Report

Principles of digitalisation and IT-OT integration

ICT security – Robustness in the petroleum sector 2020

Authors:

Geir K. Hanssen, Tor Onshus, Martin Gilje Jaatun, Thor Myklebust, Maria Ottermo, Mary Ann Lundteigen

Report No:

2023:00189 - 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

Principles of digitalisation and IT-OT integration

ICT security – Robustness in the petroleum sector 2020

KEYWORDS
Digitalisation
ICT security
OT system
Regulations

VERSION
1.0

DATE
2023-02-06

AUTHOR(S)
Geir K. Hanssen, Tor Onshus, Martin Gilje Jaatun, Thor Myklebust, Maria Ottermo, Mary Ann Lundteigen

CLIENT
Petroleum Safety Authority Norway

CLIENT'S REFERENCE
Arne Halvor Embergsrud

PROJECT NO.
102022556

NO. OF PAGES/APPENDICES
37/1

SUMMARY
The purpose of this report is to provide the industry with a greater understanding of ongoing digitalisation, status and challenges, and how this development should be managed going forward.

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

The report is a translation of the SINTEF report 2021:00057 (in Norwegian).

PREPARED BY
Geir K. Hanssen

SIGNATURE 

CHECKED BY
Lars Bodsberg

SIGNATURE 

APPROVED BY
Maria Bartnes

SIGNATURE 

REPORT NO.
2023:00189

ISBN
978-82-14-07958-6

CLASSIFICATION
Unrestricted

CLASSIFICATION THIS PAGE
Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
1.0	2023-02-06	Translation of SINTEF report 2021-00057

Image crediting:
Page 13: Based on Illustration from McAfee
Other images: Self-produced or Pixabay (Pixabay License)

Table of contents

Executive summary

Introduction

The objective of this report is to address the digitalization in the Norwegian oil- and gas sector and highlight challenges, in particular related to cybersecurity and operation technology (OT), and to provide recommendations to the industry and to Ptil.

The work is mainly based on analysis of documentation, interviews, and meetings. Both operators and suppliers have been interviewed.

Digitalization in the industry

The petroleum industry is undergoing an extensive process of digitalization, driven by considerable opportunities but also facing challenges. All actors in this industry have added digitalization to their agendas, and some with a solid anchoring in their strategies, aiming for more effective operations, increased extraction, and improved safety. Maturity varies though, typically related to the size of the organization, and the capacity to manage large technology-driven transformation processes. Digitalization is a trend within nearly any domain and industry, but where the petroleum industry may be considered at an earlier stage than other domains due to its strong focus on safety. This development can be seen as part of the development of Industry 4.0 where physical devices are connected with distributed ICT-systems, building on technologies such as machine learning, Industrial Internet of Things (IIoT), new communication technologies, autonomous systems, etc. These are all technologies which enables production, transfer, storage and exploitation of very large data from operations, which enables improved processes, exploiting information technologies. Examples are automation, expert systems, and digital twins. We already see an extensive use and benefits from this class of technology, but several challenges remains to be resolved before we see the full potential. The fundamental challenge is to understand and manage limitations with respect to guidelines and requirements from the authorities, which creates a fundamental basis for safety in the industry.

Identified challenges

The ongoing development is complex, even for highly competent organizations that already are advanced users of technology. It is challenging to build a complete understanding of the development, but it seems obvious that the transition towards increasingly data-driven operations is at the core of the challenge. Increasing amounts of data are being produced and retrieved from the operational systems in what can be defined as edge solutions, and then processed in centralized IT-systems, meaning that data in some cases must be transferred through systems and infrastructures that was not intentionally designed for this extent of data flow. Large amounts of data also needs to be stored and processed with sufficient capacity, e.g. in cloud solutions while at the same time being secured against access and influence by outsiders. Last but not least, new data-intensive services also put a demand on data control and data quality.

This development challenges the relationship with suppliers, both those that are well established as well as new actors that are offering data-intensive, cloud-based services. It can be hard to see where and how net-based digital services are offered and how they are maintained, and how to manage these. On the other side, some suppliers may not have the needed insight themselves regarding cyber security and fundamental principles on independence and segregation of safety systems. Data is an important asset and the ownership of data is also being challenged.

Digitalization does in general increase the coupling between systems and thus challenge information security, in particular when systems and equipment is located near operational systems and where the safety systems potentially can be affected. Well established principles such as boundary protection and layered architectures are being challenged. The industry are seeking relevant guidelines and several actors are referring the IEC 62443 series, but where development and the level of maturity are yet not in place.

All actors do have similar challenges and there is a clear need to increase joint competency, preferably as a joint effort; the challenges of the industry – and the solutions – are of common interest. In particular, it is important to build a shared understanding and a standard for fundamental principles for information security. This is particularly important in relation to operational systems that are being influenced by information technology. NAMUR Open Access and OPC UA seems to gain focus in the industry as a common view on interoperability, but do as well require coordination and increased knowledge on use and limitations.

Recommendations

Based on the understanding of the digitalization, and findings from interviews, a set of recommendations are given to the industry.

- A joint effort to increase competency and collaboration
- Standardization (or selection of standards) for interoperability and information security
- Increased emphasis on data *quality* and *integrity*
- Increased awareness of the role as data *owner*
- Increased emphasis on the flow of data, especially in existing systems
- Increased focus on digitalization for improved safety, beyond ambitions on efficiency

Followingly, recommendations are provided to Ptil:

- Develop the role as a driving force to increase competency, although within the mandate of Ptil
- Monitor the development on data transport and technologies for coupling systems, in particular in relation to operational systems
- Contribute to clarify regulations in the light of the technological development
- Contribute to the effort on establishing a joint reference architecture (NAMUR OA is relevant) and a joint standard for interoperability (OPC UA is relevant)
- Coordinate guidelines and follow-up of production and drilling companies, which have common challenges

1 Introduction

1.1 Background

The Petroleum Safety Authority Norway has commissioned SINTEF to investigate various aspects of the topic of ICT security — robustness in the petroleum sector. The primary objective has been to obtain knowledge concerning risks, threats, vulnerabilities and the importance of ICT security for industrial systems. The aim of the project has been to improve the understanding of ICT security in the petroleum industry and thereby increase the industry's resilience against undesirable incidents. SINTEF has also provided input for updating the Petroleum Safety Authority Norway's regulatory framework for monitoring ICT security.

The following is a brief description of the six subprojects:

Data quality

The aim was to examine which data sources and data are used in industrial ICT systems and how data is handled and processed prior to being made available in the office network. Strengths and vulnerabilities relating to data quality and the protection of data are discussed.

Memorandum – ICT security in the petroleum industry

SINTEF has prepared a memorandum to clarify how ICT security in the petroleum industry is regulated by the applicable regulatory framework. The memorandum also sheds light on the expectations of the authorities, and presents an overview and status of the petroleum industry's focus on ICT security in recent years.

Guidelines for ICT security

Guidelines have been prepared for the Norwegian petroleum industry to supplement the core ICT security principles set out by the Norwegian National Security Authority (NSM). The guidelines are tailored to the solutions that are typically employed in the petroleum sector, while retaining the flexibility to address the key elements of the petroleum industry's ambitions for digitalisation.

Model-controlled operation

The report summarises knowledge and recommendations concerning the secure use of data from model-controlled operations. Particular emphasis is afforded to the quality assurance of models and communication between software solutions in drilling operations.

Principles of digitalisation and IT-OT integration - *this report*

The purpose was to describe and assess how digitalisation and the use of cloud services affect industrial ICT systems, and the security solutions that need to be implemented to ensure secure use of cloud services. The Petroleum Safety Authority Norway's regulations are particularly built upon a pillar of segregation and independence as strategies for establishing safety and security.

Communication networks

The aim was to investigate external communications roles that data networks can provide in the event of hazard and accident situations. The report describes challenges associated with the risks and vulnerabilities in data networks and makes specific recommendations for improvements.

This project is part of a larger ICT security initiative at the PSA. Key issues for the PSA include:

- How does the industry manage change processes relating to the introduction of new technology?
- How will digitalisation impact HSE conditions and risk management?

SINTEF's work with this project is largely a continuation of previous projects carried out by DNV GL and SINTEF within the same thematic area [1].

1.2 Objectives and purpose

The primary objective of this report was to provide the industry with a greater understanding of the principles for digitalisation in the oil and gas industry in the Norwegian sector.

The following four objectives were defined:

1. Assess status and plans, including probable applications of digitalisation, and thus principally cloud technology, in OT systems and integration with IT systems at operators (within the Petroleum Safety Authority Norway's area of responsibility).
2. Evaluate known experiences with cloud technology as an important digitalisation and system integration trend from the same and similar industries to determine typical ICT security challenges and good practice for managing these, including ensuring independence between systems, with special emphasis on emergency shutdown systems (ESD). It was also relevant to assess systems for performance monitoring of field equipment (for example, can monitoring of closure time for ESD valves adversely affect safety functions?)
3. Describe and assess how the use of cloud services/digitalisation impacts OT systems, what impact this may have on ICT security, and which ICT security solutions have to be implemented for secure digitalisation, for example, the use of cloud services, and possibly what limitations exist.
4. Provide input for updating the guidelines to the Petroleum Safety Authority Norway’s regulatory framework for monitoring ICT security in IT and OT systems.

This report places the spotlight on the ongoing digitalisation of both existing and new installations and is based on information that was obtained from operating companies, drilling companies and providers.

1.3 Restrictions

The following restrictions apply:

- Emphasis has been placed not only on the current solutions, but also on challenges in the near future that the industry is working with today. The report is therefore not intended to provide input regarding the long-term developments, but rather the ongoing developments – based on experiences from the present day.
- The companies and respondents were selected with the intention of ensuring that there was the best possible access to expertise, however our findings were based on information, statements and assessments from individuals, a factor that which will naturally influence the information that is collected.
- All information collected was treated confidentially and the report will therefore not disclose information that is specific to individual companies. The report has also been presented in such a

manner that it is not possible to trace findings back to individual companies, and the intention was to present an overall picture of the industry.

1.4 Terms, definitions and abbreviations

1.4.1 Terms and definitions

Definitions are used to ensure that we have an equal understanding of key terms, however definitions can in themselves limit the understanding of a term, and there are often multiple definitions of the same term. Therefore, in some instances we have deliberately included multiple definitions of the same term.

Term	Definition/description	Reference
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, both individually and collectively.	PSA 2020 (ptil.no) [4]
Cloud	Storage and processing of data on externally connected infrastructure that is connected to the internet.	This project
Cybersecurity ***	The protection of equipment (components and devices) and physical processes that are vulnerable through ICT.	SINTEF 2019:00361 [5]
DevOps	Integrated iterative process for development (Dev) and operation (Ops)	
Digital Security ***	Protecting “anything” that is vulnerable because it is connected to or otherwise dependent on information and communications technology.	National Strategy for Digital Security 2019 [6]
Digital Twin	A digital reconstruction of something that exists in the real world. This can be a representation of a physical object, a place, a system, a process, or even a human being. The digital representation mirrors the real thing, and learns and changes in line with what it represents.	Digital Norway [7]
Edge	Processing and storage of data in close proximity to the collection and use of data.	This project
Fog	Processing and storage of data collected from edge equipment and potentially integrated with cloud solutions.	This project
ICT Security ***	Protection of information and communications technology (hardware and software, as well as communication systems).	SINTEF 2018:00572 [8]
ICT security measures*	Measures to protect ICT systems and information against intended and unintended incidents.	NOU2015: 13 [9]
Information Technology (IT)	Technology that processes information.	This project
Internet of Things (IoT)****	Technology that provides the ability to remotely monitor and control products by connecting them to the Internet.	Digital Norway [10]
Operational Technology (OT)	Technology that supports, controls and monitors industrial production, control and safety functions.	This project
Risk (1) **	Risk means the consequences of the activity and its associated uncertainty.	Guidelines to Section 11 of the Framework Regulations [11]

Term	Definition/description	Reference
Risk (2) **	Risk can be expressed as a combination of the probability and consequence of an undesirable incident.	NS 5814:2008 [12]
Risk (3) **	Risk can be expressed as the relationship between the threat to a given asset and this asset's vulnerability to the specified threat.	NS 5832:2014 [13]
Security (1)	Security involves protection against hazards and threats which could cause undesirable incidents.	NOU2015: 13 [9]
Security (2)	Protection of assets such as people, the external environment, equipment and information	SINTEF 2018:00572 [8]
Vulnerability (1)	The inability of an analysis object to withstand the effects of an undesirable incident and to restore to its original state or function following the incident.	NS 5814:2008 [12]
Vulnerability (2)	An expression of the problems that a system experiences in operating when exposed to an undesirable incident, and the problems that the system experiences in resuming its activities after the incident has occurred.	NOU2015: 13 [9]

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

**) Risk (1) is an example of a qualitative definition of risk, while risk (2) and risk (3) are examples of definitions for describing risk, cf. [14]

***) Digital security is used synonymously with ICT security and cybersecurity [6].

****) Can be expanded to IIoT – Industrial Internet of Things – equipment designed for industrial use (sensors, instrumentation, etc.).

