who should be contacted if other nation-states are involved • Verify that the response time of suppliers is as stated in contracts. • Detecting missing agreements/contracts with suppliers

Backdrop:
On Tuesday, two weeks ago, new components from a specific supplier were inserted in the IACS network.

Description of scenario:
Part 1: The SOC gets an alarm that information is attempted to be sent to an IP address which is not defined in the firewall present in the network connected to IACS.

Part 2: After investigating this event, the technicians find spyware present in the systems. The spyware seems to be gathering information about the architecture, components, and different security mechanisms around IACS. This kind of information gathering may be used to perform an advanced attack against the company later.

Part 3: After further investigations, the technicians believe that the spyware has entered the IACS network via a backdoor in a new component from a specific supplier.

Justification of the scenario:
Stuxnet and the ongoing SolarWinds attack are examples of malware attacks where suppliers are used to gaining knowledge of vulnerabilities in systems that they deliver to customers. Hence, they are used as an attack vector. The consequences of such an attack may be financial loss, material damage, and even loss of lives. These aspects makes such a scenario both relevant and realistic.

Information about a installation or the operator might not seem as critical as disruption of a system. But, it is important to keep in mind that criminals can use gathered information to plan and execute an attack later on. Therefore, information gathering should be treated as seriously as any other attack as it is difficult to differentiate if it is an ongoing attack or information gathering.

Nation-states and other APTs like organized crime, who have a lot of resources, are potential actors of such an attack. Attackers may only want to show their strength by being present in the systems or showing that they can perform such an attack. Today's warfare is different from what it used to be, where the digital domain arises as the new platform to show strength.

Exercise Plan:

Time duration	Total of 3 hours, including introduction and first evaluation.
Prerequisites	• Training of employees on log analysis
Participants	• SOC employees • Relevant IT experts • Relevant IACS personnel • Platform management • Liaison from PSA, government authorities, and NSM • Supplier • Emergency response team

Example questions	*Part 1:* *Technical:* • How to proceed to figure out what caused the alarm? • How can you determine if there are other suspicious activities in the networks? *Procedure:* • How to proceed to figure out what caused the alarm? • Who should be contacted and involved? *Part 2:* *Technical:* • What consequences may this spyware have? • What entrance may the spyware have used? How to locate it in order to stop the malware? • How to determine if any other components are affected by the spyware? • Should the awareness of the attacker's presence be hidden from the attacker? If yes, how to stop the attacker then? • How to get the spyware out of the systems? *Procedure:* • What consequences may this spyware have? • Who should be contacted and involved? NSM? The government? PSA? • Should the awareness of the attacker's presence be hidden from the attacker? If yes, how to stop the attacker then? • Should emergency preparedness be set? *Part 3:* *Technical:* • How do we handle the infected component? • How can we remove the actor without triggering the actor to perform damage? • How can we be sure that the attacker is removed from the systems?

	Procedure: • What are the different roles and responsibilities present in procedures for such a situation? • How do we handle the infected component? • How to approach the suppliers? • Consider who should be contacted. The government? NSM? PSA?
	Discussion and reflection: • Who may the threat actors be? • How to reveal the attacker? ◦ Is it even possible? • How would the actions discussed in the previous parts vary according to different threat actors? • How could the backdoor have been discovered earlier? • Discuss the routines for inserting new components • Are the contracts we have with suppliers specific enough when it comes to cyber incidents?
Variations	None
Suggestions to playbook	*Further input to the scenario:* • The attacker knows he has been discovered and starts to change values of physical devices from the components in the IACS-network

	Possible threat actors: • Nation-states • An attack group with a financial motive/wanting to insert malware • An environmental activist/group • Other suppliers who are interested in specially designed solutions *Possible motivation for the attack:* • A supplier delivers specially-adapted components to operators. An attacker may be interested in this type of information to compete as a supplier by offering the same solution.

Scenario 4 - Disconnection of Detectors

Purpose:

Technical:	• Increase competence of distinguishing a cyber attack from technical faults • Increase competence on how to troubleshoot the disruption of detectors
Procedure:	• Practice procedures around events that may be either technical errors or cyber attacks • Increase the competence for cyber related incidents

Description of scenario:

Part 1: Three technicians working the night shift in the control room observe that the gas detectors suddenly stop responding. The disruption happens simultaneously for all of the gas detectors. All other detectors are still working as intended, and no further changes in the system are noticed.

Part 2: A technician uses diagnosis software to try to find the error. The technician contacts the detectors to retrieve a diagnosis, but the detectors are not responding. The technicians can not find any technical faults when troubleshooting and suspect that a cyber attack may progress.

Part 3: The technicians receive a phone call from SOC that they have been compromised and that they currently are under cyber attack.

Justification of the scenario:
One of the operators from the interviews had this scenario as an example from an actual event. In that example, the gas detectors had been disconnected for 17 hours before measures were initiated. The reason behind that specific event was a technical error but could also have been caused by a cyber attack. Increasing the awareness that "technical errors" actually can result from a cyber attack amongst the control room operators is necessary. There are several possible causes for such an event, e.g. fog, technical error, electrical error or a cyber attack.

Exercise Plan:

Time duration	Total of 2 hours, including introduction and first evaluation.
Prerequisites	• Training of employees on log analysis

Participants	• First line personnel:
	  ◦ Control room operators
	  ◦ Maintenance personnel
	• Platform management
	• IT security experts

Example questions	*Part 1:* *Technical:* • When should the error be manually checked? Could it wait until the morning? • Is this a serious event?

	Procedure: • When should other personnel be informed? • When should the emergency response team be contacted? • Is this a serious event? *Part 2:* *Technical:* • What other components should be investigated for infection? *Procedure:* • What are the procedures for the first-line personnel? • Who should be contacted now? • What other components should be investigated for infection? ◦ Are there any procedures for this? • If suppliers are involved, what is the response time stated in the contract? *Part 3:* *Technical:* • How should we avoid that other areas get infected as well? • How can this situation be solved?
	Procedure: • Who should be contacted? • What are the procedures for the first-line personnel? • Who has the responsibility for contacting the media, PSA, etc.?

	Discussion and reflection: • How can you distinguish whether it is a cyber attack or if it is just a technical error without saying that it is not likely? • How should the correspondence between the technicians working the night shift and the SOC-personnel be organized?
Variations	• Other sensors or detectors can be disconnected. • Involve the emergency response team. • Fog may lead to detectors not responding, and this can be added to the exercise if there is a need for a more complex scenario.
Suggestions to playbook	*Further input to the scenario:* • The scenario can develop after the disconnection is discovered. The facilitator can add more severe consequences as the scenario is played out.

Scenario 5 - IACS Insider Attack

Note:
Part 3 and 4 of the scenario are only expedient in pure procedure exercises.

Purpose:

Technical:	• Raise awareness on how to identify malicious content in relevant logs • Verify that the procedures for restore are in place ◦ Employees know how to switch to backup systems

Procedure:	• Practice procedures of handling suspicions against employees

Description of scenario:
Part 1: One of the SOC-employees discovers unusual network traffic in one part of the IACS network. It seems that information has been sent through ports that are not usually used.

Part 2: After closing the ports, technicians start investigating the traffic and discover that spyware is responsible for the unusual traffic.

Part 3: After checking logs, it was discovered that the specific ports were enabled last Tuesday at 03.41 AM. When checking the list of employees at work that day, there is a reason to believe that an employee, working with technical maintenance of IACS, from a high-risk country is responsible. The company is aware that the home country may pressure citizens to do such operations, which increases the suspicion.

Part 4: The employee admits to have installed the spyware and enabled the specific ports. The employee explains the actions by telling the management that his family was threatened in the home country.

Justification of the scenario:
Employees responsible for technical maintenance often have competence in the different networks and systems of an operator. In addition, they have easy access to the systems as it is their job to work with them. This access makes it easy for them to perform such changes if they have bad intentions or experience pressure, making this scenario relevant. Having a scenario that may be adapted to enable hands-on experience like this is also favorable for the participants and makes the scenario valuable.

Exercise Plan:

Time duration	Total of 3 hours, including introduction and first evaluation.
Prerequisites	• Training of employees on system restore • Training of employees on checking logs

Participants	• SOC • Relevant first-line personnel • Platform management • Emergency response team • Relevant liaisons
Example questions	*Part 1:* *Technical:* • How to proceed to figure out what has happened? • Are other parts of the network infected? • What actions can be handled internally, and what actions need to be outsourced? *Procedure:* • How to proceed to figure out what has happened? • Who should be contacted? • What actions can be handled internally, and what actions need to be outsourced? *Part 2:* *Technical:* • How should the spyware be removed? • How can we figure out who is responsible for this malicious action?

	Procedure: • What procedures are in place to handle spyware? • How can we figure out who is responsible for this malicious action? • Who needs to be informed about the incident? *Part 3:* *Procedure:* • How to approach the suspected employee? • Should external resources be contacted? • Who should talk to the suspect? • Who needs to be informed about the incident? *Part 4:* *Procedure:* • What should be the consequences for the employee? • How to inform other employees? • How to handle media? • Who should be contacted? (PSA, police, government)

	Discussion and reflection: • What are the internal procedures for handling an insider who has experienced threats from an outside actor? • What procedures are present to mitigate the probability of an insider attack? ◦ Should other procedures be established? ◦ Should we have a procedure for having a conversation about the risks of hiring someone from a high-risk country when relevant? • Should some positions be closed for people from high-risk countries? • Do we understand the current insider threats? How can we stay updated on how this threat changes?
Variations	• Different systems can be affected by the attack
Suggestions to playbook	None

Scenario 6 - Industrial Internet of Things (IIoT)

Note:
This scenario is best suited for a technical group of participants.

Purpose:

Technical:	• Verify if we know how to identify if data values from IIoT-devices are manipulated

Procedure:	• Raise awareness of how the IIoT devices can be used as an attack vector • Be aware of the procedures present for ensuring data quality from incoming data from IIoT devices

Description of scenario:
IIoT monitoring devices are monitoring the drilling process. The data from the monitoring devices have been stable over time, but the values have changed in the last four days. Based on analysis and interpretation of the new information, onshore personnel decides that changes should be made in the production. They send the new change requirements to the platform personnel.

The changed values were a result of an attack. The attacker had tampered with the data sent from the IIoT monitoring devices to the onshore personnel, and the data were not representable for the actual values obtained by the monitoring devices.

Justification of the scenario:
IIoT devices are vulnerable to cyber attacks as they are connected to the Internet via Cloud, and new threats arise as they are integrated into the petroleum sector. The devices may be manipulated and show wrong values, which may lead to decisions based on incorrect information. Hence, such scenarios should be reflected upon.

Exercise Plan:

Time duration	Total of 1-2 hours, including introduction and first evaluation.
Prerequisites	• The company has implemented IIoT devices • Knowledge of IIoT devices and their use • A threat and vulnerability analysis for the IIoT devices is conducted
Participants	• Relevant people from the land organization

Example questions	*Technical:* • What technical procedures are present when the land organization decides to make changes to the drilling process? How is the data ensured to be correct? • How can these types of attacks/manipulations be mitigated? • How can these types of attacks/manipulations be discovered quickly? • How is the integrity of this type of data ensured? *Procedure:* • What procedures are present when the land organization decides to make changes to the drilling process? How is the data ensured to be correct? • Who is responsible for the data quality? • How is the integrity of this type of data ensured?
Variations	• The attacker can block the signals from the IIoT device such that the onshore personnel receives no data • Attacks against the IIoT devices can be varied based on the threat and vulnerability analysis.
Suggestions to playbook	None

Scenario 7 - Access to IACS via Remote Support

Purpose:

Technical:	• Raise awareness of how a two-factor hijacking attack can be performed and discovered • Verify if we are able to discover a two-factor hijacking attack and analyze changes made to a system
Procedure:	• Raise awareness of how a two-factor hijacking attack can be performed and discovered • Reflect around remote access for suppliers • Be aware of procedures around observations of double logins

Backdrop:
A supplier receives an e-mail, from what seems to be one of the coworkers, with an attachment with relevant information. The attachment is opened and looks legit.

Description of scenario:
Part 1: A system supplier of IACS is contacted by an operator to check some values the operator thinks look suspicious and is asked to log on urgently. The supplier logs in remotely to IACS to check these values. Immediately when logging in with two-factor authentication, the supplier gets an error message and is requested to log in again via two-factor. Once successfully logged in, everything looks normal. A few weeks later, a technician working for the operator discovers a new backdoor in one of the systems.

Part 2: After investigating how the backdoor has entered, the technicians find a double login of the supplier, which logged in remotely to IACS a couple of weeks ago. It seems like every time the supplier logs in he gets two active sessions. When investigating the actions performed by this specific supplier, it seems like there are two different users performing different changes at the same time.

Justification of the scenario:
Operators can use remote support to get support from suppliers or other technicians onshore. By performing a two-factor hijacking attack, explained in "suggestions to

playbook", an attacker can gather information about the systems in use and later use this information to perform an attack. This type of attack can also be performed against technicians or others who have remote access and access to perform changes to the systems. However, this type of hijacking attack requires that the technician works from outside the control room as other login methods are used once inside a control room.

