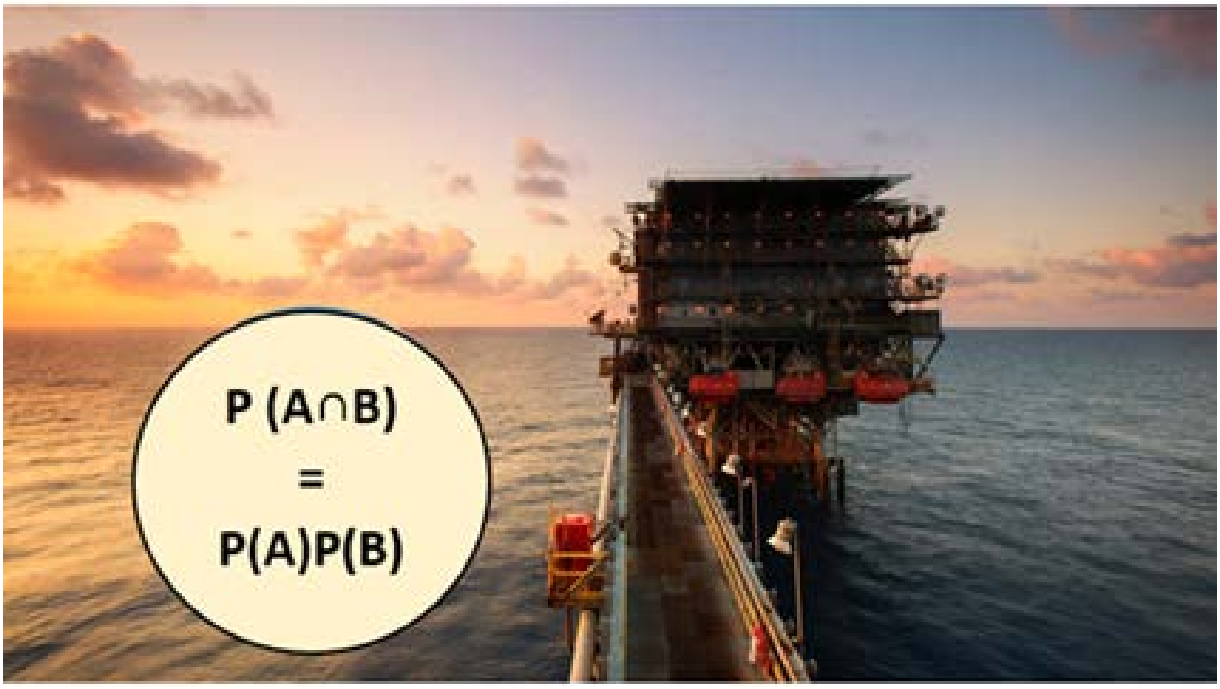

Report

ICT security and independence

Authors:
Tor Onshus, Lars Bodsberg, Stein Hauge, Martin Gilje Jaatun, Mary Ann Lundteigen, Thor Myklebust, Maria Vatshaug Ottermo, Stig Petersen, Egil Wille

Report No:
2023:00188 - 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

ICT security and independence

KEYWORDS
Regulations
ICT security
OT systems

VERSION
1.0

DATE
2023-02-06

AUTHORS
Tor Onshus, Lars Bodsberg, Stein Hauge, Martin Gilje Jaatun, Mary Ann Lundteigen, Thor Myklebust, Maria Vatshaug Ottermo, Stig Petersen, Egil Wille

CLIENT
Petroleum Safety Authority Norway

CLIENT'S REFERENCE
Arne Halvor Embergsrud

PROJECT NO.
102025521

NO. OF PAGES/APPENDICES
56

SUMMARY
The Petroleum Safety Authority Norway's (PSA) regulations set requirements for independence between systems in both the Management Regulations and the Facilities Regulations. There are also equivalent requirements in, for example, IEC 61508 and IEC 61511, which are cited in the guidelines to the regulations. This report assesses whether these requirements will be challenged by possible future technical solutions and how these requirements can be met.

Our focus is on major accidents and not dependencies that can result in lost production only. When assessing ICT security in industrial ICT systems (OT systems), we mainly address availability and integrity related to intentional incidents.

The report is a translation of the SINTEF report 2021:01387 (in Norwegian).

PREPARED BY
Tor Onshus

SIGNATURE *Tor Onshus*
Tor Onshus (7. mar. 2023 08:24 GMT+1)

CHECKED BY
Ranveig Kviseth Tinmannsvik

SIGNATURE *Ranveig Kviseth Tinmannsvik*
Ranveig Kviseth Tinmannsvik (7. mar. 2023 10:16 GMT+1)

APPROVED BY
Anita Øren

SIGNATURE *Anita Øren*
Anita Øren (13. mar. 2023 10:36 GMT+1)

REPORT NO. 2023:00188
ISBN 978-82-14-07957-9
CLASSIFICATION Unrestricted
CLASSIFICATION THIS PAGE Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
1.0	2023-02-06	Translation of SINTEF report 2021:01387

Table of contents

Executive Summary

The Petroleum Safety Authority (PSA) Norway's management regulations and facilities regulations both have a requirement for independence between systems. In addition, there are similar requirements in e.g. IEC 61508 and IEC 61511 that are referred to in the guidelines to the regulations. This report assesses whether these requirements are challenged with possible future technical solutions and how these requirements can be met. We focus on major accident risk and not dependencies that can lead to lost production. When assessing industrial ICT systems (OT systems), our focus is on intentional acts and events, and we look specifically at functional safety (including availability and integrity).

Key questions are how the industry complies with the requirements for independence and how this may develop in the future. Our impression is that systematic analyses that assess dependencies are generally missing and based on this it is fair to conclude that independence is not sufficiently documented.

The development with reduced manning on the offshore facilities and increased information transfer from offshore to land continues and may also be a prerequisite for the future survival of the oil and gas industry. A general requirement from the operators has emerged that all relevant information from offshore located systems should be made available so that it can be analyzed on land. This represents a challenge to safety to avoid negative impacts and potential accidents on the facilities.

One sees that the layered Purdue model, which is intended, among other things, to protect the OT systems from unwanted influences, is undermined, and that many new connections between the OT systems and the surroundings arise. Each connection is not necessarily a problem, but in total they may represent a challenge to functional safety and security.

Maintaining independence will also depend on how ICT security is ensured, and solutions for IT/OT usually have many common functions and systems that need to be safeguarded. Existing instrumented safety systems (SIS) and process control systems must be protected from digital attacks, as they are often not suitably designed to protect against unexpected data traffic and malicious actions. If the development with increased complexity continues, the challenges of securing these systems will increase, as the number of attack points and error mechanisms increases.

Both today's systems for managing field equipment, 5G and new edge and IIoT devices can, unless protected against, be granted access directly into OT systems without authentication and work permits to save time and bureaucracy. This, of course, increases efficiency, but can also represent undesirable access and influence from actors with malicious intents.

There are many standards and initiatives dealing with the protection of OT systems against undesirable influence via communication, but the field remains immature. Nevertheless, it seems that different parts of the standard series IEC 62443 "Security for industrial automation and control systems" are used by major actors. The IEC 62443 series is very comprehensive and contains several parts, including technical specifications and technical reports. The different parts are to a varying degree updated or available in official versions, and e.g., substandard 1-1 and 2-1 are over 10 years old. It can be challenging and resource-demanding to obtain an overview, hence updated guidance on how to implement the standard will be of great benefit to the industry.

We recommend the PSA Norway to consider adjusting section 5 of the management regulations and section 32-34 of the facilities regulations with associated guidelines, to highlight the importance of ICT barriers. We

see an emerging need for the definition of barriers to be expanded from controlling energy to also encompass the information area, e.g., that protection against unwanted data flow and subsequent negative impacts is treated as a barrier function.

Even though key parts of IEC 62443 are not available in updated versions, we recommend that the PSA Norway refers to (parts of) the IEC 62443 series in the guidelines to sections 32 to 34 of the facility regulations. In particular, IEC 62443-3-3 contains several system requirements (and substandard 4-2 corresponding component requirements) that, if implemented, can contribute to independence.

1 Introduction

1.1 Objectives and purpose

The overall objectives of the assignment are:

> Identify and assess how, through the design and delivery of new ICT systems and IIoT solutions, the industry safeguards the Petroleum Safety Authority Norway's (PSA) requirement that the process control and safety systems perform their intended functions independently of other systems and are not adversely affected.

The secondary objectives of the assignment were to:

a. Assess how the process safety and security systems can be adversely affected by each other and by other ICT systems and IIoT solutions, including connections to provider-based cloud solutions outside the OT domain.
b. Assess the extent to which the PSA's requirements for independence will be met.
c. Propose measures which can ensure that the process safety and security systems are not adversely affected by other ICT systems and IIoT solutions.
d. Assess whether there is a need for changes to requirements for independence in the PSA's regulations and what standards are referred to in the PSA's guidelines.

This project is centred around Sections 32-34 of the PSA's Facilities Regulations [43], which state the following:

> *"The system [including fire & gas, emergency shutdown and process safety] shall be able to perform the intended functions independently of other systems."*

The following is stated in the guidelines:

> *"The system may have an interface with other systems as long as it cannot be adversely affected as a consequence of system failures, failures or isolated incidents in these systems."*

The project is part of the focus on ICT security in the petroleum sector (2018-2021), for which DNV and SINTEF have prepared a number of reports for the PSA that investigate various aspects of the topic of ICT security in industrial systems[41]. Both literature reviews and interviews with actors in the industry and with representatives from other sectors and government authorities have been used.

1.2 Restrictions

The assignment placed an emphasis on analysing the new ICT systems and IIoT solutions that are in the process of being used or that may, in the short term (typically a 5-year perspective), be used in Norwegian petroleum activities.

We specifically assess the following requirements in Section 34 (Process safety system) of the PSA's Facilities Regulations: [43]

> *"The process safety system shall be able to perform the intended functions independently of other systems, i.e. that the process safety system is in addition to systems for management and control and other safety systems and that the process safety system can have an interface with other systems if it is not adversely affected as a consequence of system failures, errors or isolated incidents in these systems."*

This section also sets the requirement that the process safety shall be designed with two independent levels of safety to protect equipment, i.e. that the safety levels shall be protected against dependent fault, such that an isolated fault does not lead to the failure of both safety levels, and that the process safety system shall be designed in such a way that it enters or remains in a safe state if a fault occurs that can prevent the system from functioning.

The requirements that the regulations presently set for independence are at a functional and relatively overarching level. We assess whether these independence requirements can be specified and operationalised. In the project, we particularly assess possible additional functional requirements that could complement the current regulations.

We place emphasis on:

- A comprehensive approach to Sections 32-34 of the PSA's Facilities Regulations, including the requirement that the facility shall be designed with two independent levels of safety ("no single fault") and maintain a safe state if a fault occurs.
- Potential challenges relating to safety rather than production regularity.
- "Lift your eyes" – what new systems/solutions will be “coming round the corner” in the next five years.
- Going in-depth on issues relating to new ICT systems/IIOT solutions (for example, OPC Unified Architecture, NAMUR Open Architecture, 5G) rather than well-known challenges in existing systems/solutions.
    - How can new ICT systems impact independence? (For example, achieving independence with different localisation of equipment and system is toned down.)
    - How to compensate when existing protection in a layered structure is removed by "open/flat solutions" (for example, the need for quantum-resistant encryption is not important in the current systems.)
- Assessment of offshore production facilities.
- Overall recommendations for regulatory development rather than specific proposals for text in the regulations.
- Challenges in keeping the systems separate when moving parts of management and control onshore (or to another facility).

The following two principal topics are addressed:

1. New ICT systems and IIoT solutions. (What will be provided in the next 5 years?)
2. Assessment of security. (How to maintain security in the ICT systems/solutions of tomorrow?)

By ICT systems and IIoT solutions, we mean new systems/solutions that can be brought online in the next five years. Unless otherwise specifically stated, the term ICT systems will include both systems and solutions in this report.

1.3 Terms, definitions and abbreviations

1.3.1 Terms and definitions

In Table 1:, we have attempted to adapt terms used in international standards to Norwegian terms. The Norwegian term “sikkerhet” in particular creates challenges because both” safety" and "security" can be used for this everyday speech.

Table 1: Key terms and definitions that are used in the report.

Term	Definition/description	Reference
Authentication	Measure for establishing the validity of a transfer, message or originator, or a means of confirming a person's authorisation to receive certain categories of information.	IEC 62443-1-1 [26]
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 or collectively.	PSA, Words and Expressions [46]
Black channel	Parts of the communication channel are not designed, developed or validated in accordance with IEC 61508, only the endpoints (sender and receiver).	IEC 61784-3 [17]
Cybersecurity	Protection of ICT systems against ICT attacks which can impact confidentiality, integrity and availability of ICT systems. (Note: Some standards also include the term unintended incidents)	IEC 62443-1-2 [26]
Data diode ("Unidirectional gateway or data diode")	Network component which guarantees that when there is a connection between network A and network B, data can only flow from A to B, but not from B to A.	Jones et al [19]
Digital signature	A mechanism for verifying the sender of a message, as well as for determining whether the message has been unlawfully changed after being sent by the sender. The message is signed using a private key (known only to the sender), however can be verified by the corresponding public key (known to everyone). Normally used with a public key infrastructure (PKI).	SINTEF [55]
Hazards	Potential circumstances that could lead to an undesirable incident.	NS 5830:2012 [37]
Functional safety	In this report, we have interpreted this as the protection of human life and health, the environment and material assets through OT systems. "Part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers".	IEC 61511-1 [16]
Hash	A cryptographic checksum that generates a fixed-length result based on a variable amount of data that is fed in. It must be computationally infeasible (“impossible”) to find either: (a) a data object that maps to a pre-specified hash result (the one-way property), or (b) find two data objects that map to the same hash result (the collision-free property).	SINTEF [55]

Term	Definition/description	Reference
ICT system	All systems that perform their functions by sending, receiving, storing, processing and converting information from other systems.	The Office of the Auditor General [49]
ICT attacks	Acts carried out with the intention of damaging or impacting an ICT system.	The Office of the Auditor General [49]
ICT incident	An incident which can impact the confidentiality, integrity and availability of ICT systems. ICT incidents include both intentional acts and unintended incidents	The Office of the Auditor General [49]
ICT incident management	Activities that are performed to stop or limit damage to ICT systems and network resources impacted by incidents or actions that threaten security, and then restore to a secure state.	The Office of the Auditor General [49]
ICT security	Protection of the ICT systems, the interaction between the systems, the services provided by the systems, or information processed in the systems.	NOU 2018:14 [36]
Information security	Ensuring that information does not become known to unauthorised parties (confidentiality), is not changed unintentionally or by unauthorised parties (integrity) and is available as required (availability). The term information security is often used synonymously with ICT security. Information security also includes information that is not exchanged and stored in ICT systems or electronically in some other manner.	The Office of the Auditor General [49]
Industrial Automation and Control System (IACS)	A collection of personnel, hardware, software, procedures, and guidelines that can affect or influence secure operations.	IEC 62443-1-1 [26]
Integrity (of ICT system)	That the information which is processed in the systems, and the services associated with the systems are not altered without authorisation.	IEC 62443-3-1 [26]
Communications Channel (Channel)	Specific communications link in a conduit.	IEC 62443-1-1 [26]
Client	Device or application that receives or requests services or information from a server application.	IEC 62443-1-1 [26]
Confidentiality (of ICT systems)	That the information is only accessible to processes, devices and people who should have lawful access.	IEC 62443-1-1 [26]
Message authentication code (MAC)	Also known as keyed hash function, and typically used between two parties that share a secret key, to authenticate information exchanged between the two parties.	Cheswick [5]
Node	A device in an ICT network. For example, a router, server, or switch	IEC 60050 [14]
Profile (fieldbus)	Defines functional safety for a given fieldbus protocol. Most fieldbuses have their own profile for functional safety, for example, PROFISafe for PROFIBUS and PROFINET.	IEC 61784-3 [17]
Protection profile	Set of security requirements that are independent of implementation and can be applied for evaluating specific user needs.	IEC 62443-1-2 [26]
Proxy	Process which acts "on behalf of" another process, often in a firewall. For example, if there is a need to contact an email	FFI [11]

Term	Definition/description	Reference
	server inside a firewall, one will often connect to a proxy on the firewall that will then forward on messages. A proxy will typically be more basic than the service it represents, and therefore easier to evaluate/secure.	
Risk	Risk means the consequences of the activity and its associated uncertainty. The term “Consequences” is used here as a collective term for all of the consequences the enterprise could potentially cause. The term is not only limited to the final consequences for the enterprise in the form of, for example, injury to or loss of human life and health, harm to the environment and material assets, but also includes conditions and incidents that could cause or lead to these types of consequences.	PSA, Words and Expressions [46]
Router	Functional device that establishes a path through one or more computer networks and forwards packets.	IEC 60050 [14]
Safety	Freedom from unacceptable risk.	IEC 62443-1-1 [26]
Security	Measures for protecting a system.	IEC 62443-1-1 [26]
Server	Functional device that provides services to workstations, to personal computers, or to other functional devices on a computer network.	IEC 60050 [14]
Zone	Grouping of logical or physical devices based on risk, criticality, function, location, access or other criteria. A system can be divided into multiple zones.	IEC 62443-3-2 [26]
System Under Consideration (SUC)	Defined collection of IACS components (including relevant network infrastructure) that together form an automation solution. An SUC consists of one or more zones, as well as related conduits. All devices that are part of the SUC belong to either a zone or a conduit.	IEC 62443-3-2 [26]
Switch	Device that receives signals from a number of inbound lines and forwards these on according to specific rules. (Switches in a telephone network are usually known as switchboards)	IEC 60050 [14]
Vulnerability	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.	NOU 2000:24 [35]
Security measures	Measures for reducing risk associated with intentional undesirable acts.	NS 5830:2012 [37]
Availability (of ICT systems)	The ability of the ICT system to be in a state which enables it to perform a necessary function under certain conditions at a given moment or over a given time interval, provided that the necessary external resources are in place.	IEC 62443-1-1 [34]
Threat	A possible unwanted action which could trigger a negative consequence for an entity's security.	NS 5830:2012 [37]
Conduit	Logical grouping of communications channels with common security requirements, which connect two or more zones.	IEC 62443-1-1 [26]
Undesirable incident	An incident that can have an undesirable impact on an asset and result in a negative consequence for the party that owns, manages or derives benefit from a material or immaterial resource.	NS 5830:2012 [37]

1.3.2 Abbreviations

The abbreviations used in the report are shown in Table 2.

