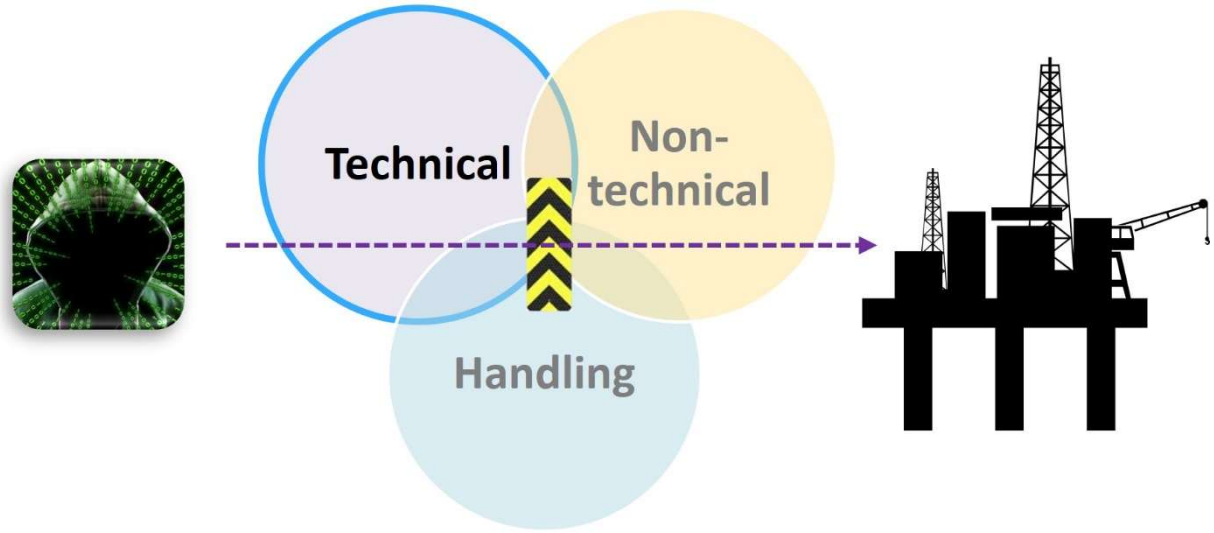

Report

ICS cybersecurity barriers and associated requirements

Authors:
Knut Øien, Christoph Thieme, Martin Gilje Jaatun

Report No:
2025:00700 - Unrestricted

Client:
The Research Council of Norway

SINTEF Digital
Postal address:
Postboks 4760 Torgarden
7465 Trondheim, Norway
Switchboard: +47 40005100
Postmottak.Digital@sintef.no
Enterprise /VAT No:
NO 919303808 MVA

Report

ICS cybersecurity barriers and associated requirements

KEYWORDS
Barriers
Barrier management
Cybersecurity barriers
Cybersecurity measures
Barrier requirements
Oil and gas industry

VERSION
1.1

DATE
2025-10-29

AUTHORS
Knut Øien, Christoph Thieme, Martin Gilje Jaatun

CLIENT
The Research Council of Norway

CLIENT'S REFERENCE
326717

PROJECT NO.
102020847

NO. OF PAGES
88

SUMMARY
This report is the first of three summary reports from the cybersecurity barrier management project. It summarizes new knowledge and guidance on technical cybersecurity barriers, covering the following activities:

i) Identification of cybersecurity barriers and associated requirements
ii) Assessing the status of cybersecurity barriers
iii) Allocation and verification of security levels

The other two reports cover non-technical cybersecurity barriers, and the handling of cybersecurity threats, vulnerabilities and barrier impairments.

All three reports are summarized in a fourth report – a guidance document.

PREPARED BY
Knut Øien
SIGNATURE

CHECKED BY
Geir K. Hanssen, Acting Research Director
SIGNATURE

APPROVED BY
Maria V. Ottermo, Research Manager
SIGNATURE

REPORT NO. 2025:00700
ISBN 978-82-14-07267-9
CLASSIFICATION Unrestricted
CLASSIFICATION THIS PAGE Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
0.5	2025-05-14	Draft version of WP1 report for commenting by CDS-forum Working Committee
0.8	2025-06-12	Draft version of WP1 report for commenting by project partners
1.0	2025-09-01	Final version (internal)
1.1	2025-10-29	Final version (unrestricted)

We used ChatGPT 5 (Open AI, 2025) to assist in the language editing. All outputs were critically reviewed and revised by the authors.

Table of contents

1 Introduction

1.1 Background

Barriers are safety and security measures aimed to detect and contain failure, hazard, or accident situations (safety), and threat, vulnerability, or attack situations (security), at an early stage, to prevent their escalation and to limit their impact.

Barriers complement preventive controls, such as safe, secure, and robust design solutions. While preventive controls are intended to maintain control and prevent unwanted events, barriers are designed to help regain control or minimize harm when such events occur. Both are considered risk-reduction measures; however, specific regulatory requirements apply to the implementation and performance of barriers.

Barriers are generally a combination of technical and non-technical measures, with the non-technical measures aligned to the implemented technical ones, ensuring a balance between investments in technology and non-technical means.

The overall objective of the Cybersecurity Barrier Management (CBM) project is to generate new knowledge and provide guidance for managing cybersecurity barriers as a continuous process throughout the development and operation of Industrial Control Systems (ICS) in the petroleum industry. The project addresses both technical and non-technical aspects, aiming to bridge the safety and cybersecurity domains. This overarching objective is pursued through three secondary research objectives, each of which is supported by a defined set of activities that establish its scope.

The secondary research objectives have been to provide new knowledge and guidance for:

1. Identification of cybersecurity barriers to protect ICS from cyberattacks, and development, implementation, and verification of associated requirements.
2. Integrating non-technical elements in cybersecurity barrier management.
3. Establishing procedures to ensure that cybersecurity threats to ICS are resolved and barrier impairments handled.

These three parts, illustrated in Figure 1, are documented in three summary reports: (1) a *Technical* Barrier Report [1] (this present report), (2) a *Non-technical* Barrier Report [2], and (3) a Barrier *Handling* Report [3].

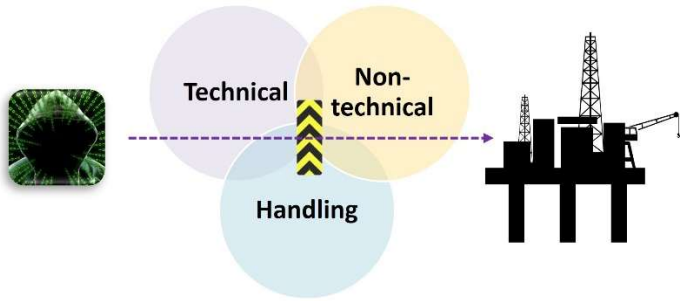

Figure 1.1 The three main parts of the CBM project

A fourth report, the cybersecurity barrier management guidance document [4], is based on the three summary reports. They provide more details and also references to additional background documents.

1.2 Purpose and scope

The aim of this report is to provide new knowledge and guidance on technical cybersecurity barriers, covering the following activities:

i) Identification of cybersecurity barriers and associated requirements
ii) Assessing the status of cybersecurity barriers
iii) Allocation and verification of security levels

The overall scope of this report is related to the three activities and corresponding challenges:

1. How to identify cybersecurity barriers and barrier elements?
2. How to develop, implement and verify cybersecurity barrier requirements?
3. How to assess the cybersecurity barrier status?
4. How to verify security levels of cybersecurity systems and components?

The first two challenges are related to the first activity, and one to each of the two last activities. In addition, a fifth challenge on how to integrate safety and cybersecurity barrier management is related to the barrier management guidance document but is also covered in this report.

Detailed discussions and adaptations of the scope have persisted throughout the project, starting with input from partners and advisors to the overall project and the entire scope of the technical barrier management part, and continuing through iterative work on each of the three specific activities listed above. The scoping is addressed in internal working memos, and the result is partly reflected by the limitations described below.

1.3 Approach

The primary research approach is iterative empirical research, in which exploration and analysis are conducted through multiple iterations in close collaboration with industry partners, advisors, subject-matter experts, and professional forums. This work on *cybersecurity* barrier management also builds upon earlier research on *safety* barrier management, in particular work documented in Hauge and Øien [5], which was carried out in close collaboration with the PDS-forum[1], a professional forum on reliability of computer-based safety systems. Similarly, the research described in this report was developed in active cooperation with the CDS-forum[2], a professional forum for cybersecurity of industrial automation and control systems. The forum's Working Committee served as an advisory board to the CBM project throughout its execution.

Detailed methods include literature search, document reviews, interviews, workshops, and participation in webinars, seminars and conferences. This report also incorporates industry practices, best practices from industry standards and guidelines, and academic publications documented in internal working memos.

1.4 Limitations

Industry practices on cybersecurity barrier management are mainly described in classified company documents for which the research team had limited access, e.g., cybersecurity risk assessments, topology diagrams, and asset inventories. Thus, the guidance provided is high-level and generic. Some examples are given, but without covering all topics in detail.

[1] https://pds-forum.com/
[2] https://cds-forum.com/

In the context of the CBM project, "identification" of cybersecurity barriers does not encompass the initial establishment or the assessment of the need for barriers. Rather, it begins once the barriers have been defined—either as part of a new project where decisions on barrier implementation have already been made, or in relation to an existing installation with established barriers.

With respect to cybersecurity requirements, our primary focus is on the IEC 62443 series of standards [6], in alignment with the CDS-forum statutes. These statutes aim to bridge the gap between technical safety and cybersecurity based on the standards IEC 61511 [7] (PDS-forum) and IEC 62443 (CDS-forum). Therefore, IEC 62443 requirements are used as examples in this report.

This report addresses parts of the challenge on how to develop, implement and verify cybersecurity requirements, focusing on the development or establishment of cybersecurity barrier requirements. While verification is partially addressed, implementation falls outside the scope of this research project and remains the responsibility of asset owners who apply the guidance provided.

1.5 Structure

Chapter 1 introduces the document, followed by Chapter 2, which describes the barrier concept, regulatory requirements, and a definition of cybersecurity barriers. Chapter 3 provides background on cybersecurity perspectives and initiatives from public authorities, regulators, and the industry, along with findings from standards, guidelines, and academic literature reviews. Chapter 4 consists of a methodology for identifying barriers and their requirements. Chapter 5 gives guidance on monitoring and follow-up of cybersecurity barriers. Chapter 6 is about the integration of safety and cybersecurity barrier management, while Chapter 7 provides discussion and conclusions. Abbreviations and definitions are found in Appendix A, and requirement classifications are in Appendices B (IEC 62443-2-1) and C (IEC 62443-3-3).

2 The barrier concept, regulatory requirements, and definition of cybersecurity barriers

The petroleum industry faces the risk of major accidents, which can cause multiple fatalities and massive oil spills. Therefore, it is crucial to reduce these risks to an acceptable level [5].

Requirements for risk management are outlined in the **Management Regulations** Chapter II (§§ 4-6), covering Risk Reduction (§ 4), Barriers (§ 5), and Management of Health, Safety, and the Environment (§ 6). This document focuses on §§ 4 and 5 [8].

MR § 4 Risk reduction

> *In reducing risk as mentioned in Section 11 of the Framework Regulations, the responsible party shall select technical, operational and organisational solutions that reduce the likelihood that harm, errors and hazard and accident situations occur.*
>
> *Furthermore, barriers as mentioned in Section 5 shall be established.*
>
> *The solutions and barriers that have the greatest risk-reducing effect shall be chosen based on an individual as well as an overall evaluation. Collective protective measures shall be preferred over protective measures aimed at individuals.*

It is important to note that *solutions*, such as cybersecurity measures, that reduce the likelihood that harm, errors and hazard and accident situations occur, are part of risk reduction in normal situations (normal operation), and as stated in the second subsection: *Furthermore,* barriers shall be established. They constitute risk reduction in abnormal situations.

A common illustration of barriers is the "Swiss Cheese model" [9] which depicts multiple layers of protection, also known as "defense in depth".

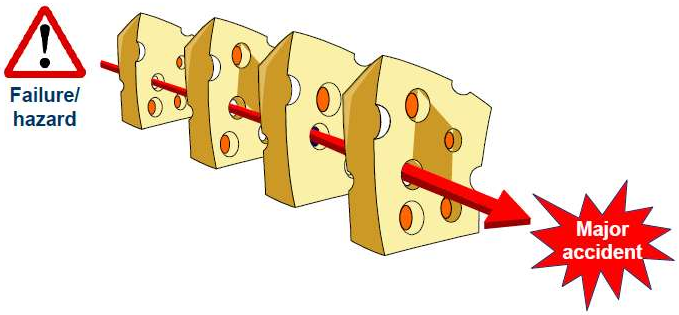

Figure 2.1 Swiss Cheese model (adapted from Reason, 1997) [9]

With multiple barriers in place, major accidents are considered "low probability, high consequence" events. However, even multiple barriers can sometimes be insufficient, leading to major accidents, as illustrated by the alignment of holes in the Swiss Cheese model (Figure 2.1). Individual barriers are not perfect, may not be independent, and may not be adequately compensated for if impaired. Therefore, several requirements in MR § 5 address the capabilities of barriers.

MR § 5 Barriers

Barriers shall be established that at all times can

a) identify conditions that can lead to failures, hazard and accident situations,

b) reduce the possibility of failures, hazard and accident situations occurring and developing,

c) limit possible harm and inconveniences.

Where more than one barrier is necessary, there shall be sufficient independence between barriers.

The operator or the party responsible for operation of an offshore or onshore facility, shall stipulate the strategies and principles that form the basis for design, use and maintenance of barriers, so that the barriers' function is safeguarded throughout the offshore or onshore facility's life.

Personnel shall be aware of what barriers have been established and which function they are intended to fulfil, as well as what performance requirements have been defined in respect of the concrete technical, operational or organisational barrier elements necessary for the individual barrier to be effective.

Personnel shall be aware of which barriers and barrier elements are not functioning or have been impaired.

Necessary measures shall be implemented to remedy or compensate for missing or impaired barriers.

The Petroleum Safety Authority (PSA), now the Norwegian Ocean Industry Authority (Havtil), has clarified the difference between barriers and non-barriers in the Barrier Memorandum (PSA, 2017) [10], including providing barrier-related definitions. Figure 2.2 illustrates the distinction between MR § 4 (safe and robust solutions) and MR § 5 (barriers).

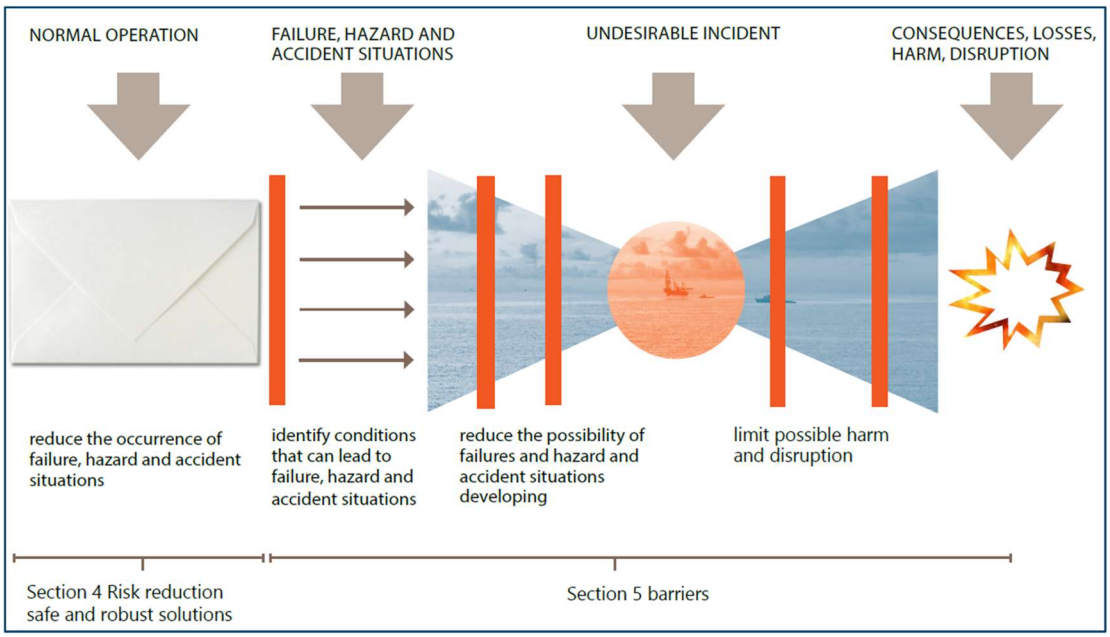

Figure 2.2 Barriers versus "safe and robust solutions" (PSA, 2017) [10]

Risk reduction through safe and robust solutions, as required in MR § 4 Risk Reduction, pertains to normal operation. Barriers, as defined in MR § 5 Barriers, are activated during abnormal situations, outside the normal operation "envelope" (illustrated in Figure 2.2).