Exercise Plan:

Time duration	Total of 2 hours, including introduction and first evaluation
Prerequisites	• The operator uses remote support from suppliers • Two-factor authentication is used for remote login • Training of employees on checking logs • Training of employees on system restore
Participants	• Employees from the SOC • Employees with remote access • Platform management • Relevant experts

Example questions	*Part 1:* *Technical:* • How could these two events correlate? • Which logs should be checked in order to figure out how the backdoor was established? • How to remove the observed backdoor? • Could there be more changes made to the system or other systems? • Can we know if the attacker is still present in the system? ◦ If present, how can we remove the attacker from the system? *Procedure:* • How could these two events correlate? • Who should be contacted? ◦ Should external resources be involved? • Should the emergency response team be contacted? *Part 2:* *Technical:* • Can we know if the attacker is still present in the system? ◦ If present, how can we remove the attacker from the system? • How can the double logins be taken care of? *Procedure:* • Who should be contacted? • How can the double logins be taken care of? • What procedures are present for abnormal actions from a supplier? • How to approach the targeted supplier?

	Discussion and reflection: • How can this type of attack be discovered? • How to raise awareness of this threat? • What can an attacker gain from the information gathered? • How can we protect our systems to avoid double logins and hijacking of the two-factor authentication system? ◦ Do we have any protection for this today?
Variations	• The attackers may have compromised an employee instead of a supplier.
Suggestions to playbook	*Potential explanation of the attack:* • An attacker has compromised the supplier by targeted phishing e-mails and luring the supplier to install malware. Once the target logs in remotely to the industrial site, the malware will move the Remote Desktop to an invisible extension of the laptop screen. It will then ask the target to log in again via an error message. The malware further provides remote control of the invisible Remote Desktop to the attackers. Once the target closes the remote connection, the attacker will also lose its connection. *Indicative questions to the participants:* • Could there be something wrong with the supplier's computer causing the double login? • Could the supplier's computer be compromised?

Scenario 8 - Disruption of Safety Systems

Note:
This scenario is recommended to use in either a procedure-oriented or technical exercise and not a combined one. A combined exercise may lead the participants in different directions, and the learning outcome will be reduced.

Purpose:

Technical:	• Verify that technicians/employees know how to examine the software of SIS when suspecting something malicious
Procedure:	• Practice procedures of cooperation between experts from the land organization and offshore personnel, when the land organization does not have physical or logical access to systems • Practice procedures where SIS systems do not work as intended

Backdrop:
A couple days ago, an update was made on the fire- and gas system from a service laptop.

Description of scenario:
Part 1: An employee working at the platform noticed the smell of gas from one of the gas pipes when walking by. The employee decides to call the control room operators to see if any of the gas detectors in that area have been notified about such an event. In the control room, nothing unusual is observed, and an employee from the maintenance personnel is sent out to manually check the specified area. When manually checking the gas level, it is seen that it is too high, and the detectors should have notified the control room. Since this situation has high severity, the experts on land need to be involved to a severe extent.

Part 2: It is suspected that the update of the fire- and gas system has made some changes to the code present in SIS, like increasing the limit set for the gas detector to generate an alarm. This will make the systems not notifying too high gas levels, which could cause great danger. The systems must be recovered as soon as possible.

Justification of the scenario:
The TRITON malware, used in 2017 and 2019, targeted SIS systems in the Middle East and shows that with enough resources and time, it is possible to get into one of the most critical systems and control it. As the TRITON malware demonstrated that this was indeed possible, it is important to exercise on similar scenarios as an attacker's control over SIS is critical and unwanted. In addition, this scenario will exercise the cooperation between onshore and offshore personnel, which makes it complex and relevant to exercise on.

Exercise Plan:

Time duration	A total of 4 hours including introduction and first evaluation.
Prerequisites	None

Participants	• Platform management
	• Experts from the land organization
	  ◦ Safety experts
	  ◦ Security experts
	• Control room operators
	• Liaison from PSA, government authorities, and NSM

Example questions	*Part 1:* *Technical:* • What may have caused the gas detectors to not send an alarm to the control room? *Procedure:* • What are the routines if someone smells gas and there is a suspected gas leakage? • Who should be notified about the gas leakage? • Are there any other gas leakages present on the platform? • How can we coordinate the help from onshore personnel? • How should the communication between on- and offshore personnel be conducted?

	Part 2: *Technical:* • How should the update be examined to reveal if there is malicious content there or not? • How to state if there is a correlation between the update and the lack of generating an alarm? • How should the systems best be recovered? *Procedure:* • How can we coordinate the help from onshore personnel? • Who should be contacted? • Who can locate and fix the source of the problem? *Discussion and reflection:* • What could have been the consequences if the gas leak was not discovered? • How can we prevent this from happening again? • Are our procedures good enough?
Variations	• Plant shutdown: A SIS manipulation attack can lead to a reduction in operation or even shutdown. This can be done by creating operational uncertainty or tripping the safety "fail-safes" to halt operations. • Unsafe physical state: Attack scenario where the attacker creates an unsafe physical condition that might cause physical damage.
Suggestions to playbook	None

4.4.5 Feedback on Scenarios

To improve our scenarios, we gathered feedback from several interviewees. In this section, we want to present the feedback received on the first draft of the scenarios. This feedback may show common pitfalls to avoid when developing scenarios for cyber attacks against IACS to be used in tabletop exercises. The feedback presented was taken into consideration for the final scenarios presented in Subsect. 4.4.4, hence contributed to improving them.

After we finished the first draft of the scenarios, we called in for a new round of interviews. Seven out of the eight interviewees from the first round participated in these feedback interviews. We chose to conduct all the interviews in two weeks as we wanted to compare the feedback received in the interviews. This way, we were able to make the changes that applied to most of the respondents. We received feedback on both a general level and a more detailed level for specific scenarios. The general feedback is presented in this section while we considered the detailed feedback when improving the different scenarios.

Themes and Content for the Scenarios

We varied the themes chosen for the scenarios, which the interviewees appreciated. By choosing different themes for the different scenarios, the scenarios will give the participants experience with handling various types of events. The themes for the scenarios were also considered realistic by the interviewees. The main themes for the scenarios were something the interviewees agreed could potentially happen. Still, the interviewees pointed out that some technical details were wrong or lacking for the scenarios to be considered entirely realistic. We received feedback and suggestions on what to add and change to make the scenarios more technically realistic.

We also received feedback on the content of the scenarios. Some of the scenarios made in the first draft contained extraction of sensitive information and extortion with this kind of information against the operators. Several interviewees made us aware that the petroleum industry does not consider stolen information as a critical consequence. The values of this industry lie in the production of oil and gas, which will be one of the top assets to secure. A stop in production will do more significant harm than information disclosure, and we should focus our scenarios on elements that affect the production.

Although business information might not be that sensitive for the industry, scenarios could still be directed towards extracting information about the structure and systems of an organization. Another interviewee stated that an adversary could later use this information in an attack affecting production. Besides, the interviewees also pointed out that information gathering on a supplier's product and systems

could cause significant harm to the suppliers. If an adversary got specific information on specialized systems from the supplier, they could use it to make similar products and systems. The supplier would then lose its competitive advantage and could be faced with economic loss.

Another concern that was highlighted by the interviewees, which we had not addressed in our collection, was the tampering of the safety systems, SIS. If the safety systems were disrupted, it could potentially lead to a dangerous situation. As a worst-case situation, this could lead to material damages and loss of lives. Based on this concern, they advised us to add such a scenario to our scenario collection.

Some of the scenarios made in the first draft originated as a cyber attack in IACS and evolved to other areas, like personnel responsibility. One of the interviewees advised us to remove the parts of the scenario description that were not directly directed towards a cyber attack against IACS. However, none of the other interviewees advised us to remove them.

As we considered developing a more complex scenario, we asked for suggestions from the interviewees. We then received a suggestion on creating a scenario that revolved around the cooperation between offshore and onshore personnel. The interviewee addressed that the onshore personnel often hold advanced knowledge in their expertise fields, but they do not have physical access to the platform. A scenario that challenges this cooperation would therefore be favorable.

The final feedback we received for the themes and content of the scenarios was that it is hard to shut down a platform with a cyber attack. There exist a lot of security barriers and backup options. In our first draft of the scenarios, we had one scenario that required such a shutdown. After the interviews, we saw that the scenario was unrealistic and unaccepted among the interviewees, which led us to exclude it from our scenario collection.

Size and Complexity

The interviewees considered the size of the scenarios as suitable for a tabletop exercise. One of the interviewees found it beneficial that the organizations could scale the scenarios both up and down. This way, the organizations can adjust the scenario and fit it to their purpose of conducting the exercise. The interviewee pointed that this was a strength with scenarios.

Several interviewees pointed out that many of the participants of these exercises would be employees with no specific competence in cyber security. Because of this, the scenarios should not be too complex. In the first draft of the scenarios, we added a point of diversion to confuse the participants. We decided to remove this

information after the feedback interviews to let the participants focus on the more relevant sequence of events.

Applicability

At this stage, the intention of the scenarios was to use them in tabletop exercises with the possibility of practical sections. One of the interviewees pointed out the difficulty with using these scenarios in pure practical exercises as many of them required well-developed malware. It was suggested to use pattern fields that simulated different viruses without being malicious to get abnormal results in the logs and trigger the antivirus system. Based on these results, the participants should be able to differentiate malware from regular traffic. For scenarios with technical details that are difficult to simulate, the interviewee stated that a pure discussion would be sufficient when conducting the exercise. Based on this finding, scenarios that might not enable any practical aspects is still valuable to include in the scenario collection.

Some of the scenarios might be technically challenging for the participants to play through. Some of the interviewees, therefore, recommended adding specific technical training to the prerequisites. By having these prerequisites, one avoids that the exercise stops because of technicians not knowing how to check logs, perform a restore, or other technical procedures. This aspect is relevant whether the participants check the logs practically or discuss their way through it.

The participants should not have access to the scenario ahead of the exercise, and the interviewees encouraged us to specify this when presenting the scenarios. One of the interviewees had an experience with an exercise where the exercise leaders' technical competence was lacking. The leader asked for help from someone who was to participate in the exercise. By helping the leader, the participant knew how to solve the scenario and the exercise was completed perfectly. As a result, the exercise management could not verify if the participants would have solved the scenario without knowing it in advance. In addition, the participants did not achieve the desired learning outcome as the discussion was not triggered to a desirable extent when one of the participants knew the details in the procedures beforehand.

Scenario Description

The interviewees highlighted some points for the structure of the scenario description. We were made aware that all scenarios should include the attack source and how it was detected. One of the interviewees also mentioned that if the scenario description is too technical, some of the participants might argue on the technical details, which may weaken the exercise's outcome. A suggestion was, therefore, to remove specific technical information. In addition, the scenario should not have a defined end. It is

up to the participants to discuss their way towards an end and a conclusion of the scenario.

Justification

The interviewees seemed satisfied with having the justification section to show the relevance of the scenarios and hence have the participants accept them. They also highlighted that it was wise to use previous, similar attacks in this section to actualize the content of the scenario. For instance, we can use SolarWinds and Stuxnet to justify why it is vital to have a scenario on supply chain attacks and exercise on such a scenario.

Participants

We received feedback from several interviewees that we should add more participants to the suggested participants for each scenario. In particular, platform management should be included in almost all exercises, and the interviewees also recommended including experts from different fields. For instance, IT experts should often be involved as we focus on cyber attacks in this project. In addition, liaisons from various authorities, like PSA and the police, should be included where relevant. Liaisons are representatives that ensure the communication between several people or groups [Dic21b]. As an example, in the petroleum industry, a liaison from PSA provides a valuable collaboration between the offshore personnel and PSA.

According to one interviewee, there is no need to include suppliers in the list of participants. In the scenarios and exercises where it would be expedient to have the suppliers, the participants already present would determine if they should contact the suppliers or not. According to this interviewee, this should be a part of the exercise.

Example Questions

One of the interviewees suggested that we should sort the example questions into technical and procedure-related questions. This structure will make it easier for the participants to find the questions and tasks relevant to them, and the exercise will go smoother. The discussion and reflection questions were supposed to be questions for participants in the exercise. Some of the interviewees had experience with asking those types of questions during exercises, and their experience was that the participants stayed quiet with no one responding. The participants might not have experience discussing these types of questions or reflecting on the topic, making it hard for them to participate in those questions. According to the interviewee, this part should, therefore, only be for exercise management.

4.5 Validation

To validate our scenarios and criteria, we conducted two different activities. We used semi-structured interviews to validate both the criteria and example scenarios through validation interviews. These interviews were held with the operators previously interviewed. To validate the scenario description of the example scenarios, we also conducted a test with two fellow students.

4.5.1 Semi-structured Interviews

To validate that the lists of criteria and scenarios were realistic and expedient, we invited three of the previous respondents to validate them. All of these respondents are employees in operator companies. Two out of three respondents wanted to contribute. The interview guide used throughout the interviews is presented in App. A.

Lists of Criteria

The interviewees validated the criteria in both lists to be relevant and valuable. The first interviewee agreed with all the criteria presented but had some minor comments that gave a better clarification of the intention of the criteria. In addition, the interviewee suggested adding a new criterion. This criterion involved preparing reports and other documents needed for the exercise using the scenario and have these available during the exercise. This way, the scenario and exercise would reach its potential to a greater extent.