Table 2: Abbreviations used in the report.

Abbreviation	Description
AAS	Asset Administration Shell
BPCS/PCS	Basic Process Control System/Process Control System
EUC	Equipment under control
FR	Foundational Requirements
HMAC	Hash-Based Message Authentication Code - Message authentication code which is implemented with the assistance of a cryptographic hash function according to a specific pattern.
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
ICT	Information and Communications Technology
IIoT	Industrial Internet of Things
IoT	Internet of Things
IPL	Independent Protection Layers
IT	Information Technology
LOPA	Layer of Protection Analysis
MAC	Message Authentication Code
ML	Maturity Level
MTP	Modular Type Package
NEK	Norwegian Electrotechnical Committee
NOA	Namur Open Architecture
NORSOK	The Norwegian shelf's competitive position
NOU	Norwegian Official Reports
NS	Norwegian Standard
NSM	National Security Authority
OPA	Open Process Automation
OPC	Open Platform Communication
OPC UA	OPC Unified Architecture.
OT	Operational Technology
PCS	Process Control System
PKI	Public Key Infrastructure
PFD	Probability of Failure on Demand
PSA	Petroleum Safety Authority Norway
RAMI 4.0	Reference Architectural Model Industrie 4.0
RE	Requirement Enhancement
SAS	Safety and Automation System
SIS	Safety Instrumented Systems
SL	Security Level
SPR	Security Protection Rating
SR	System Requirement
UDP	User Datagram Protocol

1.4 Report structure

Chapter 2 provides the background to the assignment, what is meant by independence and how to model independence. This chapter illustrates the connection between functional safety and ICT security and how these attributes can be influenced by both unintended and intended incidents. The conclusion of the chapter provides examples of typical connections between control and safety systems (OT systems) in petroleum activities on the Norwegian continental shelf.

Chapter 3 summarises requirements for independence in relevant standards and guidelines.

Chapter 4 provides an assessment of possible new dependencies in connection with the implementation of new ICT systems and solutions, including increased use of 5G. This chapter is based on interviews with companies, a literature review and SINTEF's experience and expertise in relation to OT systems.

Chapter 5 provides an assessment of possible measures to combat cyberattacks that could impact critical functions in OT systems.

Chapter 6 discusses how new solutions may lead to possible dependencies and adverse effects and whether or not the PSA's requirements for independence can be said to be fulfilled.

Chapter 7 discusses whether the PSA's regulations should be updated in relation to updated standards and guidelines for ICT security.

Chapter 8 summarises SINTEF's recommendations regarding measures within the industry and the PSA, as well as the need for further work on knowledge acquisition.

2 Present status

2.1 Background to the assignment

OT systems on a facility which were previously separated from the outside world are being modernised and becoming increasingly complex and interconnected with IT systems. This opens up the possibility of more holistic solutions, including management and monitoring from countries where OT systems have multiple connection points with the company's IT systems and extensions to external networks such as cloud solutions via the internet. This means that the traditional distinction between IT systems and OT systems is being challenged. IT equipment is also increasingly being used to safeguard OT functions. Examples are monitoring, maintenance, and configuration systems for field instruments that have traditionally been viewed as IT systems because they do not directly influence production.

The greater complexity of ICT systems entails that new dependencies are introduced, and that the systems are therefore more closely linked. This may mean that the facilities will become more difficult to understand, operate and, not least, maintain, and that in emergency situations it may be more difficult for the operator to obtain an overview of the situation.

2.2 What is meant by independence

In purely mathematical terms, two incidents (A and B) are independent if $P(B|A) = P(B)$. This means that incident B has the same probability of occurring, irrespective of whether A occurs (and vice versa). This also entails that the probability of two independent incidents occurring simultaneously is given by the product of the probabilities: $P(A \cap B) = P(A) \times P(B)$. If this is not the case, the two incidents are dependent.

When calculating the probability of failure on demand (PFD), the β factor is used to indicate the degree of dependency.

Various forms of dependency can arise, and the starting point we use in this project is the following qualitative classification of dependency (not necessarily mutually exclusive).

1. *Functional dependency*, i.e., a system is dependent on another system to function.
2. *Cascading failures,* i.e., that failures in one system occur due to failures in another system — can be linked to both hardware and software failures.
3. *Common components*, i.e., that the same component or module is part of multiple systems – can also include common software.
4. *Common localisation* that enables the systems to be subjected to common influence from either the surroundings (external influence) or operational personnel (human influence).

Some dependencies between systems and components can be obvious, such as a pump requiring cooling to function, or having a common ESD and PSD valve, while other dependencies – for example, common networks or the same software – *may* be more difficult to detect.

Dependencies are often created as a result of technological development, operational and financial assessments, increased standardisation in projects and software upgrades. Some examples of connections and dependencies that are now more or less common in the Norwegian petroleum industry include:

- Dependencies between the process control and process shutdown systems (common operator stations and common communication channels for the control system and security systems).
- Dependencies between security systems and other safety-critical systems and functions, for example, between the seawater and fire water systems, between ballast control and emergency ballasting and between heating, ventilation, and air conditioning (HVAC) and fire & gas systems.
- Common components such as firewalls, network components, operator stations/HMI, configuration tools, clock systems, and domain controllers.

From a security perspective, dependencies are generally undesirable, for example between security systems and the control system, however there can be major design-related, financial and/or other advantages from using such solutions.

2.3 Modelling and analyses of dependencies

The present reliability and risk analyses generally take a relatively rough approach when it comes to modelling dependencies. This is discussed in somewhat more detail for some key analyses.

Quantitative risk analyses such as TRA (Total Risk Analysis) often include all physical areas and safety functions on a facility and cover most incident categories that contribute to the risk of a major accident. Therefore, by their nature, these analyses are relatively rough and rarely consider details related to the complexity and connections between the systems. For example, common components, common influences, cascading failures or operational dependencies are analysed to a limited extent. For hydrocarbon incidents, the analysis normally starts in the event of a leak, which means that the control system and the process shutdown system have not been subject to much analysis. Mostly generic data is used, which implies that average performance of technical systems and personnel is assumed. There is thus often a limited analysis of underlying causes of failures and correlations. Potential dependencies and vulnerabilities in, for example, user interfaces and networks, are therefore rarely detected in risk analyses (or other analyses). It should also be noted that the primary purpose of the overall risk analyses is to verify an acceptable overall risk, as well as provide input for design at a relatively rough level, and that it is therefore not certain that these analyses are suitable for delving into the type of detail that will be required to analyse possible dependencies and links.

Reliability analyses, including Safety Integrity Level (SIL) analyses, normally focus on individual systems, and therefore often go into greater detail with these than in the case of a TRA (where reliability of safety systems often appears as branch probabilities on an incident decision tree). However, since reliability analyses normally examine individual systems, it is in their nature that connections to and dependencies on other systems can quickly fall outside the scope. The same arguments also largely apply to FMECA analyses (Failure Mode, Effects and Criticality Analyses). However, there is not much variation between the analyses and there are of course exceptions to these general considerations.

Layer of Protection Analysis (LOPA) has become a popular method for determining risk reduction requirements and performance requirements for different layers of protection (security functions). On the Norwegian continental shelf, this methodology is often used as an alternative or supplement to Norwegian Oil and Gas 070's guideline for the use of IEC 61508 and 61511 [33] (with deterministic minimum SIL requirements). Simply put, the steps in LOPA are as follows:

1. Identify undesirable incidents.
2. For a given event, identify how often protection is needed to avoid this (demand rate).
3. Identify independent protection layers (IPL) to avoid undesirable incidents.
4. Determine the risk reduction requirements for the various IPLs that provide protection.

These analyses normally derive their input parameters/numerical values from predefined tables and then multiply the probability of failure on demand (PFD) for each of the independent protections together to estimate the performance of all identified layers of protection seen in context.

Since the LOPA methodology itself places limited emphasis on specific assessments of possible dependencies, the quality of any such assessments will largely depend on the competence of the LOPA team and, of course, the time and resources allocated for the analyses. Some other primary challenges related to the follow-up of LOPA analyses include:

1. It has not been verified that the demand rate and reliability of IPLs have the values retrieved from the tables.
2. It is not always verified in operations that the IPLs are maintained in such a way that they retain the assumed performance throughout their lifetime.
3. It is highly demanding to verify that assumptions related to the dependability of manual intervention are fulfilled in operation.
4. It has not been verified that the protective layers are truly independent (that $\beta = 0$).

These observations are also supported by an article written by the original developers of LOPA [3].

2.4 Functional safety and ICT security – unintended and intentional risk elements

Historically, a distinction has been made within the industry between administrative computer systems (office support systems) which process data and information (IT and ICT systems) and computer systems that monitor and control operations (OT systems) on production and drilling facilities. In PSA's regulatory framework, the term ICT systems is used to refer to systems that address the need to obtain, process and disseminate data and information (cf. Section 15 of the Management Regulations [44]). Industrial ICT systems are generally used to refer to OT systems that can manage changes in physical equipment and processes such as control and monitoring systems and security systems. PSA's area of authority in relation to ICT systems is primarily focussed on industrial ICT systems (OT systems) and particularly systems that have a barrier function (safety systems).

In Figure 1 attempts were made to demonstrate why ICT security is also important for functional safety and major accidents.

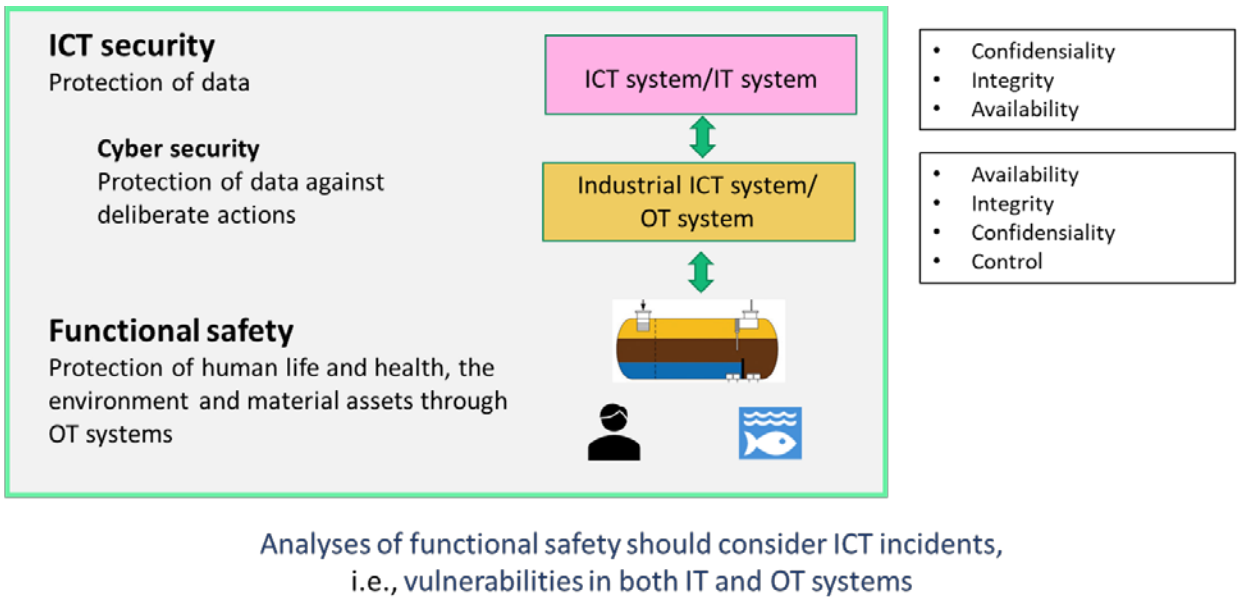

Figure 1 Functional safety, Cyber security and ICT Security.

Technical safety, including functional safety, has traditionally been linked to the need to protect people and the environment from the uncontrolled flow of energy because of unintended incidents and error states. Technical safety encompasses many different types of technical barriers, while functional safety is normally used for barriers implemented with electrical/electronic and programmable systems.

The figure shows that functional safety is impacted by ICT security in both IT and OT systems, and that ICT incidents include both intentional acts and unintended incidents. Important attributes in the ICT system are confidentiality, integrity, and availability. Confidentiality and the protection of data and information against intentional (malicious) acts are often emphasized in IT systems, while availability related to unintended events and error states is often emphasized in OT systems.

As a result of new connections and dependencies between different systems, the energy area and information area will increasingly cross over. An attempt was made to illustrate this in Figure 2, which shows how intended and unintended risk elements can influence both the information and energy areas and how these two areas impact one another. The figure also illustrates measures (barriers) that can be introduced to prevent undesirable consequences. The model is the starting point for a new methodology known as CyPHASS [12], [13] which is designed to systematically identify connections between potential accident situations and loss of control with the information domain.

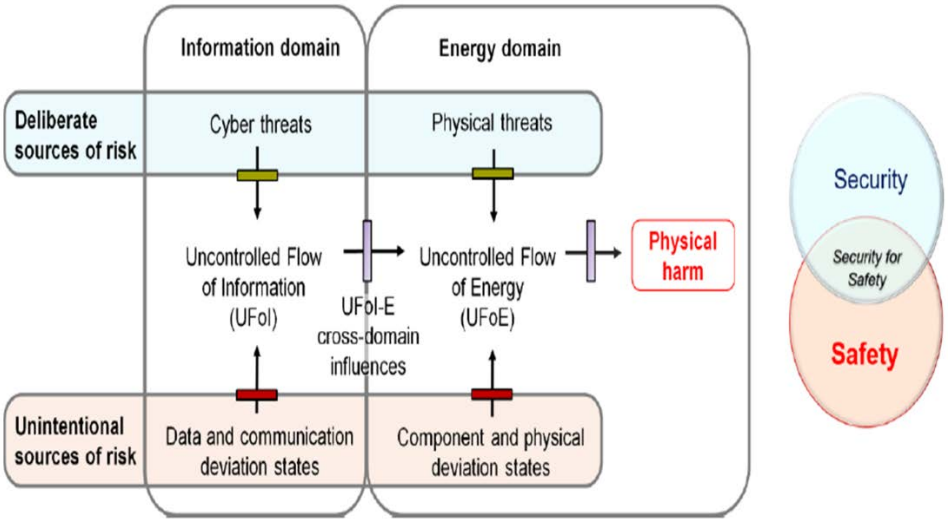

Figure 2 Unintended and intended errors and how these can cause physical harm [Adapted From [13]]

It should be noted that the PSA's regulations and traditional barrier management have primarily been about controlling energy, and that the information area has been relevant to the extent that it can adversely affect the energy area and have the potential to cause physical harm. Whether or not the regulations should be amended as a result of closer connections between the two areas is discussed in more detail in chapter 7.

2.5 The current systems and solutions

Figure 3 and Figure 4 below show typical sketches for production facilities and drilling rigs, as well as examples of data flow between IT and OT systems according to the Purdue Model that some suppliers now want to challenge. It is noted that there may be several variants of the figures for specific facilities.