Despite the PSA's clarifications and barrier definitions, distinguishing between barriers and non-barriers remains challenging, especially for cybersecurity barriers compared to safety barriers.

The PSA distinguishes between barriers and non-barriers also by referring to performance influencing factors (PIFs). Therefore, there are three categories of risk measures: safe and robust solutions or control measures used during normal operation, barriers, and PIFs, as illustrated in Figure 2.3.

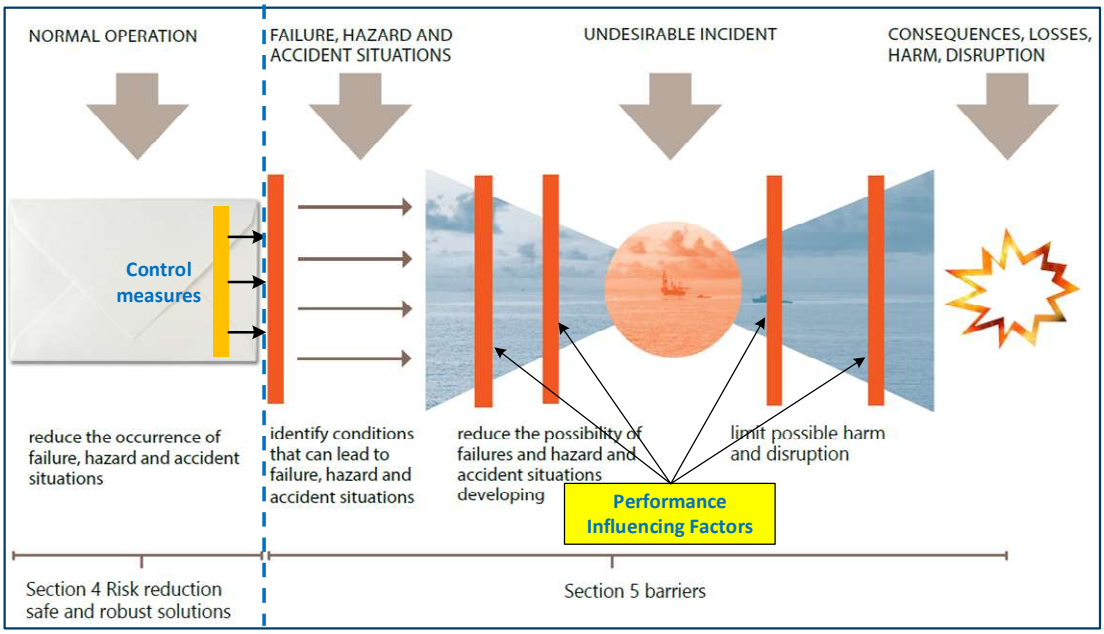

Figure 2.3 Bow-tie model distinguishing between types of measures or solutions

Barriers are depicted as red bars[3], safe and robust solutions (control measures) as an orange bar, and PIFs as a yellow box influencing the barriers (without being a barrier by themselves).

The barrier-related definitions provided by Havtil in the petroleum regulations are included in Appendix A. We follow these definitions since our approach to cybersecurity barrier management is company-neutral and aligns with the regulations. However, note that the guidelines and the Barrier Memorandum [10], where most definitions are found, are not normative. Therefore, there are somewhat divergent definitions of barriers in the petroleum industry.

The latest Barrier Memorandum ("Principles for Barrier Management in the Petroleum Industry") [10] explicitly includes security, stating that using barrier management principles for security incidents promotes a systematic approach to identifying, establishing, and maintaining barriers. It implies that the definitions of security barriers (including cybersecurity barriers) are the same as those for safety barriers. A barrier, including a cybersecurity barrier, is defined as:

> *A measure intended to identify conditions that may lead to failure, hazard and accident situations, prevent an actual sequence of events occurring or developing, influence a sequence of events in a deliberate way, or limit damage and/or loss.*

[3] Bow-ties with a single "top event" can be misleading, as a sequence of events involves a chain of propagating events with corresponding barriers. Preventative and mitigating barriers exist throughout the entire chain of events, not just in relation to one selected "top event."

Note that this definition covers barriers against any type of "failure, hazard, and accident situations." For cybersecurity barriers, this corresponds largely to "vulnerability, threat, and cyber-attack situations."

In addition to general requirements for barriers in the MR § 5 [8], the **Facilities Regulations** Chapter V (§§ 29-40) [11] cover requirements for physical (safety) barriers. The guideline to FR § 34a Control and monitoring system [12] states: "Control and monitoring systems may be interfaced with other systems, but it should be ensured that this does not weaken the system. In addition, Offshore Norge Guideline No. 104 should be used as a basis for protecting against ICT-related hazards."[4] This guideline provides information security baseline requirements (ISBRs) for security controls and measures. These are not referred to as barriers and can be considered general cybersecurity measures, managed as part of cybersecurity management, but not necessarily as part of cybersecurity *barrier* management.[5] ISBRs consist of both barrier and non-barrier requirements.

The Facilities Regulations [11] also include definitions (§ 3) covering safety system and safety functions (addressing technical barrier elements) as stated in Appendix A. These definitions are part of the regulations and thus normative. Additionally, the Facilities Regulations includes requirements to safety functions (§ 8):

> *Facilities shall be equipped with necessary safety functions that can at all times a) detect abnormal conditions, b) prevent abnormal conditions from developing into hazard and accident situations, c) limit the damage caused by accidents.*

Given that safety functions align with barrier functions, cybersecurity barriers may be defined as:

> *A cybersecurity barrier is a measure intended to a) detect abnormal conditions, b) prevent abnormal conditions from developing, or c) limit the damage caused by cyber incidents.*

Other barrier-related definitions (e.g., barrier function and barrier element) are found in Appendix A.

A note on referencing industry standards: Guidelines to regulations often recommend industry standards to meet regulatory requirements. These regulatory guidelines are not legally binding, so actors can adopt other solutions. If a recommended solution is chosen, it is generally assumed that regulatory requirements are met. If other solutions such as different standards or company-specific procedures are adopted, they must be documented to be at least as good as if not better than the recommended ones. This is explained in the **Framework Regulations**, § 24 Use of Recognized Standards [14], and it means that e.g., IEC 62443 can be used instead of NOROG 104.

[4] Offshore Norge Guideline No. 104, previously known as NOROG 104, is referenced in this document as NOROG 104 [13].

[5] This is similar to safety measures covering much more than barriers, i.e., safety management is broader than safety *barrier* management.

3 Background for the project

3.1 Perspectives from public authorities

The Lysne Committee found petroleum regulations lacking specificity regarding digital threats and recommended that the Petroleum Safety Authority (PSA) require barriers for digital vulnerabilities (NOU 2015: 13) [15]. This recommendation aims to extend the robust safety tradition in health, safety, and environment (HSE) to the digital realm. While HSE has long focused on barriers and barrier management, NOU 2015: 13 highlights the need for better testing and verification of barriers against ICT incidents, though it does not provide examples or definitions of such barriers. This was followed by the white paper Meld. St. 38 (2016-2017) [16].

3.2 Perspectives and initiatives from the regulator

NOU 2015: 13 and Meld. St. 38 (2016-2017) led to four years of grants (2018-2021) for the PSA to improve ICT security in industrial systems, resulting in 22 knowledge reports[6]. However, these reports did not define or describe how to identify cybersecurity barriers.

Before this, the PSA focused on safety barrier management, publishing Barrier Memorandums in 2011, 2013 [17], and a major update in 2017 [10]. The 2017 update included security but did not define cybersecurity barriers, suggesting that the general barrier definition applies. The memorandums also did not specifically address barrier identification, apart from describing the breakdown from barrier functions to elements.

Explicit ICT security and cybersecurity requirements are scarce in petroleum regulations. Only two explicit requirements are found in the guidelines: § 29 of the Management Regulations [18], which mentions ICT events as reportable, and § 34a of the Facilities Regulations [12], which references NOROG 104 [13]. Consequently, cybersecurity requirements must be derived from guidelines or standards like NOROG 104 or IEC 62443. It should be noted that in 2019, the authorities sent a letter[7] to the industry outlining which regulations and sections they considered relevant to ICT security.

The key finding about cybersecurity barrier requirements is the distinction between having a cybersecurity measure in place (*requirements about*) and performance requirements for these barriers (*requirements to*). Standards and guidelines mix requirements for cybersecurity measures with general functional performance requirements. Cybersecurity measures include the barriers themselves (related to identifying cybersecurity barriers), while performance requirements in MR § 5 apply to the barriers. This distinction is crucial when establishing a cybersecurity barrier management system.

3.3 Initiatives by the industry

When referring to *"the industry,"* we primarily consider two oil and gas companies in the Norwegian petroleum sector. These companies have compiled requirements for cybersecurity measures in performance standards, integrated cybersecurity barrier management with safety barrier management, and established approaches for identifying cybersecurity barriers, as briefly outlined below. Certain challenges are also highlighted.

[6] https://www.havtil.no/en/explore-technical-subjects2/technical-competence/news/2021/ict-security---robustness-in-the-industry/

[7] https://www.ptil.no/contentassets/cdf45185805f4c14bc7caf03f6853d08/2019_1176-brev-handtering-av-iktsikkerhet.pdf

Requirements to cybersecurity measures compiled in performance standards

The companies have established operational performance standards (PSs) for cybersecurity, titled *Safety & Automation System Security* and *Cyber Security*, respectively. One of the companies has also produced a technical report that supports its PS; however, this report does not define or identify specific cybersecurity barriers. Instead, it addresses cybersecurity requirements more generally and does not focus on barrier-specific requirements. The report is based on the broader frameworks of IEC 62443 [6] and the NIST Cybersecurity Framework (CSF) [19], which encompass overarching security measures.

The other company's performance standard (PS) document, which is based on NOROG 104 [13], outlines cybersecurity performance requirements and references barrier functions and elements. However, it does not provide a clear definition of cybersecurity barriers. The accompanying Barrier Management Manual primarily addresses safety barriers and defines barrier elements in a way that is similar, but not identical, to the definitions provided by the PSA in Appendix A. As for the first company, this company's PS emphasizes general cybersecurity requirements—comparable to those in IEC 62443—rather than specifying distinct cybersecurity barriers.

Integration of cybersecurity barrier management with safety barrier management

The companies have integrated cybersecurity barrier management with their existing safety barrier management regimes, driven by increased attention to cybersecurity reporting to top management. Their approaches differ due to varying safety barrier management methods and the use of different cybersecurity standards (IEC 62443 vs. NOROG 104). The Cybersecurity Barrier Management (CBM) project aim has been to develop a flexible, common approach for the petroleum industry, accommodating these differences.

In industry initiatives, performance standards include requirements based on standards like IEC 62443 [6] and NOROG 104 [13], implicitly treating all cybersecurity measures as barrier measures. This contrasts with the PSA's approach, which distinguishes barrier measures from other cybersecurity measures. We advocate for this distinction to align with PSA reasoning and facilitate consistent integration of cybersecurity and safety barrier management.

Identification of cybersecurity barriers

Two complementary approaches for barrier identification were identified (in internal working memos [20], [21]): 1) Event sequence and functional top-down approach, and 2) Asset inventory bottom-up approach. These methods ensure comprehensive identification of barriers in safety barrier management.

In cybersecurity barrier management, both approaches have been applied, though not in combination. The first approach faces challenges in achieving a sufficient breakdown from barrier functions to barrier elements, while the second approach is constrained by limited access to complete OT asset inventories—particularly in brownfield environments.

Applying the approaches individually therefore raises concerns about completeness. *How can we ensure that all barrier functions, sub-functions, and elements are identified?* This question is addressed in Section 4.1.

3.4 Findings from cybersecurity standards and guidelines, and academic literature

Standards/guidelines like NIST CSF [19], IEC 62443 [6], IEC 63069 [22], ISA-TR.84.00.09 [23], and NOROG 104 [13] rarely define 'cybersecurity barriers,' using terms like countermeasure, security measure, and safeguard instead. We will focus on IEC 62443 as an international standard, despite its draft challenges, in favor of local

guidelines like NOROG 104 [13]. IEC 62443 currently uses 'countermeasure,' but this may change to 'security measure' in the future.

In a previous literature review [24], we searched for publications on identifying cybersecurity barriers and barrier elements. We reviewed the use of the term 'cybersecurity barriers' but did not specifically search for definitions. Few publications used the term, and none provided a definition.

We conducted preliminary testing to identify cybersecurity barriers based on PSA (2017) [10], distinguishing between safe and robust solutions, barriers, and performance influencing factors (PIFs) as described in Chapter 2. This was tested on countermeasures from ISA-TR.84.00.09 (2017) [23]. Results are documented in an internal working memo [21] and an IEEE article [24].

The assignment of countermeasures to various categories can be disputed and should be justified. However, the essence is that cybersecurity barriers are only one category of cybersecurity measures, following the PSA's reasoning.

4 Identification of cybersecurity barriers and associated requirements

4.1 Complementary approaches and rationale for a standards-based method

How can we ensure all barrier functions, sub-functions, and elements are identified? This question forms the basis for the methodology outlined in this chapter. Recall from the limitations in Section 1.4 that "identification" of cybersecurity barriers does not encompass the initial establishment or the assessment of the need for barriers. Rather, it begins once the barriers have been defined—either as part of a new project where decisions on barrier implementation have already been made, or in relation to an existing installation with established barriers.

Barrier identification in safety barrier management typically combines a top-down approach—based on event sequences and functional breakdowns—with a bottom-up approach using asset inventories. Hauge and Øien [5] highlight methods such as barrier grids, hierarchical functional breakdowns, and barrier logic diagrams. Any new equipment identified as barriers during and after implementation is also included.

This chapter introduces a new approach: starting with security measure requirements from relevant standards and guidelines. Combined with other methods, this helps ensure comprehensive identification of all barrier functions, sub-functions, and elements (as shown in Figure 4.1):

I. Top-down approach: Identification of barrier functions using event sequences, and breakdown into sub-functions and elements
II. Bottom-up approach: Identification of barrier elements from the asset inventory
III. Standards-based approach: Identification of barrier functions from security measure requirements in standards and guidelines, and breakdown into sub-functions and elements

Continuous identification of additional barrier elements during and after implementation apply to all.

The first approach often begins with selected scenarios from risk assessments (e.g., network, physical, or supply chain entry points), using tools like barrier grids or bow-ties to map barrier functions along the event chain. However, since scenarios are always limited in scope, some barrier functions, sub-functions, and elements may be missed.