1.4.2 Abbreviations

Abbreviation	Description
HMI	Human Machine Interface
HSE	Health, Safety and the Environment
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
IF	Facilities Regulations (*Innretningsforskriften*)
ICT	Information and Communications Technology
ISO	International Standardization Organization
IT	Information Technology
LAN	Local Area Network
NEK	Norwegian Electrotechnical Committee
NKOM	Norwegian Communications Authority
NOG	The Norwegian Oil and Gas Association
NORSOK	The Norwegian shelf's competitive position
NOU	Norwegian Official Reports
NS	Norwegian Standard
NSM	National Security Authority
OT	Operational Technology
PC	Personal Computer
PLC	Programmable Logic Controller

Abbreviation	Description
PSA	Petroleum Safety Authority Norway
RF	Framework Regulations (*Rammeforskriften*)
SAS	Safety and Automation System
SF	Management Regulations (*Styringsforskriften*).
SIS	Safety Instrumented Systems
SLA	Service Level Agreement
TCP	Transmission Control Protocol

1.5 Methodology and implementation

This work was primarily based on a document review, interviews, and working meetings. The work was carried out by an interdisciplinary project team with expertise in, among other things, communications systems, ICT security, emergency preparedness, as well as petroleum regulations and standards within these fields. The research literature (appendix A) was also screened.

Interviews were conducted with several companies in connection with this. For the sake of anonymity, the names of the companies have not been disclosed. Interviews were conducted with 5 operating companies and 1 provider. Observations were also made of a total of 6 interviews conducted in sub-assignment 2 (Data Quality), 3 (ICT Security) and 5 (Model Controlled Operation).

1.6 Report structure

Chapter 2 provides a brief introduction to digitalisation, which is aimed at a non-technical target group.
Chapter 3 provides an overview of important findings in the dialogue with the companies.
Chapter 4 summarises the most important recommendations for the industry and the PSA, and provides input for further knowledge acquisition.

In addition to figures and tables, we use fact boxes (green boxes on the left-hand side of the page) and result boxes (blue boxes on the right-hand side of the page). The same colours are used for tables, i.e. result tables are blue.

2 Digitalisation - a brief introduction

This chapter provides a brief introduction to the term “digitalisation” and related terms such as cloud technology and cloud-based service models. The introduction is geared towards developments and needs in the Norwegian oil and gas industry and is intended to lay the foundation for later parts of the report that discuss important findings from document analyses and interviews with actors in the industry. The introduction is at a generalised level and is aimed at a wider audience who do not necessarily have in-depth ICT expertise. References to additional information are made where relevant.

2.1 A brief introduction to digitalisation

Digitalisation is a broad term, however can be understood as being a trend in which data and digital technologies are used to improve existing organisations and processes. This is nothing new, however we are now seeing that information and communications technology are increasingly being used to establish new data-intensive services and functions, and that data and processing power are increasing in scope, and becoming more widely distributed and more accessible at lower cost.

Digitalisation is about taking advantage of the opportunities that digital enabling technologies provide for improving, renewing and innovating.

Therefore, digitalisation is not simply about technology, but is equally about the willingness and ability to change.

Digital 21 [2]

Virtually all modern organisations have a relationship to digitalisation, whether this be as users, recipients and/or providers of digital services. This is a development that is being driven by ever larger and more advanced software systems with high capacity, increasing amounts of data and an increasing degree of connectivity between systems over the internet as a communication channel with a high level of flexibility and capacity. This is driven by the prospects of better operations and greater profits, where data is utilised to create new knowledge and streamline processes, for example, through increased automation and simplification of manual processes. For the oil and gas industry, this may include improving the efficiency of drilling and production processes, better safety and reducing emissions. A well-known example from other domains is the banking and finance industry, where data and web-based ICT solutions have long since replaced what used to be extensive manual processes. The benefit of this has been easier access to new, faster and better services for customers, who can perform most tasks anywhere at any time. This correspondingly enables there to be savings, new services and more efficient operations for the banks. The degree of manual processes has significantly decreased over time. We see the same situation in the oil and gas industry, where the development has progressed from the introduction of solutions such as e-operations in the 1990s – where ICT enables integrated operations centres that improve efficiency [15] – to the present situation where increasingly more data is collected and used to develop new services, for example, based on digital twin and cloud services.

Digitalisation has reached a scope that encompasses virtually all areas of society and industries, including most definitely the oil and gas industry. However the development in this industry can be said to be in the start phase when compared with other industries. This development is often related to the term “Industry 4.0”, or the Fourth Industrial Revolution, which alludes to closer interaction between software, hardware and organisation – essentially in manufacturing enterprises. These are also referred to as “cyber-physical systems” where physical equipment is connected to distributed software-based systems, and realised based on innovative technologies such as machine learning, industrial internet of things (IIoT), new communications technology, autonomous systems, etc.

Despite digitalisation in the oil and gas industry being a clear trend both in Norway and internationally, it is a development that is in its early phase, and it is difficult to form a complete picture of the development for the actors in the industry and, not least, of where it is heading [16]. At a generalised level, the objective is "intelligent oil fields", "intelligent drilling", and "intelligent pipelines". These are obscure terms without clear definitions, however when a term such as "the digital oil field" alludes to technology that replaces or streamlines human and repetitive tasks, the "intelligent oil field" alludes to technology that also creates, analyses and applies knowledge. An "intelligent oil field" can be described through the following functions: 1) real-time access to data, 2) analysis of the status quo, trend analysis, and optimisation, 3) operational integration, 4) automated control. As an indication of potential, empirical data suggests that "intelligent oil fields" can increase productivity by 2-8%, with 2-6% better extraction [16].

While digitalisation is a concept with serious potential, we are also talking about major growth in complexity and the distribution of data that also need to be managed. Old equipment and new equipment are digitalised, and large amounts of data are produced, collected, analysed and used in new ways which we do not yet fully understand the potential and limitations for. This requires expertise and major resources and is challenging to manage, even for large organisations that generally have a high level of expertise. Many actors make the decision to use various forms of cloud solutions as an alternative to developing and operating their own inhouse capacity.ll of the major actors have adopted cloud solutions, typically from the large market leaders such as Microsoft (Azure), Amazon (AWS), IBM (Cloud), etc. 'Cloud' is a term which insinuates that a customer or user is spared the complexity and responsibility of physical storage, processor capacity, resource pooling and scalability by entrusting this to an external provider. In this way customers avoid having to develop their own operational expertise, capacity and infrastructure, and can instead focus on their core business. These providers typically have data centres with enormous capacity and that service many customers simultaneously to realise efficiency gains. In such instances, there is often little control over where data is physically stored and processed.

Cloud computing:

A computing capability where the architecture surrounding massive clusters of computers is abstracted from the applications using it and a software and server framework (usually based on virtualization) provides clients scalable utility computing capabilities to elastically provide many servers for a single software-as-a-service style application or to host many such applications on a few servers.

NIST [3]

Alternatively, if it is important for a customer to have a greater degree of control over the storage and use of data, a customer can establish its own private cloud solutions in its own infrastructure. The customer can then influence and control the physical implementation (processor, storage, network, etc.). These can be referred to as 'fog' or hybrid solutions and can also be connected with purely cloud solutions. This therefore places greater demands on the customer's own expertise and investments in infrastructure, and there is a lower degree of flexibility. Another important term is 'edge'. This is a solution that is located in close physical proximity to equipment or systems. This is typically in instances in which there is a requirement for a high degree of security, control and performance/response time, and data cannot be permitted to be stored in a cloud solution. Lack of control or predictability with regard to availability, uptime, and response time (where data is transported via the internet, which has unpredictable and variable performance) due to physical location may be reasons for this. The downside is that there is then not the same scope for compiling and processing data across systems.

Different types of services are often mentioned in connection with cloud solutions:

- Infrastructure-as-a-Service (Iaas), where infrastructure capacity is purchased, for example, storage space or processor capacity.
- Platform-as-a-Service (PaaS), where capacity is purchased on a virtual system platform, for example, virtual Windows servers, databases, etc.
- Software-as-a-Service (SaaS), where one purchases the service the software provides instead of the software itself to operate this even in own infrastructure, for example, an analysis system.

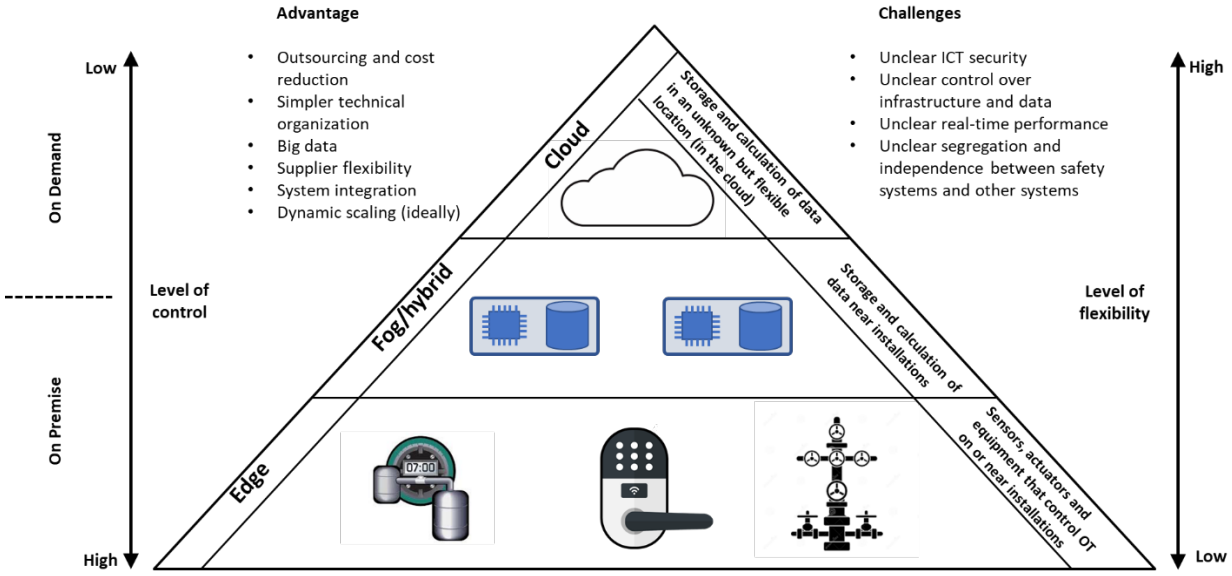


Figure 1 Edge, fog and cloud computing

'Cloud', 'fog', and 'edge' indicate a range between the degree of control on the one hand and flexibility on the other (Figure 1). For purely cloud solutions, where all data is stored and processed in a data centre that is located outside the organisation and operated by a provider, there will be a higher degree of flexibility and needs-based access to resources, however a lesser degree of control. Capacity can be purchased as required, without having to scale own infrastructure, however relinquishes a degree of control over what happens with the data, how it is protected, and who has access. This must therefore be potentially expressed in contracts

and agreements, and in the follow-up by the provider. Conversely, if one stores and analyses data close to operational activities (in physical proximity to sensors and actuators, often on the same network – hence the name 'Edge') there is a high degree of control, but little flexibility and one must assume the costs and responsibility of managing infrastructure and operations oneself or possibly enter into an agreement with a provider and follow this up. Fog, or hybrid, suggests an intermediate variant, where data and processing are located more centrally, for example, in their own internal data centre, where there is still proximity to the equipment that is being controlled. The advantage therefore is that this can be physically placed in a system infrastructure with established mechanisms for information security (firewall/DMZ). Hybrid can also indicate combined solutions between local and distributed capacity. The degree of control will be greater, however the degree of flexibility will be lower.

