Report

Regulation of ICT security in the petroleum sector

ICT security - Robustness in the petroleum sector 2020

Authors:

Knut Øien, Lars Bodsberg, Martin Gilje Jaatun, Thor Myklebust, Tor Onshus

Report No:

2023:00190 - Unrestricted

Client:

Petroleum Safety Authority Norway

SINTEF Digital
Postal address:
Post Box 4760 Torgarden
7465 Trondheim, Norway

Switchboard: +47 40005100

info@sintef.no

Enterprise /VAT No:
NO 919 303 808 MVA

Report

Regulation of ICT security in the petroleum sector

ICT security - Robustness in the petroleum sector 2020

KEYWORDS
Regulations
ICT security
OT systems

VERSION 1.0	**DATE** 2023-02-06

AUTHORS
Knut Øien, Lars Bodsberg, Martin Gilje Jaatun, Thor Myklebust, Tor Onshus

CLIENT Petroleum Safety Authority Norway	**CLIENT'S REFERENCE** Arne Halvor Embergsrud
PROJECT NO. 102022556	**NO. OF PAGES/APPENDICES** 39 (3 appendices)

SUMMARY

The purpose of this report is to clarify how the protection of information and communication technology (ICT security) in the petroleum industry is regulated under current regulations and to shed light on the expectations of the public authorities in the field of ICT security.

This report is one of six SINTEF reports from the project entitled: "ICT security – Robustness in the petroleum sector 2020". The project has collated knowledge concerning risks, vulnerabilities and ICT security for industrial ICT systems.

The report is a translation of the SINTEF report 2021:00054 (in Norwegian).

PREPARED BY Knut Øien	SIGNATURE Knut Øien
CHECKED BY Ranveig Kviseth Tinmannsvik	SIGNATURE Ranveig Kviseth Tinmannsvik Ranveig Kviseth Tinmannsvik (3. mar. 2023 18:10 GMT+1)
APPROVED BY Maria Bartnes	SIGNATURE Maria Bartnes

REPORT NO.	**ISBN**	**CLASSIFICATION**	**CLASSIFICATION THIS PAGE**
2023:00190	978-82-14-07959-3	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
1.0	2023-02-06	Translation of SINTEF report 2021:00054

Image crediting:
Cover page: Equinor

Table of contents

Preface

The petroleum industry is characterised by rapid change and ambitious plans for the increased use of digital technology throughout the value chain. Some key words are robotisation, artificial intelligence, machine learning, big data processing, changing work processes, and new forms of collaboration and business models.

Digitalisation is facilitating closer interconnection and increased data flow between different computer systems, support systems, sensor data, databases and people. This is contributing to more efficient work processes and better analyses and decisions. Digitalisation will offer better security through expanded access to and more efficient use of real-time and historical data, both internally and externally in an organisation. However, as information from control and security systems becomes more widely available in administrative office systems and in "the cloud", this could cause control and security systems to become more vulnerable and increasingly attractive targets for cyberattacks. Attacks on office systems can be a springboard into industrial ICT systems.

A key aim of this document is to clarify how ICT security in the petroleum industry is regulated under the current regulations and, in particular, to provide an overview of the regulations applicable to market operators who may not be as familiar with them.

The document also presents an overview of the background and status of the major initiative within the field of ICT security in the petroleum sector which began in 2018 and ends in 2021. The status was assessed in relation to the expectations of the overarching authority, including signals given in the *National Cyber Security Strategy for Norway* (2019). This also constitutes an update for the overarching authority concerning the status of the ongoing work.

The document has been created as a SINTEF report, but is formulated as a concise memorandum, in much the same way as other Petroleum Safety Authority Norway (PSA) memoranda, such as *Integrated and unified risk management in the petroleum industry* (2018). It was prepared by SINTEF for the PSA and is thus viewed from an external perspective. It is therefore not viewed with the PSA's own eyes but may provide a basis for a future PSA memorandum on ICT security as viewed from the PSA's own standpoint, for example after the major initiative relating to ICT security has ended in 2021.

The document covers selected topics within ICT security and should also be seen in the context of other work by the PSA, such as the aforementioned memorandum on risk management (2018) and the barrier memorandum (2017), presentations given by PSA in various professional forums, and ICT security audits. The latter is not covered to any great extent in this document, as the reports on these audits are generally confidential.

In order to achieve a high level of ICT security, it is envisaged that individual companies will acknowledge the potential for serious ICT incidents which could impact on industrial ICT systems.

Knut Øien
Senior Researcher, SINTEF Digital
January 2021

Executive summary

Introduction

This document describes how ICT security in the petroleum industry is regulated in current regulations, and it provides an overview of the background for, expectations of, and status of the major ICT security initiative in the petroleum sector that started in 2018 and expires in 2021.

Industrial ICT systems and ICT security

In the petroleum sector, the term IT system is usually used for office systems, OT system or industrial ICT system are used for industrial control and security systems, and ICT system is used as a common term for IT and OT systems. Similarly, ICT security is generally a broad term, not having an unambiguous definition, whereas a focus for the Petroleum Safety Authority (PSA) is the industrial ICT systems (OT systems) and thus "OT security" as part of ICT security.

Background and expectations from the authorities

The Lysne Committee's report *Digital Vulnerability - Safe Society* (2015) and the White Paper on *ICT Security - A Joint Responsibility* (2016-2017) were key documents that led to the major initiative in ICT security in the petroleum sector (2018-2021). This includes recommendations and expectations related to the transfer of the safety tradition within health, safety and environment (HSE) to the digital area, the establishment of regulations for digital vulnerabilities, clarification of the role and capacity of the Petroleum Safety Authority Norway and collaboration with response teams for ICT incidents. Furthermore, there are expectations for the work with ICT security in general in the *National Strategy for Digital Security* (2019) and specifically for the Petroleum Safety Authority Norway in the annual assignment letters from the Ministry of Labor and Social Affairs.

General information about the petroleum regulations

The HSE regime in Norwegian petroleum activities mainly applies functional principles and is based on internal control, where the companies have an independent responsibility for HSE through internal management systems and processes. The operator and licensee are also required to follow up that everyone who performs work for them complies with requirements given in the health, environment and safety legislation (duty of care). The regulations consist of five regulations pursuant to the Petroleum Act (and several other laws), guidelines for the regulations, as well as reference to recognized standards, norms and guidelines.

ICT security in the petroleum regulations

ICT is not specifically mentioned in the Petroleum Act, and the regulations are function-based where ICT security is generally covered, but only to a minor extent is mentioned explicitly. Furthermore, NOROG 104 is the only ICT-related reference to standards, norms or guidelines. There is an ongoing discussion in the industry about regulatory reference to other ICT-related standards, norms and guidelines. This applies in particular to the IEC 62443 series (standards and technical reports defining procedures for implementing secure industrial automation and control systems (IACS/OT)).

ICT security - robustness in the petroleum sector

During the first three years of the initiative *ICT Security - Robustness in the Petroleum Sector* (2018-2021), 18 reports have been prepared for the PSA by IRIS, DNV GL and SINTEF. These are briefly described, and an assessment has been made of the status of the initiative in relation to expectations and recommendations in the *National Strategy for Digital Security* (2019), the Lysne Committee's report (2015) and the assignment letter from the Ministry of Labor and Social Affairs (2020). Most of the 18 reports provide recommendations for measures and further knowledge acquisition. Many of these are linked to the expectations and recommendations from the authorities, which the PSA can use in the continuation of the ICT security initiative.

1 Introduction

1.1 Objective

The aim of this document is to clarify how ICT security in the petroleum industry is regulated under the current regulations and, in particular, to present an overview of the regulations applicable to players who may not be as familiar with them. A description is also given of the background to and status of the major initiative within the field of ICT security in the petroleum sector which began in 2018 and ends in 2021.

The document is intended to help companies in the petroleum industry further develop their own practices relating to ICT security in industrial ICT systems within the framework of current regulations.

1.2 Target group

The target group for the document is anyone with a particular responsibility for deciding, formulating, implementing and following up on ICT security in the petroleum industry, including players with a limited knowledge of the PSA's regulatory framework.

1.3 Background

The Petroleum Safety Authority Norway (PSA) has commissioned SINTEF to investigate various aspects of the topic of ICT security — robustness in the petroleum sector. The main aim was to collate knowledge concerning risks, threats, vulnerabilities and the importance of ICT security for industrial ICT systems. The project aims to help improve the understanding of ICT security in the petroleum industry and increase resilience with regard to adverse events. SINTEF has also provided input for updating of the PSA's regulatory framework for monitoring ICT security.

The project forms part of the project relating to ICT security in the petroleum sector (2018-2021), for which SINTEF has prepared six reports for 2020, with this report constituting one of these. All of the reports, including the reports prepared in 2018 and 2019, are briefly described in section 6.2.

1.4 Definitions

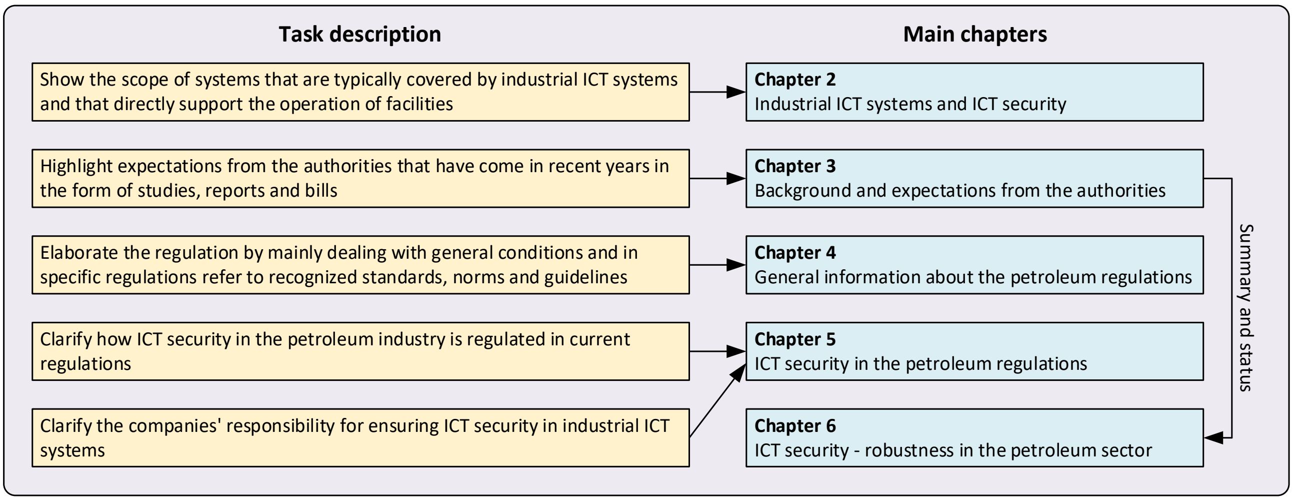
Definitions are used to ensure that we have a consistent understanding of key terms, but definitions can in themselves limit the understanding of a term, and there are often multiple definitions of the same term. In the table below, we have selected and compiled some terms relating to ICT security that are used by overarching authorities and the PSA. The PSA has created a separate website “Terms and expressions” which explains terms and phrases based on how they are used in the petroleum industry (see https://www.ptil.no/en/technical-competence/terms-and-expressions/). It should be noted that the terms may have different meanings in common parlance and in industries other than the petroleum industry.

Term	Definition/description	Reference
Defined hazard and accident conditions (DSHAs)	A collection of possible observable incidents which the companies must defend against in order to pursue prudent petroleum operations	PSA, Guidelines to the Activities Regulations, Section 73
Barriers*	Measures intended to prevent a specific sequence of events from occurring or to guide such a course in a specific direction to limit damage and/or loss. The function of such barriers is ensured by technical, operational and organisational elements, individually and collectively.	PSA, Terms and expressions
HSE	A collective term which, in the petroleum industry, encompasses consideration for people, the environment and material values	Report to the Storting 12 (2017–2018)
ICT security/Digital security/Cyber security	The protection of "anything" that is vulnerable because it is connected to or otherwise dependent on information and communication technology	National Cyber Security Strategy for Norway 2019
ICT security measures*	Measures to protect ICT systems and information against intentional and unintentional events	NOU2015: 13
Information and communication systems	Systems which address the need for the collection, processing and dissemination of data and information	PSA, Management Regulations, Section 15
Integrity (of ICT systems)	That ICT systems, the information that is processed in the systems, and the services associated with the systems are not altered unintentionally or without authorisation	NOU 2018: 14
Confidentiality (of ICT systems)	That ICT systems, the information that is processed in the systems, and the services associated with the systems are only available to those who should rightfully have access	NOU 2018: 14
Risk	The consequences of the activity and its associated uncertainty	PSA, Guidelines to the Framework Regulations, Section 11
Security	Security involves protection against hazards and threats which could cause undesirable incidents	NOU2015: 13
Vulnerability	An expression for the problems that a system experiences during operation when exposed to an undesirable incident, and the problems that the system experiences in resuming its activity after the incident has occurred	NOU2015: 13
Availability (of ICT systems)	That ICT systems, the information that is processed in the systems, and the services associated with the systems are available where and when they are needed by users	NOU 2018: 14
Threat	An intentional undesirable act	NSM 2015
Uncertainty	Concerns a lack of information, understanding or knowledge	Report to the Storting 12 (2017–2018)

*) The term "barrier" is rarely used in ICT security standards. Instead, terms such as measures, countermeasures and defence mechanisms, protective mechanisms, solutions, etc. are used.