Additionally, the first approach includes breaking down barrier functions into sub-functions and elements through a hierarchical functional breakdown, as mentioned in the Barrier Memorandum [10]. The level of detail varies—some methods use a single layer of functions and elements, while others incorporate multiple sub-function levels for greater depth.

In the new method described in detail in this chapter (Approach III), scenarios are not used. Instead, we begin with security measure requirements from standards and guidelines (e.g., IEC 62443), based on the assumption that these cover most relevant barrier functions by addressing a wide range of abnormal situations. These functions represent a subset of all security measures, as categorized by PSA in the Barrier Memorandum [10]. This approach is expected to yield a more comprehensive identification of barrier functions than scenario-based methods. Any gaps in the standards can be filled by adding additional barriers. Barrier functions are broken down into one level of sub-functions, with the option to extend further if needed.

Using publicly available standards to identify relevant barrier functions (Approach III) avoids dependence on confidential scenario data required in Approach I. Similarly, the asset-based bottom-up Approach II often involves sensitive information, which is particularly challenging in cybersecurity and brownfield settings.

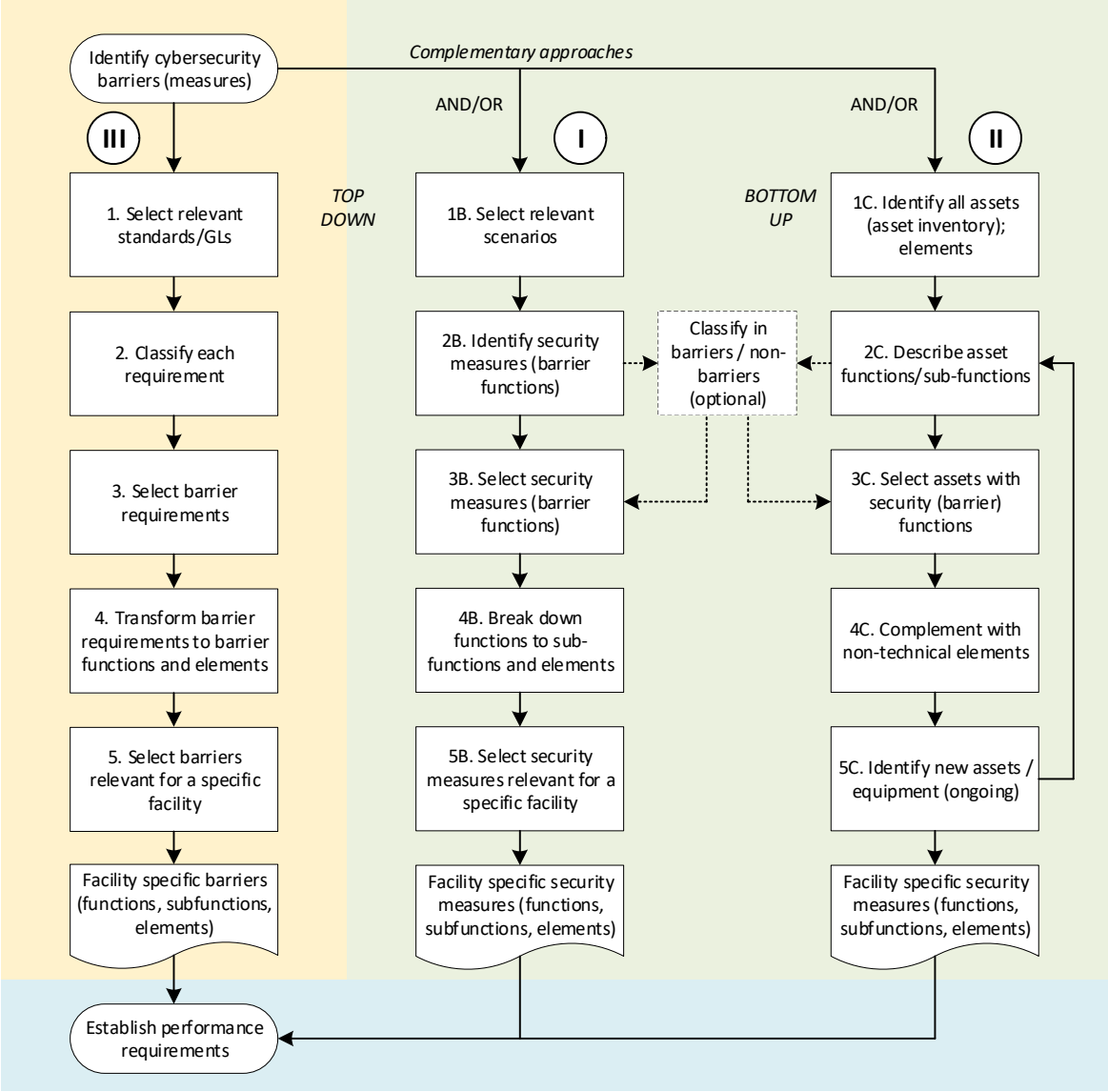

Figure 4.1 Approaches for identification of cybersecurity barriers

Companies, with their access to all necessary information, can choose any approach or combination of approaches. And, as indicated in Figure 4.1 for Approach I and II, they can also choose whether or not to classify the security measures in barriers and non-barriers. Such a classification is not needed to fulfil FR § 34a; however, regarding the fulfilment of MR § 5, omission of classification is not in accordance with the Barrier Memorandum.

One benefit of Approach I is that event sequence diagrams, like barrier grids and bow-ties, help visualize barriers. They can show multiple barrier impairments within the same event chain, which is crucial for assessing consequences and risks. For more details on Approaches I and II, refer to Hauge and Øien [5] for production facilities, and NSA/DNV [25] for drilling rigs, and the Barrier Memorandum [10].

4.2 Principles

The methodology is built on five main principles.

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)[8]
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

The methodology differentiates between barriers and non-barriers as per the Barrier Memorandum (PSA, 2017) [10]. Non-barriers are also covered according to the fifth principle. General cybersecurity requirements (covering both barriers and non-barriers) are referred to in the guidelines to FR § 34a [12]. Asset owners decide on managing non-barriers similarly to barriers.

A methodology has been developed to identify cybersecurity barriers and requirements based on the five principles, using a preferred cybersecurity standard or guideline and a top-down approach.

4.3 Methodology step-by-step

The nine-step methodology includes the first five steps for identifying cybersecurity barriers and elements, and the last four for establishing performance requirements and verifying their fulfilment.

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)

The steps are illustrated in a flowchart in Figure 4.2.

Each step includes a description, justification/explanation, and examples/elaboration. We focus on the international standard IEC 62443 for exemplification, using parts IEC 62443-2-1 [26] and IEC 62443-3-3 [27]. The Security Program Elements (SPEs) in Part 2-1 are crucial for asset owners, while the mapping of each security requirement to the Security Levels (SLs) in Part 3-3 is key for determining Security Levels (SLs). The security requirements in Part 3-3 are structured in Foundational Requirements (FRs). SPEs and FRs are the only requirement structures included in IEC 62443-1-1 [28].

[8] We refer specifically to the Barrier Memorandum, which now explicitly includes security. It states that applying barrier management principles to security incidents promotes a systematic approach to identifying, establishing, and maintaining barriers. While this "hypothesis" has been questioned, our approach shows that using the same classification of barriers and non-barriers as in safety barrier management is feasible, supporting the hypothesis. However, the suitability of this classification for cybersecurity remains open to debate.

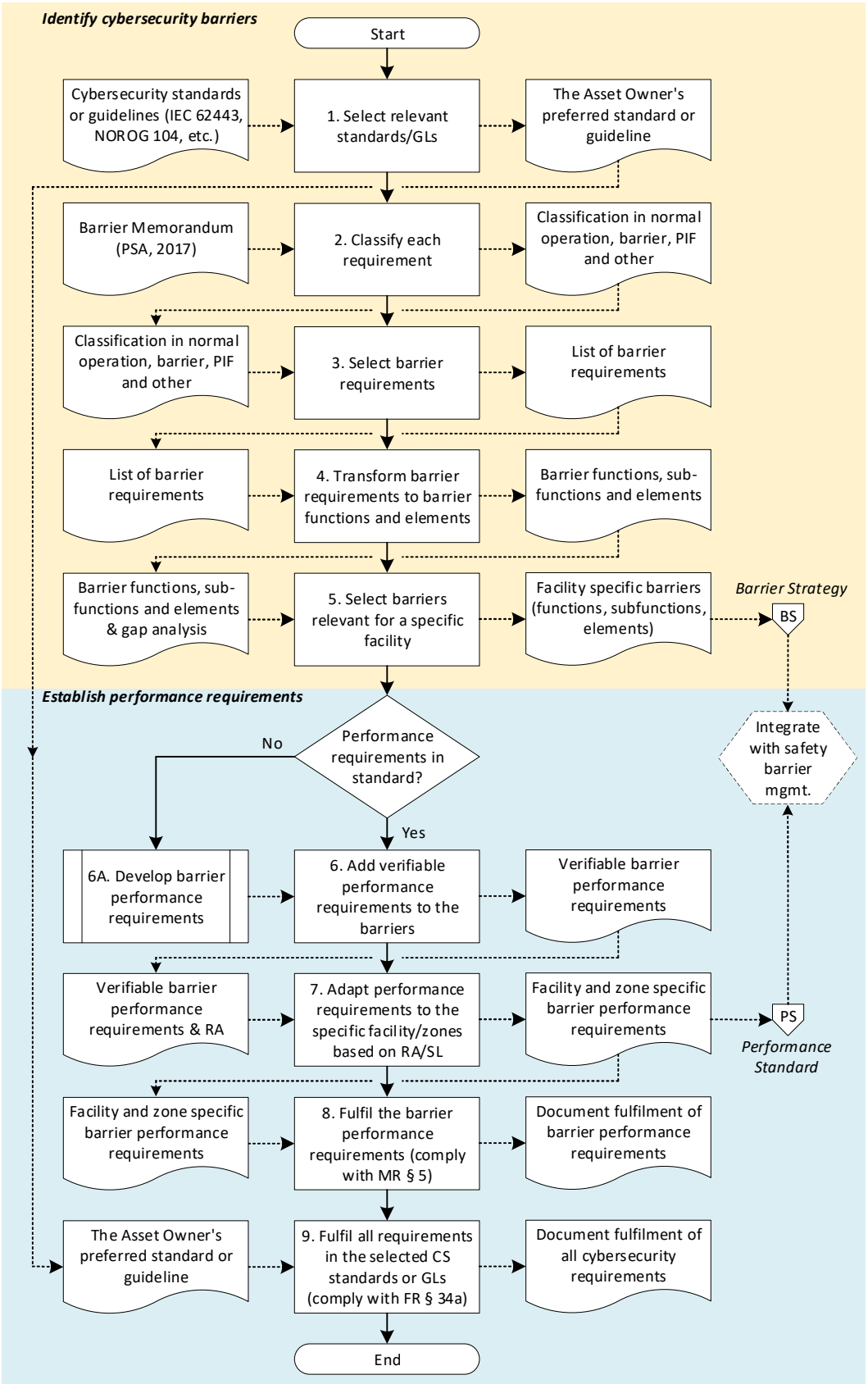

Figure 4.2 Flowchart of methodology

4.3.1 Step 1: Select relevant standards/GLs and extract cybersecurity requirements

Relevant cybersecurity standards and guidelines (e.g., IEC 62443 [6] or NOROG 104 [13]) are selected, and requirements are extracted (typically in an Excel sheet). These cover a wide range of cybersecurity measures, assumed to include all relevant barriers.

Companies with requirements compiled in performance standards (PSs) or technical reports (TRs) can use these as a starting point if they follow the PSA's reasoning, which views cybersecurity barriers as a subset of all cybersecurity measures. Considering all cybersecurity measures as barriers requires defining performance requirements for all measures, as per MR § 5 [8].

Justification/comments

Requirements about security measures are included in relevant cybersecurity standards/guidelines, categorized as Foundational Requirements (FRs) and System Requirements (SRs) in IEC 62443-3-3 [27]. Although there are no complete lists, security measures can be derived through a systematic review of all requirements (cf. Step 2).

The methodology should be industry-wide and 'company neutral,' allowing the use of any external cybersecurity standards/guidelines or in-house documents as a starting point. This approach ensures broad coverage of cybersecurity requirements, with a specific focus on barriers. Consequently, the classification between barriers and non-barriers (Step 2) and selection (Step 3) are less critical, as non-barriers can be addressed through the broader set of cybersecurity requirements (eventually in Step 9).

Example/elaboration

All 87 requirements from IEC 62443-2-1 [26] and 51 system requirements from IEC 62443-3-3 [27] (excluding requirement enhancements – REs) are extracted. Companies may also include other requirements, such as those from other parts of IEC 62443 (e.g., Parts 2-4, 4-1 and 4-2).

4.3.2 Step 2: Classify each requirement

Each requirement is classified according to the Barrier Memorandum [10] into: i) safe and robust solutions (normal operation), ii) barriers, and iii) performance influencing factors (PIFs). If none fits, an 'other' category is used, covering general cybersecurity foundation or aspects. A requirement can belong to multiple categories. The decision tree in Figure 4.3 aids this classification. Complete assessments in Step 2 are documented in Appendix B and C for IEC 62443-2-1 and IEC 62443-3-3, respectively.

When assessing *safe and robust solutions* versus *barriers*, we refer to normal operation (keeping control) for the former and abnormal situations (regaining control) for the latter. In the cybersecurity domain, normal operation of *flow of information* is analogous to normal operation of *flow of energy* in the safety domain (Carreras Guzman et al. 2019) [29], covering both information in transit and at rest.

Justification/comments

This classification and interpretation of barriers comply with regulations and align with the safety domain, facilitating consistent integration of cybersecurity and safety barrier management. Currently, the industry lacks a harmonized use of the term 'barrier,' with cybersecurity 'barriers' based on a broad view of security measures.

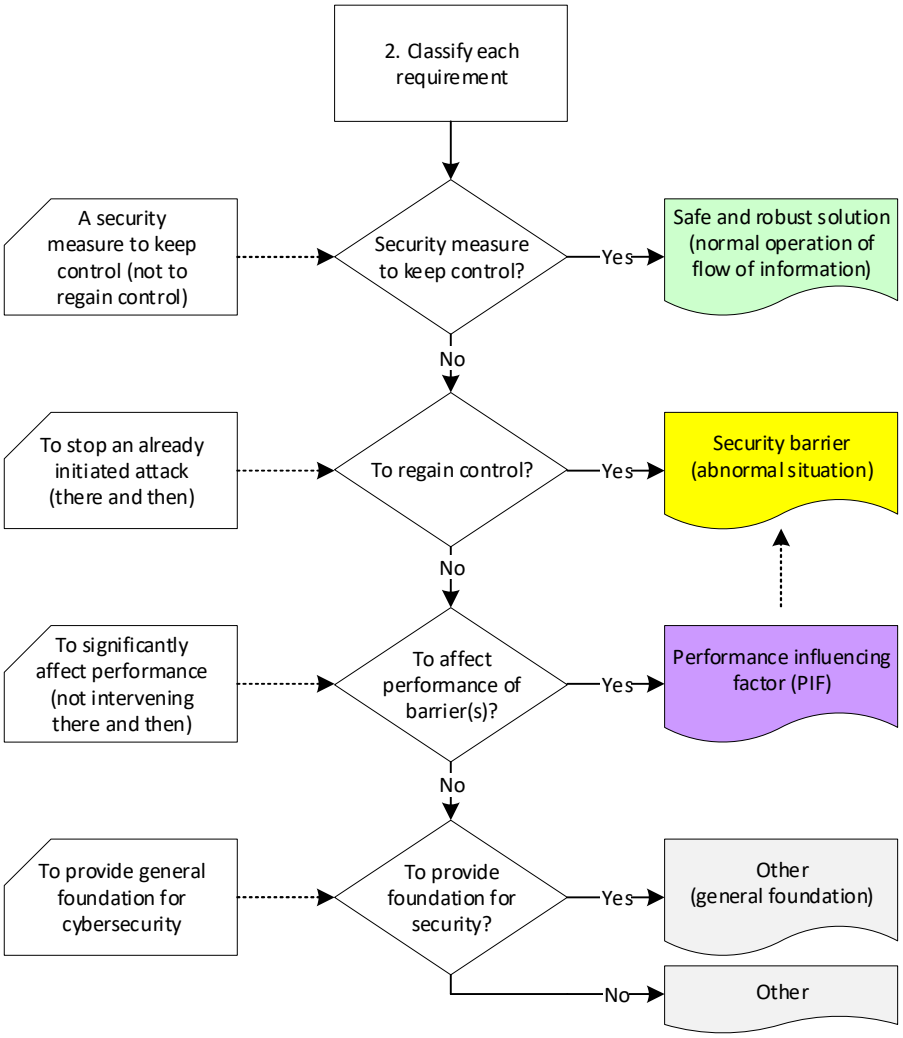

Figure 4.3 Decision tree for classification of requirements

The PSA interpretation of barriers emphasizes detection and response, balancing prevention, which accounts for about 95% of cybersecurity requirements (cf. internal working memo [21]). Cybersecurity measures that detect and mitigate ongoing intrusions are analogous to systems outside normal operating conditions. According to PSA (2017) [10], 'barriers are measures that offer protection in failure, hazard, and accident situations.' Thus, during an ongoing cyber-attack, barriers are essential.