An important consequence of digitalisation is the shift in responsibility for information security. When all equipment and systems are controlled by one and the same organisation, the organisation is naturally enough also responsible for all aspects of information security, and therefore has the ability to exercise a large degree of control (assuming there are good principles and the correct use of technology). When infrastructure, platforms and/or software-based services are moved out of the organisation in whole or in part, some of the responsibility for information security (but not all) is also outsourced. Figure 2 demonstrates how, in principle, the degree of digitalisation, from outsourcing of only infrastructure to outsourcing software, shifts this responsibility. When the provider assumes more of the responsibility, it is of course important that the customer is able to set requirements and verify that this responsibility is being handled in an optimal manner.

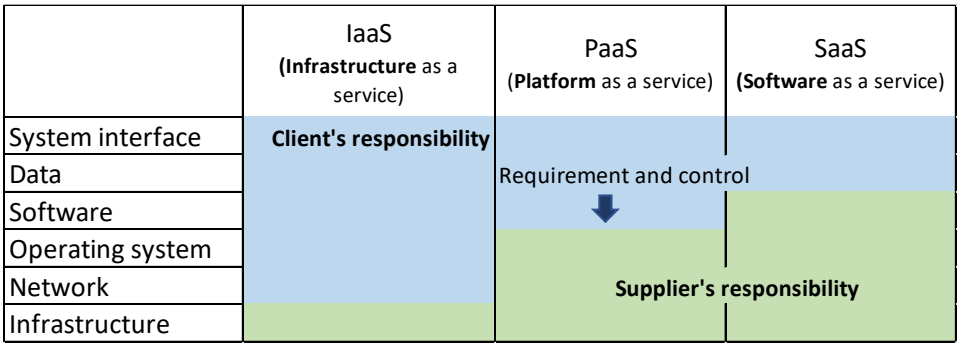


Figure 2 Shift in responsibility and control of information security

This range of control and flexibility is of fundamental importance to organisations with high-risk activities and that are reliant on advanced data-intensive solutions to control risk. In many ways, the oil and gas industry is a typical example of this. Simply put, management may want a rapid development to achieve quick gains, while the operations and production divisions will see challenges down to OT. In other words, there may be tension between management/strategy and operations that could influence priorities, competence building, and development work.

2.2 Benefits from digitalisation and why this is an important trend

The Digital 21 [2] report identifies the oil and gas activities in Norway as one of 10 important areas in which digitalisation will create new opportunities and the increased competitiveness that will be necessary when facing the expected lower oil prices and stronger competition from new forms of energy. In short, digitalisation is regarded as key to improving efficiency and a prerequisite for the industry's long-term viability. The report refers to McKinsey's estimate of potential annual savings from digitalisation on the Norwegian continental shelf of NOK 30-40 billion.

«Digitalization technologies contribute significantly to reduce costs and improve recovery.»

OG21 rapport [1]

The OG21 Report 'Norway's oil and gas technology strategy for the 21st century' [1] presents an analysis of the industry and concludes that digitalisation technologies will contribute to significant cost reductions and increase extraction capacity. The report makes special mention of following six technologies as being "digitalisation technologies":

- Field model optimization
- Big data exploration analytics
- Wired pipe (drill string with signal cables)
- Automated drilling control
- Predictive maintenance
- Unmanned platforms

These are all technologies that can be described as *data-intensive*, i.e. that they are based on the extensive collection and processing of data. This can be data from the OT layer, for example, temperature, pressure, or other data from reservoirs, drilling, etc. If this data is collected with a high resolution and frequency, for example in a cloud solution with high storage and processing capacity, it can, for example, be utilised for predictive maintenance (large amounts of data from many instances over an extended period) that could potentially result in lower maintenance costs. Another obvious example of the utilisation of data is the construction of models or digital twins that can optimize, for example, drilling. This technology is already relatively mature. See also the separate report on model-controlled operation [17].

The next generation of data-intensive services will benefit from machine learning technology (ML) that has the potential to utilise large amounts of data better than traditional solutions based on classical (deterministic) algorithms and mathematical models. A machine learning system can interpolate predictions and classifications about future situations (new data) based on learning from existing data. Simply put, an ML system is effective for finding new links in known amounts of data, however has problems making good predictions outside of known amounts of data (extrapolation). Therefore, an ML system trains itself to make decisions that are not based on a pre-defined algorithm. In other words, it is not a trivial matter to understand *how* and *why* the system does what it does and can simply be described as a 'black box' [18]. A notable example is Google's AlphaZero, an ML system that trains itself to master chess by playing against itself within the game's basic rules. The system is virtually unbeatable within its known domain, however does not know what to do if the rules change.

Johan Sverdrup is a specific example of a comprehensive digitalisation project in the oil and gas industry in which the development project has developed its own Digital Roadmap with two overarching objectives: 1) to ensure that the large amounts of data that need to be collected can be used effectively to optimise the management of the reservoir, and 2) explore new means of working to ensure an effective operation [19]. In practice, this is effectuated in the form of solutions for better (data-based) decision-making support and automation of processes. Examples are improved drainage strategy, optimisation of well placement, and automated production.

In addition to efficiency gains, there are also potential security and safety benefits. New data-intensive services can provide assistance and, in the long term, partially automate critical operations, for example, drilling, with better kick detection that reduces the risk of well control incidents with the potential harm to operators/drillers and others. Therefore, new digital services can improve the reliability and effect of existing barriers, however this is predicated on these solutions themselves not introducing new weaknesses or threats. There is safety potential in digitalisation which has probably thus far not been fully understood and exploited. This should be an equally important driver of developments to more efficient operations and extraction. If good quality data about a facility or operation is collected, this creates opportunities for improving information and situational awareness for the operator, for example, via handheld solutions or VR or AR solutions. Better access to good quality information can contribute to improved safety. One can also envision solutions that benefit from information about the operator's location that, together with data concerning ongoing activities, can be used to improve safety. There are potentially many such examples that should be explored.

Potensiale for produktivitet og utvinning

"From the available statistics, intelligent oil fields can increase production by 2%–8 % and recovery by 2%–6%..."

Oil and Gas 4.0 era:
A systematic review and outlook [17]

Alongside the purely technical benefits, digitalisation in the industry also offers opportunities for closer collaboration and new forms of cooperation between actors and suppliers. Virtually all actors have a digitalisation process and there is obvious potential in developing knowledge and sharing experiences based on common needs, issues and solutions. This also includes opening the door to the sharing of data across organisations.

2.3 Cloud technology from an oil and gas perspective

The terms used when we talk about cloud technology can be unclear, however can be exemplified in the following model (based on the Purdue Model) which depicts the typical division of a facility into levels, for example, a platform.

Edge implies that data is processed *close to* where the data is located and that it is not generally transferred to a central system over a large distance. This can be data that is obtained from equipment with sensors and actuators in the OT layer such as valves, pressure gauges, vibration meters, etc. There may also be data from IIoT equipment. The aim is to ensure performance/response time (direct connection or few detours for data) in addition to making it easier to maintain ICT security by keeping production, transport and processing of data in, for example, layer 1. Edge computing will also reduce problems relating to data integrity and quality, because transporting data upwards in the layer model via multiple systems (historians, Pie servers, etc.) can result in data being affected, for example, if data from a sensor is converted to other formats. On the other hand, the consequence of edge computing is that data and functionality have limited availability and applicability for other systems. Although edge implies close proximity between data and processing, it may still also be possible to share data with other systems. Foundation Fieldbus is an example of already established technology that possesses the characteristics of an edge device, because the application can be placed on a sensor or actuator.

Fog can be an internal service at a higher layer – Level 3 (OT) or Level 4 (IT). Fog collects more data from Edge equipment, typically IIoT devices, and thereby provides greater potential value through the collation of data and analysis of data from multiple data points. Data is in relatively close proximity to the operation and, in principle, the system owner itself has to take responsibility for infrastructure, operations and maintenance – including necessary measures for information security. A Fog service can also be connected to Cloud services at even higher layers.

Cloud indicates that data and functionality are physically located outside of the architecture, however can be operated either internally (on premise) or by a cloud provider (on demand). Cloud solutions can have high storage and processing capacity, which is relevant in terms of the increase in the data produced in a modern facility. There is again a balance between control and flexibility; a cloud server in its own infrastructure provides more control, particularly for protecting and using data, while purchasing services from a cloud provider gives more flexibility when capacity can be purchased according to varying needs, however part of the control responsibility is transferred to an external provider.

Figure 3 shows how these terms can be placed in a typical layered architecture.

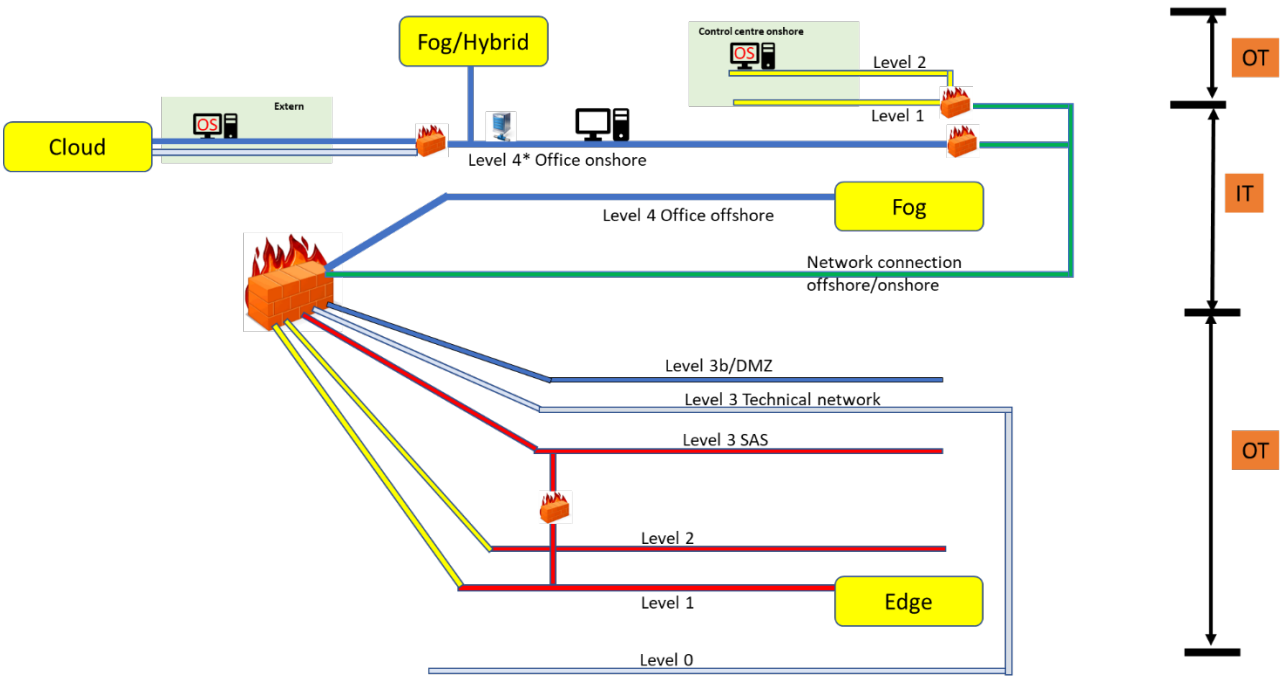


Figure 3 Cloud-Fog-Edge mapped with a physical Purdue Model

Most operators and some of the suppliers have made major investments in cloud technology such as Microsoft Azure or Amazon Web Services or IBM Cloud – this is driven by an increased need for *capacity* and *flexibility*. Strategic partnerships have also been entered into with cloud providers to ensure there is both expertise and capacity, as well as to protect data when, among other things, it is specified *where* the data centre is geographically located, for example, to keep it within the EU area and therefore in accordance with the applicable regulations. Separate cloud solutions from traditional providers, for example, ABB Utility Sky, are also used.