1.5 Report structure

The report structure is illustrated in Figure 1. The main chapters are linked to the remit from the PSA.



Task description
Main chapters
Show the scope of systems that are typically covered by industrial ICT systems and that directly support the operation of facilities
Chapter 2
Industrial ICT systems and ICT security
Highlight expectations from the authorities that have come in recent years in the form of studies, reports and bills
Chapter 3
Background and expectations from the authorities
Elaborate the regulation by mainly dealing with general conditions and in specific regulations refer to recognized standards, norms and guidelines
Chapter 4
General information about the petroleum regulations
Clarify how ICT security in the petroleum industry is regulated in current regulations
Chapter 5
ICT security in the petroleum regulations
Clarify the companies' responsibility for ensuring ICT security in industrial ICT systems
Chapter 6
ICT security - robustness in the petroleum sector
Summary and status

Figure 1 Main chapters versus task description

Abbreviations are given in Appendix 1, the PSA's explanation of relevant regulatory requirements regarding ICT security in a letter to the industry is included in Appendix 2, while a larger version of Figure 3 (key documents) is shown in Appendix 3.

2 Industrial ICT systems and ICT security

2.1 What are IT systems and OT systems?

In the PSA's regulatory framework, the term "information and communication systems" (ICT systems) is used to refer to systems which address the need to obtain, process and disseminate data and information (see the Management Regulations, Section 15 *Information*). The term "industrial ICT systems" is used to refer to OT (Operational Technology or Operational IT) systems which bring about changes in physical equipment and processes such as control and monitoring systems and security systems.[1] The distinction between IT systems (office systems) and OT systems is illustrated by a simplified version of the Purdue model[2] in Figure 2 (SINTEF, 2021. *Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer / Basic principles for ICT security in industrial ICT systems*).

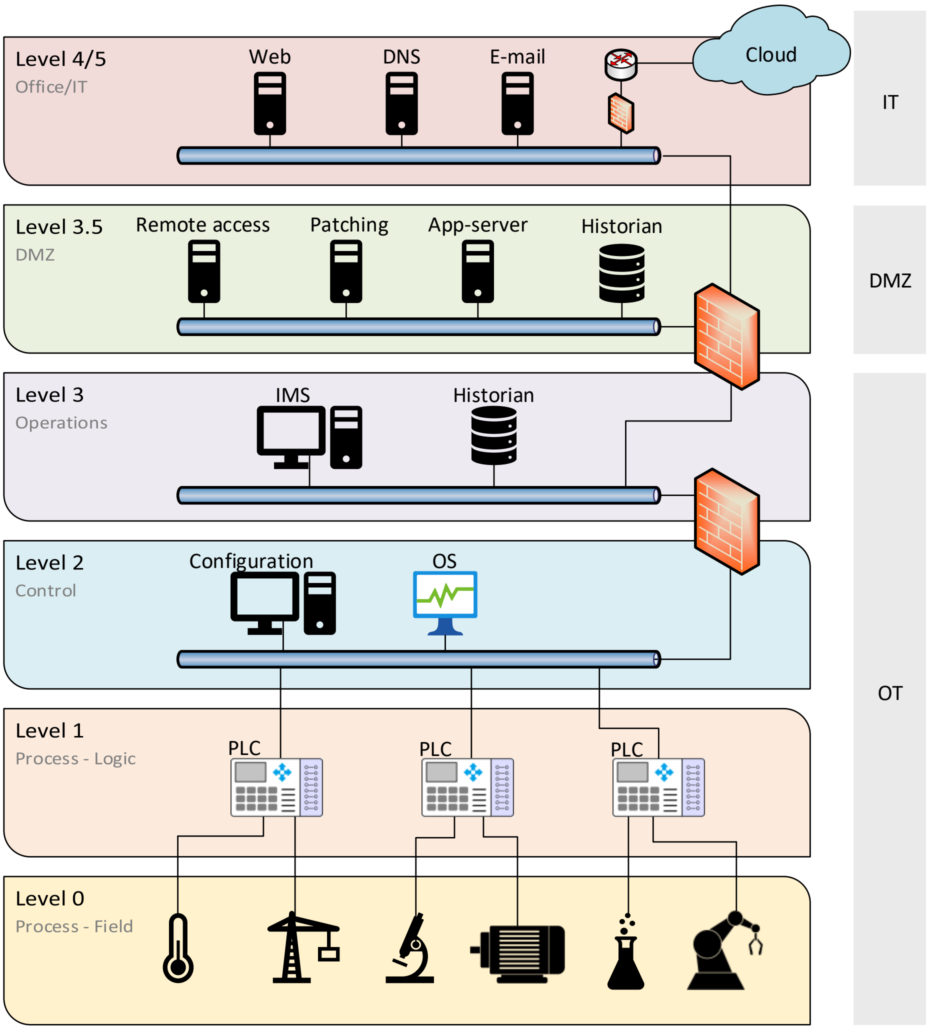


Figure 2 Simplified Purdue model to illustrate the boundary between IT and OT

[1] In (English) standards and frameworks, various terms are used to refer to industrial ICT systems, including SAS (Safety and Automation System), ICS (Industrial Control System), IACS (Industrial Automation and Control System) and SCADA (Supervisory Control and Data Acquisition).

[2] The Purdue model was developed by Theodore J. Williams and a consortium at Purdue University (Williams, 1992). Figure 2 is a simplification and the exact content is not discussed further here.

In somewhat simplified terms, the boundary between IT systems and OT systems passes through the De-Militarised Zone (DMZ)).

Historically, a distinction has been made within the industry between administrative computer systems which process data and information (IT and ICT systems) and computer systems which control production (OT systems). OT systems on a facility which were previously separated from the outside world are being modernised and becoming increasingly complex and interconnected with IT systems. This is opening up the possibility of more unified solutions, including management and monitoring from land where OT systems have multiple connection points with the company's IT systems and extensions to external networks, such as cloud solutions via the internet.

Both IT systems and OT systems include computers, networks, operating systems, applications and other programmable and configurable components.

2.2 Overview of constituent systems

Table 1 gives examples of a possible division between IT and OT systems on fixed and mobile facilities.

Table 1 Examples of a possible division between IT and OT systems on fixed and mobile facilities

IT and OT systems
IT systems
Performance monitoring systems
Condition monitoring (e.g. rotating equipment, valves, cranes)
Personnel record systems
Telecommunication systems*, PA, alarm and emergency communication systems, CCTV, radio communications
Radar, helicopter navigation
Collision warning, meteorological data
OT systems
Management and control systems for production facilities and onshore facilities, including application units
Management and control systems for drilling and wells, including application units
Safety systems (fire and gas detection, emergency shutdown, pressure relief, process shutdown, fire-extinguishing water supply)
Safety-critical marine systems (positioning systems, ballast systems, bilge systems, weight and stability monitoring systems)
Systems for ensuring the detection and mapping of acute pollution
Ventilation systems
Power distribution and control, including emergency power
Metering
Crane and lifting systems

* May also form part of an OT system, e.g. in connection with remote operation

2.3 What are ICT security and OT security?

The term “ICT security” does not have an unambiguous definition. It has interfaces with, or is perceived as being synonymous with, information security, cyber security and digital security (NOU 2018: 14 *IKT-sikkerhet i alle ledd / ICT security at every stage*).

NOU 2018: 14 also notes that the terms in some documents are used entirely or partially synonymously, while in others they are accorded different meanings. In addition, use of the term “ICT security” has changed over the years. Traditionally, the protection of networks and systems has been given considerable emphasis, while today the term has come to more broadly encompass information that is processed in the systems and networks, as well as the services that the systems provide. NOU 2018: 14 adopts this broad understanding of the term, and notes that the security-related goals of ICT security are *confidentiality*, *integrity* and *availability* (see the definitions in section 1.4).

Each enterprise will weigh the security-related goals differently depending on the purpose that it has or is intended to support, and the requirements and risk picture that it has to relate to. Based on these objectives and their weighting, protection will encompass technological, human and organisational barriers, which are intended to counteract undesirable digital incidents, the ability to detect such incidents and subsequent response in order to restore a secure state for the ICT systems.

Industrial ICT systems (OT systems) are a particular area of focus for the PSA, as is therefore “OT security”, where the security-related goal *availability* is the most important. A safety system must be available in the event of a need to protect human life and health, environment and material values.

A more detailed explanation is given in SINTEF (2021). *Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer (Basic principles for ICT security in industrial ICT systems).*

3 Background and expectations of the overarching authority

3.1 Overview and timeline (investigations, reports and propositions)

An important backdrop to the work relating to ICT security, both within the petroleum sector and in other sectors, are key policy documents and the national and international risk picture. This is illustrated in Figure 3. A larger version of the figure can be found in Appendix 3. (The year stated in the text indicates the document that is being referred to).

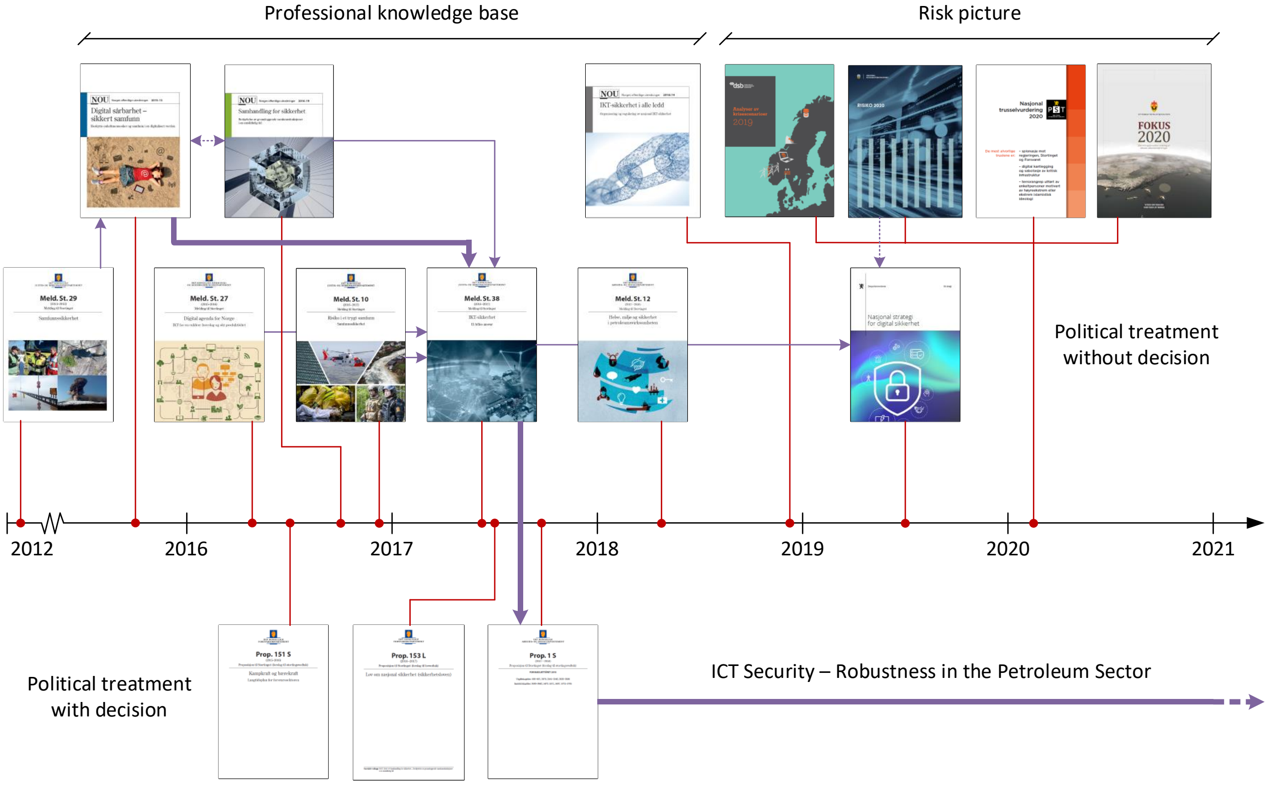

Professional knowledge base
Risk picture
NOU
Digital sårbarhet – sikkert samfunn
NOU
Samhandling for sikkerhet
NOU
IKT-sikkerhet i alle ledd
Analyser av krisescenarioer 2019
RISIKO 2020
Nasjonal trusselvurdering 2020
FOKUS 2020
Meld. St. 29
Samfunnssikkerhet
Meld. St. 27
Digital agenda for Norge
Meld. St. 10
Risiko i et trygt samfunn
Meld. St. 38
IKT-sikkerhet
Meld. St. 12
Helse, miljø og sikkerhet i petroleumsvirksomheten
Nasjonal strategi for digital sikkerhet
Political treatment without decision
2012
2016
2017
2018
2019
2020
2021
Political treatment with decision
Prop. 151 S
Kampkraft og bærekraft
Prop. 153 L
Lov om nasjonal sikkerhet (sikkerhetsloven)
Prop. 1 S
ICT Security – Robustness in the Petroleum Sector

Figure 3 Key documents for the work relating to ICT security published in recent years[3]

The figure is not exhaustive. Particular emphasis has been placed on including the documents that directly led to the major initiative concerning *ICT security — Robustness in the petroleum sector* (2018-2021), indicated by thick arrows.

