Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P3765-cd

Cybersecurity Barriers and Performance Requirements

Knut Øien

SINTEF Digital, Trondheim, Norway. E-mail: knut.oien@sintef.no

Martin Gilje Jaatun

SINTEF Digital, Trondheim, Norway. E-mail: martin.g.jaatun@sintef.no

Christoph Thieme

SINTEF Digital, Trondheim, Norway. E-mail: christoph.thieme@sintef.no

The cybersecurity barrier management project aims to develop new knowledge and guidance to secure industrial control and safety systems against cyberattacks. With several threat actors targeting the petroleum sector, the number of publicly known cyberattacks is increasing, revealing a larger threat landscape. At the same time, extensive digitalisation of the sector has led to increased vulnerability. Cyberattacks against control and safety systems in the petroleum industry can cause physical damage to facilities, harm personnel, and affect security of gas supply to Europe. Barrier management systems have been introduced for traditional safety against accidental events, but to a lesser extent against intentional events such as cyberattacks. In this paper, we focus on the identification of cybersecurity barriers, and the development of corresponding cybersecurity barrier requirements, i.e., how well the barriers should perform. The main research approach is iterative empirical research where the research and exploration are carried out in several iterations in close interaction with industry partners, advisors, experts and professional forums. A literature survey has been performed and considerations about the distinction between cybersecurity barriers and non-barriers have been made. The main result described in this paper is a nine-step methodology for identification of cybersecurity barriers and establishment of performance requirements for the barriers. This includes a definition of cybersecurity barriers. However, a definition is not sufficient in itself to distinguish between cybersecurity measures that are considered cybersecurity barriers versus those that are considered non-barriers; expert insights in cybersecurity measures are a prerequisite for the identification of cybersecurity barriers and the establishment of performance requirements.

Keywords: Barriers, barrier management, cybersecurity barriers, barrier requirements, security measures, oil and gas industry.

1. Introduction

Barriers are measures intended to detect failure, hazard and accident situations at an early stage, reduce their potential for propagating and limit harm and disruption. Barriers supplement safe and robust solutions aimed at preventing failure, hazard and accident situations arising (PSA 2017). Safe and robust solutions are control measures to prevent loss of control, whereas barriers are used to regain control or prevent the propagation of chain of events and limit damage.

1.1. *Purpose and scope*

The aim of the work described in this paper is to provide new knowledge and guidance on identification of cybersecurity barriers and barrier elements, and development of cybersecurity barrier requirements.

Requirements for the establishment of barriers are included in the Norwegian petroleum regulations: Management Regulations Section 5 (MR § 5) (Havtil 2023a). These requirements are not restricted to specific types of events or consequences, i.e., they are also relevant for cybersecurity. However, the industry has focused extensively on safety related to major hazards, with just a few – and very different – initiatives to establish cybersecurity barriers and to integrate this into safety barrier management. Thus, the ambition of the project *Cybersecurity*

Barrier Management (CBM) is to provide a common approach for cybersecurity barrier management in the petroleum industry (i.e., a company neutral approach).

An issue related to the identification of cybersecurity barriers and development of cybersecurity barrier requirements is the lack of an explicit definition of cybersecurity barriers.

1.2. *Regulation, standards and previous work*

1.2.1. *Regulations*

General definitions of barriers, barrier functions and barrier elements are provided in the Barrier Memorandum (PSA 2017), but no specific definition of a cybersecurity barrier is included. This may imply that the general definition of a barrier also applies to cybersecurity barriers.

In addition to elaborating on the regulations regarding barrier management, in particular MR § 5 in Havtil (2023a) and providing barrier definitions, the Barrier Memorandum explains the authorities reasoning about barriers, including the differences between barriers and non-barriers, which are essential for the identification of cybersecurity barriers. The essence is that cybersecurity barriers are only one category of cybersecurity measures. Other categories include risk reduction during normal operation (control measures) and performance influencing factors (PIFs) affecting the performance of barriers.

1.2.2. *Cybersecurity standards and guidelines, and academic literature findings*

The relevant standards and guidelines, such as NIST Cybersecurity Framework (NIST 2024), IEC 62443 (2024), IEC 63069 (2019), ISA-TR.84.00.09 (2017) and NOROG 104 (2016), rarely use the term barrier; thus, they do not include any definition of cybersecurity barriers. They use other terms like countermeasure, security measure, safeguard, etc.