The asset owner should define the consequence classes for the assessment, such as health and safety, environment, confidentiality, regularity, and availability. This has implications for the integration of safety and cybersecurity barrier management, which is addressed in Chapter 6.

Barriers are measures that directly affect the sequence of events. For organizational barrier elements (i.e., the human part), 'front-end' personnel are considered, while 'back-end' personnel are not barriers but may be PIFs if they significantly impact barrier performance. According to PSA (2017) [10], a PIF must have a significant effect. PSA (2017) [10] also notes that a broad definition of barriers (‘anything that may help prevent an incident occurring or limit damage’) makes it difficult to define verifiable performance requirements, as currently practiced in the industry regarding cybersecurity barriers.

Example/elaboration

Table 4.1 shows examples of classification for the three requirements COMP 2.1-2.3 of sub-element COMP 2 Malware Protection within SPE 4 Component Security in IEC 62443-2-1 [26]. The 'other' column is not shown.

Table 4.1 Examples of classification of requirements (from IEC 62443-2-1)

COMP 2 – Malware protection	Requirements	Normal	Barrier	PIF	Assessment
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			Safe and robust solution. Avoid getting into failure, hazard and accident situations by ensuring malware are not present prior to use.
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		It is a barrier preventing events developing by detecting malware and prevent it from executing.
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	Testing affects the performance of the anti-malware (the barrier); thus, it is a PIF (it has a significant impact).

Checking components for malware before use is a safe and robust solution, part of normal operation, to keep control (not to regain control). Malware protection acts as a barrier by detecting and preventing malware execution[9]. Testing impacts the performance of anti-malware (the barrier) and is thus a PIF.

COMP 2.2 is an example of a requirement *about* having a cybersecurity measure in place (i.e., the barrier itself), while COMP 2.3 specifies the performance of that measure, making it a PIF. COMP 2.3 is a verifiable performance requirement per MR § 5, whereas COMP 2.2 is not. Examples of control measures in normal operation, apart from COMP 2.1 (malware free components before use), include screen lock, authentication, authorization, background checks, and data classification.

Table 4.2 shows examples from IEC 62443-3-3 [27], FR 7 Resource Availability (RA), using all three categories. SR 7.6 and SR 7.7 are requirements related to normal operation, SR 7.1, SR 7.3, SR 7.4 and SR 7.5 are barrier requirements, and SR 7.8 is related to both normal operation and barrier. The 'other' column is not shown.

The requirement enhancements SR 7.1 RE1 and RE2, and SR 7.3 RE2, are included as barrier sub-functions (BSF), whereas SR 7.6 RE 1 is included as a control sub-function. SR 7.3 RE1 is a PIF and can be used as a performance requirement. In general, the requirement enhancements (REs) are most often specific ways of achieving the system requirements (SRs), i.e., they are sub-functions.

Asset owners may reassess and adjust the classification of requirements and justifications for IEC 62443-2-1 (Appendix B) and IEC 62443-3-3 (Appendix C). As stated in some of the assessments in Table 4.2, the classification may depend on the consequence categories included (i.e., whether a requirement is critical for safety or production). Also, relationships between similar requirements in the various parts of IEC 62443 should be considered. IEC 62443-2-1 provides cross-references to Parts 2-4, 3-3 and 4-2. However, it should be noted that the cross-references are sometimes not directly comparable, or only partly overlapping.

[9] The distinction may be debatable. COMP 2.1 aims to avoid failure, hazard, or accident situations, while COMP 2.2 focuses on preventing such situations from developing, starting with detection.

Table 4.2 Examples of classification of requirements (from IEC 62443-3-3) – FR 7

Req. ID	Requirement title	SL	Requirement	Normal	Barrier	PIF	Assessment / comments
SR 7.1	Denial of service protection	1	The control system shall provide the capability to operate in a degraded mode during a DoS event.		X		Protection of safety systems in DoS situations.
SR 7.1 RE 1	Manage communication loads	2	The control system shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.		X		Included as barrier sub-function (BSF)
SR 7.1 RE 2	Limit DoS effects to other systems or networks	3	The control system shall provide the capability to restrict the ability of all users (humans, software processes and devices) to cause DoS events which affect other control systems or networks.		X		Included as barrier sub-function (BSF)
SR 7.2	Resource management	1	The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.			X	Resource exhaustion which is not caused by DoS attacks (addressed in SR 7.1) is caused by unintended intensity in flow of information or unintended intensity in processing of information. This influences the performance (response times, capacity) of the control system; thus this is a PIF (e.g., of SR 6.2).
SR 7.3	Control system backup	1	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		Back-up is a barrier. Consider a ransomware shutting down your control system, the recovery of that system (from a previously taken backup) is way outside normal operation. However, it may not be safety critical (e.g., only affecting production), thus it depends on the consequence classes included.
SR 7.3 RE 1	Backup verification	2	The control system shall provide the capability to verify the reliability of backup mechanisms.			X	Included as performance requirement (PR BE-T)
SR 7.3 RE 2	Backup automation	3	The control system shall provide the capability to automate the backup function based on a configurable frequency.		X		Included as barrier sub-function (BSF) and performance requirement
SR 7.4	Control system recovery and reconstitution	1	The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.		X		Recovery is a barrier. However, it may not be safety critical (e.g., only affecting production), thus it depends on the consequence classes included.
SR 7.5	Emergency power	1	The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.		X		To prevent loss of function of security mechanisms. Switching to emergency power is outside normal operation.
SR 7.6	Network and security configuration settings	1	The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.	X			This is part of normal operation. Recommended network and security configurations are "robust and secure" design.
SR 7.6 RE 1	Machine-readable reporting of current security settings	3	The control system shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.	X			Included as a sub-control function and part of normal operation.
SR 7.7	Least functionality	1	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.	X			Hardening prior to operation. Normal sound secure solutions.
SR 7.8	Control system component inventory	2	The control system shall provide the capability to report the current list of installed components and their associated properties.	X	X		This is part of normal operation, but it can also be used to detect unintended/ unauthorized installation of software, similarly to SR 3.2, in such a use-case this would be a barrier.

4.3.3 Step 3: Select barrier requirements

Requirements classified as barriers (functions or systems) are selected, forming a 'barrier profile' according to IEC 62443, which is a subset of all requirements.

Justification/comments

The CBM project focuses on barriers, not the broader perspective of all cybersecurity measures in general cybersecurity management. The subset of barriers is part of cybersecurity *barrier* management.

Example/elaboration

Of the 87 requirements in IEC 62443-2-1, 33 relate to barriers (Appendix B). Of the 51 system requirements (SR) in IEC 62443-3-3, 28 relate to barriers (Appendix C). The requirement enhancements (REs) in IEC 62443-3-3 are only partly covered, as they depend on the risk assessment and SL-T (Security Level – Target) of each zone. Thus, they are not included in the numbers provided above.

Table 4.3 provides two examples (including REs) of requirements from IEC 62443-3-3 relevant as barrier requirements. This includes REs as sub-functions or PIFs to the barriers. SR 6.2 is from FR 6 Timely Response to Events (TRE), and SR 7.3 is from FR 7 Resource Availability (RA).

Table 4.3 Examples of classification of requirements (from IEC 62443-3-3) – FR 6 and FR 7

Req. ID	Requirement title	Requirement	Normal	Barrier	PIF	Assessment / comments
SR 6.2	Continuous monitoring	The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner. (NOTE: Response time is a local matter outside the scope of this standard.)		X		To detect security breaches. Detection is a barrier function.
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		Back-up is a barrier. Consider a ransomware shutting down your control system, the recovery of that system (from a previously taken backup) is way outside normal operation. However, it may not be safety critical (e.g., only affecting production), thus it depends on the consequence classes included.
SR 7.3 RE 1	Backup verification	The control system shall provide the capability to verify the reliability of backup mechanisms.			X	Included as performance requirement (PR BE-T)
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		Included as barrier sub-function (SBF2) and performance requirement

SR 6.2 and SR 7.3 are barrier requirements that can be transformed into barrier functions in Step 4. SR 7.3 RE 1 is a PIF that can serve as a performance requirement (PR) for the technical barrier element (BE-T) (in Step 6). SR 7.3 RE 2 is a sub-function of SR 7.3. A backup is used as part of recovery and restoration (SR 7.4) and could be considered part of the recovery barrier function, i.e., as a sub-function[10]. However, the further breakdown to barrier elements will be the same.

4.3.4 Step 4: Transform barrier requirements to barrier functions and elements

Barrier requirements are transformed into barrier functions, sub-functions, and elements using a functional top-down hierarchy. This transformation is illustrated in Figure 4.4.

We distinguish between three types of barrier elements: Technical, Human, and Operational (THO). 'Human' refers to front-end personnel directly involved in activating a barrier, avoiding confusion with 'organizational' (cf. PSA, 2017 [10]), which may imply back-end personnel like management. Operational barrier elements are the actions or activities personnel must perform to realize a barrier function (PSA, 2017) [10]. See Appendix A for definitions.

[10] The act of taking backups could strictly be considered part of normal operation, whereas using a backup during an abnormal situation is a barrier function/sub-function. However, it needs to be available before recovery.

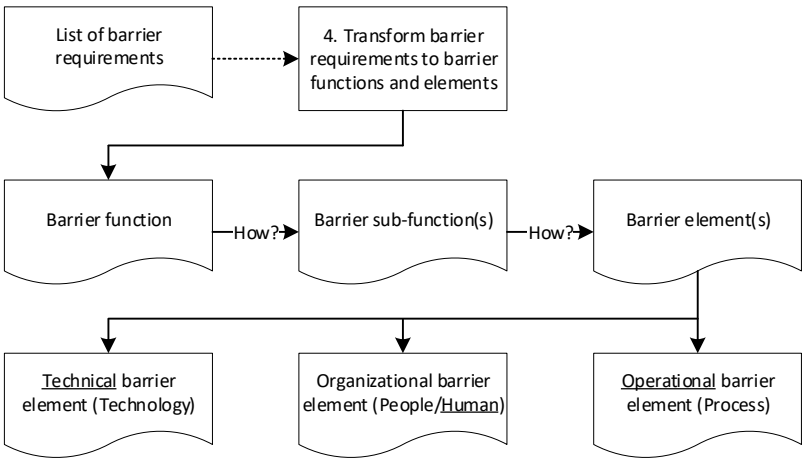

Figure 4.4 Transforming barrier requirements to barrier functions and elements

Justification/comments

This step uses a barrier hierarchy, a well-known approach also referred to by the PSA (2017) [10], as shown in Figure 4.5.

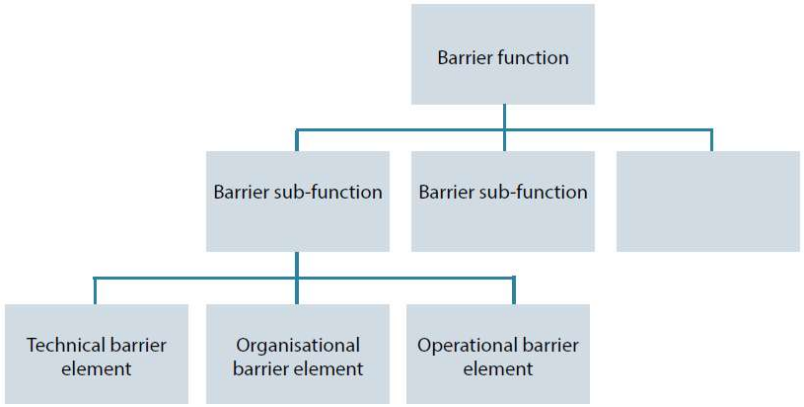

Figure 4.5 Barrier hierarchy (adapted from PSA, 2017) [10]

Example/elaboration

Continuing from Table 4.3, Table 4.4 shows the transformation of barrier requirements to barrier functions and sub-functions. The transformation to barrier functions is based on the *requirement description* (see underlined text), while sub-functions are derived from the *rationale and supplemental guidance* in IEC 62443-3-3 [27]. Extracts of the guidance for system requirements SR 6.2 and SR 7.3 are provided below.

Extract of the rationale and supplemental guidance for SR 6.2: "Control system monitoring capability can be achieved through a variety of tools and techniques (for example, IDS, IPS, malicious code protection mechanisms and network monitoring mechanisms). … mechanisms such as SIEM[11] are commonly applied to correlate individual events into aggregate reports which establish a larger context in which the raw events occurred."

Extract of the rationale and supplemental guidance for SR 7.3: "The availability of up-to-date backups is essential for recovery from a control system failure and/or mis-configuration. Automating this function ensures that all required files are captured, reducing operator overhead."

[11] SIEM – Security Information and Event Management

Table 4.4 Examples of transforming barrier requirements to barrier functions and sub-functions

IEC 62443-3-3 Requirements				Barrier functions and subfunctions	
Req. ID	**Requirement title**	**SL**	**Requirement**	**Barrier function(BF)**	**Barrier sub-function (BSF)**
SR 6.2	Continuous monitoring	2	The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner. (NOTE: Response time is a local matter outside the scope of this standard.)	Detect, characterize and report security breaches in a timely manner	Intrusion detection Intrusion prevention Malware protection Network monitoring Event management
SR 7.3	Control system backup	1	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.	Conducting back-ups	Capturing required files
SR 7.3 RE 1	Backup verification	2	The control system shall provide the capability to verify the reliability of backup mechanisms.	Not relevant (NR)	NR
SR 7.3 RE 2	Backup automation	3	The control system shall provide the capability to automate the backup function based on a configurable frequency.	Not relevant (NR)	Automation of back-up function

Note that SR 7.3 RE 2 represents a sub-function, so the underlining in Table 4.4 pertains to the sub-function. SR 7.3 RE 1 is only relevant for verification, which will be addressed in Step 6. Not relevant (NR) means not relevant as barrier function or sub-function.

Table 4.5 (an extension of Table 4.4) shows the further breakdown from barrier sub-functions to barrier elements, distinguishing between the three types of barrier elements.