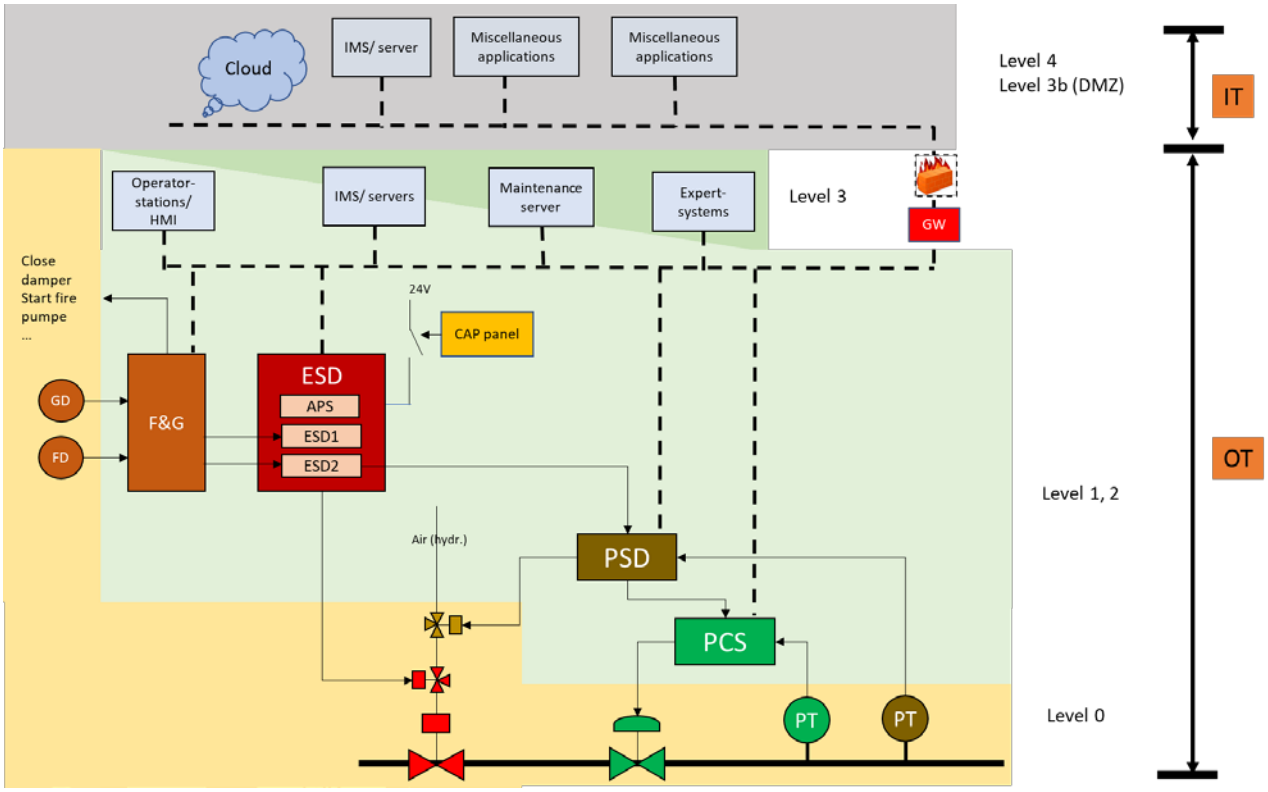

Figure 3 Typical connection between industrial ICT systems on production facilities.

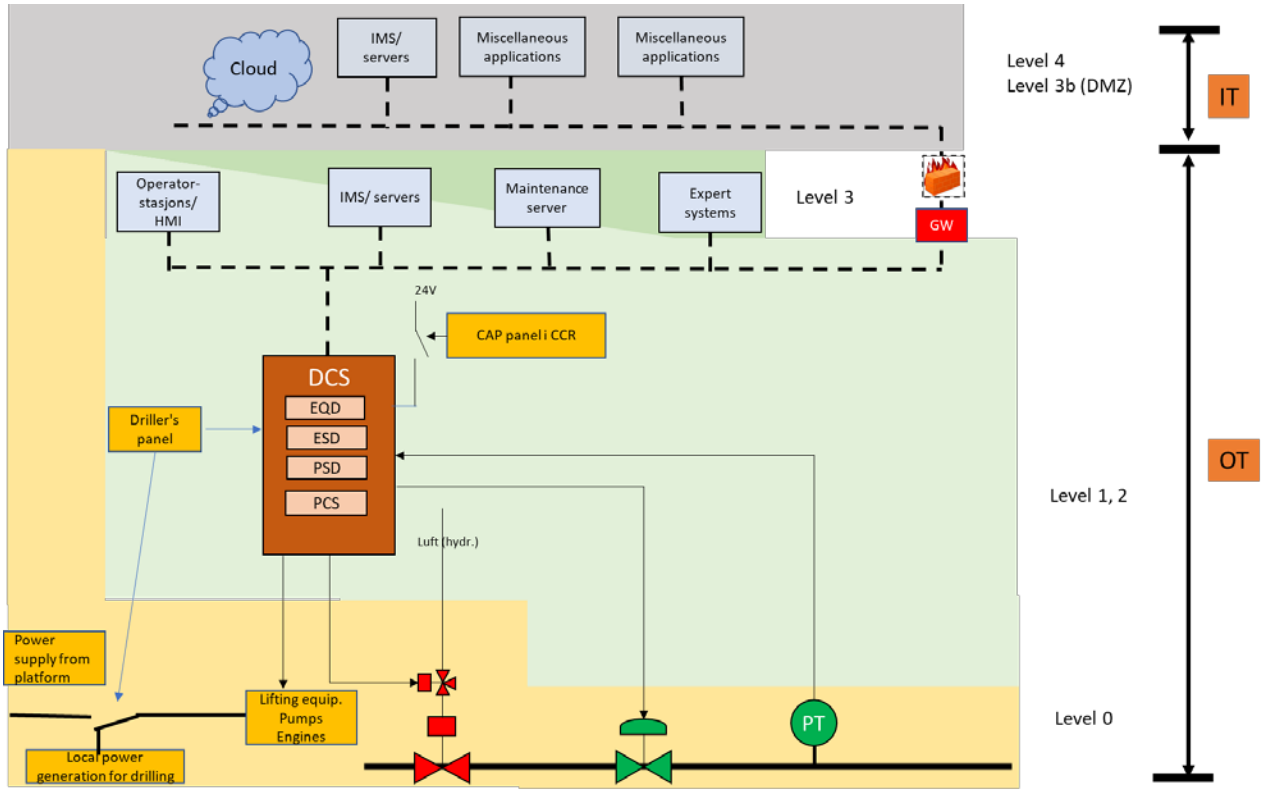

Figure 4 Typical connection between industrial ICT systems on drilling rigs.

The current facilities primarily have three separate instrumented safety systems (SIS), in addition to the control system. These four systems are collectively referred to as the SAS (Safety and Automation System):

- Process Control System (PCS)
- Process ShutDown (PSD)
- Fire and Gas (F&G)
- Emergency ShutDown (ESD)

In connection with drilling, there are also some special systems and parameters in addition to those mentioned above, for example:

- Blowout Preventer (BOP)
- Circulation and maintenance of drilling fluid (Fluid column)
- Rotation speed of the drill bit
- Pressure down in the well

In addition to SAS solutions, there are many other systems that belong to OT and that need to be managed in the same manner, without being integrated into SAS. Some examples include:

- Standalone devices without a connection to SAS (Control Class 3, NORSOK I-002 [34])
- Fiscal metering
- Control systems used for drilling
- Critical marine systems such as positioning, ballast and bilge well systems.

According to the definition of IT/OT, monitoring, maintenance, and configuration systems for field instruments will not be part of the OT, because they do not directly influence the process/production.

The division of levels for the current solutions and systems are largely based on the principles shown in Figure 5.

Among other things, the reason for having this division of layers with several logical levels is that the systems that currently implement the (safety) functions described above are not designed for the current threat landscape and must be protected from undesired outside influence.

There are also solutions in which attempts are being made to differentiate in a PCS network and an SIS network to reduce the possibility that errors on the PCS side will adversely affect the SIS. This can limit traffic on the SIS network, however there are normally still many messages that need to be let through, such as to/from the common user interface and sync signals. Appendix G of Norwegian Oil and Gas 070 includes some conditions for being able to use a common network.

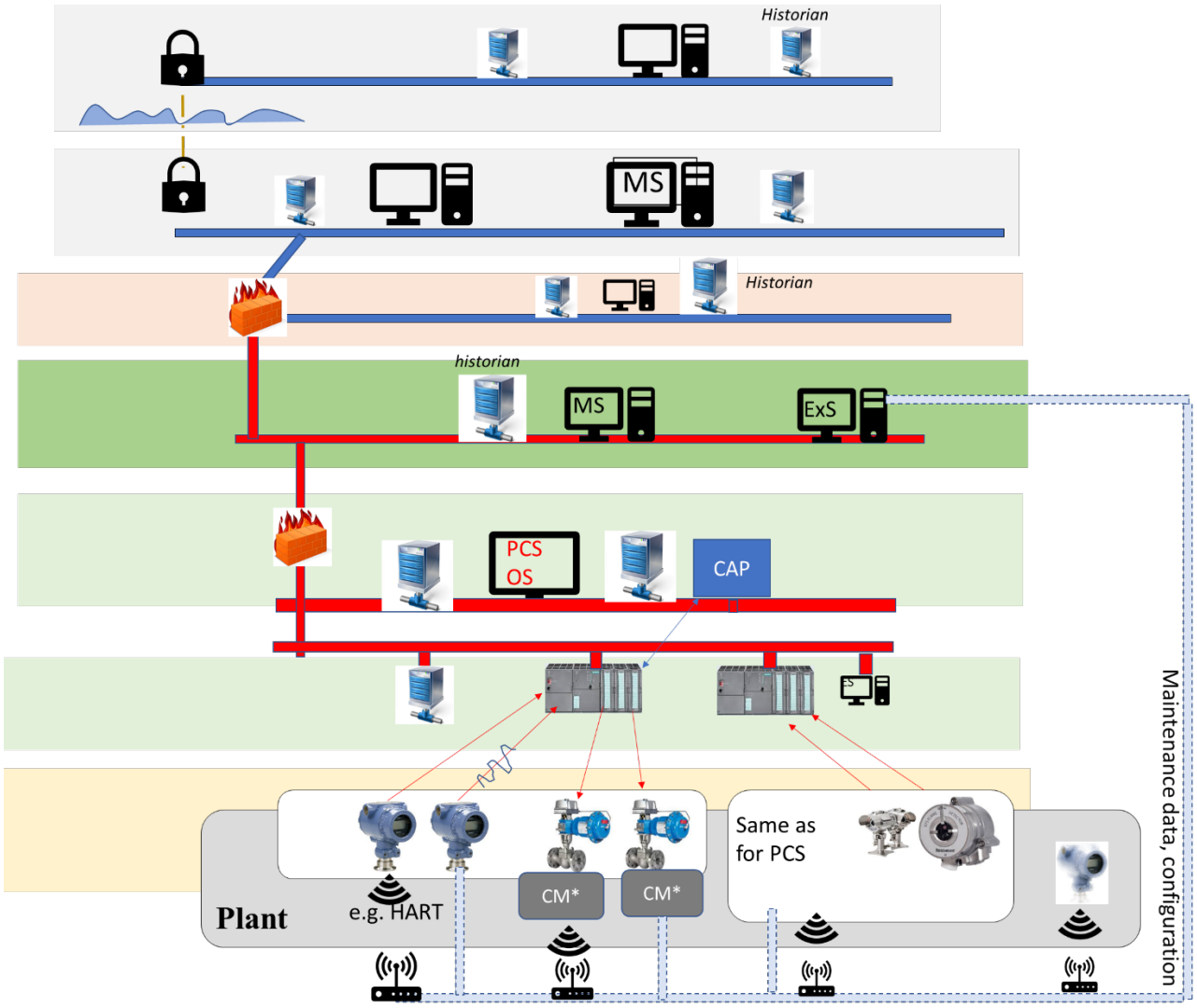

Figure 5 Typical current division of levels for protection of the OT systems.

3 Standards and guidelines and requirements for independence

In the following, some relevant standards and guidelines are discussed, with an emphasis on requirements for independence and proposed solutions in addition to what is stated in the PSA's regulations.

3.1 IEC 62443

IEC 62443 [26] is a series of standards that were developed to protect industrial communication networks and OT systems. The 62443 series is considered by many actors to be a natural framework to follow in order to build and safeguard security in OT systems, and is, among other things, central to DNV's class notation: Cyber Secure for maritime OT systems[8].

One of the basic concepts described in IEC 62443-3-2 is to divide systems and networks into appropriate zones and conduits, to group functions and devices based on criticality, and to delimit/minimize the consequences of undesirable incidents, see Figure 6. In addition, zones and conduits will protect devices and the connections between them from undesirable outside influences.

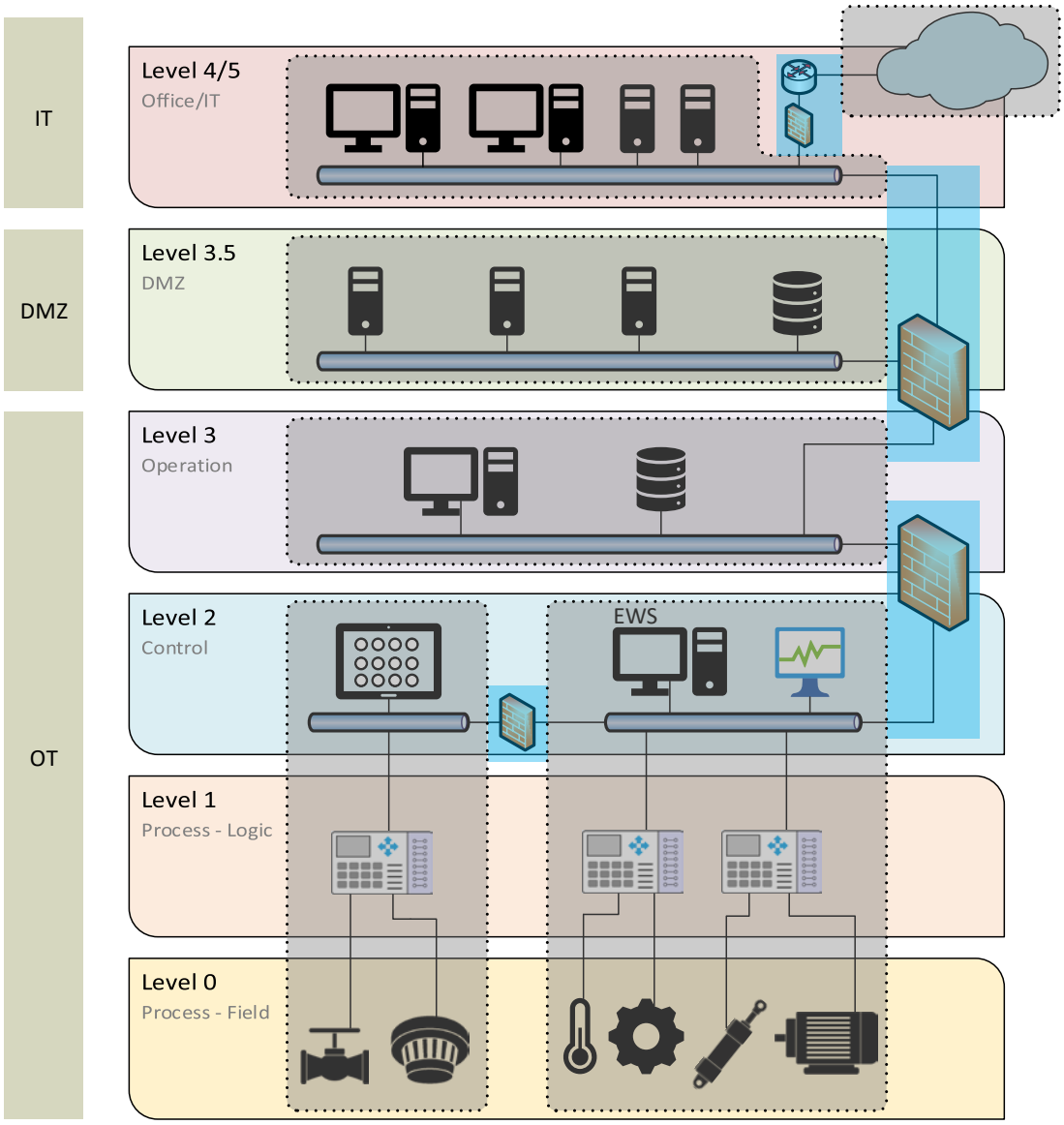

Figure 6 - Example of network topology with zones (grey) and tunnels (blue).

The 62443 series proposes selecting network topology and security barriers based on risk assessments, and thus the degree of independence may vary between different applications/interpretations of 62443.

A key term in IEC 62443 is the "Security Level" (SL). The concept focuses on the fact that zones and conduits should be graded at different levels (SL1–SL4), and IEC 62443-3-3 and IEC 62443-4-2 describe this as being requirements for systems and components included in the different zones. Based on a risk assessment, these security levels represent a framework for determining the necessary protections and measures. The higher the SL, the greater the assessed risk and the higher the level of protection there should be against any malicious attacks.