In a literature review (Øien et al. 2022), we searched for publications on how to identify cybersecurity barriers and barrier elements, and we reviewed the use of the term cybersecurity barriers. Very few publications in our review used the term barrier, and no publications provided a definition of cybersecurity barriers.

1.2.3. *Industry initiatives*

When referring to "the industry", we are mainly considering two companies. Both companies have developed performance standards (PSs) for cybersecurity, which are added to the about 20-25 safety performance standards that they already use. The PSs cover general cybersecurity requirements, i.e., not limited to cybersecurity *barrier* requirements.

Both companies have integrated cybersecurity barrier management with the already existing safety barrier management regime, one reason being increased attention to cybersecurity through reporting of barrier status to top management. Since the approaches used by the two companies regarding safety barrier management are very different, so are their approaches to cybersecurity barrier management. This is also due to the use of different standards or guidelines for cybersecurity requirements (i.e., IEC 62443 (2024) versus NOROG 104 (2016)). This is the background for the ambition of the CBM project to provide a common approach for cybersecurity barrier management in the petroleum industry (i.e., a company neutral approach). This approach needs to be flexible, to account for the differences in safety barrier management regimes and different preferences regarding cybersecurity standards or guidelines.

2. Research Approach and Methodology

The main research approach is *iterative empirical research,* where the research and exploration are carried out in several iterations in close interaction with the industry partners, advisors, experts and professional forums. This work on *cybersecurity* barrier management also builds on previous work on *safety* barrier management, in particular work documented in Hauge and Øien (2016), which was carried out in close collaboration with the PDS forum[a] (a professional forum on reliability of computer-based safety systems). Similarly, the work described in this paper is carried out in close interaction with the sibling CDS forum[b] (cybersecurity of computer-based control and safety systems) where the Working Committee acts as an advisory board to the CBM project.

3. Results: Methodology for Identification of Cybersecurity Barriers and Requirements

The main result of the work described in this paper is a methodology for identification of

[a] https://pds-forum.com/; [b] https://cds-forum.com/

cybersecurity barriers and development of corresponding performance requirements. The methodology is built on five main principles as shown in Table 1.

Table 1. Main principles for the methodology

1. It should be company neutral
2. It should be independent of selected requirements, standards, and/or guidelines
3. It should follow the regulations, definitions and reasoning of the authorities (i.e., PSA/Havtil)
4. It should be suitable for integration with (different regimes of) safety barrier management
5. It should also consider security measures not defined as barriers

In the methodology described in this paper, we distinguish between barriers and non-barriers according to the Barrier Memorandum (PSA, 2017); however, we also cover the non-barriers according to the fifth principle. Reference is made to the Facilities Regulations Section 34a (FR § 34a) (Havtil 2023b) for general cybersecurity requirements. It is up to the asset owners to follow up on non-barriers in a similar manner as barriers.

The methodology consists of nine steps, the first five covering identification of cybersecurity barriers and the last four covering establishment of performance requirements to the cybersecurity barriers, including verification of fulfilment of the requirements in the last two steps. The steps are listed in Table 2.

Table 2. The nine steps of the methodology

1. Select relevant standards/guidelines and extract cybersecurity requirements
2. Classify each requirement
3. Select barrier requirements
4. Transform barrier requirements to barrier functions and elements
5. Select barriers relevant for a specific facility
6. Add verifiable performance requirements to the barriers
7. Adapt performance requirements to the specific facility/zones
8. Fulfil the barrier performance requirements (comply with MR § 5)
9. Fulfil all cybersecurity requirements (comply with FR § 34a)

For each step, a description is followed by justification/explanation and examples/elaboration. We pay particular attention to the international standard IEC 62443, and we use this standard for exemplification.

The two parts IEC 62443-2-1 (2023) and IEC 62443-3-3 (2013) are used as examples in explaining the methodology. The Security Program Elements (SPEs) in Part 2-1 are the most relevant requirements for the asset owners/ operators, and the Foundational Requirements (FRs) in Part 3-3 are fundamental for determining Security Levels (SLs). These are the only two requirement structures included in the new draft version of Part 1-1 (IEC 62443-1-1-WD:2023). For Part 2-1, we use the new draft version (FDIS) from 2023.

3.1. *Step 1: Select relevant standards/guidelines and extract cybersecurity requirements*

Relevant cybersecurity standards and/or guidelines are selected and requirements extracted.

3.1.1. *Justification/explanation*

Security measures are included as part of requirements in relevant cybersecurity standards/ guidelines, and the requirements are grouped in different categories (such as Foundational Requirements (FRs) and System Requirements (SRs) in IEC 62443-3-3 (2013)). There are no single lists of security measures in these standards/guidelines; however, the security measures may be derived through a systematic review of all the requirements (cf. step 2).