NORs (Norwegian Official Reports) are often used to obtain a technical knowledge base, which can then be followed up by political consideration in reports to the Storting (without any recommendations regarding a decision) or propositions to the Storting (with recommendations regarding a decision: S — Storting decision and/or L — Legislative decision).

The technical basis is also continually supplemented by annual reports on the national and international risk picture, indicated in Figure 3 with the most recently published reports[4]. These are published by the National Security Authority (NSM), the Norwegian Police Security Service (PST) and the Norwegian Intelligence

[3] NOU 2015: 13 *Digital vulnerability — secure society* (page 61) contains a timeline of key reports and ICT security initiatives in Norway during the period from 2000 to 2015.

[4] NSM *Risks 2020*, PST *Nasjonal trusselvurdering 2020 (National threat assessment 2020)*, NIS *Fokus 2020 (Focus 2020)*, DSB *Analyser av krisescenarioer 2019 (Analyses of crisis scenarios 2019)*.

Service (NIS), while the Norwegian Directorate for Civil Protection (DSB) publishes reports every few years, most recently in 2019. NSM, PST, NIS and the National Criminal Investigation Service (KRIPOS) also submit classified reports to the Norwegian government.

The risk picture covers all relevant sectors in Norway, including the petroleum sector and attacks which are aimed at industrial control systems. NSM considers the state administrations and enterprises in defence, aerospace, maritime, *petroleum* and power to be at risk (NSM, 2020), while NIS notes that cyberattacks include operations which target *industrial control systems* (NIS, 2020). This situation is not new and is also based on incidents which occurred before the foundations for the initiative relating to ICT security in the petroleum sector were laid.

In addition to reports to the Storting, the *National Cyber Security Strategy for Norway* constitutes an important policy document for the work relating to ICT security. This was last published in 2019 (first published in 2003 and subsequently revised in 2007 and 2012). It is noted that the preface written by Prime Minister Erna Solberg only refers to two documents. These are the report from the Committee of Digital Vulnerabilities in Society (the *Lysne Committee*) on digital vulnerabilities in Norwegian society (NOU 2015: 13 *Digital vulnerability — secure society*) and its follow-up through the first Report to the Storting which exclusively deals with digital security (Report to the Storting 38 (2016-2017) *Cyber Security - A joint responsibility*.

These are the same two documents that directly led to the major initiative relating to *ICT security — Robustness in the petroleum sector* (2018-2021). A political decision and appropriation were made in connection with the consideration of the National Budget for 2018 (Prop. 1 S (2017-2018) and Recommendation 15 S (2017-2018)). The recommendation from the Standing Committee on Labour and Social Affairs stated that the initiative will be carried out over a period of four years: *"... that a proactive effort is important to prevent vulnerability in both operating systems and information management systems. The government has therefore strengthened ICT security over a four-year period in the amount of NOK 5.9 million in 2018."*

Recommendations submitted by the Lysne Committee (NOU 2015: 13) are described in section 3.2, while a summary assessment of the status of the work relating to these recommendations, described in Report to the Storting 38 (2016-2017), is presented in section 3.3.

Other key policy documents concerning ICT security

National Cyber Security Strategy for Norway (Norwegian Government, 2019) also refers to Report to the Storting 27 (2015-2016) *Digital agenda for Norway* and Report to the Storting 10 (2016-2017) *Risk in a Safe and Secure Society*, as well as Prop. 151 S (2015-2016) *Fighting strength and sustainability* and Prop. 153 L (2016-2017) *National Security Act*.

Report to the Storting 27 (2015-2016) concerns the government's digitalisation policy, in which privacy and digital security are key elements, and Report to the Storting 10 (2016-2017) deals with societal security which encompasses digital security. Both of these are referred to in the aforementioned Report to the Storting 38 (2016-2017) *Cyber Security - A joint responsibility*.

Prop. 151 S (2015-2016) is a long-term plan for priorities in the defence sector, including digital security. It also concerns NSM, which reports to the Ministry of Defence (but is administratively subject to the Ministry of Justice and Public Security). NSM's annual risk picture is otherwise the only risk picture to be highlighted in the *National Cyber Security Strategy for Norway* (2019). In addition, both NSM and other players such as PST, NIS and DSB are briefly mentioned in an appendix to the *National Cyber Security Strategy for Norway* (2019). This also includes the Norwegian Communications Authority (Nkom), which has a special responsibility with regard to security and preparedness in electronic communications networks and services. Nkom also publishes annual reports, most recently EkomROS 2020 *Den digitale grunnmuren satt på prøve*

(The digital foundation put to the test), which, in addition to reviewing incidents, identifies key risk areas in the coming years (Nkom, 2020).

Prop. 153 L (2016-2017) concerns a new Security Act, which was announced on 1 June 2018 and came into force on 1 January 2019. Clarifications concerning, and the extent to which it will impact on, the petroleum sector are ongoing. Responsibility for determining which enterprises should be covered by the Security Act rests with each individual ministry (NOU 2018: 14 *IKT-sikkerhet i alle ledd / ICT security at every stage*). Prop. 153 L (2016-2017) refers to NOU 2015: 13 and Report to the Storting 38, as well as Report to the Storting 10, but is based directly on the Security Committee's (the *Traavik Committee*) NOU 2016: 19 *Samhandling for sikkerhet*. NOU 2016: 19 is therefore enclosed as a separate appendix to Prop. 153 L (2016-2017).

Report to the Storting 29 (2011-2012) *Social Security* contains a separate chapter on ICT security and refers to responsibility principles that are still applicable, including within the petroleum sector. Report to the Storting 12 (2017-2018) *Health, safety and environment in the petroleum industry* provides a status on the work relating to ICT security. NOU 2018: 14 *IKT-sikkerhet i alle ledd (ICT security at every stage)* looks at, inter alia, the regulation of ICT security, including the petroleum sector, what is covered by the term 'ICT security' (see section 2.3), and what can be interpreted as being *prudent* ICT security (see Chapter 6).

3.2 ICT security expectations for the petroleum sector

The *National Cyber Security Strategy for Norway* (2019) notes that Report to the Storting 38 (2016-2017) is entitled *"ICT security — a joint responsibility"* with good reason, as we all have both an interest and a responsibility in safeguarding our values. Good digital security is not an objective that the authorities can achieve on their own. It is the industry which possesses the expertise and resources that are needed to be a driver of digitalisation and innovation. It is noted that *"safeguarding digital security is primarily a corporate responsibility"*.

This is based on, and elaborated upon in, Report to the Storting 29 (2011-2012): *"ICT security is primarily a corporate responsibility. This follows from the principle of responsibility, which implies that the person who is responsible for an enterprise under normal circumstances will also be responsible in the event of a crisis situation. In practice, this means that primary responsibility for securing information systems and networks rests with the owner."*

The Norwegian government has, inter alia, the following three expectations (*National Cyber Security Strategy for Norway*, 2019):

1. That ***companies*** adopt a *risk-based approach* to cyber incidents and use recognised frameworks, standards and management systems for cyber security
2. That ***authorities and the business community*** *share information* about threats, vulnerabilities, incidents and efficient measures with relevant actors to make society better able to withstand cyber incidents
3. That the ***authorities*** share advice, recommendations and guidelines on cyber security to provide companies with *knowledge* for their security work

The Lysne Committee believes that the security and supervision regime that is in force pursuant to the Petroleum Act is not strong enough and makes the following four recommendations ("expectations"):

1. Transfer the safety tradition within HSE to the digital area
2. Assess the value of the sector's facilities and ICT systems, and establish regulations concerning digital vulnerabilities
3. Clarify the role and capacity of the PSA

4. Assess the association with the response environment for ICT incidents

These expectations are aimed at the ***authorities - including the PSA - and companies*** within the sector.

Barriers[5] and barrier management can be seen as key elements of all the Lysne Committee's recommendations, with the exception of recommendation no. 3. Barrier management has been the subject of systematic work within the field of HSE for many years and is an example of a safety tradition that can be transferred to the digital area. As regards recommendation no. 2, the Lysne Committee notes that the regulations only implicitly cover digital security and believes that the supervisory authority (PSA) should require the establishment of barriers to digital vulnerabilities. It also recommends that, pending clarifications regarding the scope of the new Security Act, work should be initiated to value and classify facilities and ICT systems. This has many similarities with selections and criticality assessments that are made in the context of barrier management. In addition to the link to the response environment, recommendation no. 4 includes a recommendation that the sector carry out drills concerning the management of undesirable ICT incidents, in order to test and verify the quality of the barriers.

Recommendation no. 3 notes that the PSA has limited capacity as regards monitoring the ICT security and vulnerability of the sectors, and that the PSA should therefore be significantly strengthened in this area.

3.3 Initiative relating to ICT security and appropriations/letters of allocation

As mentioned previously, the major initiative relating to ICT security — Robustness in the petroleum sector (2018-2021) was brought about by the Lysne Committee's NOU 2015: 13 and Report to the Storting 38 (2016-2017), and appropriations were made in the 2018 National Budget. An allocation is made to the PSA in the annual letter of allocation from the Ministry of Labour and Social Affairs (ASD 2018, 2019, 2020), which continues in 2021. The letters of allocation also reflect the requirements and expectations of the Ministry of Labour and Social Affairs as regards the PSA.

The letter of allocation for 2018 states that: *"The Petroleum Safety Authority Norway must follow up to ensure that industry players implement appropriate safeguards to identify and prevent deliberate attacks on facilities, and that preparedness is established to deal with such attacks. This also applies to the industry's ICT technology and systems which can be exploited in order to carry out acts which threaten security. In 2018, the Petroleum Safety Authority Norway's appropriation has been increased by NOK 5 million to cover the increased monitoring of ICT security. In addition to increased knowledge and competence development and the mapping of challenges, the Petroleum Safety Authority Norway must also step up its supervisory follow-up concerning ICT security. The initiative also involves work to strengthen preparedness and incident management and the performance of drills."* (ASD, 2018).

This is helping to strengthen the work relating to ICT security, without any direct link to the individual recommendations of the Lysne Committee.

The letter of allocation for 2019 contains much the same message, concluding with: *"... This initiative is continued in the form of NOK 10 million in 2019.* "(ASD, 2019). The letter of allocation for 2020 states that: *"The Petroleum Safety Authority Norway shall, inter alia, contribute to increased knowledge of opportunities and risks relating to ICT security and digitalisation."* (ASD, 2020).

[5] The Lysne Committee uses the term "barriers", but this term is rarely used in cybersecurity standards and guidelines. Instead, terms such as ICT security measures, countermeasures, protections, solutions, etc. are often used.

Status of the work relating to ICT security prior to the initiative (before 2018)

The work relating to ICT security was carried out parallel to the establishment of the initiative (2018-2021), and before Report to the Storting 38 (2016-2017) was published. This Report to the Storting therefore also included a status evaluation with regard to the four recommendations of the Lysne Committee. Amongst other things, it is noted in this report that the PSA has contributed to the implementation of self-assessments based on NOROG 104 - *Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems*[6], and that DNV GL took the initiative regarding what became guidelines for the application of IEC 62443 (DNVGL-RP-G108 *Cyber security in the oil and gas industry based on IEC 62443*). This was linked to the Lysne Committee's recommendation no. 1 (transferring the safety tradition within HSE to the digital area) — tradition of collaboration.

In relation to the Lysne Committee’s recommendation no. 2 (valuation of the sector’s facilities and ICT systems and establishment of regulations concerning digital vulnerabilities), it is noted that, although the PSA has prepared and distributed for consultation a proposal to clarify application of the HSE regulations within the field of security, including ICT security, the follow-up to the new Security Act is awaited before regulatory changes are adopted. Reference is also made to supervision conducted by the PSA relating to both security in general and ICT security in particular.

As regards the need to strengthen the PSA within the field of ICT security (the Lysne Committee’s recommendation no. 3), reference is made to the fact that the PSA participates in technical forums, both nationally and internationally, in order to secure expertise and build networks. It is also noted that additional recruitments are planned which will strengthen the PSA as regards ICT security. The PSA is also considering the possibility of preparing an annual risk picture within ICT security in the petroleum industry.

Regarding the link to the response environment for ICT incidents (the Lysne Committee’s recommendation no. 4), it is noted that, although KraftCERT has also been made available to the petroleum industry, many organisations meet the need either through agreements with NSM or via their parent company abroad.

In relation to both the Lysne Committee’s recommendations no. 1 and no. 2, it is noted in the Report to the Storting that an important impending task will be the PSA’s efforts to clarify and further develop the regulations in order to overcome the challenges that the industry is facing with regard to changes in the threat picture and increasing digitalisation. Amongst other things, this involves following up on the development of industry standards that may be referred to in the regulations.

The provisional version of the most recent Storting report on health, safety and the environment in the petroleum industry (Report to the Storting 12 (2017-2018)), dating from 6 April 2018, presents a brief status of *ICT vulnerability and security*. According to the report, the PSA has strengthened its resources relating to the supervision of ICT security; see the Lysne Committee’s recommendation no. 3. It is stressed that, like the HSE regulations, the requirements regarding security are formulated as functional requirements. The authorities believe that, although there has been an overall improvement in the work relating to security in recent years, developments will necessitate strengthened follow-up in the industry.

The status of other related work in the industry, such as risk management and barrier management, is described in Chapter 5.