Table 4.5 Breakdown from barrier sub-functions to barrier elements

IEC 62443-3-3 Requirements		Barrier functions and subfunctions		Barrier elements		
Req. ID	**Requirement title**	**Barrier function(BF)**	**Barrier sub-function (BSF)**	**Barrier element (BE) - Technical**	**Barrier element (BE) - Human**	**Barrier element (BE) - Operational**
SR 6.2	Continuous monitoring	Detect, characterize and report security breaches in a timely manner	Intrusion detection Intrusion prevention Malware protection Network monitoring Event management	IDS IPS Malware prot. m. Network mon. m. SIEM	IDS operator	Detect, characterize and report
SR 7.3	Control system backup	Conducting back-ups	Capturing required files	Back-up mechanisms	Back-up responsible	Taking back-up (manually)
SR 7.3 RE 1	Backup verification	Not relevant (NR)	NR	NR	NR	NR
SR 7.3 RE 2	Backup automation	Not relevant (NR)	Automation of back-up function	Automatic back-up	NR	NR

Barrier elements can also be based on the rationale and supplemental guidance in IEC 62443-3-3, though this mainly applies to technical barrier elements.

The descriptions in Table 4.5 are not exhaustive. For example, SR 6.2 Continuous Monitoring only elaborates on intrusion detection. Only relevant functions and systems for a given facility need to be broken down into barrier elements (BE-T, BE-H, and BE-O). For instance, IPS may not be in use.

In greenfield projects, contractors/integrators can cover Step 4 during engineering. During project execution, barrier functions are established based on cybersecurity measures (requirements) by defining a barrier profile. Contractors then review all components of each system being engineered/installed, identifying applicable barrier functions/sub-functions from the barrier profile (same as is done today optimizing the requirements for each system based on system properties). Identifying technical barrier elements for each function and sub-function is a natural part of this process.

We assume all relevant barriers are covered by cybersecurity requirements in the selected standards or guidelines. However, any missing barriers identified during design or operation, using complementary approaches (see Section 4.1), should be added.

4.3.5 Step 5: Select barriers relevant for a specific facility

In this step, barriers relevant to a specific facility are identified and selected. A gap analysis is conducted between the barrier functions and elements defined in Step 4 and those currently designed or implemented at the facility. The main aim is to identify the existing barriers. Additionally, the gap analysis can identify missing barriers.

Justification/comments

While many cybersecurity barriers may be relevant for various facilities, their applicability to the specific facility must be ensured. Requirements for a given cybersecurity barrier can differ between facilities, areas/zones, and down to individual equipment/components (cf. Step 7). If a requirement is defined as a barrier requirement, it must be specified which areas, systems, zones, components, or component types are relevant or exempt from being barrier elements for that requirement.

Example/elaboration

The selected barriers can be described in a barrier strategy (BS). Together with the performance standard (PS) from Step 7, this can be integrated with safety barrier management, as illustrated in Figure 4.2. (See [5] for typical contents of BS and PS).

4.3.6 Step 6: Add verifiable performance requirements to the barriers

Verifiable performance requirements for the barriers are added, considering that such requirements may be missing in standards/guidelines. A performance requirement is a 'verifiable requirement for the properties of the barrier elements in order to ensure the barrier is effective' (PSA, 2017) [10].

Justification/comments

Standards and guidelines often require having a cybersecurity measure in place, while performance requirements per MR § 5 pertain to how well barriers (usually barrier elements) should perform regarding properties like functionality, integrity, and robustness (PSA, 2017) [10]. If performance requirements are included in the chosen standard/guideline, they are added directly. If missing or insufficient, they must be developed and added. This is indicated as Step 6A in Figure 4.2, a subprocess that includes using PIFs to establish indirect performance requirements in addition to direct ones.

Example/elaboration

Table 4.6, continuing from Step 4 (Tables 4.4 and 4.5), illustrates adding verifiable performance requirements. It provides examples of performance requirements (PR) for each barrier element (BE) across the three categories (T-H-O). Alternatively, performance requirements can apply to barrier functions (BF) or barrier sub-functions (BSF), as shown in the first PR column. PIFs (e.g., competence) can also serve as indirect performance requirements (e.g., competence requirements, cf. the PR BE-H column).

Table 4.6 Examples of barrier performance requirements (from IEC 62443-3-3) [27]

IEC 62443-3-3 Requirements		Barrier functions and subfunctions		Barrier elements			Performance Requirements			
Req. ID	**Requirement title**	**Barrier function(BF)**	**Barrier sub-function (BSF)**	**Barrier element (BE) - Technical**	**Barrier element (BE) - Human**	**Barrier element (BE) - Operational**	**PR BF/BSF**	**PR BE-T**	**PR BE-H**	**PR BE-O**
SR 6.2	Continuous monitoring	Detect, characterize and report security breaches in a timely manner	Intrusion detection Intrusion prevention Malware protection Network monitoring Event management	IDS IPS Malware prot. m. Network mon. m. SIEM	IDS operator	Detect, characterize and report	Response time	Coverage of IDS Frequency of updating	Competence req. of IDS operator	Response time
SR 7.3	Control system backup	Conducting back-ups	Capturing required files	Back-up mechanisms	Back-up responsible	Taking back-up (manually)	Frequency of manual back-up	(RE 1)	Proportion of manual back-up Competence	Correctness of manual back-up
SR 7.3 RE 1	Backup verification	Not relevant (NR)	NR	NR	NR	NR	NR	Reliability of back-up mechanisms	NR	NR
SR 7.3 RE 2	Backup automation	Not relevant (NR)	Automation of back-up function	Automatic back-up	NR	NR	Frequency of automatic back-up	Frequency of automatic back-up	NR	NR

4.3.7 Step 7: Adapt performance requirements to the specific facility/zones

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

Justification/comments

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

Example/elaboration

As shown in Table 4.4, SL 1 is achievable with SR 7.3, SL 2 is achievable with SR 7.3 RE 1 (+ SR 7.3), and SL 3 is achievable with SR 7.3 RE 2 (+ SR 7.3 and SR 7.3 RE 1). Thus, the SL-T of a given zone determines which performance requirements to fulfil. The performance requirements are compiled in a performance standard (PS). Together with the barrier strategy (BS) from Step 5, this can be integrated with safety barrier management, as illustrated in Figure 4.2. Security level is further elaborated in Section 5.2.

For risk assessment and determining SL-T, we refer to IEC 62443-3-2 [30] [30] and DNV-RP-G108 [31]. Additionally, the adaptation of the IEC 62443 methodology to greenfield projects in the petroleum industry is discussed by Gratte (2020) [32].

4.3.8 Step 8: Fulfil the barrier performance requirements (comply with MR § 5)

This step involves ensuring that the barrier performance requirements identified in Step 7 are met, in accordance with MR § 5 Barriers [8]. It is an ongoing process that requires regular checks and verification to confirm that the performance requirements continue to be satisfied.

Justification/comments

This step is essential for effective cybersecurity barrier management during operation. The required performance must be regularly checked and verified to ensure compliance with MR § 5 Barriers. Furthermore, the barriers must be continuously monitored to detect any impairments that could compromise their proper functioning.

Example/elaboration

To verify a barrier performance requirement, both the requirement itself and its method of measurement must be operationalized. As outlined in Section 4.2.6, performance requirements can be either direct or indirect, the latter being assessed through Performance Influencing Factors (PIFs). Table 4.7 provides a simplified example for technical barrier elements (BE-T), continuing from Table 4.6. A similar verification approach applies to non-technical barrier elements.

Table 4.7 Examples of direct and indirect verification of barrier performance requirements

IEC 62443-3-3 Requirements		Barrier functions and subfunctions		Barrier elements	Performance Requirements		Verification	PIF	IPR	Verification
Req. ID	Requirement title	Barrier function(BF)	Barrier sub-function (BSF)	Barrier element (BE) - Technical	PR BF/BSF	PR BE-T	DPR BE-T	PIF BE-T	IPR BE-T	IPR BE-T
SR 6.2	Continuous monitoring	Detect, characterize and report security breaches in a timely manner	Intrusion detection Intrusion prevention Malware protection Network monitoring Event management	IDS IPS Malware prot. m. Network mon. m. SIEM	Response time	Coverage of IDS Frequency of updating	Verify coverage Verify frequency	Maintenance	Maintenance performance requirement (e.g., backlog)	Verify maintenance performance (e.g., backlog)
SR 7.3	Control system backup	Conducting back-ups	Capturing required files	Back-up mechanisms	Frequency of manual back-up	(RE 1)	(RE 1)	Maintenance	Maintenance performance requirement (e.g., backlog)	Verify maintenance performance (e.g., backlog)
SR 7.3 RE 1	Backup verification	Not relevant (NR)	NR	NR	NR	Reliability of back-up	Verify reliability	NR	NR	NR
SR 7.3 RE 2	Backup automation	Not relevant (NR)	Automation of back-up function	Automatic back-up	Frequency of automatic back-up	Frequency of automatic back-up	Verify frequency	Maintenance	Maintenance performance requirement (e.g., backlog)	Verify maintenance performance (e.g., backlog)

Table 4.7 presents the verification of direct (DPR) and indirect (IPR) performance requirements for technical barrier elements (BE-T). Indirect methods (IPRs) provide alternative verification approaches when direct methods (DPRs) are impractical or not feasible. The table includes selected examples of performance requirements and corresponding verification activities. Further details are provided in the subsequent text.

For SR 7.3, the technical barrier element is *backup mechanisms*, with the direct performance requirement being their reliability, as defined in SR 7.3 RE 1. Additional requirements—such as AVAIL 2.3 from IEC 62443-2-1—mandate the implementation of policies to verify the integrity of backup data immediately after, and at regular intervals following, the backup process.

As with all performance requirements, this must be clearly specified and operationalized. Key questions include: What constitutes integrity verification? How frequently should it be performed? And what defines acceptable performance?

Supplemental guidance to AVAIL 2.3 clarifies that *integrity* refers to the backup's ability to restore the system. If test restorations are not feasible, alternative methods—such as software validation, log reviews, or other integrity checks—should be employed to confirm data health and detect any corruption over time. Ultimately, verifying backup integrity involves ensuring that the backup is both successfully completed and capable of restoring the system. The specific operational approach depends on the available tools and chosen solutions, which may vary in terms of thoroughness.

A backup verification strategy may include the activities outlined in Table 4.8. However, these activities are context-specific and should be tailored to the company's particular needs, including both the type of activities and their execution frequency. Furthermore, what constitutes acceptable outcomes from these activities must be clearly defined—specifically in terms of the performance of the backup mechanisms.

Barrier status follow-up is categorized into short-term, medium-term, and long-term monitoring. In Table 4.8, the frequency range of "weekly – monthly" corresponds to medium-term follow-up, while "yearly" reflects long-term monitoring. These approximate timeframes are associated with the verification of performance requirements.

In addition, short-term follow-up involves day-to-day monitoring of non-functioning or impaired barriers—for example, through the use of a barrier panel.

Table 4.8 Example of control system backup verification strategy

No	Name	Description of activities	Frequency
1	Automate Backup Verification	Implement automated scripts or tools to regularly verify the backups. These tools can check for successful completion, integrity, and availability of the backup files [1)]	Weekly - monthly
2	Check Backup Logs	Review the backup logs to ensure that backups are being performed as scheduled and without errors. Look for any warnings or failures that might indicate issues [1)]	Weekly - monthly
3	Monitor Backup Storage	Ensure that the backup storage location has sufficient space and is secure. Regularly check for any issues that might affect the availability or integrity of the backup data [2)]	Weekly - monthly
4	Validate Backup Integrity	Use checksum or hash verification methods to check the integrity of the backup files. This verifies that no random errors have been introduced in the stored backup [1)]	Weekly - monthly
5	Perform Test Restorations	Perform test restorations of the backup data, regularly and after software updates, to verify that the data can be successfully restored. This helps ensure that the backup files are not corrupted and that the restoration process works as expected [2)]	Weekly – monthly (Yearly)
6	Document and Test Backup Procedures	Maintain detailed documentation of the backup procedures and test them (by following the procedures step-by-step) periodically. Ensure that the procedures are up-to-date and aligned with best practices [2)]	Yearly

1) https://www.acronis.com/en-us/blog/posts/best-practices-for-verifying-and-validating-your-backups/
2) https://csf.tools/reference/nist-sp-800-53/r4/cp/cp-9/

Each activity should be clearly operationalized to support the follow-up of the backup barrier function. This includes specifying the exact frequency of execution and defining the criteria for what constitutes a successful outcome.

Considering the performance requirement of *"reliability of backup mechanisms"* and its verification through testing, as outlined in Table 4.7 and discussed above, most of the activities listed in Table 4.8—excluding activity 6—are relevant.

For example, consider activity 2: *"check backup logs."* Assume that log files are reviewed biweekly for errors. Further, suppose a performance requirement of 90% reliability, meaning that no more than one out of ten log files may contain errors for the criterion to be met. This simplified example of how to operationalize the verification of a performance requirement is illustrated in Table 4.9.

Table 4.9 Example of operationalizing backup performance verification

Context – frequency of back-up	Daily
Direct performance requirement	90% reliability
Verification	Reviewing 10 log files from last two weeks
Rules (status)	0-1 log files with errors: Green
	2-3 log files with errors: Yellow
	4-10 log files with errors: Red

Verification methods may vary and can include traffic light systems, character scales, pass/fail criteria, and others. This example focuses on technical barrier elements (BE-T); however, similar verification approaches are applicable to human (BE-H) and operational (BE-O) barrier elements.

Chapter 5 provides details on the status of BE-T, while the non-technical barrier report [2] addresses non-technical barriers. The barrier handling report [3] focuses on the ongoing follow-up of barrier status, threats, and vulnerabilities. Follow-up on barrier impairments is typically frequent and classified as short-term. In contrast, the follow-up of Operational Security Level (SL-O) is generally considered medium-term.

Verification activity 5, *"perform test restorations,"* can be considered the true *"proof of the pudding."* Unlike other verification activities, which do not guarantee restorability, only actual test restorations can provide direct confirmation that a backup is capable of restoring the system.

This type of test is comprehensive and is typically conducted only once or twice a year. It can be compared to the testing of critical safety components such as gas detectors or shutdown valves, where backlogs in testing—part of preventive maintenance—serve as input to assessing short-term status. A backlog increases uncertainty regarding whether the barrier will function as intended when needed. This topic will be revisited in Chapter 5.

4.3.9 Step 9: Fulfil all cybersecurity requirements (comply with FR § 34a)

This step involves fulfilling all applicable requirements chosen by the asset owner to comply with FR § 34a [11], as outlined in the cybersecurity standards or guidelines from Step 1. This is a continuous process, with regular checks to ensure compliance.

Justification/comments

This process is part of general cybersecurity management, not limited to barriers. Fulfilling all cybersecurity requirements entails that classifying a measure as a non-barrier in Step 2 is not critical.

Example/elaboration

Fulfilment of cybersecurity requirements should be checked at intervals set by the asset owner. Some requirements pertain to stable cybersecurity measures, while others depend on how they are defined as performance requirements. The latter requires more frequent follow-up.

5 Monitoring and follow-up of cybersecurity barriers

The previous chapter focused on the identification of cybersecurity barriers and the associated performance requirements. It addressed the key question: *How can barriers and their elements be identified?* Additionally, it offered guidance on how to develop, implement, and verify cybersecurity barrier requirements.

In this chapter, we further examine the verification of these requirements while also exploring the following questions: *How can the status of cybersecurity barriers be assessed?* and *How can the security levels of cybersecurity systems and components be verified?*

The identified cybersecurity barriers and their corresponding performance requirements are typically documented in a *barrier strategy* and a *performance standard*, as illustrated in Figure 5.1. The figure also highlights the need to follow up on these barriers and requirements during operation—specifically, by monitoring the status of the barriers and verifying that their performance requirements are being met.