There are several definitions and variations of the terms which may be unclear. However, the most important factor is still the *need* for capacity that comes with the increasing amount of data that is produced, and consequently the inherent potential in utilising data, for example, for predictive maintenance, operator support systems, digital twins, etc. This development requires the capacity for storing and processing data that may be inappropriate or difficult to adapt to existing infrastructure, however plans can be made for this when concerning new facilities.

2.4 Expected challenges associated with digitalisation in the oil and gas industry

At a general level, the ongoing digitalisation in the oil and gas industry presents a set of new or stronger challenges relating to the protection of data (transport, storage, access). The following model (Figure 3) expands on the Purdue Model that represents well-established principles for how to ensure interconnection and data flow between the OT layers and up to the IT layer. A layered architecture with DMZ and a firewall between the layers will traditionally provide good control and information security (provided that the principles are followed). The challenge we are now seeing as a result of the trend towards digitalisation is that the need to aggregate data upwards towards the IT layer and further towards what we can describe as a new layer 6 (Cloud), and any potential instances of OT being directly impacted from such a layer are challenging the established principles. This is not necessarily a picture of the present-day situation, but rather a picture of where the development is heading. Existing infrastructure – including mechanisms for information security – is not constructed for the data flow that we are now seeing in relation to both information security and capacity (Figure 3 – green arrow). Similarly, existing OT systems are not generally constructed for connecting beyond the layer above (Figure 3 – red arrow). As part of technological development and the need to have control over data quality and performance (frequency), we may see direct connections between the OT layers and the cloud layer (Figure 3 – blue arrow). It is important to note that the interviews with the companies did not reveal that these types of connections have now been made, however signals from the supplier side indicate that this is *desirable* in terms of response time and time resolution. This is fine if it involves typical edge solutions in which data is not transferred out of the OT layer, however if the data is transferred to a cloud service, extremely good measures will be required to protect data. Some providers sell diode solutions as a protective mechanism, however it has proven difficult to get this technology to function in practice, including with challenging operations.

Naturally enough, existing installations and systems (brownfield) have limitations on integration and increased data flow. Extensions and additional equipment connected to OT systems, and particularly the safety systems, will challenge the principle of segregation and independence. However, new installations (greenfields) may be able to be designed from an early phase to produce and manage large amounts of data. The development of Johan Sverdrup is an example of such a development where technology choices, the use of data-intensive solutions and thereby new forms of work will influence developments and other installations in the future. The term 'digital field-worker' is created through new solutions for automated and digitalised work processes, digital twin, and anomaly detection models based on machine learning [20]. These are what we can call data-intensive solutions that are based on much greater production, transport and use of data than previous installations – especially from the OT layer. These are also technologies that are largely based on advanced software solutions that require a high level of capacity for storage and calculations and that enable there to be a greater degree of improvement and further development of the solutions throughout the entire life-cycle of the installation.

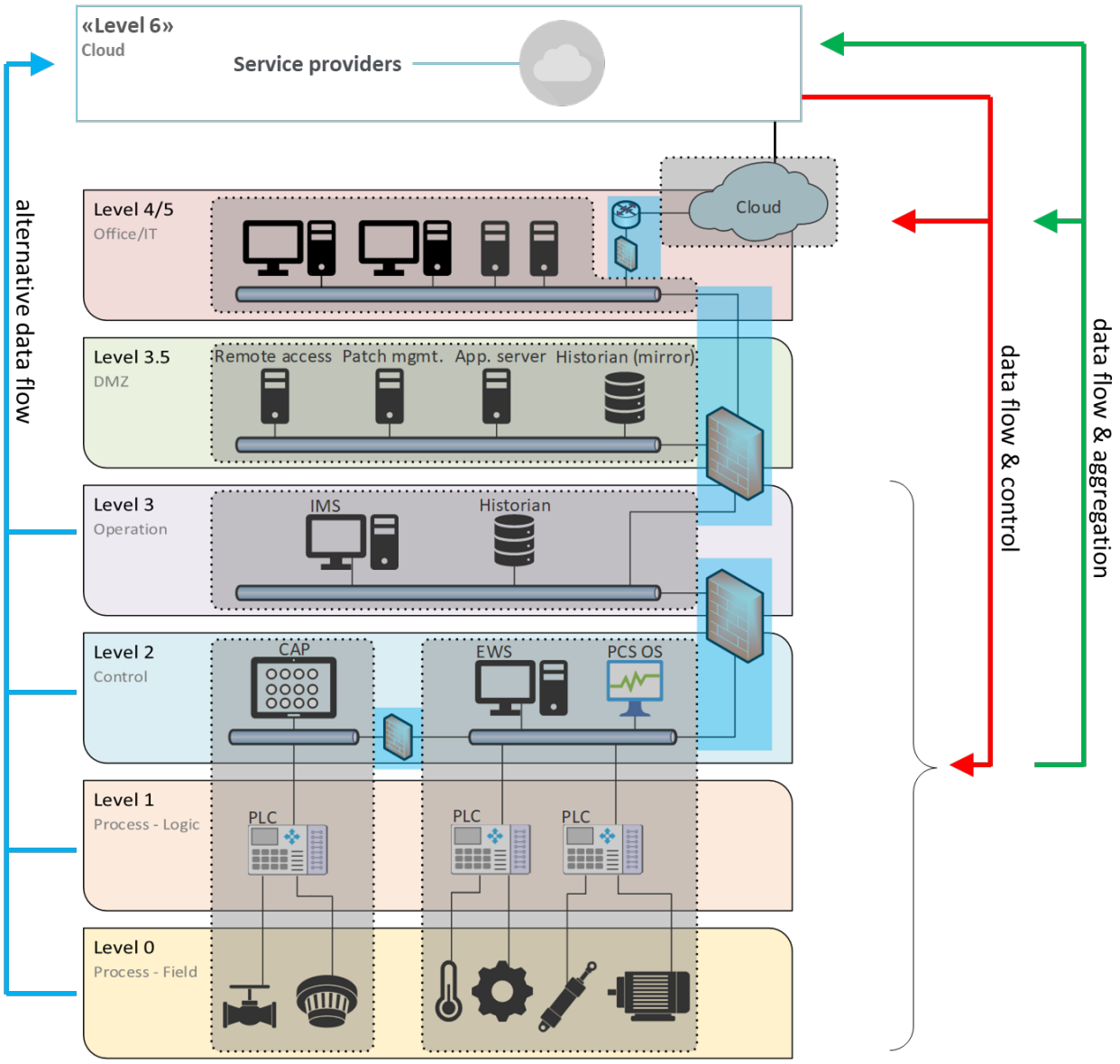


Figure 4 An "extended" Purdue Model

- **Convergence between IT and OT**
  The traditional distinction between IT and OT as different functional areas with different needs for protection, both in relation to technology and organisation, is becoming more blurred. Standard information technology and software solutions are increasingly also being used in the OT layers, with edge components in layer 0-1 (IIoT) which is connected to fog and cloud solutions from layer 2 and upwards. However, the requirements for protection of the *function* are the same – new technology and organisation must therefore offer the same level of security.

- **Competence boost**

Developments are taking place at a rapid pace and require updated expertise in digitalisation and cloud technology, new information security challenges, and how cloud-based services can impact safety. The need for expertise ranges from the organisational to technical level and stretches across operators and providers. This need is seen both at operator and drilling companies (possibilities and limitations in the technology), and on the provider side (understanding of established safety principles and regulations).

- **Increased focus on data quality**
  The production, flow and use of data in connection with OT has traditionally been limited. Now that this is growing and becoming important for both improved efficiency and better safety, it will be important to maintain adequate data *quality*. This is to realise efficiency gains, while also ensuring safety. This also includes good practices and good solutions for consolidating and aggregating data. This can be challenging, because different sources have different formats and different levels of performance. Traditional OT systems have not been developed with data sharing in mind. See the separate report for a more in-depth assessment of the need to actively ensure data quality [21].

- **Performance and availability**
  Providers of new digital and data-intensive services may set requirements for the performance of systems that send data into the solution, where, for example, it will not provide sufficient performance or resolution to retrieve data from historians. In instances in which data is retrieved from the OT layer, this could involve large amounts of data, and it may be important that data is updated at all times in order for the service to function. Flowmeter is mentioned as an example in which "you get more out of data at better frequency". Conversely, as seen from the OT side, there may be requirements for adequate response times and availability. These are requirements that can be difficult to satisfy when data flow needs to pass through all layers of security, from OT to IT. There may thus be increased pressure on *direct connection* from the OT layers (0-3) to cloud solutions, which is precisely to ensure performance for the cloud-based solutions. Requirements for performance and consistency in resolution across data streams and sources can lead to increased pressure on transport from the OT layers. Assessments of the need for increased frequency for signals and functions that do not in themselves necessarily provide added value from higher resolution must therefore be held up against both the performance of the individual service and the integrity of the facility. There is good reason to set clear requirements for these potential solutions and how ICT security is managed.

- **Information security and independence**
  Digitalisation essentially expands the attack surface: 1) Greater connectivity and data flow can create an increased number of possible pathways into systems that need to be protected, 2) processing large and complex volumes of data can increase the potential for manipulation of data and analyses, 3) larger code bases where functionality is implemented in software rather than electronics can be manipulated, 4) distributed processing of data outside of a, generally, protected layer can increase the exposure of data that is worthy of protection, and 5) standard IT infrastructure (off-the-shelf) such as OS and communications solutions can have security holes which represent a challenge when patching in an environment that is in close proximity to OT.

  In existing installations, information security is largely maintained by systems that have been developed in accordance with layered architectures with information security mechanisms between the layers, where the lowest and most critical layers at the bottom are protected via the layers above. The most critical component (for safety) - the safety systems - must be independent systems that are segregated from other systems (ref. Facilities Regulations from the Petroleum Safety Authority Norway). There are thus far no signs that safety systems such as gas and fire detection and emergency shutdown have been connected to other systems in the IT layer with an increased risk, however given the development towards data-driven

activities, there is reason to assume that these principles are being challenged, something which requires a special focus, with an explicit assessment of risk. Previous studies [22] show that emergency shutdown systems and vital parts of fire and gas systems can be on the same network as the control systems (on layer 1) in order to be connected to the same operator station and workstations, and to simplify data collection. These design choices will be even more critical if, for example, the control system is compromised, either by the system being directly impacted or through manipulation of data into the system. There will thus be a need to protect the process control system as if it were a safety system.

2.5 Screening of research into digitalisation of IT and OT

In order to formulate an overview of *the research* into the topic, a basic literature search (appendix A) was carried out. The following brief summary highlights the focus in the identified publications:

There is a clear and strong focus in the industry on the potential of big data and that data can lay the foundation for increased innovation, optimisation, improved cost-efficiency and better safety [23-25] [26, 27]. The potential to utilise the increased amounts of data that will become available for more efficient operations is not being fully exploited [27, 28]. There is also a focus on limitations with Big Data. Among other things, these relate to cybersecurity and privacy, however they have thus far not been given enough focus in regulations and standards [29]. A significant challenge is that data is still distributed in silos and greater effect is expected when access to and integration of data increase [30, 31].