[6] Reference is made to NOROG 104 in the guidelines to Section 34 a of the Facilities Regulations. The Norwegian Oil and Gas Association published a revised version of the NOROG 104 guidelines on 5 December 2016.

Status of the work relating to ICT security during the initiative (after 2018)

A description of the status of the work relating to the ICT initiative (2018-2021) at the end of 2020, i.e. after three quarters of the initiative had been implemented, which directly relates to the reports that have been published as part of the initiative, is given in Chapter 6. The reports help to provide both the PSA and the industry with a *knowledge base* for their work relating to security; see the government's expectation no. 3 in section 3.2.

4 General considerations concerning the petroleum regulations

4.1 Roles and responsibilities of the PSA

The description below of the PSA's roles and responsibilities[7] is an extract from the Crown Prince Regent's decree concerning the roles and responsibilities of the new Norwegian Petroleum Directorate (19 December 2003). The PSA was established with effect from 1 January 2004.

The PSA's remit is to set the agenda and carry out monitoring to ensure that players in the petroleum industry maintain high standards with regard to health, safety, environment and preparedness, and thereby help to maximise value creation for society. The follow-up should be system-oriented and risk-based. The follow-up should be in addition to, rather than instead of, the follow-up that the industry carries out concerning its own activities. A balance must be struck between the role of the PSA as regards high-risk/technology supervision and work-related supervision. Participation and partner cooperation are important prerequisites and principles in the work of the PSA.

The PSA will also drive the work relating to information dissemination and advisory work with respect to players in the industry, establish appropriate cooperative relationships with other HSE authorities both nationally and internationally, and actively contribute to knowledge transfer within the field of health, safety and environment in society generally. The PSA can supplement its own competence by drawing on expertise from other government agencies, institutions and companies which possess specialist expertise, in accordance with established cooperation agreements.

The PSA is responsible for conducting supervision relating to safety, preparedness and the working environment, and for performing the task of coordinating authority on behalf of the HSE authorities for the petroleum industry on the Norwegian continental shelf (approximately 80 fixed facilities, 60 rigs, 300 seabed facilities and 15,400 km of subsea pipelines) and for the collective operations on eight onshore facilities (Kårstø, Kollsnes, Sture, Tjeldbergodden, Mongstad, Melkøya, Nyhamna and Slagentangen).

The regulations require effective preparedness to be maintained at all times with a view to managing hazard and accident situations which could result in loss of life or injury, pollution or major material damage, including damage caused by terrorism, sabotage, etc.

The PSA has been delegated authority to establish more detailed regulations regarding safety and working environment in the industry, and to make individual administrative decisions in the form of permits and consents, orders, coercive fines, suspension of operations, bans, exemptions, etc.

The PSA will be the competent authority as regards technical and operational safety, including preparedness, and as regards working environment at every stage of the operation; and in connection with planning, project engineering, construction, use and any subsequent removal.

4.2 Principles (function-based, risk-based, etc.)

The HSE regime in the Norwegian petroleum industry primarily applies functional principles and is based on internal control, where companies have an independent responsibility to safeguard HSE considerations through internal management systems and processes. This entails requirements concerning risk analysis, the

[7] In addition, with effect from 17 August 2020, the PSA was delegated administrative responsibility for Act No. 21 of 4 June 2010 on offshore renewable energy production (the Offshore Energy Act), Section 5-1.

establishment of risk acceptance criteria, risk assessment and evaluation, risk management and mitigation; ref. the Engen Committee.[8]

The fact that the regulations are function-based can be seen as an overarching principle, which further entails a need for it to also be risk-based. The Engen Committee also notes that, in an international context, it is recognised that a risk-based, functional and goal-oriented regulatory framework is an effective way of regulating industries with the potential for major accidents.

Function-based

HSE regulations for the petroleum sector are largely formulated in the form of functional requirements. Unlike detailed provisions which stipulate requirements regarding specific practices and actions, functional requirements specify the results that are to be achieved, without specifying how. One of the aims behind the function-based approach is to avoid detailed regulatory provisions and highlight the responsibilities of players to identify solutions, and thereby facilitate flexibility as regards the choices of methods, procedures and technological development. This flexibility constitutes the room for manoeuvre in the regime. This room for manoeuvre enables the parties to challenge both each other and the authorities with regard to the interpretation and follow-up of frameworks and opportunities. However, the regulations are more prescriptive in certain areas. Prescriptive provisions are primarily used to regulate areas where a particular solution is desirable, or to eliminate the possibility of any doubt over minimum requirements, ref. the Engen Committee.

Risk-based

The term *risk-based* is widely used, but it does not entail an approach that is based solely on analyses and assessments of risk for the decisions that are taken. To emphasise this, the term *risk-informed* is sometimes used, including in the PSA's memorandum on *Integrated and unified risk management in the petroleum industry* (2018). In this memorandum, it is noted that the risk management and regulatory framework are based on three main categories of approaches to risk, which are: risk-informed corporate governance, the precautionary principle and the principle of "be prepared", and a dialogue between decision-makers, experts and executive personnel.

The precautionary principle applies precisely because the risk assessments are imperfect. Many requirements in the regulations, and attention to knowledge and uncertainty in assumptions, are therefore based on the precautionary principle. An example of regulations being precaution-based is that it is not permissible to disregard specific requirements, e.g. the requirement for a fire barrier between main areas. The regulations therefore contain a number of specific requirements regarding robustness. "Be prepared" is a special case of the precautionary principle. Reference is made to this in the guidelines to the Framework Regulations, Section 11 *Risk reduction principles*, where the term "risk", including uncertainty, is also described. Reference is also made here to the requirement to use best available technology, known as "the BAT principle".

Other principles

During its review of the overarching requirements and principles of the regulatory regime in the petroleum industry, the Engen Committee notes that it follows from the Petroleum Act that the petroleum industry must operate in a prudent manner, and that the organisation of licensees in Norway must have a structure and size which ensures that the licensee can take informed decisions about its operations at all times.

These are two of the principles included in Chapter II of the Framework Regulations — *Basic requirements for health, safety and the environment (Sections 9-16)*. The Framework Regulations, Section 9 *Application of the principles in Chapter II* notes that this concerns *principles* . This includes:

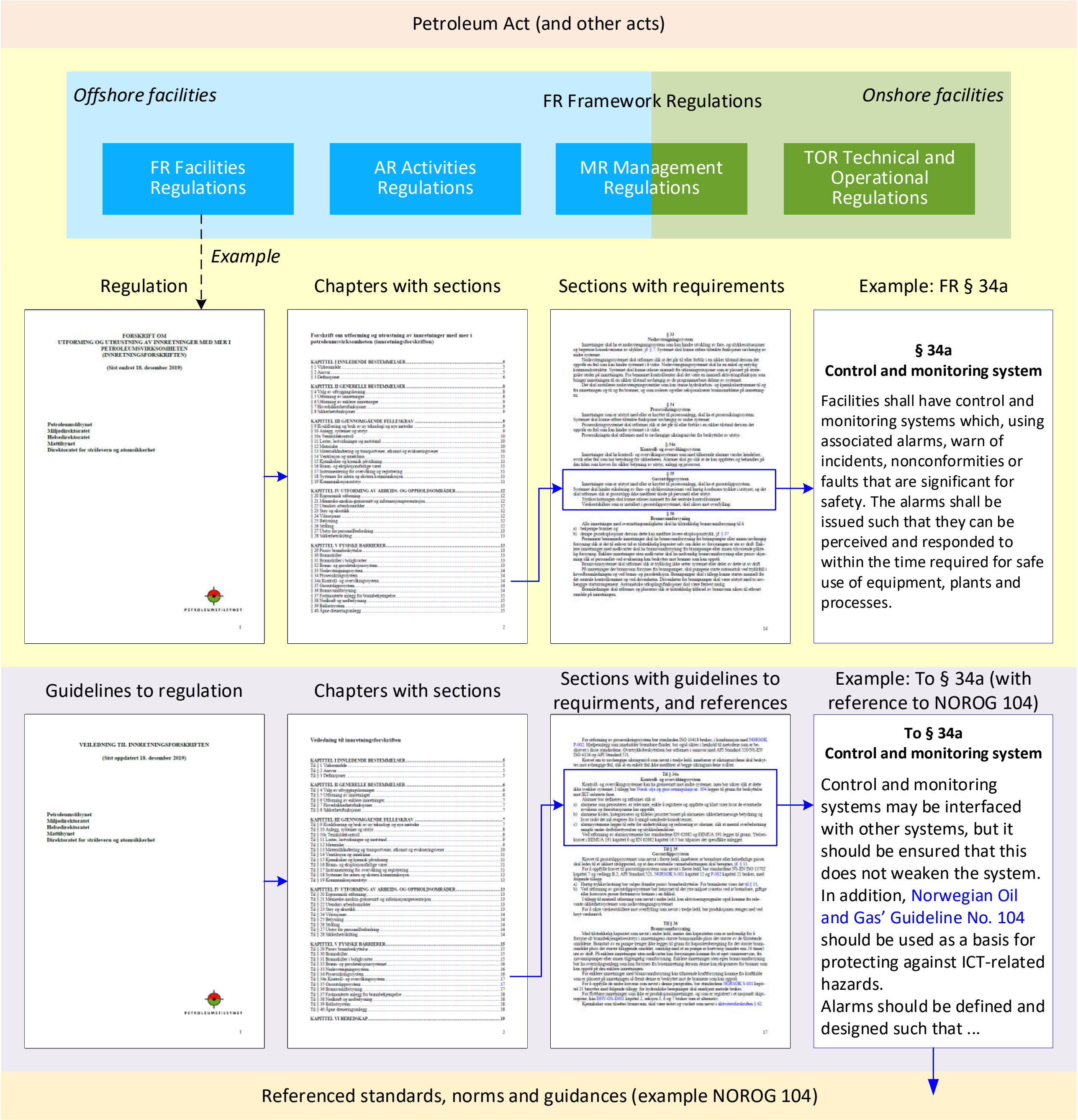
[8] *Helse, arbeidsmiljø og sikkerhet i petroleumsvirksomheten*. Rapport fra partssammensatt arbeidsgruppe, 09/2017. (*Health, working environment and safety in the petroleum industry*. Report from the party-composed working group.)

Framework Regulations, Section 10 Prudent activities
Framework Regulations, Section 11 Risk reduction principles
Framework Regulations, Section 12 Organisation and competence
Framework Regulations, Section 13 Facilitating employee participation
Framework Regulations, Section 14 Use of the Norwegian language
Framework Regulations, Section 15 Sound health, safety and environment culture
Framework Regulations, Section 16 Health-related matters

In addition to prudent operations (see Section 10 of the Framework Regulations), there is also a requirement for continuous improvement; see the Management Regulations, Section 6 *Management of health, safety and the environment*, and the Management Regulations, Section 23 *Continuous improvement.*

4.3 Structure and references (standards, norms and guides)

Figure 4 shows the structure of the regulations, with five Regulations pursuant to the Petroleum Act (and a number of other laws) and guidelines to the Regulations, as well as references to standards, norms and guides.


Petroleum Act (and other acts)
Offshore facilities
FR Framework Regulations
Onshore facilities
FR Facilities Regulations
AR Activities Regulations
MR Management Regulations
TOR Technical and Operational Regulations
Example
Regulation
Chapters with sections
Sections with requirements
Example: FR § 34a
Guidelines to regulation
Chapters with sections
Sections with guidelines to requirments, and references
Example: To § 34a (with reference to NOROG 104)
Referenced standards, norms and guidances (example NOROG 104)

§ 34a
Control and monitoring system

Facilities shall have control and monitoring systems which, using associated alarms, warn of incidents, nonconformities or faults that are significant for safety. The alarms shall be issued such that they can be perceived and responded to within the time required for safe use of equipment, plants and processes.

To § 34a
Control and monitoring system

Control and monitoring systems may be interfaced with other systems, but it should be ensured that this does not weaken the system. In addition, Norwegian Oil and Gas' Guideline No. 104 should be used as a basis for protecting against ICT-related hazards.
Alarms should be defined and designed such that ...

Figure 4 Structure of the regulations and references to standards, norms and guides

The Framework Regulations (RF) overarch the other regulations, i.e. the Management Regulations (SF), the Facilities Regulations (IF), the Activities Regulations (AF) and the Technical and Operational Regulations (TOF). The Framework Regulations and Management Regulations apply to both offshore and land, the Facilities Regulations and Activities Regulations to offshore facilities, and the Technical and Operational

Regulations to onshore facilities. The illustration of the five Regulations in Figure 4 is based on the corresponding figure in DNV GL report *Regelverk og tilsynsmetodikk (Regulations and auditing methodology)* (2020).

The five Regulations cover the areas of responsibility of a number of authorities and must be viewed in context with each other. In addition, the PSA enforces six common Regulations pursuant to the Working Environment Act. Each of these Regulations consists of a number of chapters with sections, which in turn consist of one or more requirements (*"shall"*), e.g., two requirements in the Facilities Regulations, Section 34a *Control and monitoring system*.

Guidelines to the Regulations show how the provisions of a Regulation *can* be met. The Regulations and guidelines must be viewed in context in order to obtain the best possible understanding of how the regulatory requirements are to be met.