3.1.2. *Examples/elaboration*

All 87 requirements from IEC 62443-2-1 (2023) and all 51 system requirements from IEC 62443-3-3 (2013) (not including requirement enhancements – REs) are extracted. Companies may choose to include other requirements, e.g., from other parts of IEC 62443.

3.2. *Step 2: Classify each requirement*

Each requirement is classified according to the Barrier Memorandum (PSA 2017), i.e., distinguishing between i) safe and robust solutions (normal operation), ii) barriers, and iii) performance influencing factors (PIFs). A requirement can be classified in one or more of the categories.

When we make an assessment about *safe and robust solutions* versus *barriers*, we refer to

normal operation (or keeping control) for the former, and for barriers we refer to abnormal situations (or regaining control). Also note that for normal operation in the cybersecurity domain we consider normal operation of *flow of information* (or simply normal flow of information) as an analogue to normal operation of *flow of energy* in the safety domain (Carreras Guzman et al. 2019). This also covers temporary storage (of energy or information), i.e., it covers both information in transit and at rest.

3.2.1. *Justification/explanation*

This classification and interpretation of barriers are in compliance with regulations. The same classification is used within the safety domain, which makes it easier to integrate *cybersecurity* barrier management with *safety* barrier management in a consistent manner.

3.2.2. *Examples/elaboration*

Examples of classification is shown in Table 3 for the three requirements COMP 2.1-2.3 of sub-element COMP 2 Malware protection within SPE 4 Component security (IEC 62443-2-1 2023).

Table 3. Examples of classification of requirements

COMP 2 – Malware protection	Requirements	Normal	Barrier	PIF
COMP 2.1: Malware free	The asset owner shall have policies and procedures to verify that all components and portable media (if portable media is authorized for use in the IACS) are free of known malware before being used in the IACS.	x		
COMP 2.2: Malware protection	The asset owner shall have policies and procedures related to the installation, functioning, and maintenance of malware protection mechanisms, where feasible.		x	
COMP 2.3: Malware protection software validation and installation	The asset owner shall have policies and procedures related to the testing for compatibility, approval and installation of malware protection software and any related malware signature files in a timely manner after their release.			x

Checking that components are free of malware prior to use is a safe and robust solution, i.e., part of normal operation, whereas malware protection is a barrier preventing events developing by detecting malware and preventing it from being executed. Testing affects the performance of the anti-malware (the barrier); thus, it is a PIF.

COMP 2.2 is an example of a requirement *about* having a cybersecurity measure in place, whereas COMP 2.3 is an example of a performance requirement *to* a cybersecurity measure, i.e., how well the measure should perform. Since the measure is a barrier, COMP 2.3 is a PIF. This is an example of a performance requirement according to MR § 5, whereas COMP 2.2 relates to the barrier itself, i.e., although it is a requirement, it is not a verifiable performance requirement.

Other examples of control measures being part of normal operation include e.g., screen lock, authentication, authorization, background checks, and data classification. The complete classification of IEC 62443-2-1 and 3-3 requirements are documented in Øien et al. (2024).

3.3. *Step 3: Select barrier requirements*

Those requirements that are classified as barriers (functions or systems) are selected. This is a subset of all requirements, which may be considered a "barrier profile" according to IEC 62443, i.e., a subset of all requirements.

3.3.1. *Justification/explanation*

The CBM project is about barriers and (initially) not the broader perspective covering all cybersecurity measures which is part of general cybersecurity management. The subset of barriers is part of cybersecurity *barrier* management.

3.3.2. *Examples/elaboration*

Of the 87 requirements in IEC 62443-2-1 (2023), 34 are assessed to be related to barriers, and of the 51 system requirements (SR) in IEC 62443-3-3 (2013), 28 are assessed to be related to barriers. The requirement enhancements (REs) in IEC 62443-3-3 have only been partly covered, since they will depend on the risk assessment and SL-T (Security Level – Target) of each zone.

Table 4 provides examples of barrier requirements based on IEC 62443-3-3. This also includes the REs for SR7.3, RE1 being a PIF and RE2 being a sub-function.