The "Security Level Capability" a system or component can achieve depends on the degree of fulfilment of seven types of "Foundational Requirements" (FR). These types of requirements are [26]:

- FR1 – "Identification and Authentication Control"
- FR2 – "Use Control"
- FR3 - "System Integrity"
- FR4 – "Data Confidentiality"
- FR5 - "Restricted Data Flow"
- FR6 – "Timely Response to Events"
- FR7 – "Resource Availability"

For each of the seven basic types of requirements, part 3-3 of the standard describes a number of specific system requirements (SR) and associated requirement enhancements (RE) that must be met to achieve a certain level of security (SL), and to meet, for example, SL2, all requirements that give a minimum level 2 must be met for all seven basic requirement categories (FR1–FR7).

If we look at the seven basic types of requirements (FR1 – FR7) that form the basis for a given security level (SL), it is FR5 "Restricted data flow" that has the clearest connection to independence. Chapter 9 of IEC 62443-3-3 stipulates four specific requirements (SR 5.1 – SR 5.4) with additions for "Restricted data flow". The text box on the following page provides an example of this through requirement SR 5.1. As can be seen in the text box, in order to achieve, for example, SL4, in addition to the requirement itself, one also needs to meet the three requirement enhancements.

Another key term in IEC 62443 is "Maturity Level" (ML). While SL primarily deals with technology, ML is more closely related to organisation, and documents its maturity when pertaining to the execution of various operational and maintenance-related processes and routines and deriving retrospective learning from this.

By combining SL and ML, a certain "Security Protection Rating" (SPR1 – SPR4) can be achieved based on rules that are described in more detail in part 2-2 of the standard. However, as of December 2021, only a draft version of this part of the standard was available.

Brief assessment of the IEC 62443 series

The IEC 62443 series is very comprehensive and rich in content and is well-suited for use in OT environments. It is international and well-known and thus facilitates a common understanding and effective interaction between actors. A basic concept is to divide systems and networks into appropriate zones and conduits. The philosophy of zones and conduits assists in creating independence, however, there are no specific requirements for full isolation/independence.

One drawback of this series is that it is difficult to familiarize oneself with because it contains a number of (sub) standards, technical specifications and technical reports. The different parts are also available to varying degrees in updated or official versions, which makes it extra challenging to obtain an overview. This is especially true for smaller actors, who may find that they have to devote considerable resources to familiarising themselves with standards rather than prioritising specific safety work.

SR 5.1 – Network segmentation

Requirement

The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control systems networks from other control system networks

Requirement enhancements

RE 1 - Physical network segmentation

The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control systems networks.

RE 2 - Independence from non-control system networks

The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.

RE 3 – Logical and physical isolation of critical networks

The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.

Security levels

The requirements for the four SL levels relate to SR 5.1 – Network segmentation are:

- SL-C(RDF, control system) 1: SR 5.1
- SL-C(RDF, control system) 2: SR 5.1 (1)
- SL-C(RDF, control system) 3: SR 5.1 (1) (2)
- SL-C(RDF, control system) 4: SR 5.1 (1) (2) (3)

IEC *62443-3-3 (Chapter 9)*

Substandard 3-3 contains system requirements that are linked to "Security Level" (SL) (and in sub-substandard 4-2 these system requirements are reflected in the form of component requirements). The requirements that shall be selected are produced by a risk analysis and an assessment from those who will operate/own the systems (by establishing a so-called “profile” with requirements). Application of, and possibly certification in accordance IEC 62443 is not necessarily enough to assert that a system is completely independent, however it is reasonable to expect a significant degree of independence in systems that meet strict 62443 requirements. The value of a certificate depends on the requirements included in the certification, and it is up to the certification bodies to define good requirement specifications.

Chapter 7 further discusses whether the PSA's regulations should refer to the IEC 62443 series.

3.2 IEC 61508

Similar to the PSA's regulations, IEC 61508-1 (7.5.2.6, point d) [15] also requires PCS to be independent of SIS: *"The EUC control system shall be independent from E/E/PE safety-related systems and other risk reduction measures"*. The conditions for independence are further detailed in a separate section 7.6.2.7 below.

> *The allocation shall proceed taking into account the possibility of common cause failures. If the EUC control system, E/E/PE safety-related systems and other risk reduction measures are to be treated as independent for the allocation, they shall:*
>
> - *be independent such that the likelihood of simultaneous failures between two or more of these different systems or measures is sufficiently low in relation to the required safety integrity;*
> - *be functionally diverse (i.e. use totally different approaches to achieve the same results);*
> - *be based on diverse technologies (i.e. use different types of equipment to achieve the same results);*
> - *not share common parts, services or support systems (for example power supplies) whose failure could result in a dangerous mode of failure of all systems;*
> - *not share common operational, maintenance or test procedures.*
>
> ***IEC 61508-1 (Chapter 7)***

Other than a definition of common faults, the standard does not contain a separate definition of independence, nor does it explicitly describe how to prove or document independence. Appendix D in part 6 of the standard provides checklists and a methodology for estimating the β factor when calculating redundant configurations. The lowest estimate one can have for logic is β=0.5% (0.005), and it states that it would be difficult to justify a lower value.

Brief assessment of IEC 61508

Like the PSA's Facilities Regulations (Sections 32–34), IEC 62508-1 requires that the control system is independent of the safety systems. When elaborating on the independence requirement, wording such as "sufficiently low" is used regarding the probability of simultaneous fault, something that has its parallel in Section 5 of the Management Regulations, which states barriers must be *sufficiently* independent. However, IEC 61508 elaborates somewhat on the requirement for independence by specifying that common components, auxiliary systems, and operational and testing procedures should be avoided.

3.3 IEC 61511

IEC 61511-1 [16] expresses the requirement for independence between PCS and SIS slightly differently than IEC 61508-1. In 11.2.4, the requirement is worded as follows: "*If it is intended not to qualify the BPCS to the IEC 61511 series, then the SIS shall be designed to be separate and independent from the BPCS to the extent that the safety integrity of the SIS is not compromised*".

In a note to the same requirement in IEC 61511, it is also pointed out that SIS and BPCS can use the same physical equipment if it can be shown that a fault in this equipment does not compromise safety functions implemented in SIS.

Brief assessment of IEC 61511

A reasonable interpretation of the standard is that SIS and PCS must be independent, because PCS does not normally satisfy the requirements in IEC 61511. The note is rather similar to what is stated in the guidelines

to the Facilities Regulations and notes that common components can be permitted if this does not impair the ability of the safety functions to be performed.

3.4 NORSOK I-002

A revised version of NORSOK I-002 Industrial Automation and Control Systems was released in October 2021 [34]. It covers functional and technical requirements for the design of industrial automation and control systems (IACS) for processing facilities in the petroleum sector.

Requirements that are particularly linked to the PSA's requirement that the process control and security systems shall perform intended functions independently of other systems and not be adversely affected:

Network and system security design

The IACS network and system design process shall as a minimum follow the security risk assessment for system design as defined in NEK IEC 62443-3-2.

Operational and technical requirements relevant for the design are also important to be included in the design work.

The IACS network and system design shall comply to required security level – targets (SL-T) with relevant countermeasure resulting from NEK IEC 62443-3-2 security risk assessment.

The SL-T guides which requirements and enhancements in NEK IEC 62443-3-3 that is relevant to be evaluated to ensure relevant countermeasures.

The IACS shall have a system log monitoring solution for capture and storage of system logs from all networked devices.

NORSOK I-002

IACS network architecture design

Effort shall be made to use shared network within main IACS network infrastructures based on risk assessments. The following shall be maintained in the design:

- *system independency, reliability, availability, maintainability and performance;*
- *cyber security;*
- *network monitoring and management;*
- *frame prioritization.*

Separate network management solutions should be designed for:

- *general technical network and firewall equipment, including package control system network switches connected to the network;*
- *critical technical network and firewall equipment, including package control system edge network switches connected to the network;*
- *SAS network and firewall equipment*

The IACS networks shall:

- *have capacity to handle the data load for all operational modes;*
- *be scalable with respect to capability and capacity;*
- *support quality of service (QoS) functionality;*
- *prioritise IACS dependent data traffic over non-dependent data traffic;*
- *support virtual local area network (VLAN) functionality;*
- *protect networked devices from unwanted network traffic where relevant;*
- *be able to distribute time to networked devices;*
- *support end-to-end connectivity for management data where required.*

The IACS networks should be based on recognised open industry standards.

The IACS networked devices shall not be connected to different networks by-passing installed firewalls.

The IACS network internet protocol (IP) plan shall be pre-approved by company.

The high availability firewall solution shall be a redundant firewall cluster solution with state synchronisation that support deep package inspection and intrusion detection system

NORSOK I-002

Brief assessment of NORSOK I-002

NORSOK I-002 from 2021 envisages a type of shell protection, where there are the most stringent requirements (SL4) for access to the facility, however lower, for example, for the zone containing SIS (SL1). With lower staffing levels, the use of edge devices, and IIoT, it is probable that access will need to be granted to more people and organisations more often and perhaps permanently through the access system.

When access has first been obtained to the facility and perhaps the zone, it is easier to exert both intentional and unintentional negative influence. It is therefore not evident that strict shell protection provides the best protection against major accidents.

3.5 DNV-RP-G108

DNV's recommended practice for "Cyber security in the oil and gas industry based on IEC 62443"[1] [9] provides actors in the industry with advice on how the IEC 62443 standards should be applied. A key concept in DNV-RP-G108 (and in the IEC 62443 series) is to place the facility's systems in appropriate zones, in order to prevent problems that may arise in one location from spreading to other zones. The guidelines recognize that some communication will be necessary across zones, and this communication will take place through conduits, where separate barriers (for example, firewalls) are required. DNV-RP-G108 also provides specific advice for how remote access solutions should be secured.

The guidelines provide little information about specific independence requirements; however it is worth noting that zoning itself can be a means of reducing dependence. Among other things, DNV-RP-G108 refers to the fact that two of the characteristics that should be documented for zones and conduits are "assumptions and dependencies", and a certain awareness related to dependencies is thereby forced forward.

New systems with a larger number of connections across zones will clearly "challenge" the zoning concept (in the same manner as for ISBR 4 in Norwegian Oil and Gas 104). DNV-RP-G108 also states that "*Wireless communication should be in one or more zones separated from wired communication*", which can be a challenge if one gradually sees extensive use of wireless devices and 5G when interacting with wired devices.

Brief assessment of DNV-RP-G108

DNV-RP-G108 [10] has extracted the most important elements for OT systems from a selection of IEC 62443 standards and summarised this in a practical format in order to make safety work easier for actors in the petroleum sector.

DNV-RP-G108 is based on parts 2-1, 2-4, 3-2, and 3-3 of the IEC 62443 series, of which parts 2-1, 2-4 and 3-3 are under review/being updated (see also section 3.1). Despite having been well-received in the petroleum sector, it is challenging for the authorities to refer to DNV-RP-G108, because it is partly based on draft versions from the IEC 62443 series. One should therefore be aware of which versions from the IEC 62443 series and which version of DNV-RP-G108 (which is planned to be updated) are always in effect.

[1] DNV-RP-G108 September 2017 version revised in October 2021 in connection with the name change from DNV GL to DNV.

3.6 Norwegian Oil and Gas 070, Appendix G

Norwegian Oil and Gas' guideline 070 [33] concern the implementation of IEC 61508 and IEC 61511 in the Norwegian petroleum industry and is referred to in the PSA's regulations. Appendix G of this guideline sets some technical requirements for linking between systems and demonstrates some solutions that are acceptable provided that the measures specified are implemented. Some examples are also given of solutions that are not acceptable, irrespective of the measures initiated.

Brief assessment of Norwegian Oil and Gas 070, Appendix G

The requirements and solutions described in Appendix G were written back in 2004 and are not necessarily suited to the current solutions and challenges. There is thus a need for a complete review and update of the appendix. See also chapter 8.

3.7 NSM's Basic Principles for ICT Security

The National Security Authority (NSM) has released the document "Basic Principles for ICT Security" [38], which is a set of basic principles and specific measures for protecting information systems from unauthorized access, damage or misuse. The basic principles are relevant for all Norwegian enterprises.

Brief assessment of NSM's basic principles

The basic principles are useful at an overarching level, however, do not state anything explicit about independence between systems. The recommendations/measures provided are primarily suited for protecting information systems (IT), and in the event of potential application of (present) OT systems, a somewhat adjusted procedure is recommended[52].

4 Technological trends, new ICT systems and IIoT solutions

In this chapter we will look at technological trends, technologies and solutions that may lead to new dependencies and possible adverse effects, among other things, because of new systems being able to be connected to technical networks. The following are discussed:

- Use of data diodes, see section 4.1.
- Industry 4.0, including Namur Open Architecture (NOA) and OPC Unified Architecture (OPC UA), see section 4.2.
- 5G technology and infrastructure, see section 4.3.
- Edge devices, see section 4.4.
- Handheld devices, see section 4.5.
- External connection to the OT systems, see section 4.6.

One of the primary challenges with the new solutions is that traditional layering is challenged when data is sent across autonomous components as described in, among other things, Industry 4.0. This is illustrated in Figure 7.

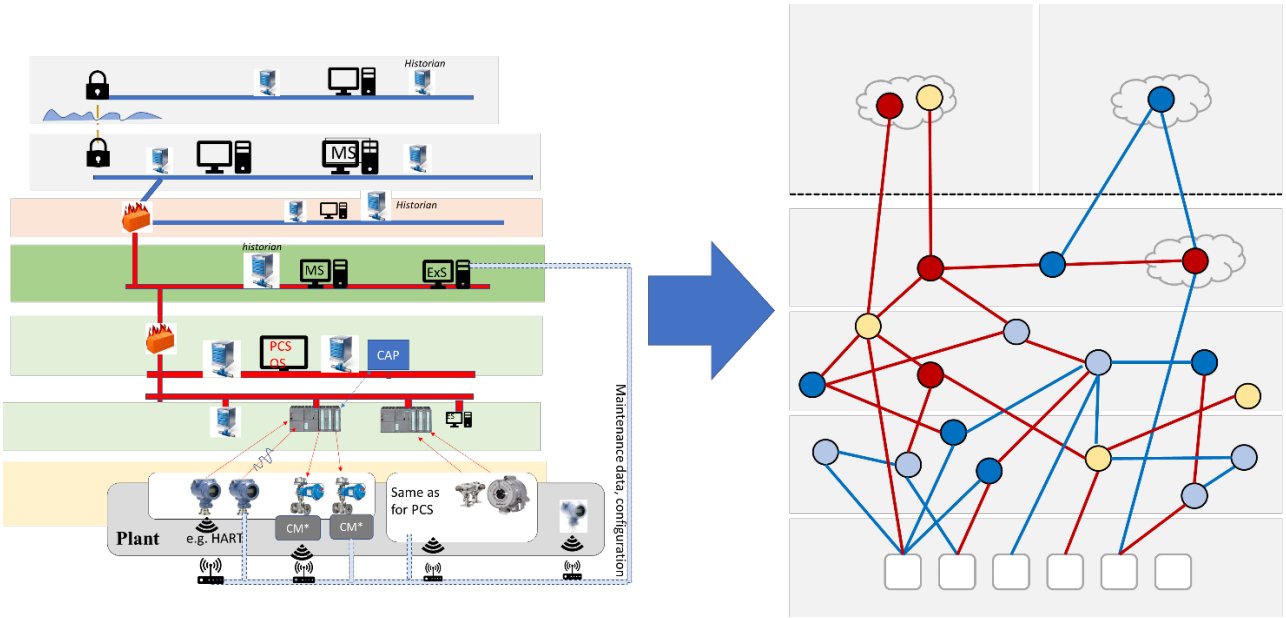

Figure 7 Future transition from the Purdue Model to open and flat structure.

4.1 Data diodes

As explained in the definitions in section 1.3.1, a data diode is a physical network component that, when connecting network A with network B, can guarantee that data can flow from A to B, but not from B to A. There are several different methods of implementing a data diode. An early proposal from Kang and Moskowitz [20] involved a trusted process that wrote to a communication buffer (i.e., a queue), and another trusted process that read from the other end of the communication buffer. However, many such data diodes were designed to ensure confidentiality in situations when writing data from a lower classification level (for

example, “restricted”) to a higher classification level (for example, “Secret”). This is in line with the Bell–LaPadula model [2], however, in our case, the situation is reversed: We want to communicate data from a high-integrity zone to a zone with lower integrity requirements, and we are not concerned with confidentiality - the decisive factor is that equipment in the latter-mentioned zone cannot impact equipment in the former (functional independence).

The solution from Kang and Moskwitz was rather complicated, and subsequent solutions exemplified by Jones and Bowersox [19] were rather based on the use of a light-emitting diode (LED) and a phototransistor. In principle, this is the same as taking a fibre-optic interface where one physically removes the return fibre (see Figure 8). There are many data diodes from different suppliers that have been evaluated in accordance with the Common Criteria at the highest level [4].