In certain areas, the guidelines refer to industry standards as a recommended way of fulfilling the requirements of the Regulations. The guidelines to the Regulations are not legally binding and players are therefore free to adopt other solutions. If a responsible player opts to adopt a recommended solution, it can normally be assumed that the requirements of the Regulations are met. If a player adopts other solutions, such as different standards or company-specific procedures, they must be able to document that the adopted solutions are at least as good as, if not better than, the recommended ones. This is explained in the Framework Regulations, Section 24 *Use of recognised standards*.

An example of a reference (*"should"*) can be found in the guidelines to the Facilities Regulations, Section 34 a *Control and monitoring system*, where reference is for example made to NOROG 104. See section 5.2 for other relevant standards which players *may* refer to, but must then document that the standard concerned is at least equivalent to NOROG 104.

The web-based version of the regulations (https://www.ptil.no/regelverk/alle-forskrifter/) also includes a link to *interpretations* of (certain sections of) the Regulations. These interpretations are presented collectively for each Regulation. In addition, there is a link to audit reports with non-conformities with respect to the relevant section.

4.4 The companies' responsibilities and the PSA's expectations

Like other areas of Norwegian working life, it is the companies themselves that are responsible for the level of HSE within their organisation. Operators and licensees are also subject to a special obligation to ensure that everyone performing work on their behalf complies with the requirements laid down in applicable health, environmental and safety legislation (the "see to it" duty).[9]

The petroleum regulations require players to establish the necessary management systems to ensure compliance with applicable regulations at every stage of their operation. This means that the players must organise their operations to ensure and verify that their operations are planned, executed and maintained in accordance with the regulatory framework established by the authorities. Follow-up by the authorities is to be in addition to, rather than instead of, the players' own follow-up (Engen Committee, 2017).

Responsibilities and expectations aimed specifically at safeguarding ICT security in industrial ICT systems are described in section 5.5.

[9] See Section 10-6 of the Petroleum Act on the duty to ensure compliance with provisions, and the Framework Regulations, Section 7 *Responsibilities pursuant to these regulations.*

5 ICT security in the petroleum regulations

5.1 Overview

ICT is not specifically mentioned in the Petroleum Act, and the regulations (the Regulations) are function-based, with ICT security being covered on a general basis, but only being explicitly mentioned to a limited extent. Exceptions are the guidelines to Section 29 of the Management Regulations, which include ICT incidents, and the guidelines to Section 34a of the Facilities Regulations, which refer to NOROG 104 (see section 4.3).

The PSA has informed the industry of a number of sections which are relevant to ICT security[10]. These are shown in Table 2, together with the sections that the Holte Committee (NOU 2018: 14) considered to be the most relevant provisions, and input from DNV GL (*Regelverk og tilsynsmetodikk*, 2020 (*Regulations and audit methodology*, 2020) concerning the sections that should include ICT security.

The Holte Committee discusses the "most relevant regulations", without indicating that these should address ICT security explicitly, while the PSA gives its understanding of how ICT security is relevant to 11 sections. DNV GL refers to 26 sections where it is relevant to incorporate the PSA's clarifications, the need for further clarifications, the highlighting of ICT security, or references to standards and guidelines.

The provision of advice and guidance concerning which sections of the Regulations and requirements are particularly relevant to ICT security is in line with the expectations and recommendations of the overarching authority; see section 3.2. However, challenges arise if only a few requirements are mentioned. This does not mean that all other sections and requirements are irrelevant — the companies themselves must still have a unified understanding of the regulations.

Similarly, it is challenging to select the sections where ICT security should be explicitly included in the regulations, both in relation to this being "complete" and the fact that other sections may be perceived as being less important for ICT security. At the same time, ICT security (ICT incidents/hazards) has already been incorporated into two sections, and the Lysne Committee (NOU 2015: 13) was clear that requirements regarding ICT security should be made clear in Regulations.

5.2 References (ICT standards, norms and guides)

In the current regulations, NOROG 104 is the only ICT-related reference to standards, norms or guides. Reference is made to NOROG 104 from the guidelines to the Facilities Regulations, Section 34 a *Control and monitoring system*, and correspondingly in the guidelines to TOF, Section 33a for onshore facilities.

Here, the following is stated in the first paragraph: *"Control and monitoring systems may be interfaced with other systems, but it should be ensured that this does not weaken the system. In addition, Norwegian Oil and Gas' Guideline No. 104 should be used as a basis for protecting against ICT-related hazards."*

[10] In a letter dated 18.9.2019 *Informasjon om håndtering av IKT-sikkerhetshendelser (Information on the handling of ICT security incidents).* See Appendix 2.

Table 2 Assessments of ICT security in the petroleum regulations

Regulation		NOU 2018: 14	PSA	DNV GL
SF	**Management Regulations**			
Section 4	Risk reduction	x	x	x
Section 5	Barriers			x
Section 7	Objectives and strategies	x		
Section 8	Internal requirements		x	x
Section 14	Manning and competence - guidelines			x
Section 17	Risk analyses and emergency preparedness assessments	x		x
Section 25	Consent requirements for certain activities			x
Section 29	Notification and reporting of hazard and accident situations to the supervisory authorities - guidelines	x	x	x
IF	**Facilities Regulations (Technical and Operational Regulations - TOF)**			
Section 8	Safety functions – guidelines (TOF, Section 10)			x
Section 9	Qualification and use of new technology and new methods (TOF Section 9)			x
Section 18	Systems for internal and external communication — guidelines (TOF, Section 22)			x
Section 32	Fire and gas detection system — guidelines (TOF, Section 32)		x	x
Section 33	Emergency shutdown system — guidelines (TOF, Section 33)		x	x
Section 34	Process safety system — guidelines (TOF, Section 34)		x	x
Section 34a	Control and monitoring system – guidelines (TOF, Section 33a)		x	x
AF	**Activities Regulations (Technical and Operational Regulations - TOF)**			
Section 21	Competence		x	x
Section 23	Training and drills		x	x
Section 26	Safety systems – guidelines			x
Section 45	Maintenance		x	x
Section 46	Classification — guidelines (TOF, Section 59)			x
Section 47	Maintenance programme – guidelines			x
Section 48	Planning and prioritisation		x	x
Section 73	Establishment of emergency preparedness – guidelines (TOF, Section 64)			x
Section 74	Shared use of emergency preparedness resources – guidelines			x
Section 75	Emergency preparedness organisation – guidelines (TOF, Section 65)			x
Section 76	Emergency preparedness plans – guidelines (TOF, Section 66)	x		x
Section 77	Handling hazard and accident situations (TOF, Section 67)	x		x

There is an ongoing debate within the industry concerning regulatory references to other ICT-related standards, norms and guides. This applies in particular to the IEC 62443 series (standards and technical reports which define procedures for implementing secure industrial automation and control systems (IACS/OT)), within security as a parallel to IEC 61508/61511[11] within security and an associated guideline, such as DNVGL-RP-G108 or similar, as a parallel to NOROG 070[12]. This is discussed in several of the reports published as part of the initiative relating to ICT security; see section 6.3.

Not all parts of the IEC 62443 series have yet been published as final editions, and the PSA is monitoring the development of both this and other industry standards to which reference may be made in the regulations.

5.3 ICT security, risk management and barrier management

The memoranda entitled *Integrated and unified risk management in the petroleum industry* (2018) and *Principles of barrier management in the petroleum industry* (2017) put forward views and guidelines from the PSA - "express the PSA's stance" - although it should be noted that they do not form part of the regulations, nor do they introduce any new requirements. Both memoranda mention ICT security.

Integrated and unified risk management in the petroleum industry

Good processes for managing risk are a prerequisite if the function-based regulatory framework is to be effective. Risk management must include security risks: *"In a unified approach to risk management, security risk (intentional undesirable incidents) is one of several considerations an organisation must take into account. Knowledge of intentional undesirable incidents as a phenomenon, and methods for implementing security measures, must form part of unified risk management."*

"A challenge many face today is that a divide runs not only between security and other disciplines, but also within the security discipline. Such divides have been seen between discipline areas for physical security, personnel security, IT (office networks) and industrial process and security systems (operational technology – OT). This has prevented a unified understanding of security-related risk."

The memorandum discusses the importance of assessing and taking account of uncertainty. Here, it is noted that, in security risk analyses, few players currently describe the knowledge strength or uncertainty, which creates an unrealistic picture of risk and leads to decisions being made on the wrong basis. For example, it is concluded that serious security incidents have such a low probability that they are disregarded, even if the underlying knowledge is weak.

Management behaviour is of great importance in a sound safety culture. The PSA refers to organisations where the management has put security on the agenda to ensure that it receives the necessary attention, and helps to ensure that continuous efforts are made to identify and manage risks associated with intentional undesirable acts.

Principles for barrier management in the petroleum industry (the barrier memorandum)

The Management Regulations, Section 5 *Barriers* require barriers to be established in order to identify circumstances which could lead to, or reduce the possibility of, errors and hazard and accident situations. ICT incidents (cyberattacks) are not mentioned explicitly as examples in the guidelines to Section 5 of the Management Regulations, but the barrier memorandum shows that the PSA includes ICT incidents. In the most recent version of the memorandum (2017), security is included as an area of application, with examples presented in the appendix. Figure 5 shows the principles for barriers used for security purposes.

[11] IEC 61508 (2010). *Functional safety of electrical/electronic/programmable electronic safety related systems*.
IEC 61511 (2016). *Functional safety of safety instrumented systems for the process industry sector*.

[12] NOG 070 (2018). *Guidelines for the Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements)*, June 2018.

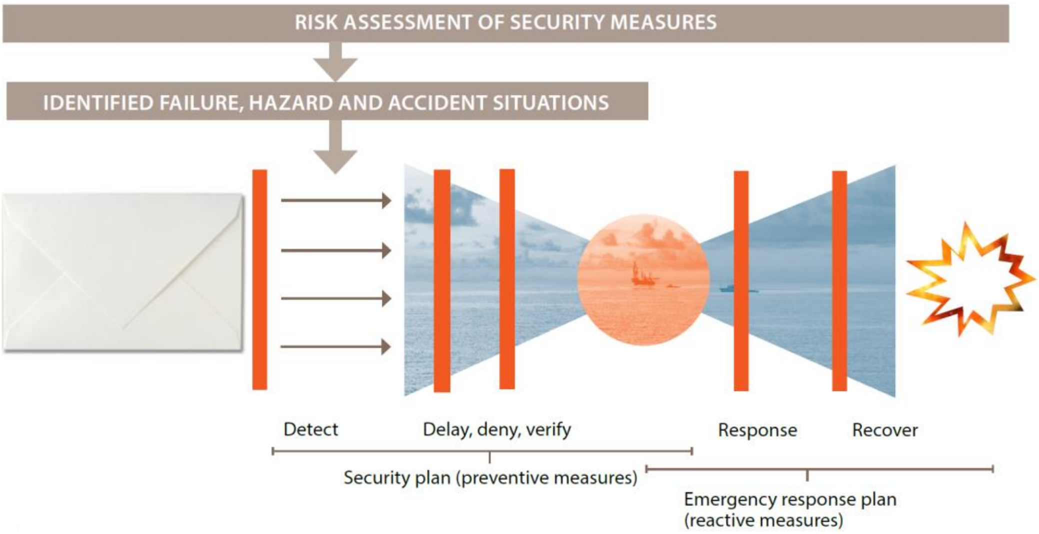

RISK ASSESSMENT OF SECURITY MEASURES
IDENTIFIED FAILURE, HAZARD AND ACCIDENT SITUATIONS
Detect
Delay, deny, verify
Response
Recover
Security plan (preventive measures)
Emergency response plan
(reactive measures)

Figure 5 Barriers used for security purposes (PSA, 2017)

"Examples of barrier functions within security include deterring, detecting, delaying, denying and verifying the existence of an attack, responding to the threat, and restoring functionality. The security plan primarily covers preventive and protective measures, or probability-reducing measures (such as reducing vulnerability), while the emergency preparedness plan covers the reactive and consequence-reducing measures. However, there will be some overlap between these two plans, as well as measures which take place simultaneously." (PSA, 2017).

It is noted that applying the principles for barrier management with regard to security incidents contributes to a more systematic approach to the actual identification, establishment and maintenance of the barriers.

5.4 ICT security and incidents (DSHAs)

Emergency preparedness is dimensioned on the basis of a set of defined situations of hazard and accident situations (DSHAs), which constitute a representative selection of hazard and accident situations; see the Activities Regulations, Section 73 *Establishment of emergency preparedness*. Drills for these must be carried out in the form of emergency preparedness drills. However, the regulations contain no fixed list of hazard and accident situations which either should or must be included as DSHAs, neither ICT incidents nor other incidents.

The regulations (Section 73 of the Activities Regulations) note that the selection of DSHAs must be *representative*. This is not something that is static, but is influenced by technological developments, societal developments and trends in the risk/threat picture; see section 3.1. The list of DSHAs for which action plans have been established in the contingency plan must be seen as a *dynamic* list which is updated as and when necessary, so that it is representative at all times. This applies to both ICT incidents and other incidents (such as the loss of external communication networks/emergency communication; see SINTEF, 2021. *Communication systems for external emergency communication*.).

ICT incidents differ from many other DSHAs in that those dealing with such an incident on board a facility (or onshore facility) rely more heavily on assistance from expertise onshore, internally or external response environments.