The second interviewee also agreed on all criteria, including the one suggested by the other interviewee. Also, in this interview, we received some minor comments on the chosen wording in some of the criteria. One of the applicable criteria was "Create stress among the participants." The word "stress" was suggested to be replaced with "challenge" or similar terms. "Stress" could be adverse for the exercise, and we should therefore not use this particular word.

We took the suggestions we received into consideration and adjusted the lists of criteria presented in Sect. 4.3 to these suggestions. Minor feedback on the rest of the scenarios are also presented in that section. We also received feedback that our lists of criteria matched our example scenarios, which was strived for during the project.

Realism of Scenarios

The interviewees considered the majority of the scenarios to be realistic. The respondent from one of the operators found seven out of eight scenarios to be realistic, where scenario six was not validated as realistic because of the respondent's little experience with IIoT.

The other interviewee considered five out of eight scenarios to be realistic. Scenario three was considered partly realistic. In part two of the scenario, words such as "seems like" and "suspects" were used. In a real-life situation, the interviewee specified that things are much more binary, and personnel at an offshore installation does not have any suspicions without checking them right away. The second scenario that was considered unrealistic was scenario seven. The respondent believed that the scenario would have been realistic for other lines of business and had also seen examples of two-factor hijacking in other sectors. Although, the respondent was unsure if it was even possible to succeed with such an attack in the oil and gas industry.

Scenario eight was validated as realistic by one of the respondents and unrealistic by the other. One of the respondents stated that a suspected gas leakage would have lead to a shut down of the platform or parts of it, and an employee would not have been sent to manually measure the gas level. However, the other operator said that it is considered normal to smell gas at a platform. Some of the toxic gasses have scent under small concentrations. If the concentration is too high, it will no longer give odor. If an employee can smell gas, that might indicate a small concentration of gas and that the levels are below what would be discovered by the gas detectors. In their situation, they would have sent a person to manually check the gas level in that area to confirm or diminish a gas leakage.

For the scenarios the interviewees did not consider realistic, they provided suggestions for improvements. We present these suggestions in Subsect. 4.5.1 below.

Expediency of Scenarios

The interviewees also found most scenarios to be expedient. One interviewee found eight out of eight scenarios to be expedient, while the other interviewee found seven out of eight to be expedient. Scenario eight was not considered expedient for the interviewee as it was not regarded as realistic in the first place. Without a realistic scenario, the interviewee could not see that the scenario could give a valuable learning outcome for the participants and the exercising organization.

It was also specified by the interviewee considering scenario three to be partly realistic that it would be expedient when we applied small changes to part two of the scenario. Based on the current scenario, it was considered to be expedient, but it would be more expedient after applying the changes.

Scenario six regarding IIoT was, by the same interviewee, considered expedient for a technical group of participants. This aspect should be specified when presenting the scenarios.

Suggested Improvements to Scenarios

In scenario one, we were encouraged to change how the ransomware was discovered. In our scenario, the ransomware was discovered in a text string in an alarm list. One of the respondents suggested changing this to a pop-up window, as this was considered more realistic. It was also recommended to replace "core generator" with "main generator" as this is the term used in the operator company.

For scenario two, one of the operators suggested connecting the 4G dongle to a server or an engineering workstation instead. The respondent was unsure whether it was technically possible for a scenario to play out as described if the 4G dongle was connected to a switch. Another suggestion was to change when the technician had performed the control from two weeks to one week. The employees are often stationed at the platform for two weeks at a time.

Suggested improvements for scenario three were to either camouflage the information gathering as something else, such as an update on the systems, or add a time perspective. If we set the time perspective of part two to a short period, like 30 minutes, the scenario was considered realistic. On the other hand, if we set the time perspective to a longer period, like one week, it would not be realistic.

For scenario four, on disconnection of detectors, one interviewee suggested adding a third part to the scenario. This part should make it clear that they were under a cyber attack.

For scenario five, on a IACS insider attack, it should appear more evident what type of ports are considered in the first part of the scenario. The interviewee suggested that we specify that it is a physical switch port.

The scenario on IIoT and the scenario on remote support did not receive any suggested improvements presented in the interviews. Although, one interviewee considered the scenario on IIoT to be relatively narrow. The interviewee suggested using the scenario in combination with one of the other scenarios presented.

For scenario eight, on a disruption of a safety system, the interviewee finding it unrealistic suggested that we changed the scenario to gas detectors not notifying when the gas level exceeds its limit values. Queries to the detectors should still work as intended, but the detectors would not notify the control room like they usually would.

Some of the suggested improvements above were taken into consideration when improving the scenarios after the validation. Thus, the presented scenarios in Sec. 4.4.4 contains some of these changes. We did not have a second validation of the scenarios after we applied these changes.

4.5.2 Test with Fellow Students

In the test with two fellow students, we wanted to verify that the scenario description of the different scenarios was understandable with enough details to start a discussion when used in a tabletop exercise. To validate this, we presented each scenario to the students part by part in the same way we would have done in a tabletop exercise with the industry.

The results of this validation were primarily positive. For seven out of the eight scenarios, the students discussed the topics and clearly showed that they understood the different situations presented. Based on this, we verified that seven out of eight scenarios had an understandable scenario description with sufficient information. For part one of scenario eight, the students started to discuss in a direction not intended for that scenario. They were closer to what we intended in part two but still not close enough to validate it as concise and valuable. This observation showed that we needed to adjust that scenario to be concise and valuable, hence expedient.

Chapter 5
Discussion

This chapter will discuss what expedient and realistic scenarios for tabletop exercises related to cyber attacks against IACS in the petroleum industry are. It will also address which criteria to evaluate in order to categorize a scenario as expedient and realistic. Hence, we will discuss the research question and sub-question presented in Chapt. 1. The questions will be discussed using the findings from Chapt. 2 and 4. We have divided the chapter into two subsections representing the two questions to be answered, respectively the sub-question, RQ 1.1, and the research question, RQ 1.

RQ 1.1 is developed to help answer RQ 1. We developed two lists of criteria for this sub-question, where one categorizes realistic and expedient scenarios, and the other categorizes an expedient scenario collection. We also use these lists to answer RQ 1. The lists will hence be a part of the answer to RQ 1 along with the scenario collection we have developed. Thus, as the sub-question is a central part of RQ 1, we will discuss it in the first section, Sect. 5.1. RQ 1 will then be discussed in Sect. 5.2. Lastly, we will discuss limitations and relevance of our study in Sect. 5.3.

5.1 Criteria Categorizing Realistic and Expedient Scenarios

To answer the sub-question asking, RQ 1.1 "which criteria must be evaluated in order to categorize a scenario as expedient and realistic?" we will justify the two lists of criteria presented in Sect. 4.3. We will go through each of the criteria and explain why those criteria must be present for a scenario to be realistic and expedient. Some of the criteria may make the scenario realistic, and others expedient, and some will be central for both realism and expediency. We will also justify how and why the criteria for a scenario collection makes the collection more expedient.

The criteria we chose to add to our lists are chosen based on the literature review and interviews with the industry. Criteria meant for other types of exercises are excluded from the list, as we have only prioritized to include criteria that fit tabletop exercises. We included criteria that were prominent and highlighted as important in

interviews and literature in the list. Also, we prioritized adding criteria mentioned in several interviews and places in the literature to the list as it showed relevance from more than one source. Some of the included criteria are only mentioned one place in the literature. However, we find them valuable to include.

5.1.1 List of Criteria for Individual Scenarios

In the following paragraphs, the criteria developed for scenarios to be realistic and expedient will be elaborated and justified.

Plausible

We have added this criterion to increase a scenario's realism. If the participants do not see the scenario as plausible, they will not consider it realistic either. A scenario describing an incident that could not become a reality would be hard for the participants to find realistic. Also, if the scenario is not seen as plausible by the participants, they can find it challenging to accept.

The importance of having a plausible scenario is confirmed by both findings from the literature and the data collection interviews. NSM, FFI and van der Merwe do all present plausible as a criterion for a successful scenario in their literature [Aut21b, MF13, VdM08]. FFI specifies that the scenario not necessarily must be the most probable event for it to be considered plausible [MF13]. The history confirms that unforeseen changes may occur [MF13]. In the validation interviews, the interviewees confirmed the criterion to be essential for the realism of a scenario.

Credible

If a scenario is credible, it increases the realism and the expediency of the scenario. A credible scenario where the participants believe the events could happen will ensure that the participants find the scenario realistic. Based on this, we included credible as a criterion for our list of criteria. Results from our literature review and a finding from a data collection interview confirm that this is a criterion that should be included.

DigDir presents that the content of the scenario should be credible for the participants and should be strived for [Age15]. FFI suggests that credibility may be achieved through involving the stakeholders in the development of the scenario in addition to having a transparent process of the development. The transparent process will connect the goal and guidelines of the exercise to the developed scenario such that it is concise, coherent, and traceable [MF13]. This approach will also ensure that the scenario is expedient by connecting the goal and the created scenario. For our project, this was done by developing the scenarios together with the industry

by getting information and feedback along the way. Also, one of the interviewees advised against having big and "fancy" scenarios and said that "boring" and realistic scenarios make them more credible, which was wanted in a scenario.

Based on Today's Threat Landscape

To make a realistic scenario, it is essential to base it on something that has a hold in the real world. Basing it on today's threat landscape enables this property and is why we chose to include it as a criterion. To fulfill this criterion, the scenario could be based on threat assessments, previous incidents, risk analyzes, or experiences of earlier exercises, incidents, and situations.

According to NSM and NVE, basing a scenario on threat assessments may help describe a scenario the company considers as a real threat [Aut21c, Lar15]. We, therefore, believe that this could be a wise starting point for the companies. Even if the threat introduced in the threat assessment is considered small, it is still present, and one cannot ignore it or argue that it is unrealistic. In the CRIOP report, the authors mention that basing a scenario on previous situations that have occurred on installations in the North Sea will make the scenarios realistic as the participants know it has happened before [JBS+11]. NVE also suggests basing the scenario on previous incidents. According to NVE, such a scenario should be considered a realistic scenario [Lar15]. Basing the scenario on previous incidents increases the realism as is it proven that it has happened before. Findings from the data collection interviews also show that basing the scenario on previous incidents increases the degree of realism of the scenario. We were advised to use this approach. Both NVE and DigDir also suggest to base the scenarios on risk analyzes [Lar15, Age15]. They further specify that experiences of earlier exercises can be used to adapt required training ahead of the exercise [Lar15, Age15]. The experiences of earlier exercises can also be used to determine areas that should be included in future exercises. Experiences from previous accidents and unwanted incidents may indicate how the company wants a given scenario to be solved and what kind of events they are exposed to.

Adapted to the Operator's Systems and Have Correct Technical Details

The scenario should be adapted to the operator's systems and have the correct technical details to make the scenario realistic and expedient. As the scenario could lose its value by not being adapted to the operator's systems and have correct technical details, we have included it as a criterion. Both information from interviews and the literature highlight this criterion.

In the feedback interviews where we presented the first draft of the scenarios, we received feedback that some scenarios had incorrect technical details, making the scenarios less realistic. According to the interviewees, participants might argue

incorrect technical details instead of the intended discussion areas, which may weaken the outcome of the exercise. In addition, the scenario may be seen as something that is not possible or relevant for their systems because of the wrong details. The authors of the CRIOP report mention the concept of specificity as crucial for scenarios [JBS+11]. This term includes that the scenarios must be specific for the installation which will play out the scenario, and hence must be adapted to the operator's systems [JBS+11]. The exercise may not be expedient if the scenario is not adapted to the exercising company's systems as they do not get to exercise on their own specific systems.

No Potential to Shut Down the Platform

According to findings from the feedback interviews, a cyber security incident that causes a platform to shut down is considered an unlikely incident. The platform systems have many barriers, and a lot of the functionality is located in their own "fire cell" environment. One could argue that a situation causing a platform to shut down is a worst-case scenario that should be included in exercises. However, as such scenarios were discouraged and the operators found such a scenario unrealistic, we recommend avoiding such a scenario for a tabletop exercise. By not having the potential to shut down the platform, we believe the scenario will be perceived more realistic and have included it as a criterion.

Fit the Participants' Knowledge Level

A scenario that does not fit the participants' knowledge level may not be expedient, and is why we have included it as a criterion.

According to the definition of an exercise used by DNV GL, an exercise should develop the organization's ability to handle an incident and to check if the current procedures and plans are suitable for the given purpose [Hål20]. One of the interviewees also stated that the objective of an exercise is to identify gaps in procedures and test what areas are in place and need improvements. Conducting an exercise where the participants do not understand what is going on or how to solve the ongoing problem may not indicate how the participants would solve the problem if it were an actual situation. In addition, the participant may not get a valuable learning outcome. These aspects lead to an exercise that is not expedient.

In addition, if the participants cannot solve the case, they may not feel a sense of empowerment, which is another criterion in the list. Gleason highlights the importance of motivating participants in a tabletop exercise, which will not be met if the scenario is not adapted to the participant's knowledge level [Gle14]. Also, Patrick and Barber address that the exercise should be a positive experience for the participants [PB01], which the scenario may not lead to if not fitted to the participants' knowledge level.