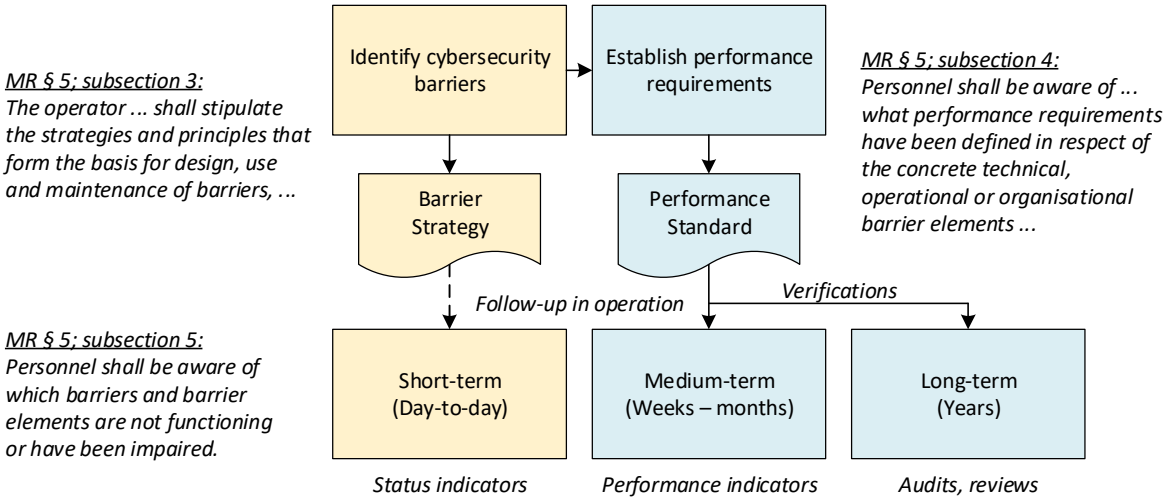

Figure 5.1 Monitoring and follow-up of cybersecurity barriers and performance requirements

The identification of cybersecurity barriers is mandated by MR § 5, subsection 3 (see also Chapter 2), while the establishment of performance requirements is required under MR § 5, subsection 4. Furthermore, providing the status of these barriers is stipulated in MR § 5, subsection 5. Verification of performance requirements, although not explicitly stated, is considered an implicit regulatory expectation.

The barriers and barrier elements included in the status overview are derived from the *barrier strategy*, whereas the performance requirements subject to verification are documented in the *performance standard*.

The barrier status should indicate non-functioning or impaired barriers—both functions and elements—in real time, i.e., reflecting the situation *now*. This is referred to as *short-term follow-up*. In contrast, verification of performance requirements is typically conducted at regular intervals over time—for example, through indicators, audits and reviews—and is categorized as *medium-term* (weeks to months) or *long-term* (years) follow-up. Each of these categories is described in the following sections.

It is important to note that *medium-term* and *long-term* follow-up are also referred to as assessments of barrier status, specifically addressing the extent to which the required performance of the barriers is being fulfilled (or not). Furthermore, since the methodology outlined in Chapter 4 includes non-barrier

cybersecurity measures (steps 1 and 9), follow-up in operation may encompass both cybersecurity barriers and general cybersecurity practices, the latter in order to fulfil FR § 34a.

This chapter includes industry practices for safety barrier management, some of which are also applied to cybersecurity barrier management.

5.1 Short-term status of cybersecurity and cybersecurity barriers

5.1.1 Barrier status panel

Providing the status of cybersecurity barriers is mandated by MR § 5, subsection 5, which states: *"Personnel shall be aware of which barriers and barrier elements are not functioning or have been impaired."* In this context, *not functioning* can be interpreted as a complete loss of function, whereas *impairment* refers to any condition between full functionality and total failure.

The regulatory requirements do not specify how personnel should be made aware of the status of cybersecurity barriers. However, in safety barrier management, a commonly used approach is to present the status via a *barrier panel*, which typically employs a *traffic light system* to visually indicate the condition of each barrier. An example of such a barrier panel is provided in Figure 5.2.

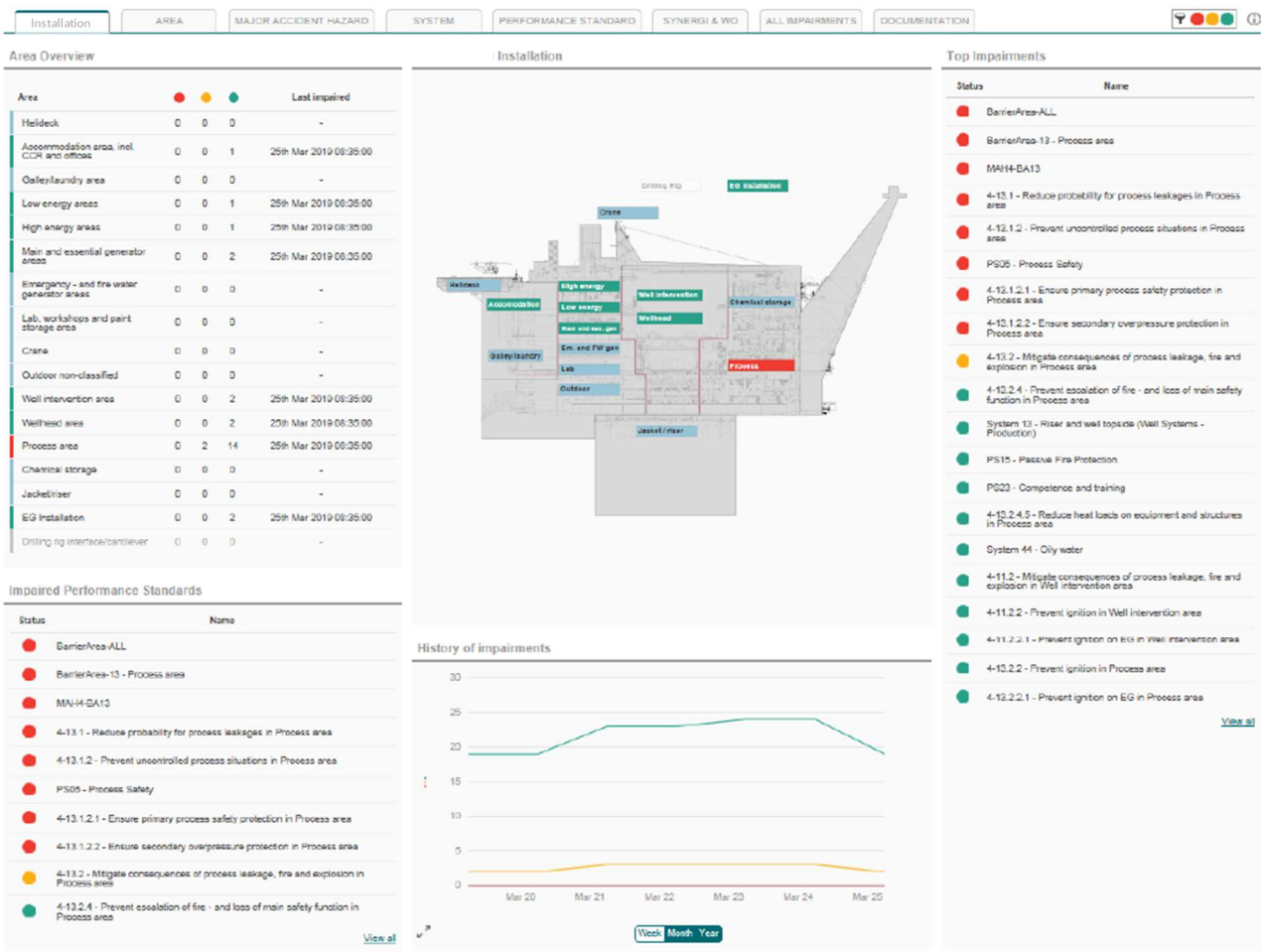

Figure 5.2 Example of barrier panel (front page)

In this example, technical barrier elements are designated as *Safety Critical Elements (SCEs)* within the maintenance system. Each SCE is assigned a specific tag, and there is an established link between the

maintenance system and the corresponding *performance standards*, where the required maintenance program for each SCE is referenced. This linkage ensures that maintenance requirements are clearly defined and traceable for each individual tag.

The status displayed in the barrier panel is derived from information automatically collected from two primary sources: the incident reporting system—which captures non-conformances—and the maintenance system, which tracks overdue preventive and corrective maintenance work orders. In addition to this automated input, manual updates to the barrier status can also be performed directly within the panel.

Status information is aggregated hierarchically, starting at the tag level and rolling up through barrier elements and functions to the area level. This structure allows users to both view a high-level status overview and drill down from the area level to individual tags for more detailed insights.

Initially, the barrier status was presented with a certain delay—i.e., not in real time. This delayed view is now referred to as the *default view*. In contrast, a new *real-time view* has been developed, although access to this version is restricted. Other companies and facilities, however, rely solely on real-time status displays.

Differences also exist in terms of the types of information included in the barrier panel. For instance, the facility shown in Figure 5.2 does not display information related to isolations (i.e., overrides or disconnections) of safety functions, whereas some other facilities do include this type of data.

It is important to note that all relevant status information is available across various source systems, regardless of whether it is compiled in the barrier panel. While the panel may aggregate some or all of this dispersed information, it can still be argued that impairment information is accessible within the individual systems—even if it is not centralized in a single interface.

The facility shown in Figure 5.2 has also integrated cybersecurity barriers into the barrier panel, albeit with certain adaptations compared to the treatment of safety barriers. This inclusion raises an important question: *Which personnel should be granted access to cybersecurity barrier status information?*

While information regarding impaired safety barriers is generally not considered confidential, the situation is markedly different for cybersecurity barriers. Due to the sensitive nature of cybersecurity, access to the barrier panel—or specifically to the *cybersecurity view*—should be restricted to personnel with a legitimate *need to know*. This approach ensures that critical cybersecurity status information is protected from unauthorized disclosure.

5.1.2 Barrier impairments and vulnerabilities

Important terms, definitions and relationships

A *barrier impairment* refers to a condition in which a barrier is partially or completely non-functioning. In safety barrier management, this concept aligns with varying degrees of failure, commonly classified into three categories: *critical*, *degraded*, and *incipient* failures. These categories are typically used in failure reports recorded in the maintenance system.

While the terms *failure*, *hazard*, and *accident* are standard within the safety domain, the cybersecurity domain more frequently uses terms such as *vulnerability*, *threat*, and *cyberattack*. Figure 5.3 illustrates the relationships among these cybersecurity-related terms, based on ontological work from the ISA/IEC 62443 series developed by the ISA 99 committee [33].

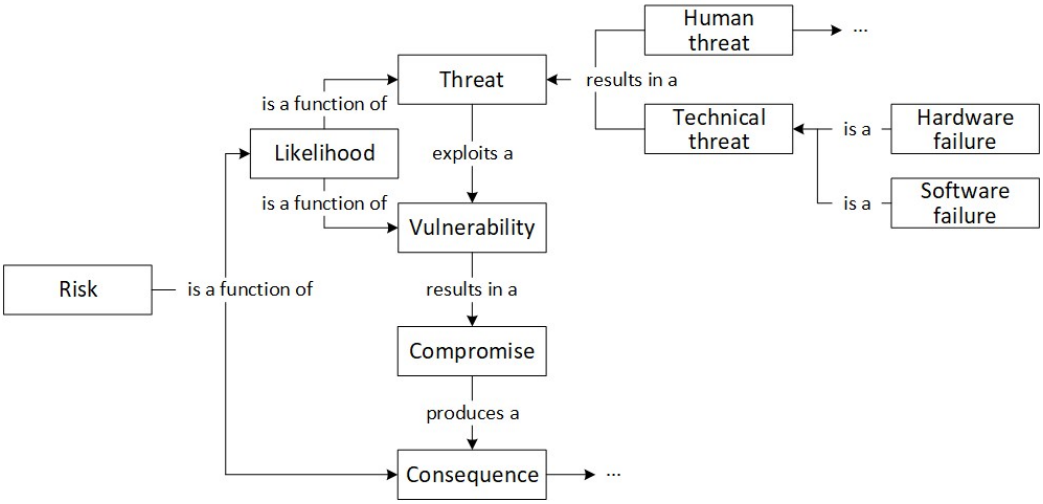

Figure 5.3 Ontology diagram of risk (adapted from [33])

Figure 5.3 illustrates the logical relationship in which a *threat* exploits a *vulnerability*, resulting in a *compromise* that produces a *consequence*. These concepts are foundational in cybersecurity risk assessment and are aligned with the ISA/IEC 62443 ontological framework.

A *threat* is defined by [28] as a *"circumstance or event with the potential to adversely affect operations (including mission, functions, image, or reputation), assets, control systems, or individuals via unauthorized access, destruction, disclosure, modification of data, and/or denial of service."* Although the definition does not explicitly reference "failure," both hardware and software failures are included in the ISA ontology as examples of *technical threats*.

A *vulnerability* is defined by [28] as a *"flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy."* The phrase "flaw or weakness" closely parallels the concept of *failures* in safety terminology, bridging the conceptual gap between safety and cybersecurity disciplines.

Finally, a *compromise* is defined as the *"unauthorized disclosure, modification, substitution, or use of information (including plaintext cryptographic keys and other critical security parameters)."* [28]

Furthermore, IEC 63069 [22] emphasizes that *"vulnerabilities should not be considered as a fault, failure or error, as defined in IEC 61508, as their origin and nature is different. Vulnerabilities should be considered as a flaw or weakness on the technologies, processes and procedures or people, as defined in IEC 62443,"* and ISA-TR.84.00.09 [23] states that *"threats exploiting vulnerabilities lead to failure."* This interpretation suggests a conceptual alignment with the model presented in Figure 5.3, where the term *compromise*—resulting from a threat exploiting a vulnerability—can be understood as analogous to *failure* in traditional safety terminology.

Although the functional safety domain explicitly defines the terms *fault*, *failure*, and *error*, and the cybersecurity domain occasionally refers to *failure* (as discussed above), it is important to note that IEC 62443 does not formally define these terms—nor does it define *flaw* or *weakness*.

Therefore, when referring to *failure* in the context of cybersecurity—such as *hardware* or *software failure*—it is advisable to adopt the same or a closely aligned definition as used in the functional safety domain. This

approach supports consistency and facilitates the integration of functional safety and cybersecurity frameworks. Refer to Appendix A for the relevant definitions.

Failures, impairments and vulnerabilities

Cybersecurity barrier failures—whether categorized as part of a *threat* or as a *compromise*—can be addressed similarly to *barrier impairments* in traditional safety barrier management. However, this raises an important question regarding *vulnerabilities*. According to ISA-TR.84.00.09, vulnerabilities can lead to failure when exploited by a threat.

Given this, how should vulnerabilities be treated when assessing and reporting the status of cybersecurity barriers? Should they be considered impairments by default, or only when specific conditions are met—such as known previous exploits, a high CVE score, or high severity through some other metric?

Figure 5.4 provides a conceptual foundation for exploring these questions and offers guidance on how vulnerabilities might be represented within a barrier status framework.