According to DNV GL, about half of petroleum operators have defined a specific DSHA for security incidents in industrial ICT systems, and numerous players say they believe it would have been useful to have an established DSHA.[13]

In addition to emergency preparedness drills linked to DSHAs, there are requirements regarding training and drills; see the Activities Regulations, Section 23 *Training and drills*. Requirements regarding training and drills for the handling of ICT incidents are not explicitly included in the regulations, as is the case with most other topics linked to ICT security, as noted in section 5.1. ICT security applies generally, where relevant. However, the PSA has clarified that Section 23 *Training and drills* of the Activities Regulations also includes ICT incidents: *The requirement concerning training and drills is also relevant to those who will deal with hazard situations in relation to ICT incidents with the industrial control and safety systems and interact with response environments."* [14]

5.5 Companies' responsibilities regarding ICT security and the PSA's expectations

Operators have a special responsibility to carry out their operations in a prudent manner and in accordance with applicable regulations. They must ensure that everyone who performs work on their behalf complies with the HSE regulations (the "see to it" duty, see section 4.4). The "see to it" duty is in addition to each individual company's duty to comply with applicable regulations. This means, for example, that operators have a responsibility to follow up to ensure that suppliers of OT systems comply with the regulations.

Despite increasing automation, the industry will be very dependent on humans in order to monitor systems and intervene if the technology fails. Systems and equipment must be designed with the aim of regaining control. Digitalisation can contribute to simplification and better support for decision-making for the personnel involved, but it can also lead to changes in roles and responsibilities and the introduction of new competence requirements for personnel. The responsible party must ensure that executive personnel possess the necessary skills adapted to changing tasks and new technologies, and that sufficient time is set aside for training and drills.

[13] DNV GL report *Trening og Øvelser* (*Training and Drills*) (2020).

[14] In a letter dated 18.9.2019 *Informasjon om håndtering av IKT-sikkerhetshendelser (Information on the handling of ICT security incidents).*

6 ICT security – Robustness in the petroleum sector

6.1 Overview and timeline

During the first three years of the initiative *ICT security — Robustness in the petroleum sector* (2018-2021), a total of 18 reports have been prepared for the PSA by IRIS, DNV GL and SINTEF, as illustrated in Figure 6. The reports are listed in Table 3 (oldest reports at the top, corresponding from left to right in Figure 6).

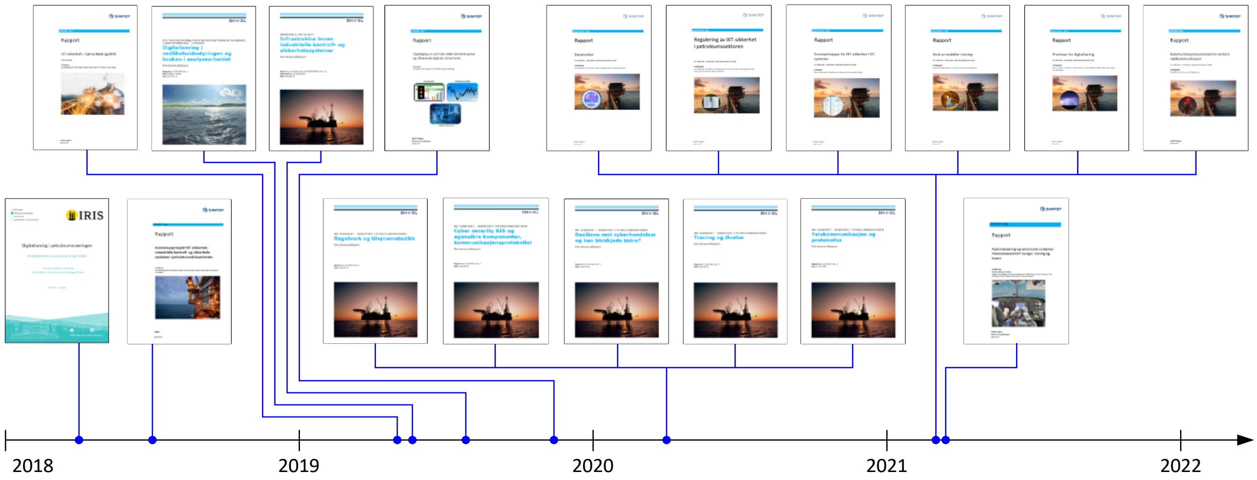


Figure 6 Knowledge reports prepared for the PSA under the ICT security initiative 2018-2020[15]

Table 3 Knowledge reports — report titles, responsible publisher and date

No.	Title	Publisher	Date
1	Digitization in the petroleum industry	IRIS	Mar. 2018
2	Industrial control and safety systems in the petroleum industry)	SINTEF	May 2018
3	HSE and Cyber Security in Remote Work	SINTEF	Apr. 2019
4	Digitalisation in maintenance management and use in analysis work	DNV GL	Apr. 2019
5	Infrastructure in industrial control and security systems	DNV GL	Jun. 2019
6	Follow-up of core safety functions and associated digital vulnerabilities	SINTEF	Nov. 2019
7	Regulations and audit methodology	DNV GL	Feb. 2020
8	Cyber security SIS and intrinsically secure components, communication protocols	DNV GL	Feb. 2020
9	Resilience to cyber incidents and can blockchain contribute?	DNV GL	Feb. 2020
10	Training and Drills	DNV GL	Feb. 2020
11	Telecommunication and protocols	DNV GL	Feb. 2020
12	Data quality in digitalisation processes in the petroleum sector	SINTEF	Jan. 2021
13	Regulation of ICT security in the petroleum sector – *this report*	SINTEF	Jan. 2021
14	Core principles of ICT security in industrial ICT systems	SINTEF	Jan. 2021
15	Use of models in drilling	SINTEF	Jan. 2021
16	Principles of digitalisation and IT-OT integration	SINTEF	Jan. 2021
17	Communications systems for external emergency communication	SINTEF	Jan. 2021
18	Automation and autonomous systems: Human-centred design in drilling and wells	SINTEF	Jan. 2021

[15] The DNV GL reports 2019 were published in early 2020, the SINTEF reports for 2020 were published in early 2021.

6.2 Obtained new knowledge

6.2.1 Brief review

The contents of the individual reports are briefly described in Table 4. This is partly based on the descriptions provided on the PSA's website.

Table 4 Knowledge reports — brief description of content

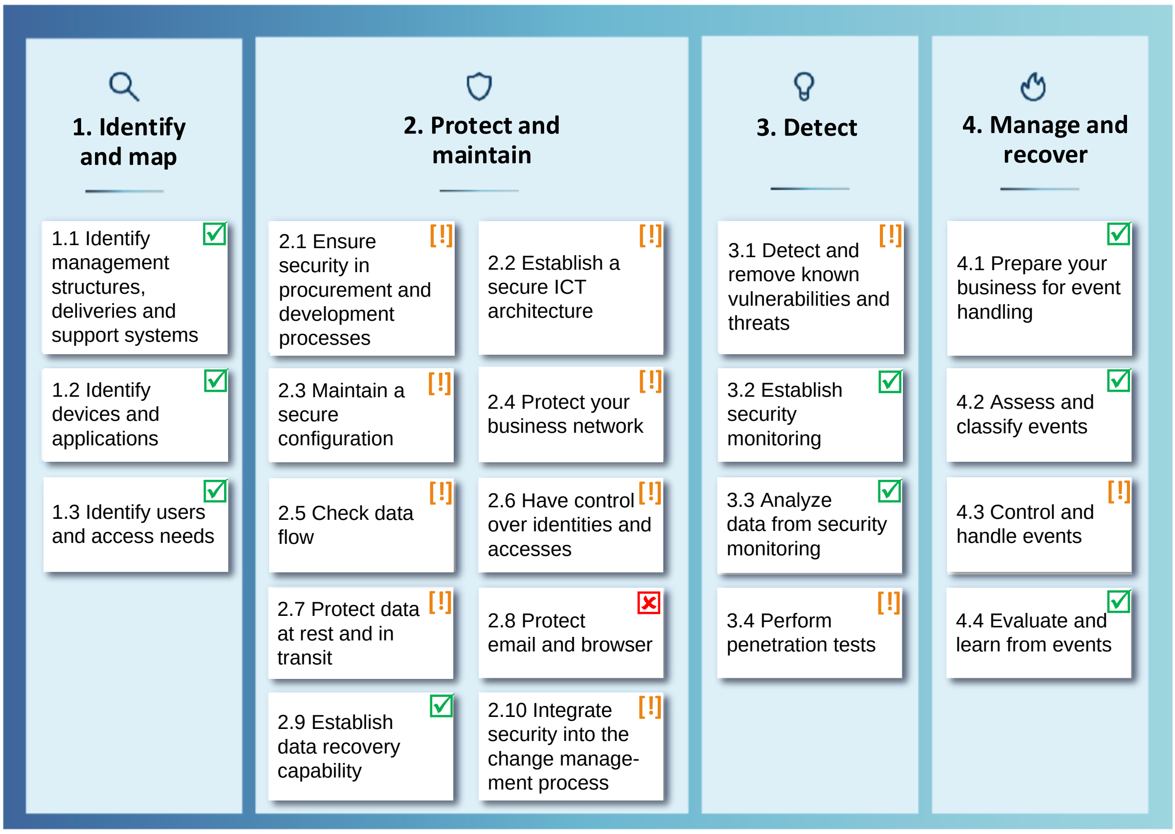
No.	Title and content
1	**Digitalisation in the petroleum industry (IRIS, 5 March 2018)** This report summarises and analyses knowledge regarding the positive and negative impacts of digitalisation on health, safety and the environment (HSE) in the petroleum industry. The main aim of this project is to provide a greater understanding of the development trends within digitalisation and their consequences for people, technology and organisation, and to make recommendations regarding strategies and measures to follow these up.
2	**Industrial control and safety systems in the petroleum industry (SINTEF, 29 May 2018)** This report is based on the changes/drivers that affect the risk picture within industrialised control technology (ICT) on facilities on the Norwegian shelf. The purpose of the report is to provide a greater understanding of the players' own and sector-based follow-up to ICT security. The report summarises key impressions from interviews with experts, including experts in the national and international response environment for ICT security (CSIRT/CERT). The report also provides an overview of relevant standards and associated regulations, as well as relevant audit methods for the PSA and the companies themselves.
3	**HSE and Cyber Security in Remote Work (SINTEF, 5 April 2019)** The principal aim of this report is to present knowledge concerning the use of remote working on the shelf. The report examines HSE consequences relating to remote working on facilities, onshore facilities and drilling rigs. The main focus is on work processes, procedures and organisation. The report also provides an overview of regulations and guidelines in the area. The report focuses on operational technology, i.e. technology that supports, controls and monitors industrial production, control and safety functions.
4	**Digitalisation in maintenance management and use in analysis work (DNV GL, 11 April 2019)** The report compiles information about the status and challenges in relation to digitalisation in the petroleum activities based on a document review and a meeting with selected companies. This provides a basis for selecting issues to investigate further in a full study. It also provides a knowledge base for potential use both internally within the PSA and in the industry.
5	**Infrastructure in industrial control and security systems (DNV GL, 21 June 2019)** The report presents an overview of infrastructure within industrial control and safety systems which are used for the management and monitoring of various processes and systems on both fixed and mobile facilities and onshore facilities. The report describes the complexity of these systems, lifespan, infrastructure structure and interfaces with various types of networks, including communication protocols from instrument/sensor level to management and control level (HMI). The report also contains a discussion of the development and possible impact that the Industrial Internet of Things (IIoT) and other trends could have on such systems when these are connected to the network structure.
6	**Follow-up of core safety functions and associated digital vulnerabilities (SINTEF, 7 November 2019)** The report collates information on the availability of data on condition and risks, condition monitoring of early fault development, and vulnerabilities due to digital solutions which could impact on safety. The objective of the project is to help the industry improve its follow-up of its own requirements concerning the status of technical, operational and organisational functions of importance for safety, and ensure that they continue to maintain the required performance at every stage of their life.
7	**Regulations and audit methodology (DNV GL, 24 February 2020)** The aim of this subproject was to assess whether the PSA's regulatory framework, in its current form, is appropriate in relation to the topic of ICT security and the threat picture within this field. A further aim was to assess whether the methodology that the PSA employs to carry out audits of ICT security is appropriate given the scope of audit objects and the threat picture.
8	**Cyber security SIS and intrinsically secure components, communication protocols (DNV GL, February 21, 2020)** This subproject considered ICT security in Safety Instrumented Systems (SIS) and how ICT security is built into the design of such systems and safeguarded in commissioning and operation. A key aspect of the delivery was to assess how the