In the petroleum industry, many employees do not have the expertise in cyber security. The companies should hence adapt the developed scenarios for cyber attacks against IACS to meet the employees' competence. One interviewee also highlighted this aspect in the feedback interviews. Adapting the scenarios to meet the competence of the employees may provide a more expedient exercise and should hence be strived to reach.

Unambiguous

To make the scenario as expedient as possible, we have added a criterion on making it unambiguous. If a scenario is interpreted the same way by the participants and not leads to any confusion regarding the content's meaning, it will probably be more expedient for the participants. It ensures that the participants all know what they should discuss. Thus, they may get a better learning outcome for the intended exercise area.

Several interviews highlighted this criterion. One of the interviewees also mentioned that ambiguities might confuse the participants, leading to a misunderstanding of the scenario content. Hence, the scenario would not be expedient. In the first draft of our scenarios, we had added information meant to distract the participants. In the feedback interviews, we were recommended to remove that part as it might lead to ambiguities among the participants. It seems like distractions could be wise to avoid in the scenarios as it may lead to ambiguities unless the author of the scenarios knows their participants well.

Concise

We have chosen to add concise as a criterion as this might increase the expediency of the scenario. Various literature address this criterion.

In the report published by NIST, they address the importance of having concise scenario descriptions [GNB+06]. If a scenario description is too long and detailed, the participants may need more time to interpret and discuss the meaning of the scenario. Using extended time on understanding the meaning of the scenario may take the focus away from the topic of the exercise [GNB+06]. If the focus is taken away from the exercise, it may lead to a less expedient exercise than desired. It is also mentioned by NSM, DigDir and FFI that even if the scenario is short, it should still include sufficient information for the participants to understand the scenario and the input from the playbook [Aut21b, Age15, MF13]. Hence, a concise scenario that both are short and precise may increase the expediency of the scenario.

Consistent

We have added consistent as a criterion as it will increase the realism of a scenario. NSM and van der Merwe address the need for a consistent scenario description [Aut21b, VdM08]. If something happens in one place of the scenario, it must not eliminate something mentioned later in the description from happening [Aut21b]. If two events happen in a scenario and do not correlate naturally, the participants might question the scenario. If the scenario described is not consistent, the participants may interpret it as unrealistic and not plausible.

Hazard Potential

Scenarios should have a hazard potential to be evaluated as expedient. Because of this, we have added it as a criterion to our list.

The authors of the CRIOP report mention hazard potential explicitly as a criterion for scenarios [JBS+11]. Focusing on situations that will affect the company will also allow the participants to prepare themselves for such incidents. Also, the participants may see such situations as more important as the consequences might be more extensive. If exercising on situations that do not have the potential of causing any damage, it may not be as valuable or expedient. The scenario and exercise should give a valuable learning outcome for the exercising company and participants. Hence, they should exercise on larger, more advanced incidents and situations.

Define Targeted Assets

Targeted assets and how they are affected should be defined in the scenario to increase the scenario's expediency. Both the direct and indirect assets that are affected by the attack should be included, and it should also be explained how the targeted assets are affected according to NSM and DSB [Aut21b, fCP16]. This will increase the scenario's expediency as it appears clear what the intention of the scenario is. Thus, it is easier for the participants to exercise correctly and get a valuable learning outcome. This argumentation is the essence of why we have included this criterion in our list.

Presented in Multiple Parts Where Appropriate

To make the exercise feel more realistic, the scenario description can be divided into multiple parts. FFI addresses that when splitting a larger scenario into smaller parts, it will be possible for the participants to focus on specific tasks or threats presented [MF13]. This criterion may be expedient if the participants should discuss several tasks or threats during a tabletop exercise. NVE is also stating that it will be expedient to present more extensive exercises in several parts and have inputs from the playbook, which again will require the scenario to be more complex [Lar15]. A

scenario presented this way may increase the realism and expediency of the exercise, and the participants may get a feeling of how an actual incident would have progressed. Hence, we have included it as a criterion in our list.

Includes the Source of Attack and How It Was Detected

We have included this criterion as we believe it contributes to participants exercising on intended areas and makes the scenario more realistic. This criterion was a suggestion from an interviewee, indicating that it is also valuable for the industry.

By including the attack source and how it was detected, the participants will get sufficient information to understand the scenario and discuss the intended areas. If this information is left out, there could be blanks in the scenario that the participants have to interpret themselves. This interpretation could lead to different participants taking the exercise in various directions. Naturally, the participants interpret the information slightly differently. Still, the scenario creators should ensure that the participants could not interpret the theme and essential information so differently that it affects the exercise's expediency. Also, if this information is lacking, the scenario could be ambiguous. An ambiguous scenario could steal time from the exercise. All aspects above could contribute to making the scenario less expedient. Therefore, one should include the attack source and how it was detected to make the scenario expedient.

Also, adding this information to the scenario may increase the realism of it. By explaining how the attack originated and was detected, the participants may accept that it could happen, hence find it realistic. In addition, this information shows the scenario is thought through such that all aspects in the scenario are connected. This aspect may also increase the realism of the scenario.

No Defined End

We have included this criterion in our list as we believe it will make the scenarios more realistic. Findings from an interview with one of the operator companies suggested that the scenario descriptions should not have a defined end. When discussing the scenario during an exercise, the decisions made by the participants should define the outcome of the incident. By not adding a defined end to the scenarios, it may make the scenario feel more realistic, as the end will depend on the actions taken by the participants.

All Participants Can Contribute

This criterion is added as we believe it will make the scenarios more expedient for the participants using it in an exercise. In a tabletop exercise where all participants discuss

the same scenario, all present participants must get a valuable learning outcome from the exercise. Patrick and Barber address in *Tabletop Exercises - Preparing Through Play* that such exercises should allow for meaningful participation by all participants [PB01]. Results from our interviews support this opinion. This finding requires that the scenario also is adapted to involve all participants and make them contribute. The expediency of the scenario will increase along with the participation of all involved participants. According to NVE, there is no purpose in having sections of the scenario where only one group of the participants can contribute [Lar15]. Only having one group contributing may lead to other participants seeing the exercise as meaningless and irrelevant, and the exercise could lose its potential [Lar15]. If some participants cannot contribute, the scenario and exercise will not be expedient, as they might not get a valuable learning outcome.

Trigger Discussion and Cooperation

As the scenarios are meant to be used in tabletop exercises, where discussion is the main element, the scenario should enable discussion and cooperation. This criterion is supported by findings from DSB and findings during our interviews [fCP16]. If this criterion is not met, it could lead to the scenario and exercise being unsuccessful and hence not expedient. Making people cooperate is essential for both technical and procedure-oriented exercises. Cooperation should therefore be a criterion independent of the focus and purpose of the scenario and exercise.

Challenging

For the scenario to give a valuable learning outcome and hence be expedient, it needs to challenge the participants. Thus, we have included a criterion on this aspect. DSB, NVE, and van der Merwe state in their literature that the exercise should challenge the participants and the current assumptions about the company [fCP16, Lar15, VdM08]. For the exercise to challenge the participants, the scenario needs to do so as well. Using a scenario that challenges the participants may make the exercise more expedient. Actual incidents would most probably challenge the participants and the exercising organization, so they need to exercise such challenging situations. A scenario that does not challenge the participants may also not give a valuable learning outcome. The participants may already know how to handle the situation described, and they might, therefore, find the scenario and exercise trivial.

Creates a Sense of Empowerment

We have added this criterion as we believe that the scenario may become more expedient by fulfilling it. According to Patrick and Barber, creating a sense of empowerment for the participants will ensure that it is a positive experience and provides a solid learning outcome and training value for both the participants and the

exercising company [PB01]. In other words, this will make the scenario and tabletop exercise expedient. Also, NVE and Gleason highlight the importance of motivating the employees by using a scenario and exercise which gives them the experience of mastery [Lar15, Gle14]. If the participants do not feel a sense of empowerment, they might lose interest in the exercise and not see the value of conducting it.

Not Known to the Participants in Advance

Based on an experience from one interviewee where one of the participants of an exercise knew the scenario description in advance, the interviewee recommended we add this criterion. Based on this recommendation and the fact that the criterion might make the scenario more realistic and expedient, we included this criterion.

DSB states that concrete dilemmas and problem descriptions can be kept secret for the participants until the exercise starts [fCP16]. Most real-life situations occur unannounced, and exercising on a situation that one is not prepared for may increase the realism of the exercise. If a participant knows the scenario former to the exercise, the evaluation of the exercise may not reflect how the situation would have been handled if it was an actual incident. The evaluation of the exercise may thus not reflect what areas need improvement. It may also be difficult to measure if the goal and purpose of the exercise were met.

To summarize, if the scenario is known to the participants in advance, it may make the scenario less expedient. On the other hand, DSB suggests that it may be an advantage if the participants can make necessary preparations ahead of the exercise [fCP16]. Because of this, we suggest keeping the scenario description secret former to the exercise. However, we recommend informing the participants about the exercise topic.

Fulfills the Exercise's Purpose, Goal, Form, and Scope

We have included this criterion in the list as it makes the scenario more expedient by leading to an exercise where the company gets to exercise on what they intend to. Three sources of literature and findings from the interviews also state that this criterion, or parts of the criterion, should be considered when developing scenarios.

Before developing the scenario, the exercise's purpose, goal, form, and scope are usually set. Purpose tells why the exercise is conducted, e.g., raise awareness around the fact that situations that look like technical faults may be caused by cyber attacks, while the goal states the intended outcome of the exercise. An example of a goal could be to have raised the participants' awareness that cyber attacks may cause technical faults. As these aspects are slightly different, we have decided to include both of them in the criterion. The form of the exercise is added because scenarios may

deviate according to what form of exercise should be used. The scope of the exercise will impact the scenario size and complexity. A more extensive scope will require a larger or more complex scenario. When developing the scenario, one should ensure that the scenario fulfills the aspects set in the criterion. This fulfillment ensures that the exercise will exercise what it intends, as the scenario is made specifically for the planned exercise.

NVE and DSB mention that the scenario must be adjusted to fit with the goals set for the exercise [Lar15, fCP16], while DigDir addresses that the scope and length of the scenario should reflect the goal, research usage, and purpose of the exercise [Age15]. Also, in the interviews conducted for this study, we received feedback that a purpose should be set before developing the scenario. The scenario should also correlate with this purpose at the end of the development.

Relevant Plans Are Available

In one of the validation interviews, an interviewee suggested adding this criterion to our list. By having relevant plans available, the participants do not have to spend valuable time finding these during the exercise. The plans and procedures may be included in the prerequisites given for the scenario. As we include prerequisites for our scenarios, this criterion will be relevant to include in the criteria. Having full focus on the scenario and discussion and avoiding distractions may give the participants a more valuable learning outcome. Based on this, the criterion could make the scenario more expedient and help it reach its full potential. One could argue that locating the relevant plans could be a part of the exercise and that an exercise can be used to discover lacking plans and procedures. However, the focus of a tabletop exercise should be given to the discussion of the scenario. Besides, the exercise may still discover lacking plans and procedures.

5.1.2 List of Criteria for a Scenario Collection

In the following paragraphs, we will elaborate on why and how our criteria for a scenario collection ensure the collection to be expedient. Some of the criteria in this list are directed towards the overall content of a scenario collection, whereas other criteria are directed towards each scenario to be included in a scenario collection.

Scalable

When creating scenarios for a scenario collection, the scenario must be scalable. Having scalable scenarios would increase the expediency of the collection and should hence be included as a criterion.

During an interview, one of the operators addressed the importance of having scalable scenarios that are easy to make as small or big as desired. A scalable scenario will be easier to adjust to the purpose, goal, form, and scope of the exercise. Hence, it will be easier for an operator to find a scenario that fulfills the desired outcome of the exercise. We chose to have this criterion in this list, as this is a criterion for scenarios in a scenario collection. However, when developing a scenario for a specific exercise, the scenario should fulfill the exercise's desired outcome and should thus not be scalable.

Adaptable

Also, when developing scenarios for a scenario collection, the scenarios should be easy to adapt for different actors. If they are not easy to adjust, it will be challenging to use them, and fewer actors may use the scenarios from the collection. These aspects would make the scenario collection less expedient. Thus, adaptable should be included as a criterion on how to make a scenario collection more expedient.

Different actors have different needs, and some adjustments are necessary for the actors to take the scenarios into use. The scenarios should hence facilitate this. DigDir addresses in their report that when choosing a scenario from an external scenario collection, it will need adjustments according to the specific exercise's purpose, goal, form, and scope [Age15]. Also, the scenarios' relevance, scope, and purpose should be considered by the actors when choosing from a collection. The actors should then compare the findings with their intended exercise [Age15]. Results from our interviews address the difficulties of adapting scenarios, and we were encouraged to add an exercise plan to our scenarios. The findings confirm that the adaption of a scenario could be difficult. Therefore, it should be strived to make scenarios in a scenario collection as easy to adapt as possible for the collection to be expedient.

Both Width and Depth

In a scenario collection, there should be a variation in scenarios targeting width and depth. Some users of the collection might want to exercise on more technical and deeper aspects, thus needing a deeper scenario. Other users might want to exercise on broader topics like procedures and then need a wider scenario. By having both types in a scenario collection, the collection will target a broader range of actors. Hence, the collection will be more expedient. The authors of the CRIOP report also highlight this criterion [JBS+11].