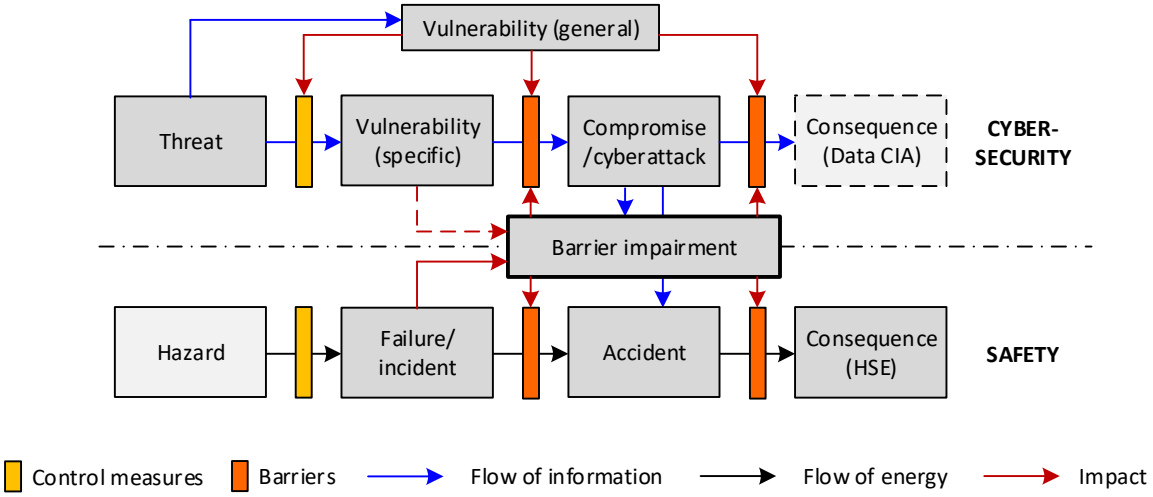

Figure 5.4 Relationship between barrier impairments and vulnerabilities

Cybersecurity focuses on controlling the *flow of information*, while safety is concerned with controlling the *flow of energy*. Under normal operational conditions, control is maintained through *control measures*. However, when an abnormal situation arises, *barriers* are required to either regain control or mitigate the consequences.

It is therefore essential to ensure that these barriers are functioning as intended when needed, and that any *impairments*—whether resulting from unintentional failures or intentional compromise—are clearly identified and communicated. Barrier impairment constitutes critical information for the effective management of both cybersecurity and safety barriers, as it directly impacts the ability to maintain system integrity and resilience under stress.

Figure 5.4 also highlights a primary concern related to *safety consequences*—specifically, the potential for a cyberattack to result in an accident with impacts on *health, safety, and the environment (HSE)*. Such outcomes typically require the compromise of both the *control system* and the associated *barriers*, often through one or more *barrier impairments*.

The specific *consequence classes* to be considered in such scenarios are determined during the *risk and barrier assessment* process, which evaluates the potential impacts and defines the scope of protection needed.

Specific and general vulnerabilities

We distinguish between two types of *vulnerability*: *specific* and *general*.

A *specific vulnerability* refers to a clearly identified weakness, typically documented in the form of a *CVE* (Common Vulnerabilities and Exposures). CVE is a standardized system for cataloguing publicly known security vulnerabilities in software and hardware. Each CVE entry is assigned a unique identifier (e.g., *CVE-2025-12345*) and includes a concise description of the vulnerability. The CVE system is managed by the MITRE Corporation in collaboration with the *National Vulnerability Database (NVD)*. Specific vulnerabilities are generally technical in nature, originating in software or hardware cyber assets—which themselves may function as cybersecurity *measures* or *barriers*.

In contrast, a *general vulnerability* is defined as any exploitable flaw or weakness associated with people, processes, design, or technology. This aligns with the broader definition of vulnerability provided in *IEC 62443*. General vulnerabilities often arise from *missing* or *deficient cybersecurity measures*, including inadequate or absent barriers, and may not be tied to a single asset or CVE.

In addition to distinguishing between *specific* and *general* vulnerabilities, we can also differentiate between the processes used to handle them.

The management of *specific vulnerabilities*, such as CVEs, is a continuous process known as *vulnerability management*. This process relies on information from third-party sources, including *external threat intelligence*, and typically involves *patching* as the primary mitigation strategy. Vulnerability management is further discussed in the third summary report on handling barriers [3].

In contrast, the handling of *general vulnerabilities* involves identifying the need to *improve existing cybersecurity measures or barriers*, or to *implement new ones*. Modifications—rather than patching—are the usual remedy. General vulnerabilities are typically identified through *regular audits and inspections* carried out by the operator, making this process especially relevant for *medium-term* and *long-term* follow-up of barriers.

If *specific vulnerabilities* are to be reflected in the *barrier status*, it would be most relevant to include them in the *short-term follow-up*, alongside traditional *barrier impairments*. In such cases, a distinction could be made between *CVEs with known exploits* and those *without known exploits*[12], as this impacts the urgency and severity of potential threats.

However, since specific vulnerabilities are typically handled through the established *vulnerability management process*, several industry partners recommend not including them in the barrier status panel, as the approach for doing so is not straightforward. Including them might introduce “noise” into the panel, since a given CVE may not be exploitable or may only be relevant for certain configurations of a barrier element.

[12] Some CVEs are known to have been actively exploited in the wild. These are often tracked in databases like the Known Exploited Vulnerabilities Catalogue maintained by CISA (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

A counterargument is that if such CVEs are first assessed for relevance, it may be reasonable to include them in the barrier panel—potentially together with the planned patch date, if applicable. This is particularly relevant for CVEs with known exploits or for those that are both applicable and critical.

In general, it is advisable not to make a barrier panel too complex, at least as a starting point. This approach is illustrated by a *dashed arrow* in Figure 5.4, indicating an optional rather than standard practice.

Ultimately, the decision rests with each company. The inclusion of CVEs in the barrier status may be reconsidered based on the specific operational context and risk posture.

5.1.3 Example: Intrusion Detection System (IDS)

IDS impairments and vulnerabilities

This section is primarily based on an internal working memo [34], where an Intrusion Detection System (IDS) was used as a case study for assessing barrier status. The work included an in-depth analysis of the relationships between barrier impairments and vulnerabilities associated with IDS. Further details can be found in the referenced working memo.

An *Intrusion Detection System (IDS)* is a cybersecurity tool designed to monitor network or system activity for malicious actions or policy violations. It analyses traffic and logs to detect unauthorized access, abnormal behaviour, or known attack patterns. When suspicious activity is identified, the IDS alerts system administrators so they can investigate and respond appropriately. There are two main types:

1. Network-based IDS (NIDS): Monitors network traffic for signs of attacks or abnormal behaviour.
2. Host-based IDS (HIDS): Runs on individual devices to monitor local activities such as file access and system calls.

IDS can be either *signature-based* (detecting known threats by pattern matching) or *anomaly-based* (flagging deviations from normal behaviour). Unlike Intrusion Prevention Systems (IPS), IDS do not block threats—only detects and reports them.

An analysis of 32 CVEs related to IDS, combined with a comparison to impairment failure modes (i.e., categories of IDS impairment failures), showed that most vulnerabilities could lead to impairments if exploited. In this sense, specific vulnerabilities (CVEs) could be incorporated into the monitoring of IDS status. However, as stated above, specific vulnerabilities will be addressed through the vulnerability management process, addressed in the Barrier Handling Report [3], where e.g., relevance, exposure, and criticality of the barrier elements are considered. The industry partners currently recommend not including specific vulnerabilities in short-term follow-up activities, such as monitoring through a barrier panel.

Overall verification of correct functioning

Similar to the backup verification strategy presented in Table 4.8 (Section 4.3.8), the proper functioning of an Intrusion Detection System (IDS) can be verified through an IDS verification strategy.

An IDS verification strategy may include the activities outlined in Table 5.1. However, as with the backup verification strategy, these activities are context-specific and should be tailored to the company's particular needs, both in terms of the types of activities and their execution frequency. Additionally, acceptable outcomes for these activities must be clearly defined—particularly regarding the performance standards expected of the IDS.

By performing these activities, organizations can help ensure that the IDS is operating correctly and providing reliable protection against potential threats.

As a reminder, we categorize barrier status follow-up into three timeframes: short-term, medium-term, and long-term monitoring. In Table 5.1, the frequency range of *"weekly – monthly"* corresponds to *medium-term* follow-up, while *"yearly"* indicates *long-term* monitoring. These indicative timeframes are linked to the verification of performance requirements, which are further discussed in Sections 5.2 and 5.3.

Table 5.1 Example of IDS verification strategy

No	Name	Description of activities	Frequency
1	Check System Logs	Review the IDS logs to ensure it is actively monitoring and recording events. Look for entries that indicate the IDS is detecting and logging suspicious activities [1)]	Weekly - monthly
2	Monitor Performance Metrics	Track performance metrics such as the number of alerts generated, false positive rates, and response times. Anomalies in these metrics can indicate issues with the IDS [2)]	Weekly – monthly (Daily)
3	Generate Test Alerts	Use tools like Metasploit or custom scripts to simulate attacks and verify that the IDS generates alerts for these activities. This helps confirm that the IDS is correctly identifying potential threats [2)]	Weekly - monthly
4	Review Configuration Settings	Ensure that the IDS is properly configured with the correct rules and signatures. Misconfigurations can lead to missed detections or false positives [3)]	Weekly - monthly
5	Update Signatures and Rules	Regularly update the IDS with the latest signatures and rules to ensure it can detect new and emerging threats [3)]	Weekly - monthly
6	Conduct Regular Audits	Perform periodic audits of the IDS to verify its effectiveness and identify any gaps in coverage. This can include reviewing detection capabilities and ensuring all network segments are monitored [1)]	Yearly
7	Use External Validation	Engage third-party security experts to conduct penetration testing and validate the IDS's effectiveness. This provides an independent assessment of the system's performance [3)]	Yearly

1) https://storables.com/home-security-and-surveillance/how-to-test-intrusion-detection-system/
2) https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf
3) https://wpgc.io/blog/intrusion-detection-systems-the-complete-guide/

In contrast, *short-term follow-up* refers to the day-to-day monitoring of non-functioning or impaired barriers—for example, through the use of a barrier panel. This section primarily focuses on short-term follow-up.

IDS status follow-up

An Intrusion Detection System (IDS) is one of the tools and techniques that can be used to fulfil the requirement *SR 6.2 "Continuous Monitoring"* in IEC 62443-3-3 (cf. Section 4.3.4 above). Examples of relevant performance requirements for the technical barrier elements—and the overall barrier function—were presented in Table 4.7. These include *response time*, *coverage of the IDS*, and the *frequency of updating*.

When compared to the activities outlined in Table 5.1:

- *Response time* is addressed in activity no. 2,
- *Frequency of updating* is addressed in activities no. 4 and 5, and
- *Coverage of the IDS* is addressed in activity no. 6.

All of these aspects are associated with *medium- or long-term follow-up* (with the exception of activity no. 2 which may be performed more frequently).

In addition, and similar to the backup verification activity *perform test restorations* (cf. Table 4.8), the IDS verification activity no. 3, *generate test alerts*, can utilize a backlog of maintenance or testing tasks as an indirect performance requirement. A testing backlog can then serve as an input for assessing the short-term status of the IDS.

This concept can be generalized to include IDS, backup systems, and other relevant cybersecurity barrier elements. A broader outline of this approach, structured similarly to established practices in safety barrier management, is provided in the next section.

5.1.4 Generalization

The day-to-day, or short-term, status of barrier functions and elements is based on information that verifies or indicates the current functioning of those functions and elements—that is, the degree to which the barriers are impaired. A common tool used for this purpose in safety barrier management is the *barrier panel*, as illustrated in Figure 5.2. This specific barrier panel has also been applied to cybersecurity barriers, as described above.

Barrier panels typically employ a *traffic light system*, where:

- *Red* indicates a critical functional failure,
- *Yellow* indicates a degraded condition, and
- *Green* indicates normal functioning.

Examples of status indicators—conditions or impairments—corresponding to red, yellow or green status of a barrier tag are provided in Table 5.2.

Table 5.2 Example of status rule set

Rule set – technical cybersecurity tags	Signal	Source
The following conditions give a **RED** status light on a barrier tag		
If tag bypassed or inhibited	INH	SAS
If health status alarm	HSA	SAS
If Pri1 PM overdue > 90 days or ½ of PM interval	PM-C	CMMS
If Pri1 CM notification, or work order open	CM-C	CMMS
If non-conformance	NC	Synergi
If known CVE has been exploited and not patched	CVE-E	CISA
The following conditions give a **YELLOW** status light on a barrier tag		
If Pri1 PM is overdue	PM	CMMS
If Pri2 CM notification, or work order open, are overdue	CM	CMMS
If known CVE has not been patched	CVE	MITRE
If none of the above, the tag shows as **GREEN** in the barrier panel		

Information that indicates a critical functional failure—giving a red status light on the barrier panel—includes:

- *Bypassed or inhibited (INH) barrier tags* provided by the Safety and Automation System (SAS). These represent functional failures, not necessarily physical failures.
- *Health Status Alarms (HSA)* associated with barrier tags, as reported by SAS.

- *Preventive Maintenance* issues, specifically overdue PM for high-priority (Priority 1, critical) barrier failures *(PM-C)*. Overdue is here defined as more than 90 days past due or exceeding half the PM interval. This information is typically provided by a Computerized Maintenance Management System (CMMS), e.g., SAP or an equivalent maintenance system.
- *Corrective Maintenance notifications or open work orders* related to high-priority (Priority 1, critical) barrier failures *(CM-C)*. Also provided by a CMMS.
- *Non-Conformances (NC)* linked to barrier tags, as reported by Synergi or another incident/deviation reporting system.
- *Common Vulnerabilities and Exposures - Exploited (CVE-E)* that remain unpatched, as identified in the CISA database.

Information that indicates a degraded functional failure—giving a yellow status light on the barrier panel—includes:

- *Preventive Maintenance (PM)* issues, specifically overdue PM for high-priority (Priority 1, critical) barrier failures. This information is typically provided by a CMMS.
- *Corrective Maintenance (CM) notifications or open work orders* related to medium-priority (Priority 2, degraded) barrier failures are overdue. Also provided by a CMMS.
- *Common Vulnerabilities and Exposures (CVE)* that remain unpatched, as identified in the MITRE database.

Note that status indicators (signals) may overlap; for example, a PM-C or CM-C may also be registered as an NC. Conversely, some status indicators may not be relevant for certain barrier elements or tags.

There are different practices regarding both the number of status indicators used and the associated rule sets. Often, status indicators only cover PM and CM, meaning that information is captured solely from the maintenance system.

Differences also exist concerning when an impairment status is visualized in the barrier panel. An impairment may be visualized as red or yellow immediately after a failure notification is reported, or it may only appear after the notification (or associated work order) has been assessed and quality assured — or even after compensating measures have been considered.

In some practices, status indicators are primarily based on NC information, i.e., data from the incident or deviation reporting system. In these cases, PM or CM tasks may become overdue before a red or yellow status is shown in the barrier panel. As a result, there is a delay between the occurrence of the impairment and its presentation in the barrier panel.

Additionally, there are rules for adjusting the status during barrier impairment handling (cf. the barrier handling report [3]) and rules or algorithms for aggregating status from the barrier tag level up to the area and facility levels.

Using the same practices for cybersecurity barrier management as for safety barrier management will facilitate the integration between cybersecurity and safety barrier management (cf. Chapter 6).

5.2 Medium-term status of cybersecurity and cybersecurity barriers

In this section, we examine the verification of the status of cybersecurity barriers on a weekly to monthly basis. We will focus particularly on the question: *How can the security levels of cybersecurity systems and*

components be verified? This is closely linked to the IEC 62443 concept of security levels and the follow-up of the Operational Security Level (SL-O).

Before addressing this question, we will introduce medium-term activities based on verification strategies, as previously discussed for backup and intrusion detection systems (IDS), along with an existing practice known as the Technical Integrity Management Program (TIMP).

It should be noted that none of these approaches are inherently limited to cybersecurity barriers. They apply to cybersecurity measures in general, unless there is a specific process for identifying and selecting cybersecurity barriers among the broader set of cybersecurity measures.

5.2.1 Medium-term verification activities

Tailored and operationalized cybersecurity verification activities should be readily available for medium-term follow-up, as discussed previously for backup mechanisms and intrusion detection systems (IDS). Relevant medium-term activities for verifying backup mechanisms and IDS are included as examples in Table 5.3. These activities should be complemented by other relevant cybersecurity barrier elements (or cybersecurity measures in general, depending on the defined scope).