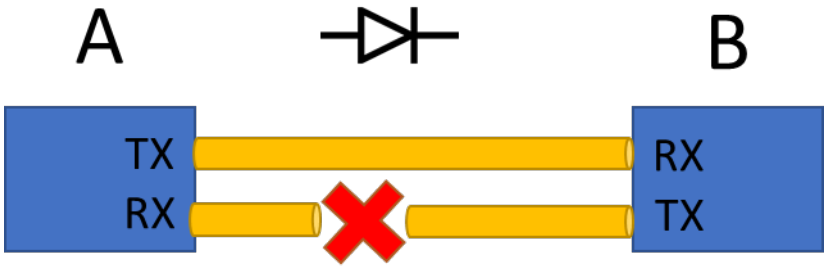

Figure 8: Conceptual description of optical data diode.

As stated in Figure 8, the data diode is an attractive solution in that it can physically guarantee that A is independent of B if the data diode represents the only connection between the two. However, it may represent a problem if there is a need for A to be updated or reconfigured from B. In that case, there would be a need to be able to bypass the data diode in some other manner. On a facility, this could be that maintenance personnel physically travel out to make the changes, which often appears cumbersome and costly. In practice, this means that many who use data diodes simultaneously create “additional solutions” which make it possible to connect to A from B (and other locations). In any event, this will mean that the independence guarantee represented by the data diode will no longer be real.

4.2 Industry 4.0

The term *Industry 4.0* describes the fourth industrial revolution, or rather an evolution in which the internet merges with production and products. The Internet of Things (IoT) is a main driving force in this development, which brings the physical and digital worlds together, and consists of four main parts: The Things, internet connections, data, and analytics[18].

In connection with *Industry 4.0* [7], new platforms are being explored for the seamless interconnection of equipment and data sharing. Industry 4.0 originated in the German manufacturing industry; however, the concept has garnered global acceptance as part of the general trend towards digitalisation.

4.2.1 Industry 4.0 and the petroleum industry

During the initial stage, the petroleum industry has placed emphasis on the development of cloud solutions in which large amounts of data from facilities are collected and shared, however this has been effectuated

without major changes in the underlying networks and systems in OT. At the same time, new initiatives are being launched from both German and global organisations that target the design of OT networks and equipment. This includes requirements and solutions for integration and data exchange between field equipment, controllers, operator stations, servers, and clients for various applications. While *Reference Architecture Model Industrie 4.0* (*RAMI 4.0*) provides the overarching framework for how system integration should occur [47], there are several competing platforms that describe how this can be solved in practice within both OT and the IT network:

- The *Open Process Automation* (OPA) *Forum* [39] proposes both requirements and standardised solutions for seamless connectivity and data exchange at levels 0-2 of the OT network, see Figure 5. Existing system providers can connect to an OPA network via an "OPA interface" or they can develop controllers with full OPA functionality. Realisation is primarily based on the communication protocol OPC UA. It can be noted that safety instrumented systems are omitted from OPA.
- *Modular Type Package* (MTP) [23] is an AutomationML-based standard [1] for configuration for displaying equipment on operator screens, alarm management, diagnostics, and meter readings. Equipment with an MTP interface can be automatically incorporated into the facility's OPC UA based information model and from which the operator stations will retrieve information.
- *Namur Open architecture* (NOA) is more of a concept than a solution for exchanging data between level 1 and 2 equipment on the OT network and higher-level systems and applications (OT, IT) and cloud solutions. It can therefore be argued that NOA takes over where OPA infrastructure ends. NOA proposes the use of a separate communications channel that is independent of the OT network, on the grounds that this is well-suited for existing facilities ("brownfields") [24]. Namur is further discussed in section 4.2.3 below.

OPA, MTP and NOA together cover functions that should have been integrated. This is the background to why German industry has developed *Asset Administration Shell* (AAS) [59][60], which is a practical approach to this. Some operator companies in Norway have identified AAS as being of great interest and have challenged the supplier industry on how AAS can be used [28]. The petroleum industry looks to, among others, German industry, which takes a more offensive stance on standardisation and digitalisation for "plug and play" solutions.

In summary, strong expectations have been created regarding the benefits of using Asset Administration Shell (AAS) to realise RAMI 4.0 (the cornerstone of Industry 4.0). At the same time, this raise concerns that the traditional divisions built into networks and between systems may be erased. It has also been observed that both tools and code, for example for AAS, are published and further developed through open websites (github) as a type of industry initiative. Even though the various platforms (OPA, MTP, NOA, and AAS) claim to safeguard cybersecurity, the solutions also represent a risk of new vulnerabilities through new network structures and means of exchanging data[22].

4.2.2 OPC UA

Open Platform Communication Unified Architecture (OPC UA) is a standard for industrial communication and information modelling that was first published in 2008[39] and has been increasingly adopted in recent years. As the name implies, OPC UA is an open standard, and the purpose of the standard is to ensure the secure and platform-independent exchange of data at field equipment level and between OT and IT. Finding good solutions for this is becoming increasingly more relevant as more field data becomes available. The OPC UA has been adopted by several sectors and is often described as the protocol that can bring data from the field equipment to the office network and/or cloud. The process industry often represents this exchange of data

using the “ISA-95 reference architecture/Purdue Model”. The OPC UA has also become more international in connection with the IEC having issued several OPC UA standards.

4.2.3 NAMUR Open Architecture

NAMUR Open Architecture (NOA) is a framework intended to simplify the introduction of principles and solutions related to Industry 4.0, digitalisation and industrial IoT in the process industry. NOA describes how information exchange between process control systems and the new area "Monitoring and Optimization" (M+O)" can be performed with open interfaces based on data diodes (see section 4.1) to ensure adequate information security (see Figure 9).

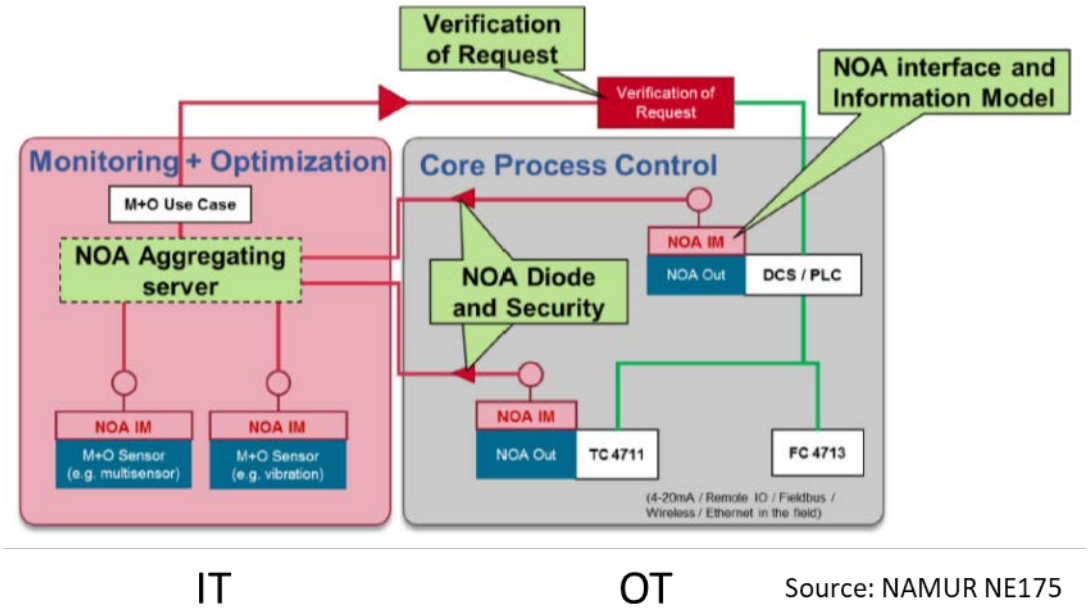

Figure 9 Information exchange between IT and OT with NOA.

NOA is intended for existing brownfield processing plants where, in terms of cost and complexity, it is unrealistic to change the basic principles of the automation pyramid and the layering in the Purdue Model. NOA shall therefore safeguard the integrity of process control systems (OT) while making data and information from controllers and I/O devices available for further analysis and processing in the IT domain (M+O). In this context, a concept known as “NOA diodes” will provide one-way communication with adequate mechanisms for information security. NOA also defines a solution for how to communicate, for example, new set points for process control from M+O back to the OT systems, however details of how this will be implemented as of November 2021 have not been fully specified.

An important limitation of NOA is that communication to and from safety instrumented systems is not part of the standard. It is explicitly stated that the concepts in NOA should not be used for this purpose. Increasing awareness of this in the petroleum industry will be important for ensuring independence by reducing the risk that NOA will, in future, be used to extract information from systems that safeguard functional safety.

4.3 5G

5G is the latest generation of mobile networks, and unlike previous generations, has been specifically designed for applications beyond traditional mobile telephony and mobile broadband. With characteristics such as high data capacity, high reliability, and low latency, 5G is intended for use in, among other things, industry, energy, health and transport.

Another new feature of 5G is the possibility of creating private networks, which are not operated or managed by the traditional mobile operators. This is essential for applications with strict requirements for performance and protection of data, such as industrial control and security systems. However, a prerequisite for private 5G networks is access to frequency resources. In Norway, the National Communications Authority (Nkom) is in the process of finalizing a new regulation for private frequencies for industry and business in the 3.8-4.2 GHz band, which will open up to local, geographically delimited frequency permits on the mainland during 2022. It is expected that equivalent regulations will also apply on the Norwegian continental shelf.

4.3.1 Architecture and technology

A mobile operator's mobile network offers wireless connection to mobile devices (user equipment), which have traditionally consisted of a mobile phone. The wireless coverage comes from a network of base stations, where each base station has a range of up to a few dozen kilometres. Thousands of base stations are therefore required to provide national coverage. This network of base stations is monitored and controlled from a centralized core network, which also handles configuration, authentication, routing, subscriptions, invoicing, etc. A simplified overview of the components in a mobile network is presented in Figure 10.

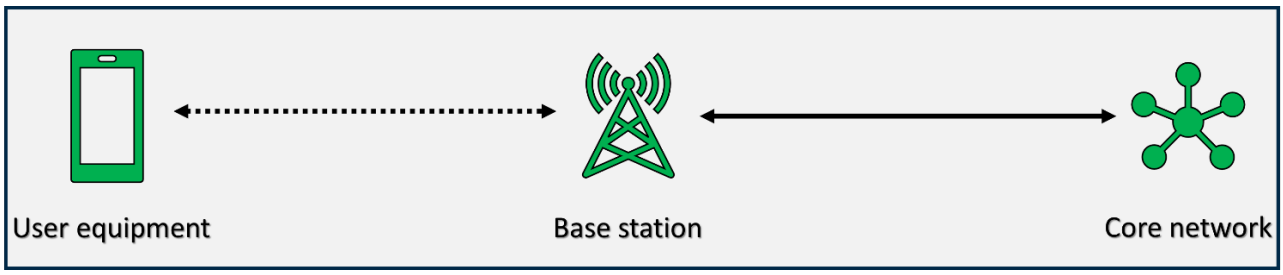

Figure 10 Components in a mobile network.

Technology and components for base stations and core networks are primarily developed by the infrastructure providers Ericsson, Huawei and Nokia, which are subcontractors to the large mobile operators.

4.3.2 Potential areas of use for 5G

5G is a collection of several radio solutions and network technologies with different characteristics, which can be customized and configured for various applications. This flexibility, combined with other innovations, enables 5G to offer:

- Wireless communication with a high level of reliability and low latency for industrial use.
- Wireless sensors with long battery life and range for IoT.
- Local data processing, which enables operations-critical data to be processed quickly and securely.
- Guaranteed capacity and quality through segregation and virtualization of various services.

These characteristics mean that there are many applications for 5G on facilities, including:

- Traditional IT applications such as digital fieldwork, audio/video, AR/VR (augmented reality/virtual reality), etc.
- Sensors for monitoring and optimization for new concepts such as IoT/digitization/NOA.
- Wireless instrumentation for process control and functional safety.
- Control signals and sensor data for drones and robots.
- Area coverage for ships, drilling rigs and possible other facilities within range.
- Emergency communications and next generation emergency networks.

The scope for 5G is illustrated in Figure 11. When viewed in isolation, 5G may not necessarily be the best solution for each of these uses, however the significant commercial benefit for a facility from 5G lies in the fact that one can use a common technology platform and physical infrastructure across many areas of use.

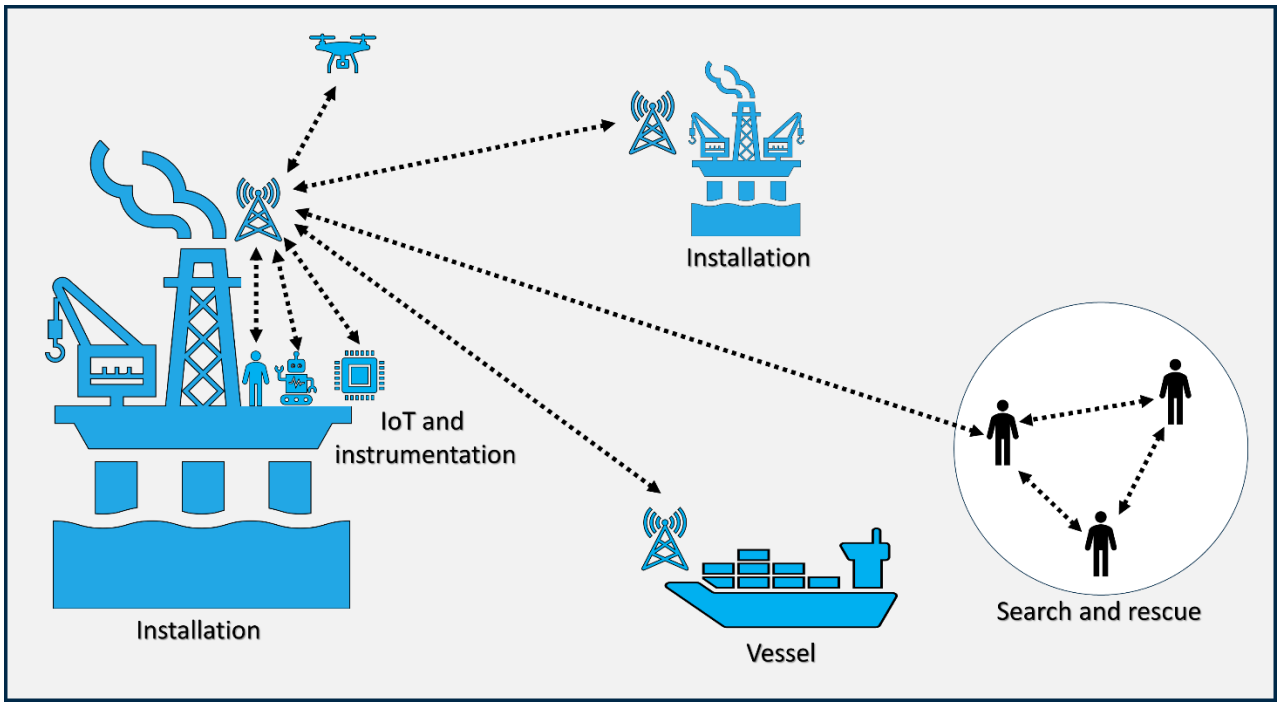

Figure 11 Identified areas of use for 5G.

4.3.3 Integration, operating models and independence

As mentioned in the previous section, the major commercial benefit of 5G is that a common physical infrastructure can be used across multiple areas of use. At the same time, this strength constitutes a risk and vulnerability since facilities now have access to infrastructure that can be used across IT, OT and IoT. By using virtualization and logical separation of various applications (also known as “network slicing"), 5G can provide a system architecture where base stations pass on data from user equipment to applications at multiple levels of the Purdue Model. A base station can therefore become a common physical component used for both IT and OT, including systems for functional safety. This is illustrated in Figure 12.