3.4. *Step 4: Transform barrier requirements to barrier functions and elements*

The transformation is carried out by using a functional top-down hierarchy from barrier functions to barrier elements. We distinguish between the three types of barrier elements using the terms Technical, Human and Operational (THO). Human points to the sharp-end personnel directly involved in activating a barrier, avoiding the use of "organizational" (cf. PSA 2017) which

may be confused with blunt-end personnel such as management who are not directly involved in the activation of barriers. Operational barrier elements are the actions or activities which personnel must perform in order to realize a barrier function (PSA 2017).

Table 4. Examples of barrier requirements

Req. ID	Req. title	Requirement	Normal	Barrier	PIF
SR 2.3	Use control for portable and mobile devices	The control system shall provide the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and c) restricting code and data transfer to/from portable and mobile devices.	X	X	
SR 7.3	Control system backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.		X	
SR 7.3 RE 1	Backup verification	The control system shall provide the capability to verify the reliability of backup mechanisms.			X
SR 7.3 RE 2	Backup automation	The control system shall provide the capability to automate the backup function based on a configurable frequency.		X	

3.4.1. *Justification/explanation*

This step utilizes a barrier hierarchy, which is a commonly known approach, also referred to by the PSA (2017). In new projects, contractors/ integrators can cover this as part of engineering.

3.4.2. *Examples/elaboration*

The transformation of barrier requirements to barrier functions, sub-functions and elements are illustrated in Table 5 and 6, continuing with SR 7.3 from Table 4.

Table 5. Example of transforming barrier requirements to barrier functions and sub-functions

Req. ID	Req. title	Barrier function(BF)	Barrier sub-function (BSF)
SR 7.3	Control system backup	Conducting back-ups	Capturing required files
SR 7.3 RE 2	Backup automation	Not relevant (NR)	Automation of back-up function

The barrier elements in Table 6 are deduced from the barrier sub-functions (manual or automatic back-up), not directly from the requirements.

Table 6. Example of transforming barrier requirements to barrier elements (technical, human and operational)

Req. ID	Barrier element (BE) - Technical	Barrier element (BE) - Human	Barrier element (BE) - Operational
SR 7.3	Back-up mechanisms	Back-up responsible	Taking back-up (manually)
SR 7.3 RE 2	Automatic back-up	NR	NR

3.5. *Step 5: Select barriers relevant for a specific facility*

In this step, barriers relevant for a specific facility are selected.

3.5.1. *Justification/explanation*

Although many cybersecurity barriers may be relevant for many facilities, it must be ensured that they are applicable for the facility in question.

3.5.2. *Examples/elaboration*

The selected barriers can be described in a barrier strategy (BS), which together with the PS from Step 7 (i.e., the performance requirements) can be integrated with safety barrier management.

3.6. *Step 6: Add verifiable performance requirements to the barriers*

Verifiable performance requirements *to* the barriers are added (i.e., how well they should perform), taking into account that performance requirements may be missing in standards/ guidelines.

3.6.1. *Justification/explanation*

Requirements in standards and guidelines are often requirements *about* having a cybersecurity measure in place, whereas performance requirements required by MR § 5 (2023a) are requirements *to* the barriers (usually the barrier elements), i.e., how well they should perform with respect to given properties. Functionality, integrity and robustness are types of properties referred to in the Barrier Memorandum (PSA 2017).

We may establish indirect performance requirements using the PIFs instead of, or in addition to, the direct performance requirements to the barriers.

3.6.2. *Examples/elaboration*

Adding verifiable performance requirements are illustrated in Table 7 continuing from Step 4 (Table 5 and 6).

Table 7. Examples of performance requirements

Req. ID	PR BF/BSF	PR BE-T	PR BE-H	PR BE-O
SR 7.3	Frequency of manual back-up	(Frequency of testing)	Proportion of manual back-up Competence	Correctness of manual back-up
SR 7.3 RE 2	Frequency of automatic back-up	Frequency of automatic back-up	NR	NR

Table 7 provides examples of performance requirements (PR) for each barrier element (BE), covering the three categories (T-H-O). Alternatively, as illustrated in the first PR column, performance requirements can apply to barrier functions (BF) or barrier sub-functions (BSF). Also, PIFs (e.g., competence) can be used as indirect performance requirements (e.g., competence requirements).

3.7. *Step 7: Adapt performance requirements to the specific facility/zones*

In this step, performance requirements are adapted to the specific facility and zone.

3.7.1. *Justification/explanation*

The same barrier may have different performance requirements in different zones depending on the risk assessment and security level (SL-T). It may also be specific for the individual equipment/components.

3.7.2. *Examples/elaboration*

The performance requirements are compiled in a PS, which together with the BS from Step 5, can be integrated with safety barrier management.