Variation in Content

The content of the scenarios should be varied for the collection to be as expedient as possible. Findings from the feedback interviews confirm that a variation in content is

valued and that it is an area that should be strived for in a scenario collection. The authors of the CRIOP report also highlight this criterion in their report [JBS+11]. Different actors could find the scenario that suits best for a particular exercise by having a variation in content. Thus, this increase the expediency of the scenario collection and should be a criterion. As we have added scalable and adaptable criteria in the list, they ensure that the individual scenarios could be varied. Hence, slight variations are already included in the collection.

Variation in Complexity

Also, the scenario's complexity should be varied to increase the expediency of a scenario collection. Both findings from the interviews and literature from NVE state that some of the scenarios should be complex while others should be less complex [Lar15]. This diversity will help meet different companies' needs. As with the two previous criteria, this criterion may ensure a wider group of users for the scenario collection as well, which is expedient.

Enables Procedure and Technical Exercises

Findings from the interviews show that the interviewees have a clear distinction between procedure and technical exercises. Some wanted us to make scenarios that gave technical exercises, while others preferably wanted scenarios to use in procedure exercises. The interviewees suggested a diversity regarding these different types of scenarios. In addition, scenarios adaptable for both kinds of exercises could also be favorable. Based on this diversion in needs for different actors, a scenario collection should include various scenarios that enable all these types of exercises. This will increase the expediency of the scenario collection.

At Least One Scenario Involving Emergency Preparedness

In a scenario collection, there should be at least one scenario involving emergency preparedness as it increases the expediency of the scenario collection. The authors of CRIOP highlight this criterion in the report[JBS+11]. Results from the interviews show that some of the interviewees wanted to have scenarios only for the emergency organization, some only for the first-line personnel, and others wanted scenarios for both. Having one scenario involving emergency preparedness in the collection allows the companies to exercise and prepare for situations that need emergency preparedness. Even if the emergency organization is exercised more often than the first-line personnel, they do have an invaluable role when larger incidents happen. Also, the criterion with hazard potential shows that at least one scenario should involve emergency preparedness for the collection to be more expedient. A scenario with large hazard potential would typically require emergency preparedness to be

set. Based on the above argumentation we find it valuable to include this criterion in our list.

5.2 Realistic and Expedient Scenarios

To answer RQ 1 which asks, "what are expedient and realistic scenarios for tabletop exercises related to cyber attacks against IACS in the petroleum industry?", we will justify our example scenarios in this section. Together with the justification of the lists of criteria in Sect. 5.1, this will answer our research question. Our example collection will be justified by first elaborating how the setup of our scenarios makes them realistic and expedient before the eight scenarios are justified in detail. In this justification, we will explain why we chose exactly those themes and the structure of the scenarios for them to be realistic and expedient for the industry.

5.2.1 Scenario Template

During our data collection interviews, we received feedback that a solid scenario description would not be sufficient to ensure that a scenario gives a realistic and expedient exercise. The interviewees desired to have additional information to help the industry adapting the scenario and ensuring that it is realistic and expedient. This additional information could mainly be seen as input to an exercise plan. We also received suggestions on adding a suggested purpose of the exercise, recommended participants, and examples of relevant questions to ask during the exercise to our scenarios. Based on the feedback received in these interviews and our perceptions, we chose to add a purpose section, a backdrop section, a justification section, and an exercise plan in addition to the scenario description. We will further justify all areas and explain how they contribute to making our example scenarios realistic and expedient.

Findings from the interviews and the report from DigDir suggest deciding and clarifying the purpose of the exercise before developing the scenario [Age15]. Further, the purpose must correspond with all phases of the scenario. Hence, it will be expedient to present some example purposes before presenting the scenario description to help the industry decide if their intended purpose with a given exercise will correspond with a scenario from our scenario collection. We have also chosen to split the purpose section in two, procedure and technical, to help the actors find purposes that best fit their intentions. We believe that this makes the scenario more expedient.

We have added a backdrop section for some scenarios to give additional information to the participants before the exercise starts. This information should lead the

participants in the right direction of the content of the scenario, which may lead to a more expedient exercise and then make the scenario more expedient.

We have decided to split most of the scenario descriptions into different parts to increase the expediency and realism of the scenario. This approach is suggested by both FFI and NVE [MF13, Lar15]. Seven out of eight scenarios are divided into several parts, which will be presented sequentially during an exercise. Each part of the scenario will provide more information, simulating the development of a real incident. Structuring the scenarios in such a way may ensure a degree of realism and expediency as it coincides with reality. The scenario regarding IIoT is considered too small to split up, and it would therefore not be expedient to divide it into multiple parts.

A justification section is added to the scenarios to increase the realism. The justification can refer to other similar attacks or incidents that show the actors using the scenarios that the events are rooted in the real world. It can also explain why the aspects of the scenario are essential to exercise on, which may increase the realism and the experience of expediency of the scenario. This section is a section we have decided to add by ourselves without any input. Despite this, we have received information from the interviewees that it is valuable. We, therefore, choose to keep it for our final delivery.

For the exercise plan attached to the different scenarios, we have decided to include several aspects to help the actors adapt our scenarios and exploit the full potential of the scenario. This way, when we present realistic and expedient scenarios, there is a greater probability that these properties are ensured when applied to a tabletop exercise. The time duration gives the participants an indication of the intended range of the scenario. This specification could help the organizations choose a scenario from the collection that fits their resources and needs. Prerequisites are added for the exercising organization to have the opportunity to fulfill them before the exercise and then get a more expedient exercise. Suppose the prerequisites are not fulfilled, e.g., training of employees on system restore. In that case, the scenario and exercise may meet challenges when discussing system restore. The participant section was a suggestion we received from the interviews. An interviewee highlighted that the exercise could be more valuable and expedient for all of them by having the right competence among the participants. Based on this, we have suggested different participants to include in each scenario.

We have added example questions for the exercising organization to see what types of discussions can be retrieved from the scenario and help them use the full depth of the scenario. The industry also suggested this section through interviews. We have further decided to structure the questions to fit with the different parts of

the scenario. Then, it should be easier for the facilitator to find the relevant questions during an exercise. The various parts of the example questions are further divided into procedure questions and technical questions, as suggested by two interviewees. This further division helps the exercising organization find the relevant questions for them. This structure may increase the expediency of the scenario and exercise. After all the different parts of questions are presented, we chose to add a section called "discussion and reflection." The questions raised here intend to allow the participants to reflect upon the scenario at the end of the exercise. Here, they could discuss how such situations could be avoided or better handled. In one of our feedback interviews, two interviewees advised us to direct these questions to the exercise management instead. The interviewees had experiences with participants not knowing such types of questions. We have chosen to keep this section with questions for the participants as we believe it will be an opportunity for them to reflect and get a better learning outcome of the exercise.

We chose to add a variations section to the exercise plan to allow the companies to use the scenario as a base and exercise on different things with the same scenario, but with slight modifications. The companies can use this section to adjust the scenario to be more expedient and realistic. The last area in the exercise plan contains suggestions to the playbook. We have included this section to give information to the facilitator of an exercise. This information could be to provide a more detailed description of events in the scenario. The section could also give explanations that can be used to make the scenario more realistic for the participants during an exercise if the facilitator finds it necessary.

5.2.2 Scenario Collection

During the interviews and literature review, we obtained general information and feedback regarding scenarios to be realistic and expedient, which we included in our scenarios. We will, in this subsection, present this general information before we justify our developed scenarios in detail. When developing our scenarios, we sought to fulfil all the criteria in the lists of criteria presented in Sect. 4.3.1 and 4.3.2. When validating our scenarios, we received feedback that there was compliance between our criteria and example scenarios.

General

After conducting the data collection interviews, we received feedback that it was desired to include practical tasks in tabletop exercises. When working on the thesis, we saw that to include practical tasks in a scenario, we needed more in-depth knowledge of the systems. As there are variations in the systems between each operator, it is not easy to create scenario descriptions, including practical tasks that are seen as realistic and expedient across the different operators. We, therefore,

decided only to focus our scenarios on tabletop exercises without practical tasks. It will hence be up to the operators to adjust the scenario also to fit practical tasks.

We have focused on developing our scenarios in a way that fits the knowledge of the first-line personnel. Findings from the interviews show that the interviewees think the first-line personnel is the ones that should be focused on in exercises directed towards IACS and cyber attacks. As cyber attacks often require a quick response, the first-line personnel should know how to quickly and precisely respond to future incidents. As the first-line personnel, including the control room operators, may not possess expertise in cyber security, the scenarios are developed to be easy to understand by all participants such that they become more expedient.

We were recommended not always to assume that the scenario should start with an attack being discovered. Other recommended approaches were to have actors observing something abnormal or suspicious. This approach may make the scenarios more realistic, as it often is uncertain whether one is under an attack or not. Abnormal actions suggested were slow updates, strange values, or something that indicated that an unauthorized user was present in the systems. We have considered this recommendation and chose to base most of our scenarios on it. Our scenarios often start by observing something abnormal, and then the scenario escalates further.

For the participants included in the exercise plan, we have chosen to include the platform management, control room operators, and IT experts for most of the scenarios. We received feedback in interviews that these groups were expedient to add to the suggested participants. The platform management should often be included for scenarios with a more significant hazard potential. Control room operators should be included as the scenario usually starts in the control room, or they are central in the scenario and should hence be exercised. As the developed example scenarios are focusing on a cyber attack, it would be natural and expedient to include IT experts in the participant list. In addition, we have included liaisons to ease the communication with different actors where needed. Liaisons were suggested to add as some of the scenarios could require communication with government authorities, PSA, the police, or others. It would then be expedient to include liaisons from the respective disciplines for the specific scenarios.

For the prerequisites, we chose to add requisites about training. More specifically, we added training on system restore and log analysis to the exercise plan for most scenarios. Adding this training ensures that the participants know how to perform such actions, specifically in technical tabletop exercises. If those prerequisites are met, the scenario will give a more expedient exercise. Thus, the participants can discuss the intended topic with a given scenario, and one may avoid the pitfall of having an exercise resulting in a training session.

We want our scenario collection to be used by several operators, and we have therefore chosen not to include too technical details in our scenarios. The technical details may vary from operator to operator, and for our scenarios, they should not be too technical. This may make our scenario collection more adaptable, which again may make it more expedient.

Scenario 1 - Ransomware

For the first scenario, we decided to make it a ransomware attack. Ransomware seems to be the top threat for the petroleum industry. During the data collection interviews, all interviewees highlighted ransomware as one of their most feared threats. The ransomware attack on Hydro, which encrypted their IT systems in 2019 [Bri19], and other ransomware attacks such as Petya and the Colonial Pipeline attack, may have led the petroleum industry to realize that this could also happen to them and lead to severe costs. Especially, the attack against Colonial Pipeline confirmed that critical infrastructure also could be victims of ransomware attacks.

Threat assessments from NSM, Europol, mnemonic, and Telenor highlights ransomware as a dominant threat in the threat landscape for Norway and Europe [Aut21c, Eur20, mA21, Nor20]. Waterfall Security Solutions dedicates three places in their "Top 20 Cyber Attacks On Industrial Control Systems" to ransomware, evolving from common to targeted, and then a zero-day ransomware [Gin20]. The NotPetya malware, described in Sect 2.4.1, also shows that malware could hide as ransomware and cause even more significant damage and severe financial loss. This type of attack can also be used as a motivation to exercise on ransomware attacks, as one can never be sure that data is regained if the ransom is paid. All aspects addressed above show that ransomware indeed is a threat that needs to be taken seriously for all industries, also industries using IACS.

mnemonic's observation of changes in the dark web, where APTs sell access and foothold on various targets to the highest bidder, is also relevant for this scenario. Ransomware-as-a-service is now a service being provided on the dark web. This service enables less sophisticated threat actors to compromise their targets, making such a scenario more realistic [mA21].

Europol, mnemonic, and Telenor highlight in their threat assessments that ransomware attacks are evolving and now often consist of two phases [Eur20, mA21, Nor20]. The first phase is encrypting and locking all systems down, while in the second phase, the attackers threaten to leak stolen, sensitive data or shut down critical services. We have chosen to escalate our scenario by adding a threat of shutting down a critical service for an offshore platform, namely the main generator. Choosing to use this generator to threaten the operators instead of sensitive data will make the scenario more realistic as this is a top asset the industry wants to

protect. We also received feedback from the industry on using a shutdown of the main generator instead of leaking sensitive data for the scenario to be more realistic.

As an entrance for ransomware, we chose to use a phishing attack. This choice was based on findings from the interviews as well as the literature review. Phishing is highlighted by several interviewees in addition to a specification of the fact the incidents targeting IACS nowadays often start in the IT network and spreads to IACS. Also, NSM's threat assessment states that phishing attacks still often succeed and that the use of e-mail as an entrance still works [Aut21c]. As our choice of phishing is based on the current threat landscape, it makes our choice realistic and hence the scenario more realistic.

In our example questions, we have included a question of whether the ransom should be paid or not. During the interviews, the interviewees told us that one should not pay the ransom regardless. Despite this, we wanted to include a question discussing the options as it is known that some companies are paying the ransom. Colonial Pipeline is one company which have paid a ransom [SW21], which increases the expediency and realism of including this question.