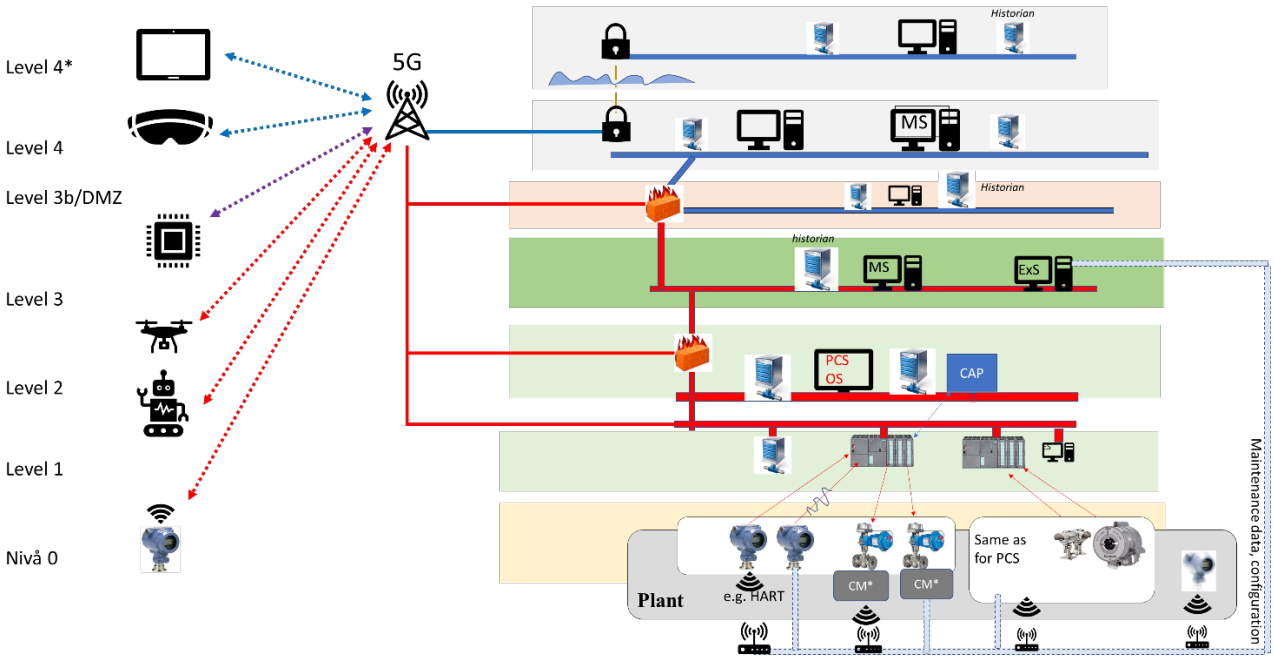

Figure 12 Integration of 5G with the Purdue Model.

Another challenge with 5G on facilities relates to value chains and operating models. At the time of writing, it is a consistent trend for industrial 5G that mobile operators will be involved in the operation and maintenance of 5G networks and infrastructure, primarily through cloud-based solutions. This applies both to the use of public infrastructure from national operating companies or whether equipment is acquired from an infrastructure provider (for example, Nokia or Ericsson). A possible (and probable) operating model for 5G is outlined in Figure 13. In this model, an imaginary operating company is installing 5G base stations on two offshore installations, with a centralized core network onshore. The operating company has access to basic monitoring and management of the 5G network via a cloud service. Via the same cloud service, the mobile operator also has much more detailed access to the setup, configuration, data flow and status of the 5G network, including change options for the setup of the base stations on the facilities.

A further challenge related to the use of 5G on facilities concerns the expected global scope that 5G will have in the coming years. As mentioned at the start, the intention is that 5G shall be used for applications within multiple domains, for example, critical infrastructure, transport, logistics, industry, health, military/defence and emergency networks. The result of this is that the national networks of the telecommunications operators are provided with common physical infrastructure that serves many societal functions. Furthermore, private 5G networks will use the same common technology platform to serve an even wider range of operations-critical applications within industry and the business sector. 5G also has complex value chains with new actors, several of which must be expected to have limited domain knowledge and understanding of, for example, industrial requirements and operating models. On the whole, this leads to a dramatic change in the risk and vulnerability landscape, where any attacks by actors with malicious intentions can have major consequences at the societal level.

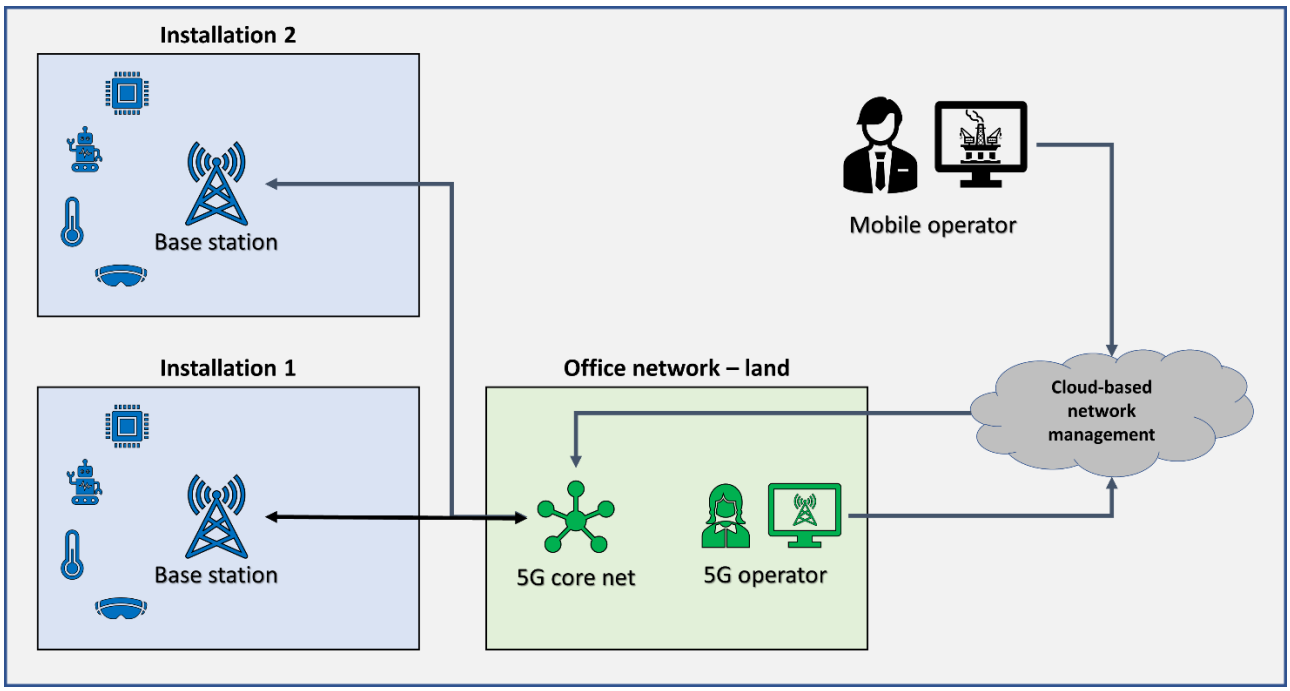

Figure 13 Possible operating model for 5G.

In summary, 5G provides new opportunities for cost savings and streamlining operations and activities across IT, OT and IoT, and many facilities are expected to have 5G infrastructure in the future. However, this technology also brings with it three categories of challenges:

- 5G base stations will become a common infrastructure used simultaneously for multilevel applications in the Purdue Model.
- The 5G business models involve cloud-based solutions where telecommunications operators have full access to configuration and setup of infrastructure on facilities
- 5G will be a common infrastructure and common technology platform that will be used in industry, transport, health, defence, emergency networks, etc., thus making it a very attractive target for malicious actors.

It should be further investigated as to whether 5G has adequate protective mechanisms (for example, network slicing, virtualization, encryption) to safeguard the principle of independence.

4.4 Edge devices

Edge devices appear to be increasingly used to extract data from the OT systems. There is no clear definition other than that they are used on the edge of the IT/OT that otherwise exists. The technology and protocols are also not unambiguous but depend on the supplier and who it is that will retrieve data. There are several reasons why these devices are used:

- Information may be lost while it is passing through the layers of the Purdue Model because there may be a desire to reduce bandwidth and storage needs, for example:
  - Messages for a time interval.
  - Not sending over all values.

- Updating values only when they have changed by a certain value in relation to when they were last sent.

- One wants to retrieve information other than what is available and installs IIoT devices that can extract other information.

Figure 14 demonstrates the principle of a possible connection of an edge device. This solution initially looks permissible; however, it must be remembered that, in order to realise a lossless transfer, a protocol that has messages in both directions must be used. One must either inquire about values or sign on to receive, and this requires good protection to prevent anything else from joining these messages.

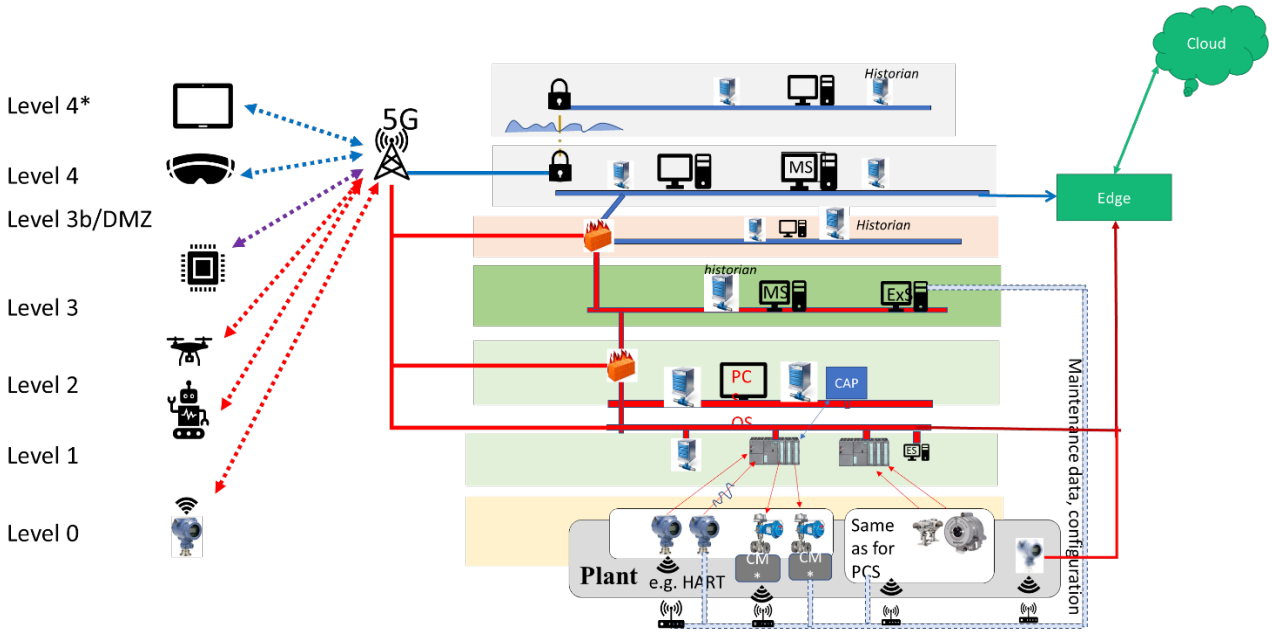

Figure 14 Connection of edge device for retrieving information.

The use of edge devices is further problematised in Figure 15, which looks at potential adverse effects for safety systems.

It is particularly where information is extracted from devices that are part of safety functions that it is critical to protect against “stowaways”. To avoid problems with operations, the PCS must also generally be protected. Such forms of protection can be demanding, especially for “cheap” devices which do not have sufficient computing power and battery capacity, particularly in wireless devices and, for example, in a pressure transmitter. As part of the OPC UA, there are possible solutions, see Section 4.2.2.

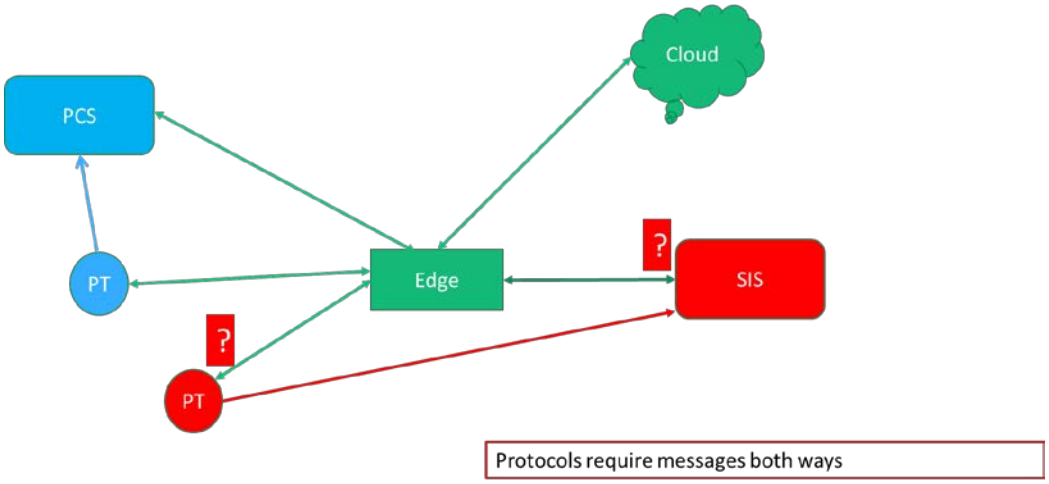

Figure 15 Possible adverse effects for SIS from edge device.

4.5 Handheld devices

Handheld devices are an example of new ICT systems that can be connected to technical networks. The information that can be presented in handheld devices *may also be used* as a basis for work in the processing facility, for example, to check the pressure and conditions of part of the process before opening a manhole for internal inspection and work. Even if all formalities, such as work permits etc., are in order, one can imagine that a dangerous situation could occur if the handheld device incorrectly shows that the pressure has been evacuated, and the operator opens the manhole because he/she trusts this information.

Figure 16 illustrates the possible data flow for values from a transmitter up to the cloud (green), where the information from different sources is connected and transferred down to a handheld device on the facility (yellow). If the information from the cloud is somehow passed through the DMZ, either to be sent to the handheld device or to be displayed on the usual screens of the operators, there will then be a challenge in securing the connection from the OT up into the cloud and back to the OT. If it is done in this manner, the cloud solution can be considered part of the OT and must therefore be protected from errors and adverse effects. Even with the solution shown in Figure 16, there are challenges associated with either the field operator or those in the control room being able to make decisions based on information generated and sent from the cloud. If it is not possible to adequately ensure the quality and connection to and from the cloud, procedures must be used to control what decisions can be made based on this information. Similar problems may also arise within drilling.

Wireless instrumentation presents some of the same challenges as handheld devices. A wireless detector can be connected to the F&G node with its own dedicated network that has nothing in common with other networks, thus entailing that the information does not have to be passed down through the DMZ. The fact that the detector uses a protocol based on the same principles as the PROFIsafe does not provide a satisfactory solution to protect against such penetration of the DMZ. See section 5.1.

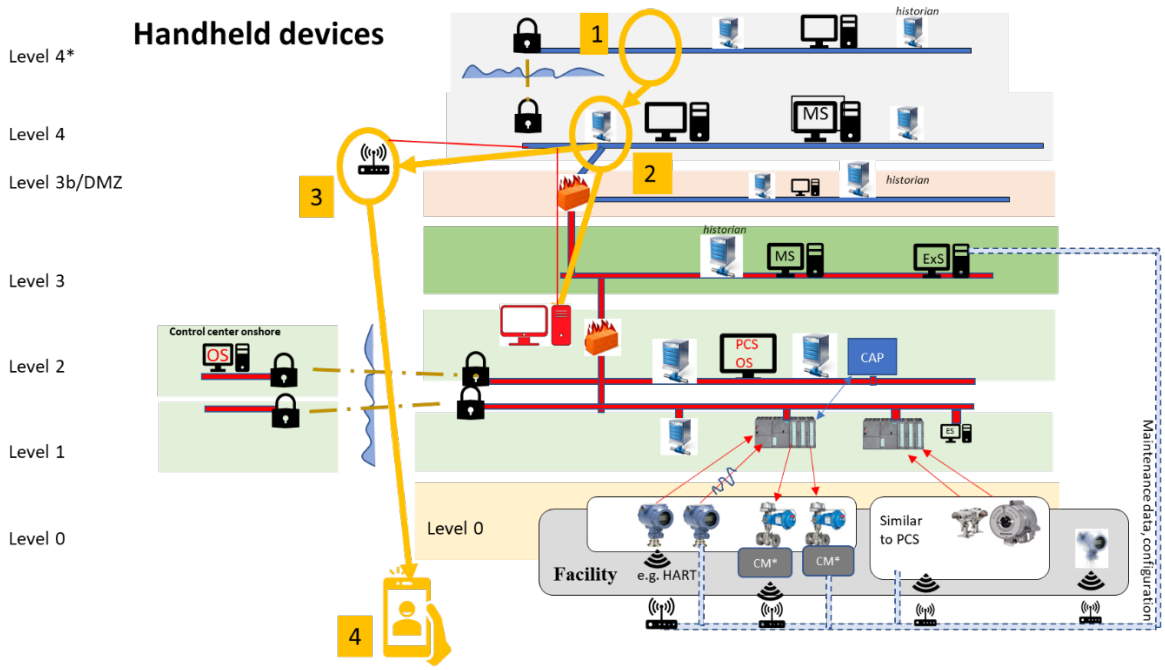

Figure 16 Illustration of logical data flow using handheld devices.

4.6 Remote access to the OT systems

Data quality and data protection are especially important when connecting remotely and accessing the IT and OT systems. Remote connections to IT systems have long been possible. The new element is that OT systems, which were previously shielded from the office network, are now becoming accessible from remote locations via connections over the internet. The motivation for this development is to reduce costs by improving efficiency and moving personnel onshore, and also to be able to provide better decision-making support to operational and maintenance personnel, for example, by allowing suppliers or other experts onshore access to the systems. By moving personnel onshore, it can also be argued that the risk associated with dangerous incidents will be reduced due to reduced exposure (consequence), which means that a safety benefit is also achieved. However, automated and remote-controlled systems will bring new risk elements, and an awareness of this is crucial.