Experience shows that there are particularly significant savings to be made from solutions relating to condition-based maintenance. The potential for better HSE has been identified, whereby increased automation reduces the need for manpower offshore, for example, by using solutions for anomaly detection[23]. New projects and developments provide major digitalisation opportunities when solutions can be planned from an early phase. Johan Sverdrup is a good example [20].

Ongoing change and digitalisation processes increase outsourcing of complex ICT solutions, which in turn can increase the risk of undesirable incidents [24]. Research thus far indicates that this risk is not well-enough understood in terms of causality, complexity and interdependence [32]. Increased digitalisation expands the risk picture and the possibility of the industry becoming a target, including from hostile states [33]. Direct attacks on OT systems are considered to be difficult to carry out at the present time (i.e. lower risk), however attacks that target IT systems have a lower threshold and can be a means of accessing OT, for example, by obtaining access to passwords or manuals [33]. This means that there must be the same standard for protecting IT systems as there is for OT systems when considering the increasing degree of connection from the well-controlled safety domain to IT systems [25, 26]. However, good ICT security is a challenge, among other things, due to greater dependence on providers[26].

The current understanding and measures for cybersecurity are not keeping pace with developments [27]. There appears to be a greater focus on digitalisation *gains* than cybersecurity in the knowledge that is disseminated [20, 31]. [20, 31].

Despite there being a major strategic focus on digitalisation and several solutions being in operation, digitalisation (in the industry) is in an early phase. This is reflected in the research, where there is a predominance of conceptual studies and where subcontractors dominate over operators. In a systematic assessment of available research, it was found that as many as 14 out of 34 articles that primarily address *challenges* rank 'cybersecurity' as the greatest challenge for IoT adoption in the oil and gas industry (internationally) [34].

This overview suggests that cybersecurity in general is the current focus of the research (2021). However, there are thus far few signs of specific issues relating to increased connectivity between IT and OT systems. Particular mention can be made of the minor focus thus far on the possible implications of digitalisation for safety systems.

2.6 Relevant experiences from digitalisation of other critical infrastructure

Many industries which are natural to compare with the oil industry have also considered using cloud to a greater or lesser degree. Norsk Vann engaged Powel and SINTEF to conduct a study that covered this issue, and this was documented in the report "Information security and cloud-based services for the water industry" [35]. This presented a selection of security requirements for cloud services that are relevant to water and wastewater plants in Norway, and many of these will also be relevant to the petroleum industry.

The focus on cloud in both the water industry and energy industry has been concentrated around the collection and processing of sensor data, where the results of processing are not directly and automatically used to manage operational control systems (SCADA). A significant difference between the petroleum industry on the one hand, and the water and energy industries on the other, is the approach to emergency shutdown systems (ESD). Energy and water are defined as critical infrastructure, and the primary focus is on security of supply, i.e. customers having water in the tap and electricity in the outlet.

The energy industry is focussed on independence, however this is primarily realised by keeping control room functions (SCADA) separate from open networks, and distribution management systems (DMS) are not able to manipulate SCADA switches directly. Similarly, as of the present date, smart electricity meters (AMS) have been separated from the control room in Norway, however this separation does not necessarily exist in the energy industries in other countries. On assignment from the NVE [36], SINTEF studied how the risk will be impacted by increased integration of these systems; and while it can be concluded that the risk increases, the report also identified several possible measures that have a mitigating effect on the risk. There is reason to believe that there will be closer integration in the future, and it is therefore crucial that ICT security measures are safeguarded to avoid power outage situations similar to those that took place in Ukraine in 2015 and 2016 [37].

Using cloud solutions transfers costs from investment (CAPEX) to operations (OPEX), and also makes it easier to rapidly scale up or down to manage, for example, seasonal variations. Economies of scale can also be achieved by cloud providers having the ability to employ an ICT security group with "critical mass" to a far greater extent than what smaller players are able to do.

The primary focus of other critical infrastructure, such as electrical power and water, is on uptime and deliverability, and less on HSE. A cyberattack does not primarily threaten HSE, but rather business operations and socially critical functions. It is also easier for that industry to go into a safe state, for example though power cuts, than for the oil and gas industry, which is dependent on special extinguishing systems functioning as intended. These differences mean that systems, routines and requirements are not directly transferable beyond general protection of cloud services.

3 Important findings

This chapter provides an overview of findings from interviews and documentation received from the companies.

3.1 What is digitalised and how?

The interviews support the notion that digitalisation in the Norwegian oil and gas industry is a very clear trend and one that affects all actors. Large companies have their own comprehensive digitalisation strategies and defined roles and functions in their organisations. Smaller players do not have the same pronounced strategies, however still have a strong awareness of and commitment to digitalisation – within the limits of their resources. It is important to note that these are not only non-binding objectives – something clearly reflected in investments, competence building, new organisational functions, and new procedures and guidelines. Digitalisation is not just hype, it is a real paradigm shift that is in full swing. As an example, Equinor has a 'digital vision' to 1) Make data available, 2) Develop competence to utilise data, 3) Predict and prevent safety and security incidents, and 4) Robotics to make work easier for humans [38].

The digitalisation trend primarily addresses the IT layer, however is also increasingly affecting OT systems, where data from SAS and operational systems (layers 0-3) is collected in order to create data-based, value-adding services. The objective is of course efficiency gains (for example, predictive maintenance), *however is also* better safety, which is achieved by, for example, establishing better decision-making support (for example, operator support for drilling operators/drillers). This means that we are now also seeing that data from OT systems is increasingly finding its way into cloud solutions or cloud-like solutions. Data is collected from various sensors and low-level equipment, for example, vibration data, temperature and pressure meters, drilling, sand monitoring, etc. This is data that is collected and consolidated over time and which forms the basis for, for example, expert systems, operator support, digital twins and models, which in turn are used to improve or support processes and people close to the OT layer, for example, drilling (model-based kick detection) and predictive maintenance. Expert systems that are currently physically located on the facility and which are managed by the provider via remote login may eventually be moved up into cloud solutions, where data and logic are placed in a different location to where the activity takes place and where one then "loses" the information security measures that one currently enjoys.

In short, data becomes more valuable the more data that has been collected at the same location or in the same system. There are currently a number of different solutions which are based on different technology, however it is reasonable to expect that the development is moving towards increasingly more centralized and standardized sources of data, which are placed in higher layers.

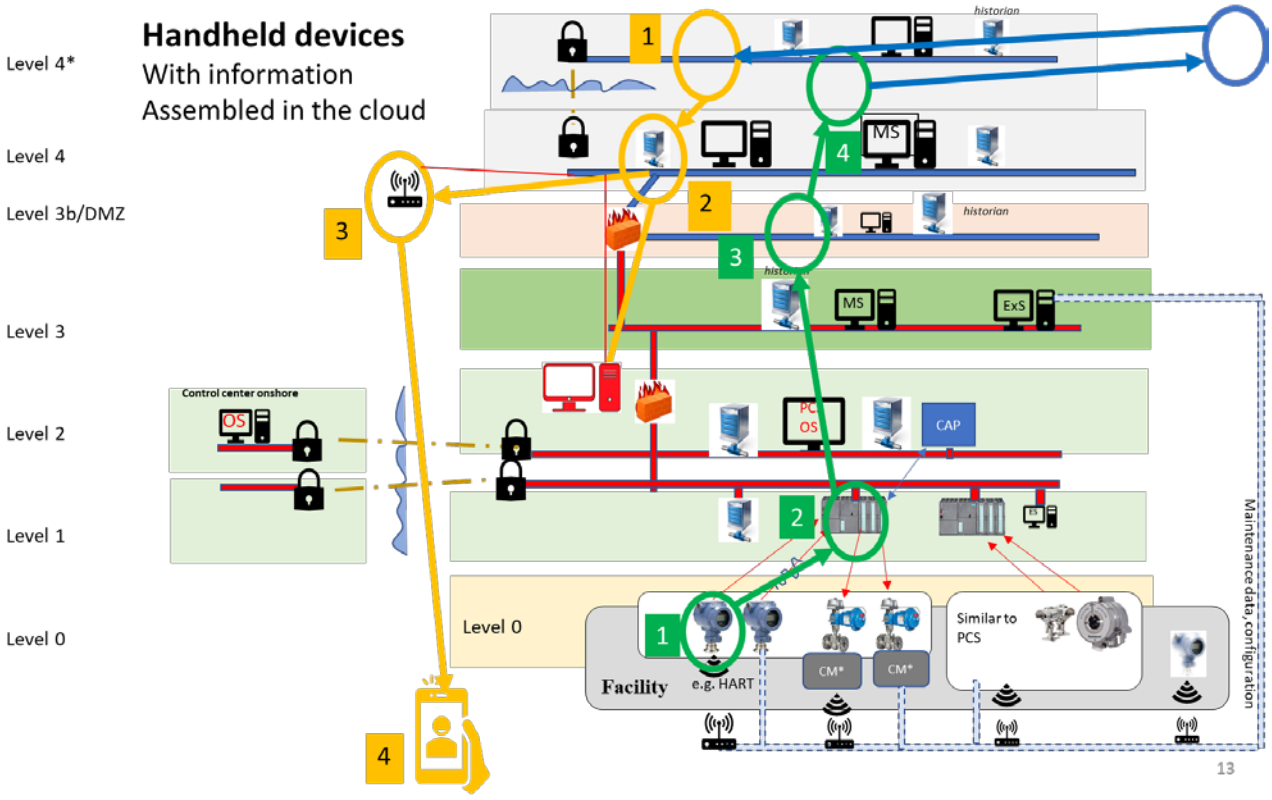


Figure 5 Possible transport routes for data

A confusing picture is painted of the present installations and how data is transported in the overall system, via which systems, and how data is processed, quality controlled, stored and, not least, protected against access from outside parties (cyber security). There are many potential pathways and technical solutions and examples are given of data that is lifted from few levels to many levels, up to IT layers and to cloud solutions. We can also distinguish between vertical integration, which is integration between OT and IT in separate infrastructure, and horizontal integration, which runs between an installation and external service provider that can further integrate with its subcontractors of, for example, Infrastructure as a Service (IaaS). Figure 5 shows a conceptual sketch of an imagined but realistic example of where data flows from the OT layers to the IT layer (including a cloud solution), and back to the operator who is out at the facility. This is very complex, and most actors have reported that they are struggling to maintain an overview – and control.

The amount of data produced, disseminated, stored, and processed is increasing and this challenges established architectures and principles for information security.

Interviews with the companies show a high level of awareness that digitalisation and cloud technology are challenging independence (ref. Facilities Regulations) and security. This is high on the agenda and no findings made in the interviews indicate deviations in relation to the safety systems. The attitude is that it is safe to retrieve data up from OT to IT, however that there are risks

associated with sending data down, for example, in the form of controlling equipment at the OT level, however there is reason to keep an eye on these developments. Four elements of uncertainty have been identified:

- **Uncertainty regarding data flow**
  Data retrieved from the OT layer up to the IT layer, or to a cloud solution, can potentially pass through many levels, systems and security mechanisms, for example, various historians, Integrated Management Systems (IMS), control systems, firewalls and switches. Some new solutions can also go beyond existing infrastructure and retrieve data directly via their own channels. Some service providers may require a direct connection in instances in which the performance in existing infrastructure is inadequate, for example, in relation to performance and response time (because it is not built for this type of use). If this concerns data that is collected from multiple sources and with a high frequency, it can be challenging to have an overview and control. This complexity is further exacerbated when, at a high level in IT or in a cloud layer, there are several systems that retrieve and use data to deliver services – especially if these are systems controlled by other actors.

- **Uncertainty regarding the processing of data**
  When data is lifted up in systems outside the OT layer, and especially in cloud solutions on leased infrastructure (on demand), it will be challenging to have control over how data is processed and stored. This generally includes control over how data is protected, how long data is stored, what happens due to changes in data, how data from multiple sources is compiled, and who has access to data if data is stored in an infrastructure shared with others. Ownership of data becomes unclear. This element of uncertainty naturally enough becomes particularly prominent in instances in which this involves data that is included in services that directly or indirectly impact the OT layer. The impression is that the companies do not have enough awareness of their role and responsibilities as a data owner.