No.	Title and content
	security principles described in IEC 61508/511 and IEC 62443 are addressed. The part-delivery also describes trends and developments in industrial ICT systems relating to network-based components.
9	**Resilience to cyber incidents and can blockchain contribute? (DNV GL, 21 February 2020)** The report explains how resilience, and associated methods, can be applied to make ICT security linked to industrial ICT systems more robust. A discussion is also presented of whether the principles of ICT security can be applied in relation to blockchain technology, and how security can be safeguarded and possibly strengthened through blockchain implementation. The report also includes a discussion of whether, on the basis of current information and available research, blockchain can make a positive contribution to the structure of resilience and enable new methods to promote cyber security relating to industrial ICT systems (OT) and at the intersection between IT and OT.
10	**Training and Drills (DNV GL, 21 February 2020)** This report makes recommendations regarding requirements and best practice linked to training and drills, including emergency preparedness for ICT security incidents which are aimed at industrial ICT systems. The divide between industrial ICT and IT is challenged, and it is noted that an attack on administrative IT systems in an office network could be a springboard towards industrial ICT systems. Digitalisation is causing information from industrial ICT systems to become increasingly available in office systems. The report therefore also makes recommendations aimed at IT systems which will indirectly impact on the company's industrial ICT systems.
11	**Telecommunications and protocols (DNV GL, 24 February 2020)** The report describes challenges and risks in current telecommunications solutions. Trends in telecommunications which could impact on security in the petroleum sector in the coming years are described. Possible measures to enhance the robustness of telecommunications solutions are discussed. There is a focus on telecommunication systems of relevance to the technical installations, both onshore and offshore, as well as circumstances concerning humans, environment and security. Systems which DNV GL believes are associated with special security challenges are discussed more thoroughly than others.
12	**Data quality in digitalisation processes in the petroleum sector (SINTEF, January 2021)** The purpose of this report is to examine what data sources and data are used in industrial ICT systems and how data is processed and processed before it is made available in the office network. Strengths and vulnerabilities relating to data quality and the securing of data are discussed. Data quality is about having access to the right data when it is needed. Data quality in ICT systems is affected by many factors. Some examples are data integrity, accuracy in data acquisition, reliability in data transfer, environment, etc.
13	**Regulation of ICT security in the petroleum sector (SINTEF, January 2021)** –– *this report* The purpose of this report is to clarify how ICT security in the petroleum industry is regulated under current regulations, including reference to recognised standards, norms and guides. The report also sheds light on the expectations of the authorities, and presents an overview and status of the initiative relating to ICT security in the petroleum industry in recent years. The report aims to help companies in the petroleum industry further develop their own practices relating to ICT security in industrial ICT systems within the framework of current regulations. It can also be used as a basis for a PSA memorandum on ICT security.
14	**Core principles of ICT security in industrial ICT systems (SINTEF, January 2021)** The main aim of this report is to provide the industry with a greater understanding of how it can apply NSM's core principles for ICT security (version 2.0) in industrial ICT systems in the petroleum industry. Relevant aspects of the Norwegian Water Resources and Energy Directorate's Power Preparedness Regulations are also assessed, and individual measures are identified in the NIST CyberSecurity Framework (CSF) which are not covered by the core principles, but are relevant to OT systems.
15	**Use of models in drilling (SINTEF, January 2021)** The purpose of this report is to discuss challenges and opportunities associated with the use of model-controlled operations, particularly regarding how the models and data from the models can be used securely and how ICT security is safeguarded. The main focus is on drilling operations. The report summarises knowledge and recommendations concerning the secure use of model-controlled drilling operations. Particular emphasis is placed on the quality assurance of models and data from models, as well as ICT security and communications between software solutions in drilling operations.
16	**Principles of digitalisation and IT-OT integration (SINTEF, January 2021)** The aim was to describe and assess how digitalisation and the use of cloud services affect industrial ICT systems, and the security solutions that must be implemented to ensure the secure use of cloud services. The PSA's regulations are particularly based around the principle of segregation and independence as strategies for establishing safety and security.

No.	Title and content
	This report puts the spotlight on the ongoing digitalisation of both old and new facilities and is based on information obtained from drilling companies and operators.
17	**Communications systems for external emergency communications (SINTEF, January 2021)** The purpose of this report is to provide the industry with a greater understanding of the role and vulnerability of communications networks, particularly in emergency preparedness situations when a defined situation of hazard and accident (DSHA) has occurred. The report puts the spotlight on external communication between sea and land in emergency preparedness situations, i.e. emergency communication with the land.
18	**Automation and autonomous systems: Human-centred design in drilling and wells (SINTEF, January 2021)** The report summarises knowledge concerning human factors in the development, testing, implementation and use of new automated technology/autonomous systems that will be useful/critical for drilling and well operations. This report collates knowledge and experience relating to automated systems in both the petroleum industry and other industries. Relevant regulations and standards for the petroleum industry are assessed.

6.2.2 Explanatory example — NSM's core principles adapted to OT systems

Core principles of ICT security in industrial ICT systems (report no. 14 in Table 4) is an example of a knowledge base which has been obtained as part of the ICT security initiative. The results are summarised in Figure 7.



1. Identify and map

1.1 Identify management structures, deliveries and support systems ✓

1.2 Identify devices and applications ✓

1.3 Identify users and access needs ✓

2. Protect and maintain

2.1 Ensure security in procurement and development processes [!]

2.2 Establish a secure ICT architecture [!]

2.3 Maintain a secure configuration [!]

2.4 Protect your business network [!]

2.5 Check data flow [!]

2.6 Have control over identities and accesses [!]

2.7 Protect data at rest and in transit [!]

2.8 Protect email and browser ☒

2.9 Establish data recovery capability ✓

2.10 Integrate security into the change manage-ment process [!]

3. Detect

3.1 Detect and remove known vulnerabilities and threats [!]

3.2 Establish security monitoring ✓

3.3 Analyze data from security monitoring ✓

3.4 Perform penetration tests [!]

4. Manage and recover

4.1 Prepare your business for event handling ✓

4.2 Assess and classify events ✓

4.3 Control and handle events [!]

4.4 Evaluate and learn from events ✓

Figure 7 Relevance of NSM's core principles for ICT security for industrial ICT systems

One of the aims was to assess the extent to which the measures contained in NSM's core principles for ICT security version 2.0 are relevant to industrial ICT systems (OT systems) in the petroleum industry. The conclusion is that, although NSM's core principles of ICT security are broadly ("80 percent") also relevant to OT systems, there are certain measures which need to be adapted or expanded in order to fully meet the need.

Each of the 21 core principles shown in Figure 7 contains between three and ten measures. If all measures within a core principle are entirely relevant to OT systems, this is indicated by ☑; if one or more measures are only partially relevant to OT systems or require further action, this is indicated by [!], while if one or more measures are not relevant to OT systems, this is indicated by ☒. Only one (2.8 *Protect email and browser*) of the 21 core principles is not relevant to OT systems, and for many of the 11 core principles that are only partially relevant, only one or a few measures are not relevant. In total, 96 out of 118 measures are relevant to OT in their entirety.

These core principles of ICT security in OT systems are particularly interesting based on the assessment of what constitutes *prudent* ICT security in NOU 2018: 14 *ICT security at every stage*, where the Holte Committee interprets "prudent" as a minimum level of security and considers that prudent ICT security is expressed clearly in NSM's core principles for ICT security. The committee claims that a company that adheres to these principles will have prudent ICT security.

This will also apply to OT systems when the core principles are adapted to OT systems as described in report no. 14; see Table 4.

6.3 Status in relation to the expectations of the authorities and the way forward

Table 5 presents SINTEF's assessment of the status of the initiative relating to ICT security (at the end of 2020), not only the contributions from the 18 reports that have been prepared as part of the initiative in particular, but also generally. The assessment was made in relation to the following expectations and recommendations set out in the *National Cyber Security Strategy for Norway* (S), in NOU 2015: 13 by the Lysne Committee (L), and in letters of allocation from the Ministry of Labour and Social Affairs (T):

S1. Apply a risk-based approach and use recognised frameworks, standards and management systems
S2. Sharing information about threats, vulnerabilities, incidents and effective measures
S3. Provide advice, recommendations and guidance concerning digital security
L1. Transfer the safety tradition within HSE to the digital area
L2. Assess the value of the sector's facilities and ICT systems, and establish regulations concerning digital vulnerabilities
L3. Clarify the role and capacity of the PSA
L4. Assess the association with the response environment for ICT incidents
T1. In addition to increased knowledge and competence development and the mapping of challenges, the PSA will also step up its supervisory follow-up concerning ICT security

Table 5 SINTEF's assessment of the status of the initiative relating to ICT security in the petroleum sector

No.	Assessment of status in relation to the expectations of the authorities	Relevant contributions
S1	Petroleum regulations are function-based, which requires risk-based/-informed decisions, with reference to standards and guides. The regulations and references to, inter alia, standards are discussed in reports nos. 2, 7, 8, 13, 14 and 17.	Nos. 2, 7, 8, 13, 14 and 17
S2	Most reports contain information on threats, vulnerabilities, incidents and/or measures. One challenge is classified information which is not available for public distribution.	Most
S3	All the reports contribute advice, guidance and recommendations to the industry.	All
L1	The Lysne Committee makes a general recommendation to transfer the security traditions within HSE to the digital area, and Report to the Storting 38 (2016-2017) presents a status for this. In the assessment of the Lysne Committee which led to the recommendation, reference is made to barriers. Barriers within ICT security are	Nos. 6, 7, 8, 10, 13 and 17

No.	Assessment of status in relation to the expectations of the authorities	Relevant contributions
	included in the appendix to the PSA's barrier memorandum; see section 5.3. Barriers are referred to in reports nos. 6, 7, 8, 10, 13 and 17.	
L2	The Lysne Committee notes that requirements regarding ICT security should be made clear in Regulations. Report to the Storting 38 (2016-2017) notes that the PSA will clarify and further develop the regulations, including follow-up of the development of standards which may be referred to in the regulations. Assessments of the regulations, including discussions concerning IEC 62443, are included, inter alia, in reports nos. 2, 7, 8, 13 and 17.	Nos. 2, 7, 8, 13 and 17
L3	The capacity has increased, as indicated in Report to the Storting 12 (2017-2018). All the reports have helped to raise competence levels, as has participation in various professional forums. Amongst other things, a new forum known as CDS[1] has been established, where the PSA is participating on the working committee.	All in relation to competence/ No. 7 in relation to capacity
L4	Status of assessment of link to response environment is described in Report to the Storting 12 (2017-2018). The response environment is discussed in reports nos. 2 and 7.	Nos. 2 and 7
T1	All of the reports have helped to boost knowledge development, and many have mapped out challenges. Audit methodology is considered in reports nos. 2 and 7, while the status of audit follow-up is described in Report to the Storting 38 (2016-2017) and Report to the Storting 12 (2017-2018).	All in relation to knowledge/ Nos. 2 and 7 in relation to supervision

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

Table 5 gives some general impressions and is not exhaustive. Most of the reports make recommendations regarding measures and further knowledge acquisition. Many of these are linked to the expectations and recommendations of the authorities specified above, which the PSA may use in the continuation of the ICT security initiative.

References

Arbeids- og administrasjonsdepartementet (2003). *Kronprinsregentens resolusjon om etablering av Petroleumstilsynet og fastsettelse av instruks om koordinering av tilsynet med helse, miljø og sikkerhet i petroleumsvirksomheten på norsk kontinentalsokkel, og på enkelte anlegg på land*.

Arbeids- og sosialdepartementet (2017). *Helse, arbeidsmiljø og sikkerhet i petroleumsvirksomheten*. Rapport fra partssammensatt arbeidsgruppe, 09/2017. (Engen-utvalget).

Arbeids- og sosialdepartementet (2018). *Tildelingsbrev 2018 – Petroleumstilsynet*.

Arbeids- og sosialdepartementet (2019). *Tildelingsbrev 2019 – Petroleumstilsynet*.

Arbeids- og sosialdepartementet (2020). *Tildelingsbrev 2020 – Petroleumstilsynet*.

Direktoratet for samfunnssikkerhet og beredskap (2019). *Analyser av krisescenarioer*.

DNVGL-RP-G108 (2017). *Cyber security in the oil and gas industry based on IEC 62443.* Sept. 2017.

DNV GL (2019). *Digitalisering i vedlikeholdsstyringen og bruken i analysearbeidet*. 11.04.2019.

DNV GL (2019). *Infrastruktur innen industrielle kontroll- og sikkerhetssystemer*. 21.06.2019.

DNV GL (2020). *Regelverk og tilsynsmetodikk*. 24.02.2020.

DNV GL (2020). *Cyber security SIS og egensikre komponenter, kommunikasjonsprotokoller*. 21.02.2020.

DNV GL (2020). *Resiliens mot cyberhendelser og kan blokkjede bidra?* 21.02.2020.

DNV GL (2020). *Trening og Øvelse*. 21.02.2020.

DNV GL (2020). *Telekommunikasjon og protokoller*. 24-02-2020.

Etterretningstjenesten (2020). *Fokus 2020.*

IEC 62443-serien (2020). *Industrial communication networks - IT security for networks and systems.*

IEC 61508 (2010). *Functional safety of electrical/electronic/programmable electronic safety related systems*.

IEC 61511 (2016). *Functional safety of safety instrumented systems for the process industry sector*.

Innst. 15 S (2017–2018). *Innstilling til Stortinget fra arbeids- og sosialkomiteen* Prop. 1 S (2017–2018).

IRIS (2018). *Digitalisering i petroleumsnæringen. Utviklingstrender, kunnskap og forslag til tiltak*. 5.3.2018.

Meld. St. 29 (2011–2012). *Samfunnssikkerhet*.

Meld. St. 27 (2015–2016). *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet*.

Meld. St. 10 (2016–2017). *Risiko i et trygt samfunn*.

Meld. St. 38 (2016–2017). *IKT-sikkerhet – et felles ansvar*.