Based on the above argumentation, this scenario is realistic. As it is a highlighted threat, and it may be realizable, the scenario is expedient to exercise. Exercising on this scenario will lead to a valuable learning outcome as this is knowledge which they need to have if such an incident should occur.

During validation of the scenarios, we received a suggestion on how to make the scenario even more realistic. The interviewee suggested that we changed the message informing about ransomware to a pop-up window instead of showing it in a text field in an alarm list. In previous interviews, we have received feedback that the message should be displayed in an alarm list instead of a pop-up window as that was more realistic. The feedback received from different interviews shows that the operators disagree on what is more realistic. Also, in the ransomware attack against Colonial Pipelines, it is perceived that the attack was discovered in a less dramatic note displayed on a control room computer [EV21]. Based on the suggestions from the interviewees and information about the Colonial Pipeline attack, we chose to remain with the alarm list. We encourage actors who are using the scenario to adapt this detail to what they find more realistic.

Scenario 2 - Attack with USB Stick Enabling 4G

The second scenario revolves around an attack where a 4G dongle USB stick is inserted into one of the switches in the telecommunication room. A 4G dongle may enable an attacker to connect to other internal networks of the system where it is plugged in. Interviewees told us that 4G and 5G now are present on some offshore

platforms enabling such an attack and making it realistic. The interviewees told us that this was a threat they had discussed internally in the company, contributing to increasing the realism of the theme for this scenario. App. B shows a map of the coverage area of Tampnet, which ensures offshore 4G connection, and the oil and gas fields on the Norwegian continental shelf. Also, this map contributes to give realism to the subject of the 4G connection on offshore platforms.

Further, the scenario implies that an insider did the job of inserting the 4G dongle. Insider threats are highlighted in the threat assessments from mnemonic and NSM as possible threats for 2021 [mA21, Aut21c]. mnemonic addresses that the risk of an insider is notably high for companies and industries with critical assets [mA21]. As the petroleum industry holds critical assets, this may increase the risk of an insider attack for them. In addition, the report from Waterfall Security Solutions gives three places of their top 20 cyber attacks against IACS to insider-attacks [Gin20]. The provided implementation of these insider attacks deviates somehow from our implementation, but the theme of the attacks contributes to making the scenario on insiders more realistic. PST and Telenor also addresses that foreign intelligence is willing to recruit sources to get information on persons and businesses in Norway and that this recruiting is increasing [Ser20b, Nor20]. In their report on the threat of intelligence against the Norwegian petroleum sector, PST also addresses that personnel working in the Norwegian petroleum sector could be approached and tried recruited by foreign intelligence [Ser20a] which gives realism to the focus on insider attacks.

Also, findings from the interviews tell us that the interviewees see insiders, both intentional and unintentional, as a threat. The interviewees told us that they feared external actors forcing or tricking employees into doing simple jobs for them, such as inserting a USB stick into a computer. According to the interviewees, employees in difficult financial situations (e.g., high gambling debt) can be willing to take inside missions for outsiders who want to sabotage an organization or retrieve some information. The risk of being caught is low, and the attack is challenging to discover, which makes the attack even more relevant in today's industry.

Further, it was stated in the interviews that there often is a lack of physical security on an offshore platform, and unlocked doors were used as an example. Lack of physical security will make it easier for an attacker to insert a USB stick. Based on the above argumentation, we believe that a scenario using 4G for an insider attack would be a realistic and expedient scenario for the petroleum industry.

In part one of the scenario, the event presented may be perceived as a technical fault, which is our intention. Findings from the interviews inferred that a cyber incident often is not considered when something that looks like a technical fault

occurs. This finding makes a scenario targeting this area expedient to use in exercises and is why we chose to add it to our scenario collection.

In the validation interviews, we received feedback from one operator that the 4G dongle should be inserted into a server or an engineering workstation instead. From previous interviews, we have received feedback that we should use a switch instead of a server. Based on this feedback, we have decided to keep the switch in the scenario and encourage the scenario users to adapt it to the technology that fits them the best.

Scenario 3 - Supply Chain Attack with Information Gathering

To succeed with an attack, it is crucial to have enough information about the targeted systems to cause as much harm, economically or materially, as desired. One way to get into the targeted system of an operator is through a supplier.

During the interviews, one operator told us that stealing or leaking information is not crucial for the oil and gas industry. Despite this, we want to enlighten that stolen information not only can be used as a means of pressure, it can also be used to plan a more significant and severe attack. Dragos states in their threat assessment that reconnaissance activity is being performed against oil and gas companies in Europe [Dra19]. PST elaborates that this reconnaissance might lead to network operations which again might lead to sabotage actions against the Norwegian petroleum sector [Ser20a]. These findings substantiate the importance of exercising in situations that might not have escalated to an attack yet.

According to NSM, attacks targeting supply chains are an increasing risk [Aut21c]. Telenor and mnemonic are also focusing on supply chain attacks in their threat assessments [Nor20, mA21], bringing supply chains into today's threat landscape. Waterfall Security Solutions includes a supply chain attack in their list of cyber attacks [Gin20]. Even though that attack is directed against hardware, it still shows the relevance of exercising supply chain attacks when talking about cyber attacks against IACS. Also, attacks via suppliers, where suppliers are used as attack vectors to gain access to the operator, were mentioned as threats during the interviews. Based on this, the scenario should be considered as a realistic scenario. Both of the operators reckoned the scenario as realistic during validation.

Attacks such as SolarWinds and Stuxnet have been used as inspiration for this scenario. Both are extensive attacks, and they show that attackers can perform much harm as long as they have enough time and resources. Threat actors that often may perform such extensive attacks, APTs, are addressed in threat assessments from Telenor, NSM, Dragos, and PST as actors that are an increasing risk in today's

threat landscape [Nor20, Aut21c, Dra19, Ser20b]. These are also elements that make this scenario realistic and expedient to exercise.

We have chosen to add suppliers to the list of suggested participants for this scenario. One interviewee in the feedback interviews advised us not to include suppliers in the list as the interviewee meant it should be a part of the exercise to contact the suppliers if needed. However, as this scenario focuses on a supply chain attack, we believe it is expedient to include them as participants from the beginning.

When validating this scenario, one of the operators evaluated the scenario as partly realistic. We were recommended to change part two of the scenario to increase the realism. We got feedback that the wording "seems like" contributed to the scenario being perceived as unrealistic, as these types of situations usually have more binary reactions. We toned down the description but kept the wording "seems like," as one can never fully understand what is happening in such a situation. As it is challenging to know the extent of such an attack, we chose to keep most of part two as it was. The operator evaluating the scenario as partly realistic also stated that the scenario could be realistic if the scenario had a short time perspective, for instance, 30 minutes. We, therefore, recommend users of this scenario to give it a time perspective they find realistic.

As supply chain attacks are highlighted in several threat assessments, and specifically for the petroleum industry in the report from Dragos [Aut21c, mA21, Nor20, Dra19], such scenario should be considered to give an expedient exercise. Both of the interviewees interviewed for validation evaluated the scenario to be expedient.

Scenario 4 - Disconnection of Detectors

Findings from the interviews inspired this scenario. One of the interviewees had one experience from when working as a technician for a supplier company. The situation that occurred made the interviewee question what it takes for the control room operators to suspect that technical faults may result from a cyber attack. The interviewee's impression was that a cyber attack is often not considered when something abnormal happens in the control systems. This focus could give the attackers additional time to perform their attack if a cyber attack was in progress. Therefore, we decided to make a scenario on the topic, as it seems to be an area that requires more focus. The situation that led to this scenario is described in detail in Sect. 4.2.3.

Because the scenario is based on a actual incident, the situation described should be considered realistic. We have chosen to let out technical details and the attack source because of variation in the systems among the possible users of these scenarios.

Therefore, users of this scenario should add the information they find necessary to make the scenario even more realistic and suitable to their exercise.

When validating the scenario, one operator recommended we added a third part to the scenario to clarify what type of attack they were facing. This part would also explain that the scenario is not about a technical fault but a cyber attack, and we chose to follow this recommendation. We did not conduct a new validation of the scenario after making the change. Still, we believe that it is reasonable to assume that it would have been validated as realistic in another round.

Because the gas detectors are crucial to the safety of the personnel offshore, it may be expedient to have such a scenario to increase the awareness that technical faults may result from a cyber attack. Gas detectors are a part of SIS, which the TRITON attack in 2017 was targeting in the Middle East. This attack shows the relevance of having such detectors in scenarios for cyber attacks against IACS. Both of the interviewees also reckoned the scenario as expedient.

Scenario 5 - IACS Insider Attack

Insider attacks are mentioned in several of the threat assessments presented in Chap. 2, Sect. 2.4.2, the interviews, and it was also mentioned in the justification of scenario two "Attack with USB Stick Enabling 4G". Using insiders to get access to critical systems may be an "easy" entrance for threat actors, and the scenario described should therefore be considered realistic.

During validation, one interviewee recommended we specified what port the unusual network traffic was going through. We chose not to specify whether it was a physical switch port or logical port as the scenario may be valid for both physical and logical ports. Findings from the interviews suggest that incorrect technical details may distract the participants and steal the focus from the exercise. Specifying on which port the traffic was discovered may distract the participants if the technicalities are wrong and steal the focus from the exercise. When using this scenario, the users must specify the port that makes the scenario realistic for the exercising company.

One respondent from the feedback interviews questioned the part of the scenario on how to handle the insider. The questioning was based on the fact that our scenarios intend to focus on cyber attacks and not personnel responsibility. To make the scenario close to an actual situation, we chose not to remove these parts of the scenarios. We believe that the scenario would feel more realistic for the participants if we include them. Therefore, the scenario is described as close to what would have been the natural development of such an incident. This natural development includes how they would have handled an insider. When using the scenario in an exercise, it is up to the organizations to determine which parts they need to include to reach

the goal and purpose of their exercise. Including all parts of the scenario will give a more complex exercise and should also be taken into consideration.

As insider attacks are highlighted as a likely threat, having exercises that include this threat is expedient. Both operators considered the scenario as expedient during the validation interview.

Scenario 6 - Industrial Internet of Things (IIoT)

Findings from the interviews show that the industry wants to take more usage of the cloud and that there is an increase in the use of IIoT in the industry. NSM also supports this finding by mentioning that sensors and other smart systems are being used to a greater extent in Norwegian businesses [Aut21c]. There are both efficiency and economic benefits of using IIoT. They allow for quick access to the data and eases monitoring of various operations [Aut21c]. The interest of IIoT in the petroleum industry and other industries contributes to increasing the realism for this scenario.

Despite the advantages of using IoT and IIoT devices, the usage of sensors is to a small extent regulated. NSM highlights that there is a risk that large amounts of information will be accessible for threat actors if using these systems [Aut21c]. In the Waterfall report presented in Sect. 2.4.2, they mention using an IIoT pivot attack to get an entry to IT and IACS networks of the target [Gin20]. We have described a less complex incident for our scenario, where the attacker can change the data sent from the sensors to onshore personnel, leading them to make decisions based on false information. As we have based our scenario on threat assessments, we find the scenario realistic. One operator validating the scenario confirmed that it was realistic, while the other operator could not validate it as realistic due to a lack of competence in that area. The first operator also stated that it was narrow and suggested to use the scenario in combination with another scenario in the collection and that it was well suited for a reflection of the topic.

As mentioned in the introduction of this section, this scenario is the only scenario in the collection that is not separated into multiple parts. We chose not to split this scenario as the first paragraph of the scenario does not indicate that the data have been tampered with. Data can change from day to day, and many factors could cause a change in the values as described in the scenario. The scenario is meant to be used as reflection and to raise awareness of how IIoT-devices could be used as an attack vector. It may also be used to verify whether the routines for verifying if data values from IIoT-devices are in place. Based on this, we believe presenting this scenario in one part makes the scenario more expedient.

We included a prerequisite stating that a threat and vulnerability analysis for

the IIoT-devices had been conducted. This analysis may be a topic for discussion during such a reflective tabletop exercise. Discussing the company's vulnerabilities and threats regarding IIoT-devices could make the exercise, using this scenario, more expedient.

Scenario 7 - Access to IACS via Remote Support

As remote access is being used to a greater extent, allowing maintenance personnel, suppliers, or onshore technicians to quickly access the systems offshore, we wanted to create a scenario on this topic. Remote access can be helpful in situations where support from technicians onshore or suppliers is needed. With remote access to the systems, the technician from the operator or supplier can fix the problem without traveling to the platform. This feature saves both time and resources. Two-factor authentication is often used to secure remote access. Waterfall Security Solutions lists two-factor hijacking as one of the cyber attacks they find most relevant today for industries using IACS [Gin20]. As two-factor hijacking is highlighted as a threat against sectors using IACS, it contributes to increasing the realism of our scenario.

For this scenario, we have also chosen to structure it as a supply chain attack. We believe this makes the scenario realistic on the same basis as the justification of scenario three, "Supply Chain Attack with Information Gathering." Supply chain attacks are highlighted in several threat assessments and interviews, making this kind of attack actual and realistic.