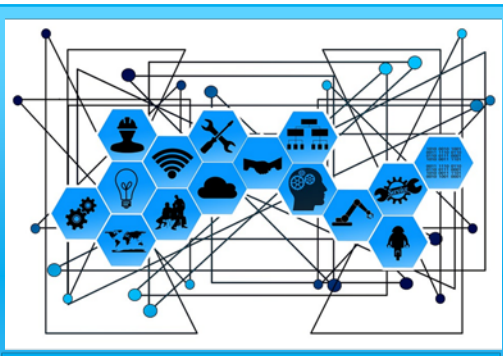
- **Uncertainty regarding the protection of data (increased attack surface)**
  Increased integration with the OT layer increases the attack surface and can impact the independence of a system, for example, SIS. This naturally becomes even more challenging the higher up the integration progresses. This is a risk that the companies are aware of and the clear principle was expressed that no systems at OT level should be directly impacted by new digital solutions in IT or cloud layers. However, there is reason to believe that this is a principle that is being strongly challenged by the potential benefits that can be specifically gained from increased data integration.

- **Uncertainty relating to data quality**
  For data-intensive services, the quality of the data will be strongly indicative of the quality of the service. For example, the quality and precision of a solution for predictive maintenance will depend on the quality of the data collected. This means that safety is reliant on the quality of data, for example, whether incorrect maintenance decisions are made. Time stamping of data appears to be a particular challenge and was mentioned by several actors. Different systems can operate in different time formats and different systems may have different performance/response times which influence timestamping. This can impact the quality of aggregated and collated data.

3.2 Relationship to the providers

Operators and drilling companies have a close connection to their providers and have, over a long time, established good practices for specifications, the use of agreed standards, contract practices and clear distribution of responsibilities, particularly for control systems and safety-critical systems in the OT layer.

This picture is also challenged by the ongoing digitalisation in the industry and we are seeing a completely new type of provider that is offering new types of services. Purely digital services means that it is becoming increasingly unclear as to *where* and *how* purely software-based, data-intensive, and web-based services are executed and how responsibility is distributed. These types of services may also have a different change regime than systems that are physically located on, for example, a platform, i.e. software that constitutes business logic can be improved and changed in a continual process of frequent updates, for example, patching when there are newly discovered threats. This is a clear trend within ICT in general because centralised software can (and should) be changed more easily than systems that need to be installed on physical machines.



The relationship to providers is challenged by an increased focus on data-intensive services.

In general terms, DevOps [39] is an extensive operating and development model for systems in which software is either located in a cloud solution or connected to the provider. Operation/use is synchronized as a continuous process, where experiences and new requirements on the user side (for example, related to ICT security) are sent back to the provider side, which can respond quickly with updates. This has little to do with the development and operation of IACS systems (in the oil and gas industry), however given the ongoing digitalisation, there is reason to expect that providers of cloud-based or connected systems may wish to promote this type of model in the future. However, it is important to note that frequent updates to operating systems which require a high level of availability and uptime will be very challenging.

We are also seeing new providers of data-intensive services that have not previously delivered to the oil and gas industry and therefore do not have the same understanding of the domain as the established players, including special requirements and guidelines for oil and gas. Furthermore, concerns have also been expressed about new and particularly small providers having the expertise and capacity to manage information security, particularly when the customer is forced into having to trust the provider because they themselves do not have the expertise and capacity. This is worth noting, particularly since these are providers that largely base their activities on the collection, processing and use of data that can definitely be said to have an impact on the safety and robustness of operations. If this is combined with the industry's own assessment that the industry itself also lacks sufficient expertise in managing information security in increasingly more connected and data-driven systems, this appears to be an important challenge that needs to be addressed. However, large companies and providers are far more robust. Among other things, established SAS providers offer digital services, which are based on in-depth knowledge of the industry and which have better solutions for information security.

Providers that base their services on compiling data from the OT layer do not necessarily have an adequate understanding of data flows and how systems are protected with the help of zones, conduits, switches, and firewalls, i.e. how systems relate to the Purdue Model that is used as a basis for the network topology on many installations and that is a prerequisite for segregation and independence. Furthermore, certain new data-intensive services will require more in terms of speed and capacity than what existing infrastructure can offer. Existing facilities were naturally enough not designed for integration with solutions in a cloud layer, and some new providers therefore want to be able to connect their solutions directly with the OT layer, primarily to collect data.

Another challenge, which is far from being new, is that some providers of systems "bundle" data and functionality. This means that the customer, for example, an operating company, does not have immediate access to its own data. Some companies expressed a desire to break up this situation, both in order to better control their own data and to be able to use data in new situations, across systems and providers. However, this challenges some providers, who then need to find new business models. If they cannot charge customers, for example, in the form of licenses, then their services and system need to be valued differently.

Some companies also reported that there are providers that request or want more data than they in fact require in order to provide their services. This is understandable from the provider's point of view because data is the entire basis for creating value, particularly with access to data from multiple customers and installations or facilities. Customers and those who own data therefore have to take a greater degree of control and manage what and how much is shared.

The companies should develop a better understanding of their role as data owner and the requirements that have to be set for providers that collect data. Ownership of data should be reflected in requirements and contracts in the same manner as requirements for functionality, performance, time, and cost. For example, it is relevant to set requirements for: 1) protecting data when data is stored and processed outside of own infrastructure, 2) access and sharing when the same infrastructure is shared between customers, 3) safeguarding data over time, and 4) utilising data beyond what is necessary for the service provided.

In principle, the need is the same as for personal data, which is now regulated by the EU's General Data Protection Regulation (GDPR). Ownership of industrial data also needs to be protected, both from a commercial standpoint and from a security standpoint. The European Commission is in the process of drafting the Data Governance Act, which will support data owners in both protecting ownership and utilising data.

3.3 Digitalisation and ICT security challenges for OT

Digitalisation that includes OT, and thereby provides increased connectivity (Figure 3) can generally create new ICT security challenges and challenge the principle of independence. Based on the interviews with industry actors, there is a clear awareness of the challenges facing ICT security, including in relation to OT, however there is still a need to understand this better and to determine the correct measures. There is a high level of complexity and this is difficult to manage – how does one control segregation/security if one does not have control over the flow, location, quality and use of data?

Despite all of the operator and drilling companies that were interviewed being strongly aware of ICT security, it is again the largest actors that have the most resources to develop expertise and capacity in the form of dedicated roles and functions, and to develop their own routines and procedures. They therefore also have an important role in sharing knowledge with the rest of the industry.

An important part of the overall picture is that the ongoing digitalisation largely takes place through collaboration with providers and through the use of new digital and data-intensive solutions and services. If these can have a direct or indirect impact on safety, it is crucial that the system owner (operator) complies with its responsibility to facilitate, control and ensure that this type of provider also satisfies the applicable requirements in the regulations: Section 18 (Qualification and follow-up of other participants) and Section 7 (Responsibilities pursuant to these regulations) of the Framework Regulations, which order the operator to *"see to it that everyone who carries out work on its behalf, either personally, through employees, contractors or subcontractors, complies with requirements stipulated in the health, safety and environment legislation."*

It is not complicated in itself to shell-proof systems to ensure that there are few routes in and out, however if the development moves towards many systems and connections, it also becomes more demanding to have control over the setup and maintenance (including patching) of firewalls and switches that provide the protection.

Some companies practice the principle that all systems that determine integrity should be hosted at the location, for example, a platform. This principle is also being challenged in the hunt for more effective data-intensive services that require the collection of larger amounts of data.

There is a clear attitude that there are risks associated with connections *down* to the OT systems, for example, automated control of OT equipment. At the same time, there is also an attitude that it is safe to retrieve data *up* from the OT systems to the IT layer or a cloud layer under the assumption that compromising data will not directly affect the OT systems. However, this assumes that it is actually a safe transfer. In principle, even solutions in which a system *can only* ask for data have possible weaknesses, for example, in the form of DOS attacks. Diodes were mentioned as a possible solution and are marketed for secure (one-way) transfer of data from an OT system to an IT system, however are not necessarily a solution that covers all needs [40].

However, what is often the case is that such control occurs manually by an operator receiving data (for example, about pressure in pipes via a portable device), that is critical for safe operations. There is currently not a high enough level of confidence in this form of control and, in practice, an operator must, in accordance with detailed procedures, verify data manually with the control room. The operator side have expressed concerns about third-party systems and compliance with processes and procedures. In principle, it makes no difference as to whether management information goes directly to the system or via humans (operator), however the consequence of incorrect information may be the same and, in practice, there is still a requirement for double control.

If many different solutions are established with multiple independent databases and possibly cloud solutions, that are based on different technologies, the *overall picture* becomes very complex, with multiple data silos that need to be managed. Some companies recognise this challenge and want to collect data in one 'super-object' or one central cloud solution. This reduces the complexity and increases the possibility of creating value-added services, however it also means that there is a very high level of vulnerability if an outside party was to be able to obtain access and impact data and services, and it is therefore important that information in such a database is not used in a manner that could impact the OT systems.

There is a major focus on the IEC 62443 series as an important tool for managing new challenges for ICT security, however this standard is still being drafted. It is important to follow up developments and understand how the principles can be applied in practice.

To manage the complexity and challenges associated with ICT security towards and in the OT layer, several actors identified NOG104, and specifically IEC62443, as a basis for this. The former is considered to have become somewhat outdated in relation to digitalisation and the latter is considered incomplete and difficult (thus far) to implement in practice. Naturally enough it is also the major players who have the resources and capacity to manage their development in accordance with the standard, and to contribute to some extent to the development of IEC 62443.

3.4 The need and willingness to cooperate across the industry

The companies that were interviewed gave the clear impression that cooperation in the industry was required in order to understand and solve the challenges while moving in the same direction, and to exploit the opportunities that digitalisation represents. A willingness to engage in this type of cooperation was also expressed. We are already seeing this through a great deal of activity in professional forums such as PDS forum and the newly-established CDS forum, which was created to address cyber-security challenges in particular. These are important meeting places that should be operated and further developed. All actors are essentially working to solve the same challenges that have a high degree of complexity and that require some form of standardisation to mitigate the need to have to manage an excessive number of different strategies and technologies. The very largest actors with the most resources are important for developing knowledge and influencing standardisation work on behalf of actors with fewer resources – this requires transparency and sharing of information. The major SAS providers have established significant expertise and know-how on digitalisation and new technologies, and professional cooperation beyond individual projects and installations would be valuable for the companies. We also see that some actors have formalised cooperation, among other things, for the development of an OPC-UA information model. This is particularly relevant cooperation for supporting the need to exchange data that requires some degree of standardisation and which will reduce tailored one-to-one solutions.

3.5 Interoperability

The clear trend is towards increased interoperability between systems in the OT layer, between OT and IT, and further towards solutions based on cloud technology. There are a myriad of solutions and technologies in existing facilities where the complexity appears to increase in the form of improvements in existing facilities and, not least, in the form of new solutions and services. It is also reasonable to expect that this trend will continue in order to exploit the potential of data-intensive solutions for more efficient operations and extraction. This entails that there will be many different technologies to deal with and, not least, many systems from many established and new providers. A unified architecture and standardisation of interoperability that balances transparency/integration and ICT security are required.

OPC Unified Architecture - OPC-UA (IEC 62541 [41]) has already been identified by some companies and appears to be a focus in the industry, both in Norway and also internationally for process automation.

Open Process Automation (OPA) is an industrial collaboration to define a standard (O-PAS) for an open, secure, and interoperable automation architecture [42]. Among other things, this includes the 'O-PAS Connectivity Framework' (OCF), where OPC UA is used to define the *interface* between different software-based or data-producing systems. OPA has conducted an assessment of various alternatives, and particular emphasis was placed on the following qualities: 1) interoperability, 2) cyber-security, 3) portability, 4) availability, and 5) discoverability. The following three principal reasons are behind the selection of OPC UA:

- It already has extensive support from providers of industrial control systems.
- Supports Open Group's development process.
- Supports the prioritised qualities (referred to above).