3.8. *Step 8: Fulfil the barrier performance requirements (comply with MR § 5)*

This step is assigned to the fulfilment of the barrier performance requirements, resulting from Step 7, in order to comply with MR § 5 (Havtil 2023a). This is a continuous process where the performance needs to be checked at regular intervals.

3.8.1. *Justification/explanation*

This process can be considered as a core part of cybersecurity *barrier* management during operation. Deviations from the required performance indicate impairment of the barrier function.

3.8.2. *Examples/elaboration*

The example is related to requirement SR 7.3 Control system back-up (and the barrier function "conducting control system back-ups"), continuing from Table 7. For the technical barrier element (back-up mechanism), the direct performance requirement "reliability of back-up mechanisms" is suggested since this fulfills the SR 7.3 RE 1 "the capability to verify the reliability of back-up mechanisms". A direct performance requirement verification is to measure and verify the reliability based on tests. However, this needs to be specified and made operational. A simplified example is presented in Table 8 where the context is daily back-ups, and the performance requirement is 90 % reliability. (Real back-up regimes are more complex).

Table 8. Example of specification of verification and status rules

Verification	Status rules
Checking 10 back-ups from last two weeks	0-1 tests fail: Green 2-4 tests fail: Yellow 5-10 tests fail: Red

The verification can provide a status using the traffic light system. A yellow or red status indicates an impaired barrier. In this case only the technical barrier element (BE-T) is covered. Similar specifications are needed for BE-H and BE-O (the non-technical barrier elements).

3.9. *Step 9: Fulfil all cybersecurity requirements (comply with FR § 34a)*

This step is assigned to the fulfilment of all applicable requirements that the asset owner has chosen to follow in order to comply with FR § 34a (Havtil 2023b), i.e., in the cybersecurity standards or guidelines resulting from Step 1. This is a continuous process where the fulfilment of requirements needs to be checked at regular intervals.

3.9.1. *Justification/explanation*

This process is part of the management of cybersecurity in general, not limited to barriers. Note

that by fulfilling all cybersecurity requirements, it is not critical that a cybersecurity measure is classified as a non-barrier in Step 2.

3.9.2. *Examples/elaboration*

Fulfilment of cybersecurity requirements should be checked at intervals decided by the asset owner. Some of these requirements will be requirements *about* a given cybersecurity measure, which is relatively stable, whereas requirements *to* the cybersecurity measure depends on to what degree they are stipulated as performance requirements. The latter would need a more frequent follow-up than the former.

4. Discussion and conclusions

4.1. *General applicability*

The general applicability of the methodology is founded on the main principles presented in Table 1. It is i) company neutral, ii) independent of selected cybersecurity requirement standards or guidelines, iii) following regulations and the reasoning of the authorities, and iv) suitable for integration with different regimes of safety barrier management.

4.2. *Remaining work and challenges*

Relevant cybersecurity standards and guidelines cover a broad range of requirements about cybersecurity measures, and it is assumed that all relevant barriers are covered, i.e., that there are no gaps in a standard such as IEC 62443. If any barriers are found to be missing, they should be added. An alternative approach is to identify barriers starting from scenarios. However, the question of completeness now concerns the scenarios instead of the requirements.

Further work could be conducted to increase the "project readiness" of the methodology. A major challenge though is confidentiality restrictions that could apply to specific projects or facilities.

4.3. *Relation to previous work*

Existing cybersecurity barrier management practices have a "dual objective". This dual objective implies complying with the general information and communication technology requirements according to FR § 34a (2023b) in addition to complying with the barrier management regulations according to MR § 5 (2023a). Although current practices ensure the fulfilment of FR § 34a, it does not mean that MR § 5 is automatically fulfilled. One reason for this is that many of the cybersecurity requirements in FR § 34a are requirements *about* having a cybersecurity measure (including barriers) in place, and not requirements *to* how well a cybersecurity measure should perform. In addition, considering all cybersecurity measures according to FR § 34a as barriers is not in accordance with the Barrier Memorandum (PSA 2017) implying that performance requirements must be defined for all cybersecurity measures, including those considered as non-barriers. However, a beneficial consequence is that the distinction between barriers and non-barriers (Step 2) does not become critically important when all measures are covered (Step 9).

The methodology described in this paper fulfils first of all MR § 5 on barriers in accordance with the Barrier Memorandum, and secondly it fulfils FR § 34a on cybersecurity measures in general.