During the interviews, phishing attacks were highlighted as a current threat. Also, Telenor, Europol, NSM and mnemonic, all mentions social engineering and phishing attacks in their threat assessments [Nor20, Eur20, Aut21c, mA21]. As the systems are more secure and harder to bypass, people are considered the weakest link. The Waterfall report also suggests using a phishing attack as a starting point for the two-factor hijacking attack [Gin20]. Based on these findings, we chose phishing as the entrance method for our scenario. By luring the supplier to open an e-mail attachment, the attacker gains control over the supplier's computer. As operators see phishing attacks as a threat and the threat is highlighted in several threat assessments, this part of the scenario should be considered realistic.

In the oil and gas industry, they often exercise on incidents where things must happen quickly, and one of the interviewees highlighted the usage of the wording "urgently" as satisfying. During the validation, the interviewee was, on the other hand, unsure whether this type of hijacking was possible in their systems. The interviewee had seen examples of two-factor hijacking in other sectors but would not validate the scenario as realistic for the oil and gas industry. The other interviewee, however, validated the scenario as realistic for the industry.

In the feedback interviews, both of the interviewees validated the scenario as expedient. One interviewee found it a particular technical scenario that could be used to raise awareness among the employees, hence be expedient for a technical group of people. The other interviewee said that this scenario described a case they had discussed internally and pointed out that we have provided the right amount of information in the scenario description. These aspects strengthen the expediency of the scenario.

Scenario 8 - Disruption of Safety Systems

Scenario eight is inspired by the TRITON malware. One of the interviewees explained a case where they updated the safety systems and received an error during the installation. Later it turned out that the reason for this error was, in fact, the TRITON malware. The fact that the malware was also present on the Norwegian continental shelf at a point in time suggests that attacks targeting other operators or companies using the same systems can also affect the Norwegian oil and gas industry. Using this malware as a basis for the scenario ensures a degree of realism to it.

Knowing what to do in situations where the SIS-systems do not work as intended is crucial to ensure safe operation at a platform. Interviewees recommended adding a scenario on SIS as this was an area of concern. It will hence be expedient to exercise on such a scenario.

The scenario is developed to have a significant hazard potential and hence include both offshore and onshore personnel. Including cooperation between offshore and onshore personnel was suggested by one of the interviewees. It was addressed that onshore personnel often hold advanced knowledge in their expertise fields and need to exercise cooperation with offshore personnel with physical access during an incident. This cooperation increases the complexity of the exercise, which is the intention of this exercise. This aspect increases the expediency of the scenario.

The first part of the scenario describes a situation where one of the employees senses the smell of gas. During the validation interviews, we received divergent feedback on whether the scenario was realistic or not. As mentioned in the results (Sect. 4.5), one operator stated that the scenario was unrealistic, whereas the other operator found the scenario realistic. We decided to leave the description as it was. Different operators might have different routines, and adjusting the scenario to these routines for it to be realistic should therefore be a task for the operator using the scenarios.

When validating this scenario, one of the interviewees mentioned that it is normal to sense a smell of gas at a platform. We believe that the scenario will give an expedient exercise as it raises awareness of the fact that malware can infect safety

systems. The safety systems are crucial to the platform's operation, and the employees must know how to handle such incidents. The scenario was also validated as expedient by one of the interviewees.

5.3 Limitations and Relevance of the Study

The study was restricted to a narrow time frame, which influenced our results of the research. Different factors may also have affected our results and relevance in this thesis.

For the interviews, we have only included respondents from two different operator companies. We interviewed two respondents from one company and one from another. The number of operators may be a limiting factor to the validation of our results. Validating our scenarios and criteria with more respondents from operators could have increased our assurance of them being valuable and useful for the industry. For the data collection and feedback interviews, we believe the selection of participants was comprehensive and complementary enough. All interviewees had valuable insight despite not working for an operator.

We have not been able to test our scenarios in exercises with the industry, which may have impacted our study. Since we have not tried them practically, we have not had the opportunity to discover areas for improvement when companies use them in practice. Due to the time constraint of the study, we did not have time to plan and conduct an exercise with the industry when starting this project. We have, however, been in contact with one company that exercises with companies in another sector that uses IACS. We interviewed them in our feedback interviews when they suggested testing one of our scenarios with a company from the energy sector. We scheduled a test in cooperation with them and the company. Unfortunately, the exercise was postponed to reasons beyond our control. This postponement resulted in the exercise being conducted after the delivery of our project. However, as they wanted to use our scenario with a company in the energy sector, we believe our scenarios could be valuable and relevant also for other industries using IACS.

We have based our lists of criteria and example scenarios on a literature review and several interviews with the industry and related sectors. With this foundation, we believe our results are suitable and useful for the petroleum industry despite not having tested them practically and only included two operators to validate them. It was confirmed during interviews that the operators were willing to take usage of most scenarios and found our criteria useful and valuable. This confirmation indicates that the scenarios and criteria will be valuable for a larger sample of the industry.

In our literature review, we searched for existing scenarios and criteria in our

field of research. We could not find any relevant results. Hence, we believe that our criteria and example scenarios are relevant for the industry. As we could not find any scenarios on cyber attacks against IACS for tabletop exercises the sector can use today, our results will hence contribute to this area of research. Also, we could not find a comprehensive list of criteria for tabletop exercises regarding cyber attacks against IACS. In fact, we could not find any list of criteria that describes how a scenario should be specified to be realistic and expedient. Some criteria were written in different guides and other literature, but none were comprehensive and explicitly adjusted to tabletop exercises. As a complete list with criteria is not available for the industry today, it makes our results relevant. Our criteria can also be used for more general tabletop exercises for most industries if slight adjustments are applied. This applicability is also a contribution to the research and increases the relevance of our results.

Chapter 6
Conclusion and Future Work

In this thesis, we have studied what characterizes an expedient and realistic scenario for a tabletop exercise, with the focus on scenarios related to cyber attacks targeting IACS. Through interview sessions and a literature review, we have gained insight into the petroleum industry and the ongoing digitalization of the sector. The report from DNV GL, *Training and Exercise* (In Norwegian: *Trening og Øvelse*), commissioned by PSA [Hål20], was used as both an inspiration and motivation. This guide identified the lack of guidelines for exercises focusing on cyber attacks against IACS today. Guidelines on exercises from other sectors were used as a base to develop our delivery. In this chapter, we will conclude with a rendering of our results and how these are relevant to the industry.

To answer our sub-question, RQ 1.1., we have developed two lists of criteria presented in Sect. 4.3 and justified in Sect. 5.1.1 and 5.1.2. One list is developed for a realistic and expedient scenario, while the other targets an expedient scenario collection. These lists include elements such as the scenario being plausible, based on today's threat landscape, not have the potential to shut down the platform, and trigger discussion and cooperation among the participants. By following these criteria when developing scenarios for a given exercise, or a scenario collection, the industry confirmed through interviews that the criteria could lead to realistic and expedient scenarios. Hence, these lists answer which criteria to evaluate to categorize a scenario as expedient and realistic.

To answer the main research question, RQ 1, we developed a collection of example scenarios presented in Sect. 4.4. This collection answers RQ 1 together with the lists of criteria from RQ 1.1. Themes included in the scenario collection are, among others, ransomware, insider attacks, and disconnection of gas detectors caused by a cyber attack. We believe that the developed example scenarios are examples of expedient and realistic scenarios for tabletop exercises related to cyber attacks against IACS in the petroleum industry, and together with the lists of criteria answer RQ 1. When developing the scenarios, we used the lists of criteria to provide realistic and

expedient scenarios. A scenario that is considered realistic, a threat to the exercising operator, and fit the participants and exercising company could give an expedient exercise. The scenarios in the scenario collection may help plan and develop new exercises, hence be valuable for the industry.

We believe the lists of criteria and the scenario collection can be used as guidelines for the industry on how best to develop and take usage of scenarios for tabletop exercises regarding cyber attacks against IACS. Despite not having tested them in practice and only validated them with two operators, we believe they are valuable and relevant for the industry. Another sector also wanted to take usage of one of our scenarios in an exercise, which we consider as a seal of approval. This also shows that the scenarios may be relevant for other sectors.

The scenarios are customized to the petroleum industry and validated as realistic and expedient by representatives from the industry. The criteria have, as mentioned, been validated as valuable by the industry. The validation indicates that the scenarios and criteria may contribute to preparedness exercises being conducted more efficiently where a valuable learning outcome is provided, which was our goal for the thesis.

As mentioned, respondents from two different operator companies have contributed in this study. To increase the value of both the scenarios and criteria, it would be valuable to conduct interviews with more operators. We did not have the opportunity to test our scenarios together with the industry. Therefore, it would also be desirable to use the scenarios in exercises with the industry and have operators use the lists of criteria when creating their own scenarios. These areas would therefore be of interest to study further.

References

[Age15] The Norwegian Digitalization Agency. Veileder i planlegging og gjennomføring av ikt-øvelser. Technical report, The Norwegian Digitalization Agency, 2015.

[Age20] Cybersecurity & Infrastructure Security Agency. Cisa issues emergency directive to mitigate the compromise of solarwinds orion network management products. [Online]. Available: https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network, 2020. Accessed: 05.02.2021.

[Aut21a] Norwegian National Security Authority. Grunnprinsipper for sikkerhetsstyring - utarbeid scenario. [Online]. Available: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/, 2021. Accessed: 01.06.2021.

[Aut21b] Norwegian National Security Authority. Grunnprinsipper for sikkerhetsstyring - utarbeid scenario. [Online]. Available: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/identifisere-og-kartlegge/utarbeid-scenario/, 2021. Accessed: 12.03.2021.

[Aut21c] Norwegian National Security Authority. Risiko 2021 - Helhetlig sikring mot sammensatte trusler. Technical report, Norwegian National Security Authority, Mar. 2021. Accessed: 23.04.2021.

[BBJ20] Agnė Brilingaitė, Linas Bukauskas, and Aušrius Juozapavičius. A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*, 88:101607, 2020.

[Bri19] Bill Briggs. Hackers hit norsk hydro with ransomware. the company responded with transparancy. [Online]. Available: https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/, 2019. Accessed: 10.05.2021.

[Con21] Redecon Consoles. What is a control room? [Online]. Available: https://redecon-consoles.com/what-is-control-room/, 2021. Accessed: 26.02.2021.

[Des18] Daniel DesRuisseaux. Cybersecurity assessment—the most critical step to secure an industrial control system. *Schneider Electric: Andover, MA, USA*, 2018.

[DG21] Renee Dudley and Daniel Golden. The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms. [Online]. Available: https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption, 2021. Accessed: 29.05.2021.

[Dic21a] Cambridge Dictionary. Fail-safe. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/fail-safe, 2021. Accessed: 13.05.2021.

[Dic21b] Cambridge Dictionary. Liaison. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/liaison, 2021. Accessed: 04.05.2021.

[DoEM21] San Francisco Department of Emergency Management. Exercise design steps. [Online]. Available: https://sfdem.org/exercise-design-steps, 2021. Accessed: 22.01.2021.

[Dra19] Dragos. Global oil and gas cyber threat perspective. [Online]. Available: https://www.dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf, 2019. Accessed: 14.05.2021.

[Eur20] Europol. Internet Organised Crime Threat Assessment 2020. Technical report, Europol, 2020. Accessed: 26.04.2021.

[EV21] Collin Eaton and Dustin Volz. Colonial pipeline ceo tells why he paid hackers a $4.4 million ransom. [Online]. Available: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636, 2021. Accessed: 29.05.2021.

[fCP16] The Norwegian Directorate for Civil Protection. Veileder i planlegging, gjennomføring og evaluering av øvelser - grunnbok: Introduksjon og prinsipper. Technical report, The Norwegian Directorate for Civil Protection, Oct. 2016.

[Fru20] Josh Fruhlinger. Ransomware explained: How it works and how to remove it. [Online]. Available: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html, Jun. 2020. Accessed: 02.02.2021.

[Gin20] Andrew Ginter. The top 20 cyber attacks on industrial control systems. Technical report, Waterfall Security Solutions, Dec. 2020.

[GL17] DNV GL. Cyber security in the oil and gas industry based on iec 62443. Technical report, DNV GL, Sept. 2017.

[Gle14] Joseph J Gleason. Getting big results by going small-the importance of tabletop exercises. In *International Oil Spill Conference Proceedings*, volume 2014, pages 114–123. American Petroleum Institute, 2014.

[GMR+18] Leif Jarle Gressgård, Kjersti Melberg, Martin Risdal, Jon Tømmerås, and Ruth Østergaard Skotnes. Digitalisering i petroleumsnæringen. 2018.

[GNB+06] Timothy Grance, Tamara Nolan, Kristin Burke, Rich Dudley, Gregory White, and Travis Good. Guide to test, training, and exercise programs for it plans and capabilities. 2006.

[Gov21] United States Government. Exercises. [Online]. Available: https://www.ready.gov/exercises, 2021. Accessed: 13.05.2021.

[Gre21] Andy Greenberg. The colonial pipeline hack is a new extreme for ransomware. [Online]. Available: https://www.wired.com/story/colonial-pipeline-ransomware-attack/, 2021. Accessed: 29.05.2021.

[Guc18] Darren Guccione. What is the dark web? how to access it and what you'll find. [Online]. Available: https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html, 2018. Accessed: 26.04.2021.