This is presently (2020) [42] a standard that is under development and for which it is particularly important to consider throughput and cyber security. It will also be a prerequisite that this is actually adopted as an industry standard, both on the system owner side and on the provider side. On the positive side, it is worth noting that this development is based on a very extensive collaboration between the leading technology players in the industry and, not least, a number of other standardisation processes and initiatives, including ISA-95, OMAC, Industry 4.0 et al.

NAMUR Open Architecture (NOA) [40] is an architecture model based on the principle that systems (OT and IT) are integrated *alongside* existing architecture (established in accordance with IEC 62443). OPC UA is the core standard in NOA for data transfer. NOA is intended to comply with ICT security requirements and is based on the principle of data direction control, whereby all systems must follow the security-by-design principle in IEC 62443.

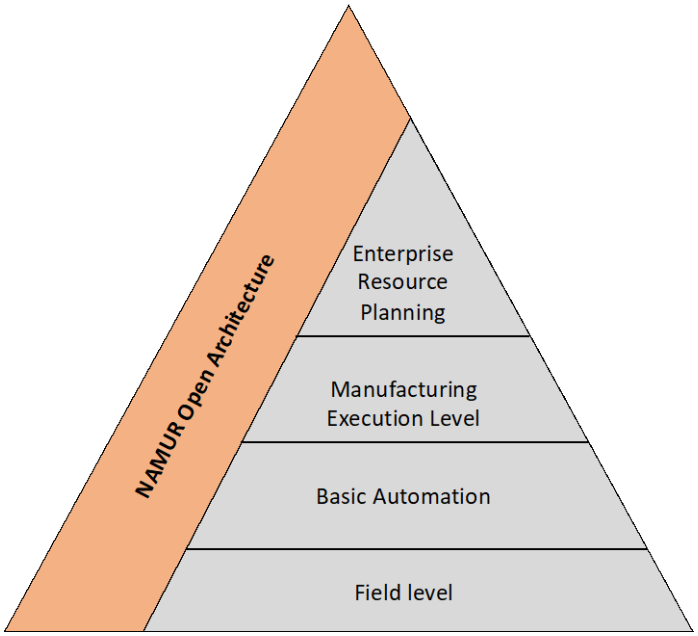


Figure 6 NAMUR Open Architecture

As mentioned, the industry is working with this, and NAMUR OA, OPC-UA, and IEC 62443 can collectively be the right initiative for meeting the need for integration, flexibility/transparency, ICT security, and a coordinated and standardized effort. However, these are standards that are *under development* and for which there is a strong need for competence building, participation in standardisation work, testing to build experience, and, not least, an extensive assessment of whether requirements for ICT security and the independence of safety systems are being met, among other things, in accordance with the PSA's regulations.

3.6 Digitalisation from a HTO perspective

Digitalisation processes naturally create a major focus on technology, however it is therefore also relevant to understand how new digital services impact people and their tasks and responsibilities. While technical safety barriers are important and although new data-intensive solutions may contribute to better safety, humans will still play an important role. We are seeing a development in which technology is simplifying, supporting or partially replacing the operator or parts of the operator's tasks and responsibilities. These can include expert systems, better access to information, digital twins, or other solutions. However, how does this impact the operator over time, and not least his/her ability to influence critical situations? If an operator with expertise and extensive experience becomes passive over time and allows the support systems to "do the job", there is reason to assume that the operator's experience and role will be weakened. On the other hand, some operations become more complex and advanced and require more from the operator. The role, responsibility and interaction with new technology are being developed.

It is important to maintain a human-technology-organisation (HTO) perspective and plan with measures that can reduce these types of consequences of digitalisation processes. Training and competence building (for example, using simulators) are natural suggestions, however there may be reason to believe that these are not being assigned enough focus. See the report "Automation and autonomous systems: Human-centred design" [43].

4 Recommendations

This chapter summarises SINTEF's recommended measures for the industry and the Petroleum Safety Authority Norway, as well as the need for further work with knowledge acquisition.

4.1 The Industry

Recommended measures for the industry are provided in Table 1.

Table 1 Summary of SINTEF's recommended measures for the industry

No.	Challenge	Recommendation
1a	The industry, including the providers, has a major *common* need for expertise that spans a wide range, i.e. digitalisation as a trend in general, and technology, and information security in the interconnection between OT and IT, including cloud solutions. The expertise is not equally distributed, and the largest actors have the greatest capacity, while the smaller actors have to rely more on the expertise of others, including that of the providers (which can also vary significantly).	Continue ongoing competence building, however to an even greater extent as a coordinated effort in the industry. It is important for the industry as a whole that the large actors take responsibility and show a willingness to include the smaller actors and to share expertise.
1b		Utilise and develop common learning arenas. CDS Forum was mentioned as one of the most important in Norway, however it is also important to invest sufficient resources in following developments in other countries, in other industries (critical infrastructure), and in international research.
2	There is a need for standardisation ranging from architecture (which includes digital services), models for interoperability, and information security in increasingly more interconnected (OT) systems.	Follow up, and contribute to, the development of the IEC62443 series – which appears to be the most relevant for information security in the industry. Similarly, the industry should also follow and, if possible, contribute to the development of common reference architecture such as NAMUR Open Architecture and OPC UA.
3	The industry considers NOG104 to be outdated, however still refers to this.	The industry should either refer to other and more up-to-date standards (see recommendation #2), or contribute to updating NOG104 and thus involve the PSA (the guidelines to Section 34a of the Facilities Regulations refer to NOG104).
4	There is and long has been a clear focus on information security in the industry, albeit with a focus on *protecting* data (storage, access, transfer, firewalls, DMZ, viruses, hacking, etc.), however there is not enough focus on data *quality* and data *integrity*. The quality of data-intensive digital services, for example, twins/models, depends *directly* on the quality of data. If the development is now moving towards closer integration of digital (data-intensive) services and OT, data quality will be just as indicative for safety as for data security.	The industry should have a clear, and preferably joint, focus on data quality. This includes a strategy and solutions for, among other things, consolidation, washing, quality control, error correction, etc. Just as the industry is looking towards the development of the IEC62443 series for cybersecurity, it should also consider following the development of similar standard initiatives for data quality, as well as research in this field. Relevant standards and guidelines can be ISWG Data Safety Guidance Version 3.2 [44], ISO 8000 *Data Quality [45],* and DNVGL-RP-0497 *Data quality assessment framework* [46].

No.	Challenge	Recommendation
5	The provider side is changing, with several providers offering digital data-intensive *services*. This includes both established providers, for example the SAS providers, but also completely new players. These providers are dependent on access to data, including from OT, and where access to data creates significant commercial value. The industry is thus far relatively immature in this area, for example, in relation to clarification of ownership of data, requirements for storage over time, and control over how data that is moved out to external parties is used and managed.	The industry should develop a better understanding of its role as a data owner and the requirements that need to be set for providers that collect data. Ownership of data should be reflected in requirements and contracts, and in the companies' follow-up of operations.
6	Digitalisation can create new challenges for information security that are not necessarily covered by existing technology, layered architecture, routines, and expertise. An increasing degree of data flow from OT layers to IT layers in existing infrastructure can create challenges, both in terms of performance and an increased attack surface. At the same time, any side channels (directly from OT to external systems) can create new information security challenges.	The industry should develop a better understanding of how digital services challenge existing architecture: 1) New transport routes for data, 2) scope of data flow, capacity and performance, 3) possible new attack surfaces, including direct channels OT-IT. Adequate information security and follow-up of providers must be established when existing systems and principles are inadequate.
7	Ongoing digitalisation appears to be primarily driven by efficiency targets, for which there is less focus on the potential for increased safety.	The industry should increase its focus on how access to digital services based on more data, with better quality and increased processing capacity, can be utilised to improve safety on installations and in operations.

4.2 The PSA

Recommendations to the Petroleum Safety Authority Norway are given in Table 2. The recommendations are based on information that has been collected from the companies and the analysis which has been made (this report). Some of the comments express desires from the industry that do not naturally fall under the PSA's function and area of responsibility. The industry considers the ongoing digitalisation to be challenging, particularly with regard to ICT security in OT systems that are connected with IT systems. The industry has generally expressed a desire for more direct and specific requirements from the PSA, however where the PSA's function and responsibility delineate the degree of detailed control. The recommendations have been adapted accordingly.

Table 2 Summary of SINTEF's recommended measures for the PSA

No.	Challenge	Recommendation
1a	The industry is calling on the PSA to provide clear guidelines for cybersecurity and safety. There is currently a great deal of uncertainty about how cybersecurity should be handled when OT is being	At the overarching level, the PSA should take greater responsibility for cybersecurity guidelines, with a particular focus on digitalisation solutions that concern the OT layer.

No.	Challenge	Recommendation
1b	increasingly impacted by digitalisation measures and the companies are currently establishing many different measures. The industry does not consider the PSA and NSM to be sufficiently up-to-date on developments. Up until now, the customers have been a greater driving force for cybersecurity than the PSA.	Guidelines that go beyond shell protection should be set, because established principles for protecting layers/functional areas are being challenged by new digital solutions and thus new connections between OT and IT/cloud.
1c		The PSA invests in further development of its own general expertise in digitalisation, and with a particular focus on technology and providers that are relevant to the industry.
2	The industry wants clearer guidelines on ICT security from the PSA. This creates legitimacy and a mandate in one's own organisation and in relation to providers and partners – and thereby a better ability to control the development.	The PSA should be visible in the discussion around challenges, choices of technology, trends, and how the PSA's regulations are understood and can be complied with.
3a	The industry itself refers to IEC62443 and NOG104 as the most relevant standards, however the former is considered incomplete and the latter as outdated (in relation to digitalisation and OT). The applicable revision 06 (audit 06) was last carried out in 2016.	The PSA supports the industry in the preparation of IEC62443 and clarifying how this standard should be applied for the industry.
3b		The guidelines to Section 34a of the Facilities Regulations refer to NOG104. The PSA should consider updating the guidelines with relevant standards (for example, DNVGL-RP-G108) or contribute to updating NOG104.
4	The industry considers the development (digitalisation) to be "chaotic" and driven by very significant objectives with serious potential, but with a complexity that is challenging. All actors are addressing challenges related to new cybersecurity challenges (OT), however in very different ways and with major variation in terms of maturity. The industry itself is calling for a common reference architecture for the industry. This will strengthen internal cooperation in the industry and with the provider side, which is increasingly also made up of digital service providers.	Based on its role, the PSA should contribute towards the establishment of a common reference architecture for the industry. NAMUR Open Architecture was mentioned as a potentially relevant common model. (Other models may also be relevant. There was no comprehensive analysis of this in connection with the assignment – this recommendation is thus far based solely on input from the industry itself.)
5	In connection with the above point, there is also a need for a unified standard/protocol for interoperability between systems internally, and for partners and providers.	The PSA should contribute to establishing a unified standard for interoperability. OPC UA was mentioned as a possible common model. (Other models may also be relevant (no comprehensive analysis has been carried out in connection with the assignment – this recommendation is thus far based solely on input from the industry itself.)
6	Production and drilling appear to be different, with the latter having operated more freely in relation to digitalisation.	The PSA should coordinate guidelines and follow-up more equally in relation to production companies and drilling companies. In principle, the opportunities and challenges they are working with (in connection with OT-focussed digitalisation) are the same.

4.3 Need for knowledge acquisition

The objective of this report has been to provide the industry with a better understanding of the premises for digitalisation. This includes a brief overview of the concept of digitalisation, the experiences and status thus far, and the measures that will drive the industry forward.