4.4. *Theoretical implications and practical applications*

Theoretical implications include i) clarifying regulatory requirements to cybersecurity in general versus cybersecurity barrier management specifically, ii) understanding the difference between requirements *about* and requirements *to* cybersecurity measures, iii) considering abnormal flow of information as an analogue to flow of energy outside normal operation (the "safety envelope"), requiring barriers, and iv) proposal of an explicit definition of a cybersecurity barrier (as stated below):

A cybersecurity barrier is a measure intended to a) detect abnormal conditions, b) prevent abnormal conditions from developing into cyber-attack situations, c) limit the damage caused by cyber-attacks.

Practical applications include that the methodology is i) flexible (i.e., company neutral), ii) complete (e.g., covering all relevant cybersecurity barrier requirements), and iii) covering also cybersecurity requirements in general (i.e., the dual objective).

The flexible, company-neutral approach is independent of specific cybersecurity standards and safety management regimes and does not require confidential company information.

However, it may result in less detailed and tailored lessons learned across companies.

4.5. *Conclusions*

The current state of integration of cybersecurity and safety barrier management in the industry does not account for a harmonized use of the term barrier. Currently, cybersecurity barriers in the industry are based on a broad view of security measures making it challenging to define and follow up verifiable performance requirements for cybersecurity barriers, and to integrate this with safety barrier management. In this paper, we provide an explicit definition of a cybersecurity barrier, and a methodology for identification of cybersecurity barriers and corresponding performance requirements in line with the regulations and reasoning of the authorities (PSA/Havtil).

A definition is useful, but not sufficient in itself to distinguish between cybersecurity measures that are considered cybersecurity barriers versus those that are considered non-barriers; expert insights in cybersecurity measures are a prerequisite for the identification of cybersecurity barriers and the establishment of performance requirements.

The methodology is not a cook-book recipe, but rather a framework which is flexible enough to take into account special features of each company. This includes the requirements from standards or guidelines that form the basis for establishing cybersecurity measures (incl. barriers) and the existing safety barrier management regime. The methodology also complies with the regulations, definitions and reasoning of the authorities. The initiatives developed by the industry have been "long journeys", and similarly, the implementation of the methodology described in this paper will require significant effort over time.

Acknowledgement

Contribution to the study presented in this paper comes from the project *Cybersecurity Barrier Management* (project number 326717), financed by The Research Council of Norway. The support is gratefully acknowledged. Also, thanks to the anonymous companies and other partners.

References

Carreras Guzman, N.H., D.K.M. Kufoalor, I. Kozine, and M.A. Lundteigen (2019). Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel. In: Beer, M., Zio, E. (Eds.), 29th European Safety and Reliability Conference (ESREL 2019). Hannover, pp. 4099–4106.

Hauge, S. and K. Øien (2016). Guidance for barrier management in the petroleum industry. SINTEF Report A27623. ISBN 978-82-14-06031-7.

Havtil (2023a). Management Regulations for Offshore Petroleum Activities. Norwegian Ocean Industry Authority.

Havtil (2023b). Facilities Regulations for Offshore Petroleum Activities. Norwegian Ocean Industry Authority.

IEC 62443 (2024). IEC 62443 series: Industrial communication networks – Network and system security. International Electrotechnical Commission.

IEC 62443-1-1 (2023). Industrial communication networks – Network and system security – Part 1-1 (WD): Terminology, concepts and models. International Electrotechnical Commission.

IEC 62443-2-1 (2023). Industrial communication networks – Network and system security – Part 2-1 (FDIS): Establishing an industrial automation and control system security program. International Electrotechnical Commission.

IEC 62443-3-3 (2013). Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels. International Electrotechnical Commission.

IEC TR 63069 (2019). Industrial-process measurement, control and automation - Framework for functional safety and security. International Electrotechnical Commission.

ISA-TR.84.00.09 (2017). Cybersecurity Related to the Safety Lifecycle. International Society of Automation.

NIST (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology. U.S. Department of Commerce.

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

PSA (2017). Principles for barrier management in the petroleum industry. Barrier memorandum 2017. Petroleum Safety Authority.

Øien, K., S. Hauge, M.G. Jaatun, L. Flå, and L. Bodsberg (2022). A survey on cybersecurity barrier management in process control environments. In Proceedings of 2022 IEEE International Conference on Cloud Computing Technology and Science, Bangkok: IEEE.

Øien, K., M.G. Jaatun, and C. Thieme (2024). Cybersecurity barrier management: Identification of cybersecurity barriers. Project memo 2024 v2.0, Internal.