[Hål20] Erling Håland. Trening og øvelse. Technical report, DNV GL, Feb. 2020.

[HF+18] Kevin E Hemsley, E Fisher, et al. History of industrial control system cyber incidents. Technical report, Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[Hig19] Kelly Jackson Higgins. Triton/trisis attacks another victim. [Online]. Available: https://www.darkreading.com/vulnerabilities---threats/triton-trisis-attacks-another-victim/d/d-id/1334388, 2019. Accessed: 16.03.2021.

[HNW+12] Espen Hoell, Cato Vivelid Nilssen, Erik Wale, Geir Nødland, and Bjørn Hoff. Beredskap og støttefunksjoner - Konsekvensutredning for havområdene ved Jan Mayen. Technical report, The Norwegian Ministry of Petroleum and Energy, October 2012.

[HS20] Guro Hotvedt and Andrea Neverdal Skytterholm. Pre-study: Scenarios for exercises on cyber attacks against iacs in the petroleum sector. Project report in TTM4502, Department of Information Security and Communication Technology, NTNU – Norwegian University of Science and Technology, Dec. 2020.

[Hyd20] Hydro. Cyberangrep på hydro. [Online]. Available: https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/, 2020. Accessed: 28.01.2021.

[IEC10] Security for Industrial Automation and Control Systems. Standard, International Electrotechnical Commision, Geneva, CH, 2010.

[iS20] i SCOOP. Operational technology (ot) - definitions and differences with it. [Online]. Available: https://www.i-scoop.eu/industry-4-0/operational-technology-ot/, 2020. Accessed: 04.11.20.

[JBS+11] Stig Ole Johnsen, Cato Bjørkli, Trygve Steiro, Håkon Fartum, Hanne Haukenes, Jasmine Ramber, and Jan Skriver. Criop: A scenario method for crisis intervention and operability analysis. Technical report, SINTEF Technology and Society, Mar. 2011.

[Job21] JobHero. What is a control room operator? [Online]. Available: https://www.jobhero.com/career-guides/interviews/prep/what-is-a-control-room-operator, 2021. Accessed: 13.05.2021.

[Koo20] John Koon. How iiot enhances industrial control systems and scada. [Online]. Available: https://www.engineering.com/story/how-iiot-enhances-industrial-control-systems-and-scada, 2020. Accessed: 15.05.2021.

[Lar15] Ann-Kristin Larsen. Øvelser - en veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen. Technical report, The Norwegian Water Resources and Energy Directorate, 2015.

[Lut21] Ben Lutkevich. Dmz (networking). [Online]. Available: https://searchsecurity.techtarget.com/definition/DMZ, 2021. Accessed: 13.05.2021.

[mA21] mnemonic AS. Security Report 2021. Technical report, mnemonic AS, Feb. 2021. Accessed: 26.04.2021.

[MF13] Stein Malerud and Håvard Fridheim. Metode for utvikling av scenarioer til spill og øvelser. Technical report, Norwegian Defence Research Establishment, 2013. Accessed: 30.04.2021.

[MK18] Albine Moser and Irene Korstjens. Series: Practical guidance to qualitative research. part 3: Sampling, data collection and analysis. *European Journal of General Practice*, 24(1):9–18, 2018.

[NEK16] Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management. Standard, Norsk Elektronisk Komite, Geneva, Vernier, 2016.

[Net21] Paloalto Networks. What is a botnet? [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-botnet, 2021. Accessed: 03.05.2021.

[Nor03] Standards Norway. NORSOK Standard T-001 -Telecom systems. Standard, NORSOK, Strandveien 18, Lysaker, Norway, December 2003.

[Nor16] Petroleum Safety Authority Norway. § 23 training and drills. [Online]. Available: https://www.ptil.no/en/regulations/all-acts/the-activities-regulations3/VI/23/, Jan. 2016. Accessed: 04.11.20.

[Nor20] Telenor Norway. De lange linjene - Digital Sikkerhet 2020. Technical report, Telenor Norway AS, Jun. 2020. Accessed: 02.02.2021.

[oF20] Ministry of Finance. Statsbudsjettet 2021: Statens inntekter og utgifter. [Online]. Available: https://www.regjeringen.no/no/statsbudsjett/2021/statsbudsjettet-2021-statens-inntekter-og-utgifter/id2768898/, 2020. Accessed: 04.11.20.

[oFN20] The Ministry of Finance Norway. Meld. st. 2 - melding til stortinget - revidert nasjonalbudsjett 2020. [Online]. Available: https://www.regjeringen.no/contentassets/f7f31a9baf3e49c1ad1fa72da5585003/no/pdfs/stm201920200002000dddpdfs.pdf, 2020. Accessed: 13.05.2021.

[OL17] Rain Ottis and Lauri Luht. Mapping the best practices for designing multi-level cyber security exercises in estonia. 2017.

[oLA18] Norwegian Ministry of Labour and Social Affairs. Health, safety and environment in the petroleum industry. Technical report, Norwegian Ministry of Labour and Social Affairs, 2018. Accessed: 21.05.2021.

[OMJA19] Nour Elhouda Oueslati, Hichem Mrabet, Abderrazak Jemai, and Adeeb Alhomoud. Comparative study of the common cyber-physical attacks in industry 4.0. In *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, pages 1–7. IEEE, 2019.

[Pau20] Kari Paul. What you need to know about the biggest hack of the us government in years. [Online]. Available: https://www.theguardian.com/technology/2020/dec/15/orion-hack-solar-winds-explained-us-treasury-commerce-department, 2020. Accessed: 05.02.2021.

[PB01] Laura Patrick and Cliff Barber. Tabletop exercises-preparing through play. In *International Oil Spill Conference*, volume 2001, pages 363–367. American Petroleum Institute, 2001.

[Pet] Norsk Petroleum. Interaktivt kart. [Online]. Available: https://www.norskpetroleum.no/interaktivt-kart-og-arkiv/interaktivt-kart/. Accessed: 20.05.2021.

[Pet21] Norwegian Petroleum. Selskap. [Online]. Available: https://www.norskpetroleum.no/fakta/selskap-utvinningstillatelse/, 2021. Accessed: 13.05.2021.

[Pra21] Mary K. Pratt. Definition: cyber attack. [Online]. Available: https://searchsecurity.techtarget.com/definition/cyber-attack, 2021. Accessed: 25.02.2021.

[Ram21] Rambus. Industrial iot: Threats and countermeasures. [Online]. Available: https://www.rambus.com/iot/industrial-iot/, 2021. Accessed: 15.05.2021.

[RMB+20] Rwamahe Rutakumwa, Joseph Okello Mugisha, Sarah Bernays, Elizabeth Kabunga, Grace Tumwekwase, Martin Mbonye, and Janet Seeley. Conducting in-depth interviews with and without voice recorders: a comparative analysis. *Qualitative Research*, 20(5):565–581, 2020.

[Rob11] Colin Robson. *Real World Research*. John Wiley & Sons, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom, 2011.

[Ser20a] The Norwegian Police Security Service. Etteretningstrusselen mot norsk petroleumssektor. Technical report, The Norwegian Police Security Service, 2020. Accessed: 25.05.2021.

[Ser20b] The Norwegian Police Security Service. Nasjonal trusselvurdering 2020. Technical report, The Norwegian Police Security Service, Feb. 2020. Accessed: 03.02.2021.

[SFS11] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82):16–16, 2011.

[Sol] Solarwinds. Solarwinds. [Online]. Available: https://www.solarwinds.com/. Accessed: 21.05.2021.

[Stø19] Ketil Støren. *Teknologivitenskap. Forskningsmetode for teknologer.* Universitetsforlaget, Universitetsforlaget AS, Postboks 508 Sentrum, 0105 Oslo, 2019.

[SW21] Scott Shackelford and Megan Wade. Colonial pipeline forked over $4.4m to end cyberattack - but is paying a ransom ever the ethical thing to do? [Online]. Available: https://theconversation.com/colonial-pipeline-forked-over-4-4m-to-end-cyberattack-but-is-paying-a-ransom-ever-the-ethical-thing-to-do-161383, 2021. Accessed: 29.05.2021.

[Tam] Tampnet. Coverage maps. [Online]. Available: https://www.tampnet.com/coverage-maps. Accessed: 20.05.2021.

[Too21] Instrumentation Tools. Industrial automation and control systems (iacs). [Online]. Available: https://instrumentationtools.com/industrial-automation-and-control-systems/, 2021. Accessed: 26.02.2021.

[Top12] Rolv Christian Topdahl. -oljå tenker alltid "worst case". [Online]. Available: https://www.aftenbladet.no/aenergi/i/1yOjK/oljaa-tenker-alltid-worst-case, 2012. Accessed: 21.05.2021.

[VdM08] Louis Van der Merwe. Scenario-based strategy in practice: a framework. *Advances in Developing Human Resources*, 10(2):216–239, 2008.

[Wil20] Jake Williams. What you need to know about the solarwinds supply-chain attack. [Online]. Available: https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/, 2020. Accessed: 10.02.2021.

Appendix

A Interview Guide for Semi-Structured Interviews

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

Introduction

In this interview, we plan to go through each scenario to evaluate if the scenarios are expedient and realistic. By expedient scenarios, we mean scenarios that give a valuable learning outcome for the participants and the exercising organization. With the term realistic, we are referring to situations the participants find plausible, hence scenarios they believe can happen in the real world.

After we have gone through all scenarios, we want to go through the lists of criteria and explain the intention with each criterion. Here, we want feedback on whether you agree with these criteria or not. If you disagree, we would like to know why.

In this round of interviews, we have chosen to conduct the interviews as semi-structured interviews. This is done to make the validation of the scenarios and criteria consistent through several interviews.

Questions Regarding Each Individual Scenario in the Scenario Collection

- Is it realistic?
    - If no:
        - What makes it unrealistic?
        - Can something be changed to make it realistic?
- Is it expedient?

    - If no:
        - What makes it not expedient?
        - Can something be changed to make it expedient?

- Do you have any other comments?

Questions Regarding the Lists of Criteria

- Are the criteria characterizing expedient scenarios?
    - If no:
        - What can be done to make the criteria characterize an expedient scenario?
- Are the criteria characterizing realistic scenarios? (Only ask this question for the list of individual scenarios)
    - If no:
        - What can be done to make the criteria characterize a realistic scenario?
- Are there any criteria that should be omitted from the list?
    - If yes:
        - Which criteria should be omitted?
        - Why?
- Are there any criteria that is missing?
    - If yes:
        - Which criteria are missing?
        - Why?
- Are there any criteria that should be changed?
    - If yes:
        - Which criteria should be changed?
        - Why?
        - How?
- Do you believe that the collection of criteria will make it easier for actors to develop scenarios that are expedient and realistic?

Ending

These sessions are the last interview sessions we are conducting. We want to thank you for contributing to our master's thesis. We have gained valuable input from these interview(s). If you would like to receive our final result, we can send it to you when the report is delivered.

Appendix B

4G Connection Coverage Map

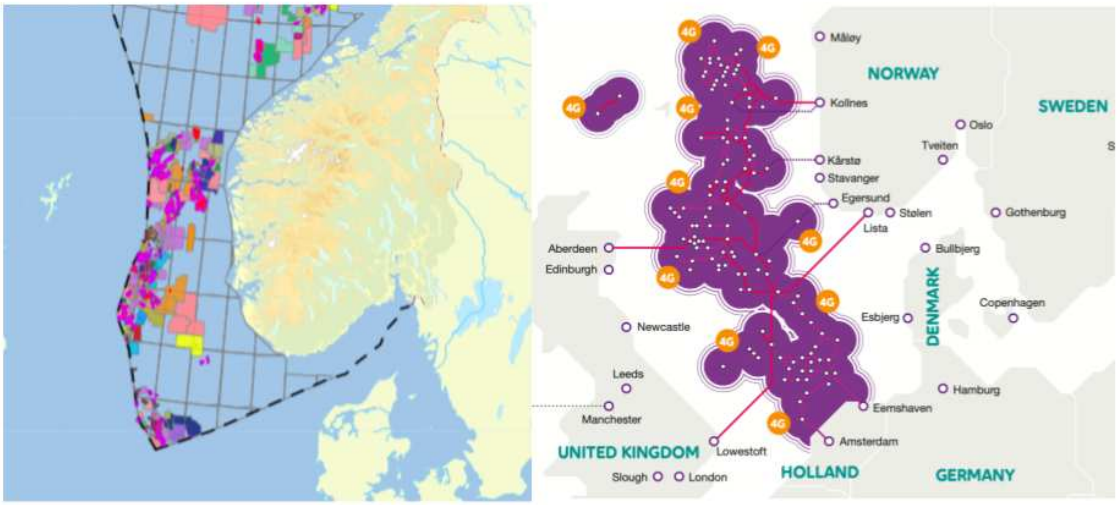

Figure B.1: Map of the Norwegian continental shelf and the coverage area of 4G from Tampnet. The Norwegian continental shelf is presented to the left, while the coverage area of Tampnet and 4G is given to the right. Adapted from Norsk Petroleum and Tampnet [Pet, Tam].

Andrea Skytterholm and Guro Hotvedt

Preparedness Exercises for Cyber Attacks Against Industrial Control Systems in the Petroleum Industry

NTNU
Norwegian University of
Science and Technology