Meld. St. 12 (2017-2018). *Helse, miljø og sikkerhet i petroleumsvirksomheten.*

Nasjonal kommunikasjonsmyndighet (2020). *EkomROS 2020.*

Nasjonal sikkerhetsmyndighet (2015). *Helhetlig IKT-risikobilde 2015.*

Nasjonal sikkerhetsmyndighet (2020). *Risiko 2020.*

Nasjonal sikkerhetsmyndighet (2020). *NSMs grunnprinsipper for IKT-sikkerhet. Versjon 2.0*. 15.04.2020.

NIST (2014). *Framework for Improving Critical Infrastructure Cybersecurity.*

NOG 070 (2018). *Guidelines for the Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements)*, June 2018.

NOROG 104 (2016). *Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems*

NOU 2000: 24. *Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*.

NOU 2006: 6. *Når sikkerheten er viktigst – Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*.

NOU 2015: 13. *Digital sårbarhet – sikkert samfunn.* (Lysne-utvalget).

NOU 2016: 19. *Samhandling for sikkerhet – Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. (Traavik-utvalget).

NOU 2018: 14. *IKT-sikkerhet i alle ledd*. (Holte-utvalget).

Petroleumsloven (lov 29. november 1996 nr. 72 om petroleumsvirksomhet).

Petroleumstilsynet (2019). *Informasjon om håndtering av IKT-sikkerhetshendelser.* Letter of 18.9.2019.

Petroleum Safety Authority Norway "Terms and expressions". https://www.ptil.no/en/technical-competence/terms-and-expressions/

Petroleumstilsynet (2017). *Prinsipper for barrierestyring i petroleumsvirksomheten. Barrierenotat 2017*.

Petroleumstilsynet (2018). *Integrert og helhetlig risikostyring i petroleumsindustrien*.

Petroleumstilsynet (2019). *Aktivitetsforskriften.* 18.12.2019.

Petroleumstilsynet (2019). *Veiledning til aktivitetsforskriften*. 18.12.2019.

Petroleumstilsynet (2019). *Innretningsforskriften*. 18.12.2019.

Petroleumstilsynet (2019). *Veiledning til innretningsforskriften*. 18.12.2019.

Petroleumstilsynet (2019). *Styringsforskriften*. 26.04.2019.

Petroleumstilsynet (2019). *Veiledning til styringsforskriften*. 26.04.2019.

Petroleumstilsynet (2019). *Rammeforskriften*. 26.04.2019.

Petroleumstilsynet (2019). *Veiledning til rammeforskriften*. 26.04.2019.

Petroleumstilsynet (2019). *Teknisk og operasjonell forskrift*. 18.12.2019.

Petroleumstilsynet (2019). *Veiledning til teknisk og operasjonell forskrift*. 18.12.2019.

Politiets sikkerhetstjeneste (2020). *Nasjonal trusselvurdering 2020*.

Prop. 1 S (2017–2018). *Justis- og beredskapsdepartementet*.

Prop. 151 S (2015–2016). *Kampkraft og bærekraft*.

Prop. 153 L (2016–2017). *Lov om nasjonal sikkerhet (sikkerhetsloven).*

Regjeringen (2019). *Nasjonal strategi for digital sikkerhet*.

SINTEF (2018). *Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten*. 29.05.2018.

SINTEF (2019). *IKT-sikkerhet - Fjernarbeid og HMS*. 05.04.2019.

SINTEF (2019). *Oppfølging av sentrale sikkerhetsfunksjoner og relaterte digitale sårbarheter*. 07.11.2020.

SINTEF (2021). *Datakvalitet ved digitalisering i petroleumssektoren*. Januar 2021.

SINTEF (2021). *Regulering av IKT-sikkerhet i petroleumssektoren.* Januar 2021.

SINTEF (2021). *Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer*. Januar 2021.

SINTEF (2021). *Bruk av modeller i boring*. Januar 2021.

SINTEF (2021). *Premisser for digitalisering og integrasjon IT – OT*. Januar 2021.

SINTEF (2021). *Kommunikasjonssystemer for ekstern nødkommunikasjon*. Januar 2021.

SINTEF (2021). *Automatisering og autonome systemer: Menneskesentrert design i boring og brønn.* Januar 2021.

Williams, T.J. (1992). *The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation*. Research Triangle Park, NC: Instrument Society of America.

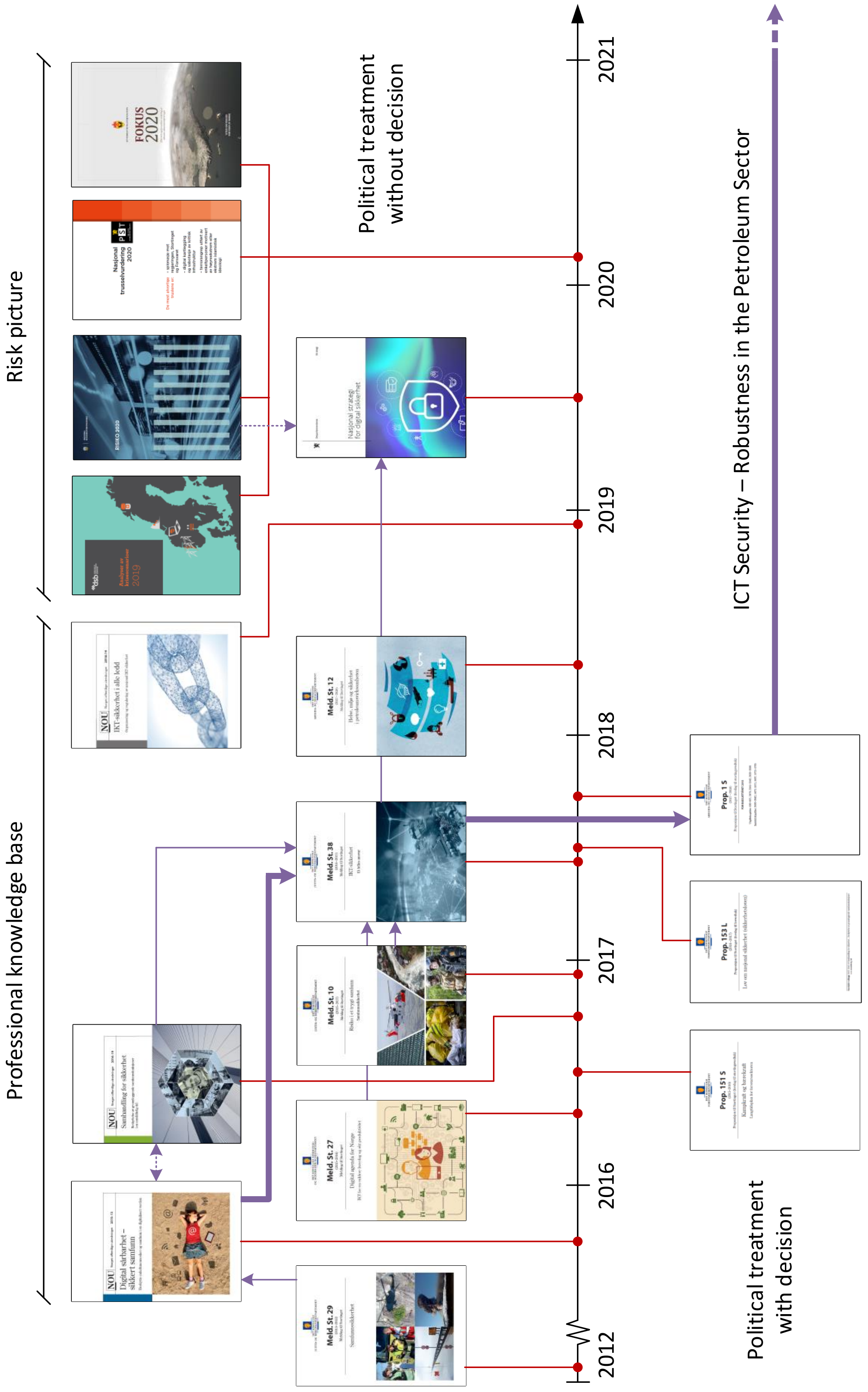
Appendix 1: Abbreviations

Abbreviation	Description
AF	Activities Regulations *(Aktivitetsforskriften)*
ASD	Ministry of Labour and Social Affairs (*Arbeids- og sosialdepartementet*)
BAT	Best Available Technology
CCTV	Closed Circuit Television
CDS	CDS-forum - Industry Forum for Cybersecurity of Industrial Automation and Control Systems
CERT	Computer Emergency Response Team
CSF	Cybersecurity Framework
CSIRT	Cyber Security Incident Response Team
DSHA	Defined situation of hazard and accident
DMZ	De-Militarized Zone
DSB	Norwegian Directorate for Civil Protection (*Direktoratet for samfunnssikkerhet og beredskap*)
Ecom	Electronic communication
NIS	Norwegian Intelligence Service (*Etterretningstjenesten*)
HMI	Human Machine Interface
HSE	Health, Safety and Environment
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
IF	Facilities Regulations (*Innretningsforskriften*)
ICT	Information and Communication Technology
IMS	Information Management System
IT	Information technology
Meld. St.	Report to the Storting (*Stortingsmelding*)
MTO	Man – Technology – Organisation
NIST	National Institute of Standards
NKOM	Norwegian Communications Authority (*Norsk kommunikasjonsmyndighet*)
NOG/NOROG	Norwegian Oil and Gas Association (*Norsk olje og gass*)
NORSOK	The Norwegian shelf's competitive position
NOR	Norwegian Official Reports
NSM	National Security Authority
OS	Operator station
OT	Operational technology
PA	Public Address
PLC	Programmable Logic Control
Prop.	Proposition
PST	Norwegian Police Security Service (*Politiets sikkerhetstjeneste*)
PSA/Ptil	Petroleum Safety Authority (*Petroleumstilsynet*)
RF	Framework Regulations (*Rammeforskriften*)
RAV	Risk and Vulnerability
SAS	Safety and Automation System
SF	Management Regulations (*Styringsforskriften*)
SIS	Security Instrumented Systems
TOF	Technical and Operational Regulations (*Teknisk og operasjonell forskrift*)

Appendix 2: The PSA's explanation of relevant regulatory requirements concerning ICT security

Regulations and regulatory text	The PSA's interpretation
Management Regulations, Section 4 Risk reduction: The responsible party [shall] select technical, operational and organisational solutions that reduce the likelihood that harm, errors and hazard and accident situations occur.	This means that solutions for ICT security must be chosen which reduce the probability of ICT attacks which cause harm, errors or hazard and accident situations.
Management Regulations, Section 8 Internal requirements: The responsible party shall set internal requirements that put regulatory requirements in concrete terms, and that contribute to achieving the objectives for health, safety and the environment.	Requirements must be set regarding how ICT security is handled, technically, operationally and organisationally.
Facilities Regulations, Sections 32-34 Safety systems: The system shall be able to perform the intended functions independently of other systems. Guidelines: The system may have an interface with other systems as long as it cannot be adversely affected as a consequence of system failures, failures or isolated incidents in these systems.	The requirement that interfaces with other systems must not have an adverse impact means that not even ICT attacks should prevent the systems from performing the intended functions.
Facilities Regulations, Section 34a Control and monitoring system: Guidelines: In addition, Norwegian Oil and Gas' Guideline No. 104 should be used as a basis for protecting against ICT-related hazards.	The guideline refers to a recognised guideline, but other standards may also be applied.
Activities Regulations, Section 21 Competence: The responsible party shall ensure that the personnel at all times have the competence necessary to carry out the activities in accordance with the health, safety and environment legislation. In addition, the personnel shall be able to handle hazard and accident situations.	The requirement concerning competence is also relevant to those dealing with hazard situations in relation to ICT incidents involving industrial control and safety systems.
Activities Regulations, Section 21 Training and drills: The responsible party shall ensure that necessary training and necessary drills are conducted, so that the personnel are always able to handle operational disturbances and hazard and accident situations in an effective manner.	The requirement concerning training and drills is also relevant to those who will deal with hazard situations in relation to ICT incidents with the industrial control and safety systems and interact with response environments.
Activities Regulations, Section 45 Maintenance: The responsible party shall ensure that facilities or parts thereof are maintained, so that they are capable of carrying out their required functions in all phases of their lifetime.	The updating and patching of software when security weaknesses are detected is to be understood as maintenance.
Activities Regulations, Section 48 Planning and prioritisation: An overall plan shall be prepared for conducting the maintenance programme and corrective maintenance activities	The requirement regarding planning entails a systematic approach regarding how the company has control over the updates that are relevant and the equipment components that must be covered by a maintenance programme.

Appendix 3: Larger version of Figure 3 - key documents


Risk picture
Professional knowledge base
Political treatment without decision
ICT Security – Robustness in the Petroleum Sector
Political treatment with decision
2012
2016
2017
2018
2019
2020
2021
Meld. St. 29 Samfunnssikkerhet
NOU Digital sårbarhet – sikkert samfunn
Meld. St. 27 Digital agenda for Norge
NOU Samhandling for sikkerhet
Meld. St. 10 Risiko i et trygt samfunn
Meld. St. 38 IKT-sikkerhet
Meld. St. 12 Helse, miljø og sikkerhet i petroleumsvirksomheten
NOU IKT-sikkerhet i alle ledd
Prop. 151 S
Prop. 153 L
Prop. 1 S
Analyser av krisescenarioer 2019
RISIKO 2020
Nasjonal strategi for digital sikkerhet
Nasjonal trusselvurdering 2020
FOKUS 2020