The biggest challenge at the present time is the complexity that comes with the already fully ongoing digitalisation in the industry. It is challenging to look at the overall picture because a change is now occurring that is impacting existing systems from a low (OT) to high (IT) level, both at the organisational and technical level, and across companies and providers. This creates a need for new knowledge:

1. There is a general need to develop expertise in the industry, both among the companies as users of and premise providers for technology, and for the providers that need to satisfy the requirements of both customers and the authorities. In the first stage, there is a need to better understand the implications of digitalisation in the industry, and thus both the organisational and technical aspects. The developments that are currently taking place are confusing, with many players, measures, technologies and new standards being developed, and where the IEC62443 series in particular is considered relevant by the industry itself. There is a need to understand the balance between opportunities and limitations, as well as develop expertise regarding the opportunities and responsibilities that the companies have for controlling and following up the providers.
2. The actors in the industry share many of *the same* challenges associated with increasing integration between OT and IT – including cloud solutions. There is thus a need for a *joint effort*, or at the very least, a consolidation towards a reference architecture and common concepts for interoperability – beyond existing layered models (Purdue) that we see are being challenged by increased data flow and new digital services, both in terms of capacity/performance and in terms of information security. NAMUR OA and OPC UA stand out as a joint initiative that could meet the needs of both established and new installations. There will be a need for new knowledge regarding applications and adaptations.
3. Data quality is directly linked to efficiency and safety if digital services impact OT. There is a need for greater knowledge of aggregation, consolidation, washing, quality control, and the use of data in value-adding digital services. This also includes knowledge about the ownership and management of data, and the distribution of responsibilities between companies and service providers. Based on this, there is a need for knowledge about how data quality is ensured in requirements for providers and in contracts. (See also the separate report on data quality in digitalisation processes in the petroleum sector [21]).
4. AI and ML are a class of technology with serious potential for applications in which there is a need to analyse large amounts of data and are thereby relevant to the industry, where access to data is strongly increasing and there is a clear focus on digitalisation. AI is considered to be one of the most important "digitalisation technologies", in addition to, among others, Big Data, Cloud and IIoT, however there is thus far little knowledge about the potential, and not least, the opportunities and limitations in relation to the present regulations. Explainable AI (XAI) in particular is a field in which there is a need for greater focus, particularly in relation to safety-critical systems.
5. Connected software systems enable DevOps models for integrated development and operations where, among other things, information and security holes can generally be more rapidly detected and rectified. However, this is a very challenging model for systems with significant requirements for uptime, availability and independence. There is thus a need for new knowledge about opportunities and limitations.

References

[1] OG21, Technologies for cost and energy efficiency (Final Report), 2019.
[2] Digital 21, Digitale grep for norsk verdiskaping, 2018.
[3] P. Mell and T. Grance, The NIST definition of cloud computing, 2011.
[4] Petroleumstilsynet. Fagstoff, Ord og uttrykk. https://www.ptil.no/fagstoff/ord-og-uttrykk/ (downloaded 14.11.2020)
[5] L. Bodsberg, Grøtan, T.O., Jaatun, M.G,. Wærø, I., IKT-sikkerhet – Fjernarbeid og HMS, SINTEF2019, SINTEF rapport 2019:00361, sluttrapport-ptil-ikt-sikkerhet---fjernarbeid-og-hms-med-underskrift-og-vedlegg.pdf. (downloaded 31.10.2020)
[6] Departementene, Nasjonal strategi for digital sikkerhet, 2019. :https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177 (downloaded 31.10.2020)
[7] Digital Norway, Hva er en digital tvilling? https://digitalnorway.com/lessons/hva-er-en-digital-tvilling/ (downloaded 19.11.2020)
[8] L, Bodsberg, Hale, B., Dahl, Ø., Grøtan, T.O., Jaatun, M.G., Moe, M. Onshus, T., Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten, SINTEF rapport 2018:00572, 2018, https://www.ptil.no/contentassets/d67ffa5187c846fe9a074d1e68f2ce1c/kunnskapsprosjekt-ikt-sikkerhet-sluttrapport-med-underskrift.pdf. (downloaded 31.10.2020)
[9] NOU 2015:13, Digital sårbarhet – sikkert samfunn. Departementenes sikkerhets- og serviceorganisasjon, 2015, https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/.
[10] Digital Norway, Hva er egentlig IoT?, https://digitalnorway.com/topic/hva-er-iot-definisjon/ (downloaded 19.11.2020)
[11] Petroleumstilsynet, Veiledning til rammeforskriften, 2019, https://www.ptil.no/contentassets/332166193108427e978accb21449436c/rammeforskriften20_veiledning_n.pdf, (downloaded 14.11.2020)
[12] NS 5814:2008. Krav til risikovurderinger, 2008.
[13] NS 5832:2014. Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse, 2014.
[14] Society of Risk Analysis, Society for Risk Analysis Glossary, 2018. https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf (downloaded 31.10.2020)
[15] S. O. Johnsen, Lundteigen, M. A., Albrechtsen, E., Grøtan, T. O., Trusler og muligheter knyttet til eDrift, SINTEF rapport nr STF38 A04433, 2005.
[16] H. Lu, L. Guo, M. Azimi, and K. Huang, Oil and Gas 4.0 era: A systematic review and outlook, *Computers in Industry*, vol. 111, pp. 68-90, 2019.
[17] M. V. Ottermo, T. Onshus, and K. S. Bjørkevoll, Bruk av modeller i boring, SINTEF rapport 2021:00056, 2021.
[18] W. Knight, *The Dark Secret at the Heart of AI*, 2017 https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/ (downloaded 20.11.2020)
[19] T. Meling, T. Bjarke, G. Veire, T. Bok, Johan Sverdrup: Lessons-Learned from the Field-Development of a North Sea Giant, *Offshore Technology*, 2020.
[20] P. Larsen, T. Tønnessen, F. Schuchert, Johan Sverdrup: The Digital Flagship," *Offshore Technology*, 2020.
[21] T. Myklebust, T. Onshus, S. Lindskog, and M. V. Ottermo, Datakvalitet ved digitalisering i petroleumssektoren, SINTEF Raport nr STF 2021:00053, 2021.
[22] P. B. Kristoffersen, O. Haugenhåtveit, and K. Omberg, Infrastruktur innen industrielle kontroll- og sikkerhetssystemer, DNV GL CyberSecurity/J-24/25154785/DNV, Rev. 1.1, 2019.

[23] J. S. Brekke, Machine learning effects on the norwegian oil and gas industry, MSc, Universidade Católica Portuguesa, 2020.
[24] A. Gezdur and J. Bhattacharjya, Digitization in the Oil and Gas Industry: Challenges and Opportunities for Supply Chain Partners, *Working Conference on Virtual Enterprises*, 2017.
[25] E. Grange, A Roadmap for Adopting a Digital Lifecycle Approach to Offshore Oil and Gas Production, *Offshore Technology Conference*, 2018.
[26] L. J. Gressgård, K. Melberg, M. Risdal, J. T. Selvik, and R. Ø. Skotnes, Digitalisering i petroleumsnæringen, International Research Institute of Stavanger AS2018.
[27] T. Kruger and E. Marotta, Big Data and Digital Transformation Summary… Three 3 Years of Panel Discussions, *Offshore Technology Conference*, 2020.
[28] E. Knutsen and M. Ileby, Harnessing data effectively to develop a low-manned platform in a remote, North Sea operating environment, *Offshore Technology Conference*, 2018.
[29] T. Nguyen, R. Gosine, and P. Warrian, A Systematic Review of Big Data Analytics for Oil and Gas Industry 4.0, *IEEE Access*, 2020.
[30] H. Devold, T. Graven, and S. Halvorsrød, Digitalization of Oil and Gas Facilities Reduce Cost and Improve Maintenance Operations, *Offshore Technology*, 2017.
[31] F. Laborie, O. Røed, G. Engdahl, and A. Camp, Extracting value from data using an industrial data platform to provide a foundational digital twin, *Offshore Technology*, 2019.
[32] S. Ertenstein and S. Løfgren, Risikovurderinger i forbindelse med outsourcing av informasjons-og kommunikasjonsteknologi (IKT) i petroleumssektoren. uis.brage.unit.no, 2018.
[33] L. Muller, L. Gjesvik, and K. Friis, Cyber-weapons in International Politics: Possible sabotage against the Norwegian petroleum sector (NUPI Report). nupi.brage.unit.no, 2018.
[34] T. Wanasinghe, R. Gosine, L. James, The Internet of Things in the Oil and Gas Industry: A Systematic Review," *IEEE Internet of Things*, 2020.
[35] J. Røstum, Jaatun, M.G., Informasjonssikkerhet og skybaserte tjenester for vannbransjen, 2018, https://norskvann.no/index.php/kompetanse/va-bokhandelen/produkt/681-a238-informasjonssikkerhet-og-skybaserte-tjenester-for-vannbransjen. (downloaded 31.10.2020)
[36] C. Frøystad, M. G. Jaatun, K. Bernsmed, and M. Moe, Risiko-og sårbarhetsanalyse for økt integrasjon av AMS-DMS-SCADA, Norges vassdrags- og energidirektorat. Rapport nr.: 8241017898, 2018, http://publikasjoner.nve.no/eksternrapport/2018/eksternrapport2018_15.pdf. (downloaded 31.10.2020)
[37] A. Cherepanov, WIN32/INDUSTROYER: A new threat for industrial control systems, White paper, *ESET (June 2017)*, 2017.
[38] Equinor. Our digital vision, 2020 https://www.equinor.com/en/how-and-why/digitalisation-in-our-dna.html (downloaded 14.11.2020)
[39] P. Abrahamsson *et al.*, Towards a Secure devops Approach for Cyber-Physical Systems: An Industrial Perspective, *International Journal of Systems and Software Security and Protection (IJSSSP)*, vol. 11, no. 2, pp. 38-57, 2020.
[40] NAMUR, NE 175 NAMUR Open Architecture – NOA Concept, 2020.
[41] I. E. Commission, IEC TR 62541-1: 2016-OPC unified architecture-Part 1: Overview and concepts, IEC, Geneva, CH, Technical Report, 2016.
[42] OPC UA Users and Experts – Conveying Knowledge and Experience: Automation.com, 2020. https://www.automation.com/en-us/products/forms/ebook-opc-technology-specifications-solutions-volu. (downloaded 31.10.2020)
[43] S. O. Johnsen, Holen, S., Aalberg, A.L., Bjørkevoll, K.S., Evjemo, T.E., Johansen, G., Myklebust, T., Okstad, E., Pavlov, A., Porathe, T., "Automatisering og autonome systemer: Menneskesentrert design," SINTEF, 2021:01442, 2021.
[44] Safety-Critical Systems Club, Data Safety Guidance Version 3.2, 2020, https://scsc.uk/publication (downloaded 31.10.2020)

[45] ISO/TS 8000-1:2011 Data Quality, 2011.
[46] DNVGL-RP-0497 Data quality assessment framework, 2017.

Appendix 1: Literature search

A search for research literature was carried out to identify relevant publications that address digitalisation which involve some of the key actors on the Norwegian continental shelf and with topics that are relevant to this report. The objective was to screen the research literature and provide an overview of what was the focus in the information disseminated. We used Google Scholar, which covers a broad spectrum of conferences, workshops and journals.

The following search string was used to define the search:

- All words: *digitalization oil safety*
- And at least one of the following words: *statoil equinor lundin akerb "aker bp"*

There was no defined time period for the search. This was to avoid excluding publications that were incorrectly registered or missing years.

The objective of the search string was to identify publications that:

- Address digitalisation in relation to the oil and gas industry in Norway, preferably with empirical data or examples from relevant actors.
- Discuss digitalisation in relation to the topic of the report.
- Provide insight into issues that have been identified.

This search resulted in 560 publications. To find relevant material, there was a step-by-step exclusion of irrelevant publications:

Step	Exclusion criteria	Excluded	Remaining
1. Search			560
2. Title	- Title obviously irrelevant - Duplicates - Not in English or Norwegian - Books or collections	450	110
3. Abstract	- Publication outside of scope	84	26
4. Full text	- Publication outside of scope - Full text is not open access	13	13