There has been a continuous development in technologies to ensure data flow via remote connection to OT systems - from a situation where everyone has access to everything in a flat technical network, to a situation where some form of data filtering function is used to control access to different subsystems. For example, VPN technology has existed since the 1990s, with protocols such as SSL and IPSec. However, without encryption, the VLAN for shielding the safety instrumented systems (as described in Appendix G.3 in Norwegian Oil and Gas 070) will only constitute "tagging" of traffic, and not provide any security against an attacker that has access to the technical network.

Typical requirements for remote access are that all connections are authorised, authenticated, encrypted and documented.

Some practices that are common to IT security when authenticating for remote users include:

- Authenticate all external users at an appropriate level to identify an external interactive user.
- Log and review all attempts to access critical systems.
- Disable the access account for a certain amount of time after failed external access attempts.
- Require re-authentication following external system inactivity.
- The authentication level required should be proportionate to the risk of the system gaining access.

Documentation for each connection involves a description of:

- the objective,
- the remote access application to be used,
- encryption and authentication technologies used,
- how the connection will be established (for example, via the Internet through a virtual private network (VPN) through a DMZ) with instructions as required,
- the circumstances that require the connection,
- the amount of time the connection needs to be open, including expected periods of inactivity, and
- location and identity of the remote client device, application, and user.

Best practice for remote connection is described in, among other things, the IEC 62443 series, together with Norwegian Oil and Gas 070 and DNV-RP-G108. Other relevant documents are NIST SP 800-46 and NIST SP 800-82.

5 Measures for resisting cyberattacks

If a System A can be subjected to cyberattacks from a System B, this would be a threat to the independence of System A. Consequently, a system will have to be protected from cyberattacks to be truly independent. In this context, we are most concerned with cyberattacks that can affect the *integrity* and *availability* of systems and data, and which can ultimately impact independence[2]. In terms of data, we can most often solve this by using the building blocks of encryption, message authentication, and/or digital signatures. It is also common to divide into different zones, which often assumes that different forms of conduits are used for communication between the zones. A special case is the use of data diodes to ensure that communication can pass from one zone to another, but not back again (see 4.1). These topics are described in more detail in the following subsections.

Software can be the target of attacks, and a successful attack can enable an actor to alter the behaviour of a system, and thereby influence its independence [6]. For proprietary software, it is important to follow good software security practices to ensure that the software does what it is intended to do, even when exposed to a malicious influence. This should of course also be the aim of software from an external provider; however, this is something one often has less control over. It will therefore often also be necessary to use network mechanisms that limit which actors are able to (attempt to) communicate with software that may impact functional safety.

5.1 Communication for functional safety

IEC 61508 states that when a safety instrumented function (SIF) is dependent on communication, the communication system should be regarded as a component in the SIF. Functionally safe communication can thus be achieved by one of two methods:

1. The entire communication channel (including the endpoints) is designed, developed, and validated in accordance with IEC 61508 and *either* IEC 61784-3 *or* EN 50159.
2. Parts of the communication channel are not designed, developed, or validated in accordance with IEC 61508, only the endpoints (sender and receiver). In this case, necessary measures for secure fault management of the communication system must nevertheless be implemented in accordance with either IEC 61784-3 or EN 50159.

Method I is called “white channelling” and requires the development of a dedicated communication system solely for safe communication. In most cases, this is very time-consuming and costly and is thus not very widespread. Method II is called “black channelling” and involves adding safety features to the endpoints of the communication in order to avoid certification of the entire communication system.

EC 61784-3 for industrial communication networks defines principles for the transmission of safety-related messages between participants in a distributed fieldbus network in accordance with requirements for black channel in IEC 61508. IEC 61784-3 also describes one set of profiles for safe communication for a selection of fieldbus standards:

- Profile 1: Functional safety with FOUNDATION Fieldbus

[2] There may also be good reasons for being concerned about confidentiality, however that is not our focus in this document.

- Profile 2: Functional safety with Common Industrial Protocol (CIP)
- Profile 3: Functional safety with PROFIBUS and PROFINET
- Profile 6: Functional safety with INTERBUS
- Profile 8: Functional safety with CC-Link
- Profile 12: Functional safety with EtherCAT
- Profile 13: Functional safety with Ethernet POWERLINK
- Profile 14: Functional safety with Enhanced Performance Architecture (EPA)

Each of these profiles is specified under IEC 61784-3-x. For example, IEC 61784-3-3 addresses functional safety for PROFIBUS and PROFINET – a profile called PROFISafe. The profiles for safe communication are based on the underlying protocols and are transferred on the same network/cable as other messages. However, the utility message is extended with the following information:

- A safety code that shall be able to detect unintended faults in messages that are of a random and systematic nature.
- Unique sender and recipient identification for the message.
- Sequence number of the message.
- When the next message should be received by the recipient.

While the profiles in IEC 61784-3 address various fault modes for communication channels, the standard is somewhat deficient when it comes to coverage of information security. Reference is made to IEC 61784-4 for fieldbus-related security and to IEC 62443 for general security, however there is no further explanation of or requirements for how it should be implemented. It is unfortunately not difficult for unauthorized parties to manipulate messages without being detected by the mechanisms of these profiles, and this can impact the safety function. There is also no protection against other traffic being adversely affected. All that these profiles ensure is that the recipient goes to a predefined safe state if any error is detected on the transfer.

One can see a development towards closer integration between process control and safety systems and, not least, that several different industrial ICT systems and IIoT solutions are being connected to technical networks. Requirements should therefore be set that even if the solution is certified in accordance with EC 61784-3, it must have sufficient mechanisms for information security. There are thus two means of protection against unauthorised access:

- Encryption of the contents of messages sent to and from SIF.
- Location of the entire SIS within a zone as defined in IEC 62443.

Of these two approaches, the first will require a change in communication elements in the SIF, with the subsequent time-consuming and costly re-certification. The second approach avoids changing the SIS by preventing unauthorised access to the communication channel using zones and conduits as defined in IEC 62443.

5.2 Encryption

An important vulnerability in the present OT systems is that they often contain older equipment that does not have built-in support for cryptography. This means that high integrity is dependent on good shell protection. Digital signatures or message authentication codes (MAC – see section 5.3), which provide the

ability to verify that data is authentic and has not been altered, are not normally used in OT systems. DNV-RP-G108 [9] contains the following recommendation:

- Symmetric encryption: AES 128 or better
- Asymmetric encryption: RSA 2048 or better
- Hash: SHA-224 or better

There has previously been a widespread misconception that encrypting a communication channel (for example, in the form of a Virtual Private Network) makes it impossible to manipulate the data that is transferred without it being detected by the recipient. However, in recent years, the IT industry has had to accept that such guarantees can only be given if one of the more specifically defined protocols for authenticated encryption is used, for example, AES-GCM [57] or AES-CCM [29].

If quantum computers become available in the short term, this will lead to dramatic changes in the algorithms and key lengths that provide adequate levels of security[58]. If this is to be considered, this may, among other things, have the following consequences:

- The current public-key algorithms that rely on discrete logarithm or factorization of large numbers (Diffie–Hellman, RSA, and ECC are the most common examples) need to be replaced with quantum-safe alternatives.
- The key length of symmetric encryption algorithms (AES) must be doubled ->256 bits or more.
- The length of hashes must be doubled (SHA3-384 or SHA3-512).

At present there is no consensus on which public-key algorithm should be chosen, however various alternatives are being developed[56]. Authenticated encryption does not appear to be an issue that receives much attention in the petroleum industry, and quantum-resistant encryption also does not appear to be something that the industry is concerned about.

Depending on the choice of profile in IEC 62443, encryption requirements may apply, and the OPC UA may also include encryption. There are also disadvantages associated with using encrypted messages within OT due to the fact that signature-based IDs (Snort, disadvantage, Bro, . . .) will not be able to detect intrusion attempts. Network monitoring will then also become more difficult. For individual applications, it is possible to consider proxy solutions that decrypt the traffic entering/exiting specific zones.

Encryption between devices in OT has not been extensively implemented on Norwegian facilities. This is partly because the equipment that is currently used rarely supports the encryption of traffic, and partly because encryption/decryption requires resources and may come at the expense of response time and the possibilities for exchanging information between the individual systems, and the operator interface may also become slower. Shell protection in the form of zones and conduits in accordance with IEC 62443 may represent a better solution for OT systems in the short-term.

There are SIL 4 certified hardwired safety systems in accordance with IEC 61508, where the logic cannot be influenced via ICT systems. The logic is not vulnerable to ICT threats, and information and status can be extracted, for example, with OPC (however, the OPC part has not yet been certified in accordance with current IEC 62443 standards). This means that the logic does not require protection against ICT threats, while the information on OPC has the same challenge as other software-based infrastructure.

5.3 Digital signatures and message authentication codes (MAC)

A digital signature relies on public and private (i.e., asymmetric) keys, which usually involves "Public Key Infrastructure" (PKI). For A to sign a message, A has to use its private key. Anyone who receives the message can then verify that the message comes from A and has not been modified during the process using A's public key. The simplest means of implementing a digital signature in conceptual terms is to take a cryptographic hash of the message and encrypt the result using A's private RSA key. The recipient can then execute the same hash operation on the message, decrypt the signature with A's public key, and compare the two results. If they match, the signature is valid.

A message authentication code (MAC) is also called a keyed hash function and is typically used between two parties that share a secret (symmetric) key to authenticate information exchanged between the two parties. The secret key is fed into the algorithm and a message (a variable-sized amount of data) and produces a value (MAC) that is connected to the message that is to be protected. If the integrity of the message subsequently needs to be checked, the MAC function can be applied to the message and the result compared with the corresponding MAC value. An attacker that alters the message would not be able to create a new correct MAC without knowing the secret key.

A common means of implementing a MAC is by using a cryptographic hash function according to a specific pattern. This is then called a HMAC.

5.4 Characteristics of zones and conduits

The concept of zones and conduits that is illustrated in Figure 6 is often cited as the solution for protection against undesirable external influence, however, these concepts do not guarantee independence. This is partly because the scope of proposed measures will depend on the application, the established SL (see section 3.1), what requirements are actually implemented, and the fact that all systems/components within a zone cannot necessarily be implemented with the given SL requirements for the zone.

Requirements for the implementation of zones and conduits are given in different parts of the IEC 62443 standard series. Below are some issues that could possibly be resolved if relevant measures are implemented:

1. A conduit between two zones *can* be made to protect against undesirable influences, including through the conduit, however this is not part of the requirements that follow directly from the level (SL) and other requirements for conduits and zones in IEC 62443. Such protection must either be realized in the conduit or at the recipient to avoid being able to influence SIS from other systems. (IEC 62443-2-4, SP.05.02). This means that requirements of the type stipulated in Norwegian Oil and Gas 070 are still necessary, see section 3.6 of this report.

2. In IEC 62443, there is a possibility that the safety instrumented systems (SIS) may be logically or physically separated in zones that are different from those containing the systems that are not safety systems (PCS). If they cannot be separated, both need to be in the same safety-related zone. (IEC 62443-3-2 Chapter 4.4.4). For devices in the same zone, the standard does not provide any protection or independence.

3. One can prevent configuration of SIS via remote access. This must also be verified by an independent third party. (IEC 62443-2-4, SP.05.09)

The measures found in 62443-2-4 are described as opportunities (or "capabilities") that a supplier should be able to offer a facility owner and are not explicitly linked to the security level (SL). On the other hand, the requirements in IEC 62443-3-3 (for systems) and IEC 62443- 4-2 (for components) are linked to an established SL, which in turn shall appear because of risk assessments. However, as discussed in section 3.1, it is the facility owner that ultimately decides which requirements should be implemented, typically by establishing a “profile”. It is therefore essential that this profile includes the requirements that are considered important for providing as much independence as possible.

5.5 OPC UA

5.5.1 PubSub as an approach to data diodes

Publish-Subscribe (PubSub) is described in OPC UA part 14 [40]. The model can generally be illustrated as shown in **Figure 17** i.e. there are one or more devices that publish data and one or more devices that subscribe to data. This takes place via “middleware” that can be implemented in different ways. All the devices can essentially be “normal” OPC UA devices that communicate in the usual manner; however one explicit option is to use a UDP datagram without a receipt. In this instance, it will be possible to place an “unidirectional gateway” (i.e., data diode – see section 4.1) between the publisher and the subscriber (see **Figure 18**).

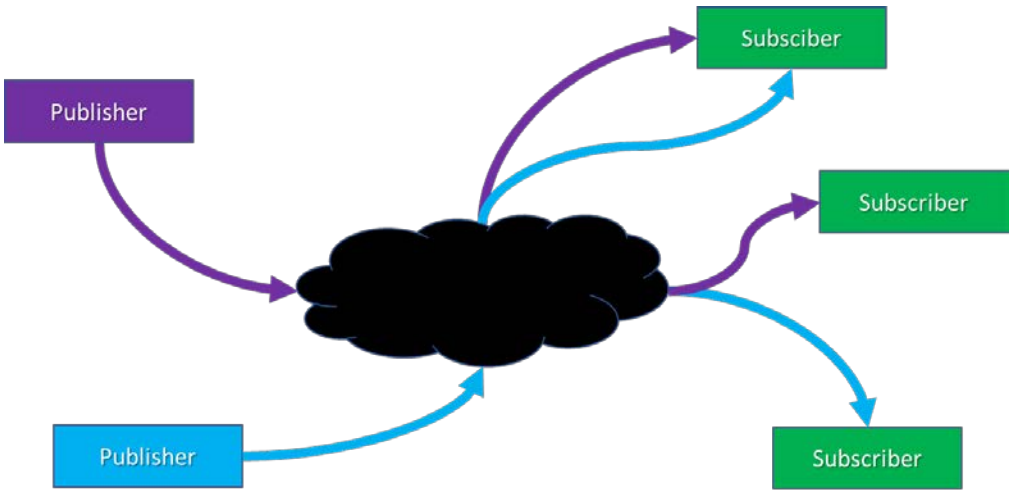

Figure 17: **OPC UA PubSub model.**

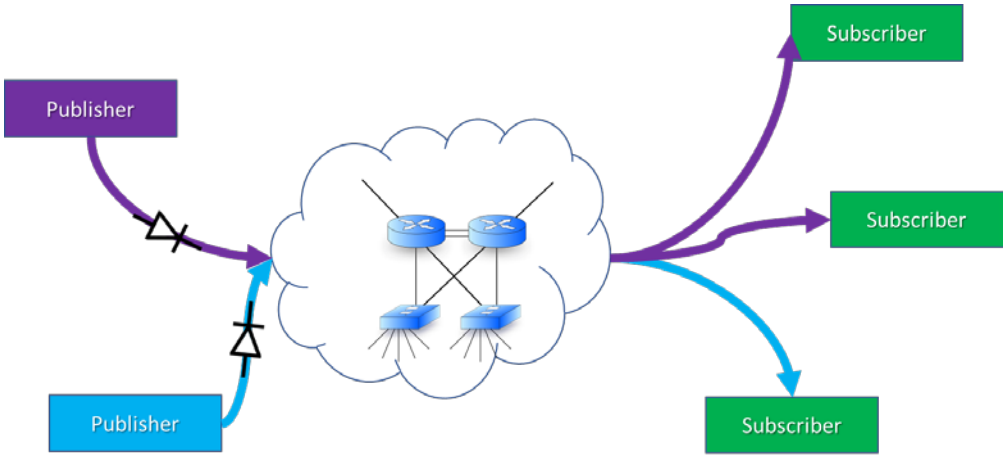

Figure 18: **PubSub without active broker, with data diodes.**

PubSub provides support signing[3] or signing and encryption. The message format is illustrated in Figure **19:**. Individual data elements are grouped into a "DataSetMessage", and several of these can in turn be grouped into a "NetworkMessage", which eventually makes up the payload in a transport protocol message (in our case, UDP). If there are multiple subscribers, UDP multicast addresses can be used, however, for our purposes, it is assumed that UDP unicast addresses will suffice.

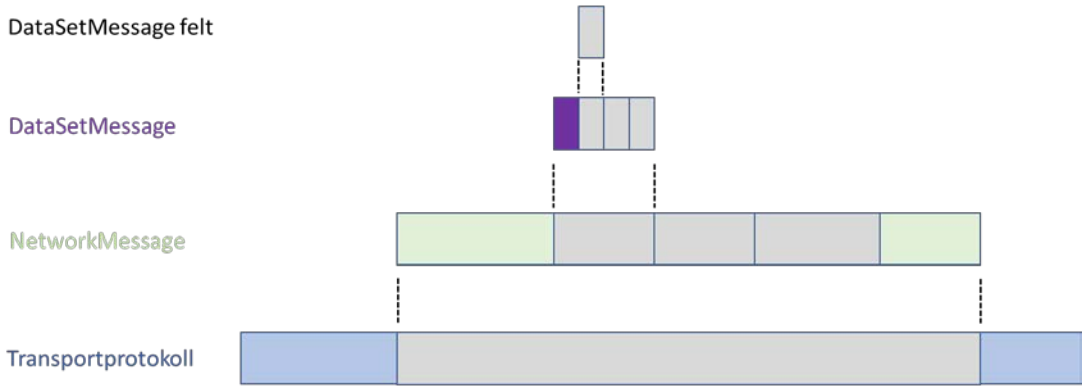

Figure 19: PubSub message format.

The data field in "DataSetMessage" (the purple field in **Figure 19:**) consists of the information specified in Table 3:. The most important elements here are an ID that identifies the sender, a sequence number, and a timestamp.

[3] It is possible that they are referring to MAC rather than digital signature, because they also mention that this requires the producer (*publisher*) and consumer (*subscriber*) to share a secret key.

Table 3: Data fields in DataSetMessage.

Field	Explanation

UDP generally makes no guarantees for timeliness, delivery receipt, order, or duplicate protection. When using a data diode, it will not be possible to request the retransmission of missing packets, however, it is possible to send multiple copies of the same packet. This must then be configured if there is a communication channel with excessive packet loss. The sequence number then makes it possible to discard the duplicate packets [40]. If UDP is used, the consumers will probably need to be adapted to enable them to work, even if some packages do not arrive.

5.6 Zero trust versus shell protection

In the early days of the computer age, computers were monolithic colossuses that filled entire rooms, and the only communication was in the form of stacks of punch cards that were carried in and out. However, the world moved on, and modern computer networks saw the light of day. At some point, computers from different organisations started to become connected, and when the Internet became public in the late 1990s, anyone could connect to any computer system. However, this opened the door to attacks and many organisations discovered that it was too difficult to protect each individual machine. This therefore resulted in the creation of shell protection of local area networks in the form of a firewall; to quote Bill Cheswick: “a hard shell around a soft, chewy centre”. [5]

In recent years, shell protection with firewalls in IT networks has proven to be challenging, partly because a number of services now require "gaps" to be made in the firewall for them to function, and partly because there are now so many mobile devices that are brought into corporate networks, and because the use of cloud networking has increased significantly. Therefore, a new trend that almost brings us back to the starting point has become popular: *zero trust computing* [21][31]. The concept is that security should no longer be based on shell protection where all devices inside the firewall are trusted, but should instead require all devices to authenticate themselves to any other device with which they intend to interact. Furthermore, all devices must then also be authorised for them to be permitted to interact with a given device.

Zero Trust Computing requires mechanisms for key distribution and key management to be in place, and often involves a PKI, despite there are also being other means of doing this. This also means that one is reliant on the use of cryptographic mechanisms in OT networks that will use this.

6 Possible dependencies and adverse effects

In this chapter, we provide some general information regarding how new solutions can lead to possible dependencies and adverse effects and also reflect on whether or not the PSA's requirements for independence can be considered to be satisfied. Possible measures to limit the new dependencies are summarised in section 8.

6.1 What do we mean by adverse effect?

In this context, we consider “adverse effect” to be that a fault or incident in a system or an associated component can impair or prevent the safety function of another system or a component in another system (a so-called dangerous failure). This could be due, for example, to common components, a functional or physical dependency, or common external effects (see section 2.2).

Adverse effects can also be failures or incidents that impact the *production capacity* of other systems or components (however do not inhibit the safety function itself). For example, a valve in the production line shuts down as a result of a failure of the hydraulic system (so-called safe faults). This is also an adverse effect, both in terms of regularity and based on the fact that shutdowns and start-ups themselves represent a risk. However, our primary focus in this report is safety-critical (dangerous) faults.

A key question then becomes whether the process safety system (PSD) or other safety systems, such as the ESD and F&G system, can be adversely affected because of failures in other systems. For example, can they adversely affect each other, can they be adversely affected by the control system, or can they be adversely affected by other ICT systems and IIoT solutions, including connections to provider-based cloud solutions outside the OT domain?

6.2 New dependencies and connections

Even in layered solutions that follow the Purdue Model, with protection of the OT systems from unwanted influence, there is a challenge when concerning connections between the different systems. This may be signals that are deliberately transferred or connections, for example, via the operator interface. It is a very challenging task to demonstrate that any fault that may occur in one system cannot adversely affect another system.

Some operate with a dedicated safety network that separates SIS from the others, however since there are deliberate connections above this separation and common operator interface, in the worst cases, the separation is no more than a reduction of the burden on the safety network.

Zones and conduits in accordance with 62443 can provide protection against unwanted external influences, however, this does not guarantee full independence. Within a zone, there are the same challenges as for the current solutions, and through conduits one can, in principle, experience adverse effects from transferring the incorrect value. As long as the value is within legal limits, it may have an adverse effect. This is comparable to the fact that 4–20 mA is within the legal limit, however, 16 mA may still result in SIS not receiving 8 mA, which should have resulted in a safe action.

The independence that occurs when segmenting networks to distinguish different systems from each other is impaired when a series of connections are established between the zones. However, the definition/delineation of a system becomes unclear when different functions are placed in different zones. According to DNV's RP-G108, different systems should be segmented into different zones, if they do not have functional or operational dependencies that require them to be in the same zone. This approach is challenged by the new solutions that have been outlined, with more/many connections across zones. Examples of this are 5G base stations that will be used across all layers of the Purdue Model and future flattening of the automation pyramid, where everyone can communicate with everyone, as defined by the OPC UA.

In the case of remote connectivity (or other cross-zone connections), there is no longer a clear connection between the system and zone. It can be argued that a system stretches across several zones since its functions are located in several different zones, however, this is not in line with the recommendation to have different systems in different zones.

Newer technologies, such as edge devices and IIoT devices, face challenges if information is to be retrieved from devices that are part of the safety systems if they use a lossless protocol that needs to send either requests or receipts to the device. It is also important to note here that NOA, which defines how to retrieve information from OT to IT using data diodes, does not include safety systems.

If one looks at the IT/OT systems as a device, there may be a good number of common components, however this may of course vary between installations. If these are not critical at the present time, there must be an assessment of whether they may eventually become critical and particularly whether they can be used as attack points. Some examples of these include:

- Firewalls and other network components
- Human-machine interfaces
- Configuration tools
- Clock system
- Systems for administering field equipment
- Domain controllers
- Backup systems
- Active directory
- 5G
- Hardware and software (hypervisor) for virtualisation
- Authentication systems
- Key management (applicable for all authentication/encryption, including for Zero Trust)

It is difficult to state anything generic about where and how these devices are currently being used, however these must be included if attack points, and dependencies are to be assessed. If the objective is to reduce these possibilities, IT and OT must at the very least have their own functions. One must also not forget the possible dependencies that may already exist in the present solutions with common networks and signals between devices both within SIS and between SIS and PCS.

Some of the initiatives for integrating information from the IT/OT systems in cloud solutions or others reveal that the levels in the Purdue Model are under pressure and that there is an opening for edge devices, IIoT and others to harvest and extract the information. Despite each connection appearing to be well-protected, the large number of connections represents a challenge because the protection is a "perishable commodity"

and needs to be updated and maintained. New challenges related to cloud solutions will also be introduced for 5G, whereby mobile operators can gain access to the configuration and setup of 5G infrastructure on installations via cloud-based services.

6.3 To what extent will the PSA's requirements for independence be met?

We can first conclude that it is difficult to provide a definitive answer to whether the requirements for independence are met. The PSA's general requirements (Section 5 of the Management Regulations) that there must be "*sufficient independence between the barriers*" is subjective and therefore difficult to verify beyond what is stated in the guidelines that *"multiple important barriers to be impaired or malfunction simultaneously, e.g., as a result of a single fault or a single incident*". This is further elaborated on in Sections 32-34 of the Facilities Regulations, which require that the fire and gas detection system, the emergency shutdown system and the process safety system respectively perform their intended functions independently of other systems, and that they are not adversely affected by failures in these systems.

The latter requirements are more tangible, and the following observations and comments can be linked to them:

- As discussed in section 2.3, the current risk and reliability analyses only contain limited detailed assessments of connections and dependencies between systems.
- Due to greater complexity and more connections, it is a very challenging task to demonstrate that any error that may occur in one system cannot adversely affect another system
- The suppliers generally do not appear to have standard documentation which demonstrates that their solution provides full independence and/or does not adversely affect other systems.
- The operators also do not have any such documentation.

If one is to attempt to provide an answer to the question in the title, it must therefore be: The requirements for independence may have been met, however there is no documentation to demonstrate this.

This discussion can also be linked to the PSA's new definition of risk, which states in the guidelines to Section 11 of the Framework Regulations that *"Risk means the consequences of the activities, with associated uncertainty."* The clarification of "associated uncertainty" entails that the degree of complexity in and knowledge of the phenomena, systems, and operations one is dealing with must be emphasised in the risk management.

Since the current risk and reliability analyses only address or study the relatively complex phenomenon of dependency to a limited extent, and documentation of independence is somewhat absent, the conclusion can be drawn that the uncertainty, and thereby the risk, associated with possible unknown dependencies is significant.

7 The need for amendments to the Petroleum Safety Authority Norway's regulations

7.1 Background

Based on recommendations from the Lysne Committee (2015), Report to the Storting (white paper) No. 38 (2016-17) on ICT security stated that:

> *"…there should be a requirement from the supervisory authority (PSA) that barriers against digital vulnerabilities should be established"* (section 13.2).

It was further stated that:

> *"PSA will clarify and further develop the regulations to address the challenges the industry is facing as a result of changes in the threat landscape and increased digitalisation. Among other things, this means monitoring the development of industry standards that can be referred to in the regulations."*

As discussed in section 2.4, the PSA's regulations and traditional barrier management have primarily involved having control of the energy area, while the information area has only been relevant to the extent that it can adversely affect the energy area and have the potential to cause physical harm. As a result of the closer connections and new digital dependencies discussed in this report, it is therefore appropriate to ask whether the regulations should further clarify the need to establish barriers against digital vulnerabilities that may result in undesirable information flow, beyond what can be immediately identified as impacting the energy area.

It is also reasonable to ask whether the PSA's regulations should be updated in relation to the standards and guidelines linked to ICT security that are referenced.

7.2 Discussion of possible adjustments to the regulations

The regulations for petroleum activities are based on certain fundamental principles which have the intention of ensuring good safety and risk management. Of key importance here is a mindset that strongly emphasises functional requirements – what one wants to achieve – rather than detailed requirements that specify the solutions and measures that have to be chosen [48]. It is natural to address the functional requirement for *sufficient independence* in the continuing discussion on the need for potential amendments and clarifications in the regulations to ensure that ICT security is taken into consideration when choosing solutions to meet this requirement.

Section 5 of the Management Regulations begins with the requirement to establish necessary barriers that will have a direct role in avoiding or reducing the risk of accidents and limiting harm. In practice, these regulations are read in the context of barriers that can control or reduce energy. The loss of control of information and data caused by digital attacks can result in incidents that weaken the traditional barriers. In the future, barriers that are intended to prevent loss of control of information and data will be of greater importance to safety at industrial facilities. SINTEF is therefore of the view that the regulations can be more explicit in terms of clarifying the need for ICT barriers, including a barrier function that prevents undesirable information flow, and how these are linked to the performance of barriers that protect loss of control of energy.

Sections 32 to 34 of the Facilities Regulations stipulate requirements that key safety systems must be able to perform the intended functions independently of other systems. In connection with the guidelines to these sections, consideration can be made to broadening the perspective of what must be considered in the requirement for independence. In addition to requirements for (sufficient) independence in the technical design and follow-up of PCS and SIS, it will be important to set requirements for sufficient independence between ICT events and possible impairment of PCS and SIS as barriers. For example, in the guidelines reference can be made to the importance of ICT barriers (counter measures) as a means of maintaining independence between barrier functions.

Some possible approaches are briefly discussed below.

7.2.1 Proposal concerning Section 5 (Barriers) of the PSA's Management Regulations

Section 5 of the Management Regulations adequately covers the overarching requirements for barriers. One option for further highlighting the area of information could therefore be to further elaborate on examples of barrier functions in the guidelines as follows:

> *Examples of barrier functions are preventing leaks, preventing ignition, reducing fire load, preventing undesirable information flow, ensuring prudent evacuation, and preventing hearing damage.*

While it could be argued that the phenomenon of independence is baked into the concepts of reliability and integrity, it could be conversely argued that the industry's inadequate focus on verifying independence could perhaps justify expanding the examples provided of performance:

> *Performance means verifiable requirements for, among other things, capacity, reliability, availability, independence, efficiency, ability to withstand loads, integrity, and robustness.*

Further elaboration of the barrier function to "*prevent undesirable information flow"* and requirements for independence can, for example, be incorporated into the next update of the PSA's barrier memorandum [45], see section 7.2.3 below. It may also be considered whether an increased focus on ICT barriers can be achieved through adjustments to other sections such as Sections 15-16 of the Management Regulations.

7.2.2 Proposal concerning references in Sections 32-34 of the PSA's Facilities Regulations

Based on discussions with the industry and SINTEF's understanding of relevant standards relating to ICT security, we recommend that the PSA considers referencing the IEC 62443 series (see section 3.1) in the guidelines to Sections 32 to 34 of the Facilities Regulations. This standard is already widely used, including internationally[4], and it contains several requirements which, if implemented, can contribute to independence. Some Norwegian operators have already now developed a "profile" which contains selected IEC 623443 requirements that they use in their projects, and it may, for example, be relevant for the PSA to use targeted supervision to further examine whether these requirements are being met.

As discussed in section 3.1, the different parts of the IEC 62443 series are available to varying degrees in updated or official versions, and this must therefore be specifically considered if the standard or selected

[4] However, the United States appears to primarily use NIST 800-82, which is thematically like the IEC 62443 series, but has a somewhat different approach in some areas. [50]

parts of this are to be referenced. In relation to determining the security level (SL) and associated technical system requirements, sub-standards 3-2 and 3-3 are particularly relevant. These have both been released in official versions from 2020 and 2013 respectively, however the latter has been opened for review.

7.2.3 Proposal concerning the PSA's Barrier Memorandum 2017

The PSA's barrier memorandum describes principles for barrier management in petroleum activities in Norway. The memorandum elaborates on and provides examples of the intentions of the regulations in relation to barrier management and contains several examples of barrier functions and performance requirements, including an appendix (7.1) that addresses physical security (preventing unauthorised access).

When considering the future challenges described in this report, and in the extension of the recommendation to include ICT barriers and define "prevent undesirable information flow" as a separate barrier function, it is reasonable that the barrier memorandum is also updated accordingly.

8 Principal conclusions and recommendations

This chapter summarises SINTEF's proposed measures for the industry and the PSA respectively, as well as the need for further work on knowledge acquisition.

8.1 Recommendations to the industry

Recommended measures for the industry are provided in Table 4:.

Table 4: Summary of recommended measures for the industry.

No.	Challenge	Recommendation	Ref.
The current solutions			
1.	There may be many common functions and systems, even in the current solutions. Some examples include domain controllers, backup systems, authentication, and active directory.	Avoiding or reducing the use of systems and components that are common to SIS and other IT/OT systems and, where this cannot be avoided, establishing multiple barriers to prevent attacks against common solutions.	6.2
2.	The current SIS and PCS systems have limited protection from digital attacks.	Despite there being a number of measures, additional measures are still required. It must be ensured that these systems are protected from attacks using other means.	2.5
3.	The effect of using separate networks for SIS and PCS may be limited, because there are a large number of messages that have to pass between these networks. Examples include synchronizing PCS in the event of shutdown and feedback on limit switches.	One should not be reliant on separate networks providing full independence and should introduce/retain other measures to avoid dependencies and undesirable influence.	2.5
4.	Data LEDs are useful for preventing the transmitter from being affected, however they are often opened for configuration and other traffic. This results in complex configuration and continual changes.	Ensure that other methods are used if OT components must be temporarily accessed externally to avoid the data diodes from being perforated by this type of communication.	4.1
5.	Safety profiles such as PROFIsafe provide poor protection from attacks.	Ensure that this communication is further protected from undesirable influences by additional mechanisms when it may be accessible from the outside (zones and conduits, etc.).	5.1
6.	The people who work with ICT security at the suppliers are not familiar enough with the independence requirements in Appendix G of Norwegian Oil and Gas 070.	This group should also be made better acquainted with these requirements.	3.6
7.	There are parts of Appendix G of Norwegian Oil and Gas 070 that are inadequate when concerning protection against influence from other systems, remote access and retrieval of information for, for example, cloud solutions.	Appendix G should be revised in connection with a future update of Norwegian Oil and Gas 070 and should also better take into consideration risk factors relating to ICT security and new solutions for sharing data between OT and IT levels.	3.6 4.6

No.	Challenge	Recommendation	Ref.
8.	It is a challenging task to meet the requirements for independence between PCS and SIS, something that is a prerequisite in both IEC 61508 and IEC 61511 for compliance with SIL.	Ensure that the requirement is met, even after the OT systems have been put into operation and the necessary exchange of signals has been implemented.	3.2