Table 5.3 Examples of medium-term cybersecurity measure verification activities

No	Name	Description of activities
1. Backup mechanisms		
1.1	Automate Backup Verification	Implement automated scripts or tools to regularly verify the backups. These tools can check for successful completion, integrity, and availability of the backup files
1.2	Check Backup Logs	Review the backup logs to ensure that backups are being performed as scheduled and without errors. Look for any warnings or failures that might indicate issues
1.3	Monitor Backup Storage	Ensure that the backup storage location has sufficient space and is secure. Regularly check for any issues that might affect the availability or integrity of the backup data
1.4	Validate Backup Integrity	Use checksum or hash verification methods to check the integrity of the backup files. This verifies that no random errors have been introduced in the stored backup
1.5	Perform Test Restorations	Perform test restorations of the backup data, regularly and after software updates, to verify that the data can be successfully restored. This helps ensure that the backup files are not corrupted and that the restoration process works as expected
2. Intrusion Detection System (IDS)		
2.1	Check System Logs	Review the IDS logs to ensure it is actively monitoring and recording events. Look for entries that indicate the IDS is detecting and logging suspicious activities
2.2	Monitor Performance Metrics	Track performance metrics such as the number of alerts generated, false positive rates, and response times. Anomalies in these metrics can indicate issues with the IDS
2.3	Generate Test Alerts	Use tools like Metasploit or custom scripts to simulate attacks and verify that the IDS generates alerts for these activities. This helps confirm that the IDS is correctly identifying potential threats
2.4	Review Configuration Settings	Ensure that the IDS is properly configured with the correct rules and signatures. Misconfigurations can lead to missed detections or false positives
2.5	Update Signatures and Rules	Regularly update the IDS with the latest signatures and rules to ensure it can detect new and emerging threats
Other cybersecurity (barrier) elements		
…	…	…

Tailored means that the barriers or measures should be relevant to the specific operator and facility, and that the verification frequency should also be appropriately adapted. As discussed regarding backup verification in Section 4.3.8, it may be more appropriate for certain activities, such as backup test restoration (activity 1.5 in Table 5.3), to be part of long-term (e.g., "yearly") follow-up instead.

Operationalized means that it must be clearly specified how the verification should be performed and what constitutes an acceptable outcome.

With reference to MR § 5, subsection 3 (abbreviated: “The operator … shall stipulate the strategies … that form the basis for … maintenance of barriers …”), the verification strategies could be included as part of the overall barrier strategy, either fully specified within the strategy itself or by referencing the maintenance management or other relevant systems. Alternatively, or additionally, such links could be provided from the performance standards.

5.2.2 Technical Integrity Management Program (TIMP)

For safety barrier management, TIMP utilizes relevant data and indicators related to technical barriers. This includes notifications from the maintenance system, backlogs of preventive maintenance (PM) and corrective maintenance (CM), test reports, inspection reports, incident reports, findings from Technical Condition Safety (TCS; abbreviated TTS in Norwegian), and dispensations.

These data points and indicators are collected and presented in the TIMP portal, where they are manually assessed by technical experts, such as system owners. Based on the status of the input data and the structured evaluations conducted by subject matter experts, barrier performance is assessed at the equipment, system, performance standard (PS), and plant levels.

The results—expressed as a score from B to E for each performance standard—are presented in a generic bow-tie diagram, as illustrated in Figure 5.5. A TIMP assessment for each performance standard is conducted every third month.

Figure 5.5 TIMP visualization of technical barrier status [5]

For cybersecurity, one company has introduced an additional performance standard (PS 23: Safety & Automation System Security), which is visualized together with the safety performance standards in the TIMP bow-tie diagram. PS 23 is added as a fifth performance standard within the Instrumented Safety Systems section of the TIMP bow-tie, positioned below PS 22.

The assessment of PS 23 follows a different approach compared to the other performance standards. The PS 23 TIMP evaluation focuses on the general condition of ICT equipment and does not consider failures of individual equipment (e.g., by checking statuses in the maintenance system). Nevertheless, the final result at the PS level is expressed as a character grade (B–E), consistent with the other performance standards, allowing PS 23 to be compared with, and receive the same focus as, the safety-related PSs.

The status assessment approach for PS 23 begins by dividing a given facility into its important systems. Each system is then assessed using a structured assessment template, organized according to the five NIST Cybersecurity Framework (CSF) functions: Identify, Protect, Detect, Respond, and Recover. Each system receives a character grade (B–E) for each of the five functions. These results are subsequently combined to calculate an overall score per system, which is then aggregated to determine the PS 23 performance score at the facility level.

Note also that some barrier panels used for short-term monitoring display a view similar to that shown in Figure 5.5 for barrier status at the PS level. This information is updated daily, but it is based solely on automatically harvested data and does not include any qualitative assessments, such as those provided in TIMP.

5.2.3 Operational Security Level (SL-O)

As described above, the question *"How can the security levels of cybersecurity systems and components be verified?"* is closely related to the IEC 62443 concept of Security Levels (SL) and the monitoring of Operational Security Level (SL-O). In other words, it must be ensured that the security levels achieved during operation (SL-O) are continuously maintained at the approved security levels that were established during design and implemented during construction: Implemented Security Level (SL-I). This approach is comparable to the concept of Safety Integrity Level (SIL) and the monitoring of "SIL in operation" as practiced within functional safety. SL-O and SL-I are new terms being introduced in [28], whereas Achieved Security Level (SL-A) is deprecated.

In addition, two related terms—Maturity Level (ML) and Security Protection Rating (SPR)—are relevant. The SPR is a function of both SL and ML, and these concepts are important for the evaluation of cybersecurity barriers.

Process for determining SL-I

SL-I is determined through a structured assessment and verification process that compares the system's implemented controls against the requirements for a predefined Target Security Level (SL-T). This ensures that the system's protection aligns with its risk exposure and operational needs. The steps described in Table 5.4 outline the typical process for SL-I determination.

Table 5.4 Outline of process for determining SL-I

Step	Description	Activities/comments
1	Define Scope – Zone and Conduit Identification	Segment the IACS into zones (groupings of assets with uniform cybersecurity requirements) and conduits (communication paths between zones), following IEC 62443-3-2. This segmentation enables tailored risk-based management of security across the system architecture.
2	Establish Target Security Level (SL-T)	Perform a comprehensive risk assessment, evaluating threats, vulnerabilities, likelihood, and potential consequences. Determine the SL-T for each zone or conduit, selecting from Security Levels 1 to 4, based on required resilience to attacker profiles ranging from casual to highly resourced adversaries.

3	Map to Foundational Requirements (FRs)	Security requirements are classified into the seven Foundational Requirements (FRs), as specified in IEC 62443-3-3. Each FR includes requirement enhancements aligned with SL 1–4.
4	Evaluate Implemented Security Measures	Assess the actual security measures implemented for each FR against the defined SL-T. Determine the SL-I for each FR by evaluating the depth, maturity, and effectiveness of security measures. Make reference to relevant standards: IEC 62443-3-3 for system-level requirements, IEC 62443-4-2 for component-level capability (SL-C), and IEC 62443-2-1 and 2-2 for organizational security practices and processes.
5	Verification and Documentation	Conduct a gap analysis to identify discrepancies between required and implemented controls. Document the SL-I per FR, for example: SL-I: [IAC: 2, UC: 2, SI: 3, DC: 1, RDF: 2, TRE: 3, RA: 1]. The overall SL-I for the zone is often taken as the minimum SL-I across all FRs, although this may vary depending on organizational policy.

To ensure accuracy and completeness, SL-I determination typically involves multiple verification methods, including design and architecture reviews, configuration and system inspections, penetration testing and vulnerability assessments, log and audit trail analysis, and tool-assisted compliance assessments (e.g., automated security checkers).

For a system or zone to be considered compliant, the achieved Security Level – Implemented (SL-I) must meet or exceed the Target Security Level (SL-T). Any discrepancy between SL-I and SL-T requires remediation. This may involve enhancing existing security measures, implementing additional security measures, or applying compensating measures along with formal documentation of any accepted residual risk.

SL-I should be periodically re-evaluated during the operational phase (then referred to as Security Level – Operational, or SL-O), especially after system upgrades, significant configuration changes, or changes in the threat landscape. Regular updates to SL-O are also recommended—e.g., on a quarterly or semi-annual basis as part of medium-term follow-up, or annually for long-term follow-up.

Process for determining SL-O

Monitoring of SL-O is illustrated in Table 5.5, using fictitious values for example zones A, B, and C. For discussion purposes, this illustrates one option (Option 1) in which the SL-O may improve over time. A second option (Option 2) will also be presented, where the SL-O cannot improve over time, instead, the SL-I is updated to a new baseline value.

Table 5.5 Monitoring of security level during operation (SL-O)

Zone	SL-I vector							SL-I	SL-O vector							SL-O
	FR1	FR2	FR3	FR4	FR5	FR6	FR7		FR1	FR2	FR3	FR4	FR5	FR6	FR7	
	IAC	UC	SI	DC	RDF	TRE	RA		IAC	UC	SI	DC	RDF	TRE	RA	
A	2	2	3	1	2	3	1	**1**	2	2	**4**	**2**	**3**	**2**	**2**	**2**
B	4	3	3	4	3	4	3	**3**	4	3	3	4	**2**	4	**2**	**2**
C	2	3	2	2	3	4	3	**2**	**3**	3	2	2	3	**3**	3	**2**

The left section of the table, highlighted in blue, represents the baseline Security Level – Implemented (SL-I), against which the regularly updated Security Level – Operational (SL-O) is compared. Each value in the SL-O vector, corresponding to the Foundational Requirements (FRs), is evaluated relative to its counterpart in the SL-I vector. Changes are visually indicated as follows: improvements are shown in *green*, reductions in security level in *red*, and unchanged values in *black*.

The table also includes overall values for SL-I and SL-O for each zone, along with indications of changes in SL-O. As described in Step 5 of Table 5.4, the overall SL-I for a zone is typically derived as the minimum SL-I across all FRs, although this approach may vary depending on organizational policy.

The rationale behind using the minimum value depends on how the FRs are conceptualized: whether they represent independent sets of security measures—akin to components in a chain (series connection)—or whether they provide overlapping or compensating effects—similar to a parallel connection. While the FRs form part of a logical defense-in-depth strategy and are structurally distinct, they address different layers of security and are not interchangeable. Because each layer plays a critical role, the FRs can be viewed as links in a chain, where the overall strength is determined by the weakest link. Therefore, using the minimum SL across all FRs as the overall SL is a defensible and conservative approach, and this methodology is applied in Table 5.5.

In the examples presented in Table 5.5, Zone A shows an improvement in its operational security level, with SL-O increasing from SL-I = 1 to SL-O = 2; this is indicated with green shading. Zone B, by contrast, has experienced a reduction in security level, with SL-O decreasing from SL-I = 3 to SL-O = 2, highlighted with red shading. Zone C remains unchanged, with SL-I = SL-O = 2, shown using the blue baseline shading.

In Option 1, these three potential outcomes are possible. In Option 2, however, any improvement in SL-O is interpreted as a system modification, which should trigger an update of the SL-I (e.g., from SL=1 to SL=2 for zone A). Consequently, Option 2 allows only two potential outcomes: a decrease in SL-O (as in zone B) or no change in SL-O (as in zone C). Although IEC 62443 does not provide clear guidance on which option to adopt, the prevailing expert view is to follow Option 2.

The most critical outcome is the decrease observed in Zone B, as a reduction in SL-O below the baseline SL-I signals a need for action—such as implementing compensating measures or other remedial actions. The values within the SL-O vector help identify which specific Foundational Requirements (FRs) require attention. This analysis applies not only to Zone B but also to Zones A and C, even if their overall SL-O is equal to or higher than the baseline SL-I, since individual FRs may still indicate areas needing improvement.

A relevant question is: how are the values of the SL-O vector determined? One approach is to repeat Step 4 from Table 5.4, but this time by assessing the *operated* (i.e., currently implemented and functioning) security measures against the SL-I baseline, rather than against the SL-T target. However, this raises a challenge similar to that faced when determining the overall SL value for a zone: namely, how to derive an overall SL for each Foundational Requirement (FR), which itself comprises a set of System Requirements (SRs) and corresponding Requirement Enhancements (REs).

As with the derivation of the overall SL from the FR vector, similar considerations must be made when aggregating SR and RE values to obtain an SL value for each FR. This includes determining whether the minimum value rule is appropriate or if another aggregation method is more justified. In fact, this issue is not limited to SL-O: the same applies when determining the SL-I FR vector, where SRs and REs must also be consolidated into a representative SL value for each FR.

Additional considerations regarding zones and conduits, Maturity Level (ML), and Security Protection Rating (SPR) are discussed in further detail in a working memo [35]. In that memo, it is proposed that the *configuration aspect* of conduits be treated as a distinct zone—specifically, a *network device configuration zone*. This approach effectively isolates the configuration functions, while the remaining parts of the conduits are conceptualized as mere communication pathways or "pipes" that do not require a Security Level (SL) assignment.

As a result of this conceptual distinction, conduits have not been included in the analysis presented above—for example, in Table 5.5—which focuses exclusively on zones and their associated SL-I and SL-O values.

5.3 Long-term status of cybersecurity and cybersecurity barriers

In this section, we examine the annual (approximately yearly) verification of the status of cybersecurity barriers. As with the medium-term follow-up discussed in Section 5.2, we introduce activities based on verification strategies (Section 5.3.1), an existing practice for Technical Condition Safety (TCS) (Section 5.3.2), and verification activities aligned with an existing cybersecurity performance standard (Section 5.3.3).

5.3.1 Long-term verification activities

For long-term follow-up, tailored and operationalized cybersecurity verification activities should also be readily available. Relevant long-term activities for verifying backup mechanisms and intrusion detection systems (IDS) are provided as examples in Table 5.6. These should be supplemented with other relevant cybersecurity barrier elements—or broader cybersecurity measures—depending on the defined scope.

Table 5.6 Examples of long-term cybersecurity measure verification activities

No	Name	Description of activities
1. Backup mechanisms		
1.1	Perform Test Restorations	Perform test restorations of the backup data, regularly and after software updates, to verify that the data can be successfully restored. This helps ensure that the backup files are not corrupted and that the restoration process works as expected
1.2	Document and Test Backup Procedures	Maintain detailed documentation of the backup procedures and test them (by following the procedures step-by-step) periodically. Ensure that the procedures are up-to-date and aligned with best practices
2. Intrusion Detection System (IDS)		
2.1	Conduct Regular Audits	Perform periodic audits of the IDS to verify its effectiveness and identify any gaps in coverage. This can include reviewing detection capabilities and ensuring all network segments are monitored
2.2	Use External Validation	Engage third-party security experts to conduct penetration testing and validate the IDS's effectiveness. This provides an independent assessment of the system's performance
Other cybersecurity (barrier) elements		
…	…	…

Note that “Perform Test Restorations” is included here as well as in the medium-term (weekly to monthly) follow-up, as some companies may find a frequency of once or twice per year more appropriate.

5.3.2 Technical Condition Safety (TCS)

As stated in Section 5.2.2, the TIMP approach within safety barrier management incorporates findings from Technical Condition Safety (TCS), among other sources. TCS and similar systems have been used for the long-term follow-up of safety barriers. TCS involves a comprehensive review and examination of compliance with internal and external requirements—covering approximately 250 requirements and 1,000 checkpoints—typically conducted every four to five years, with regular status updates provided through the "TCS status" tool. Elements of the TCS methodology are also integrated into the TIMP approach; for example, the character grading scale used in TIMP is adopted from TCS.

The TCS methodology compiles relevant internal and external safety barrier performance requirements into so-called Performance Standards (PSs), which have a broader scope than individual safety systems—that is,

a single PS covers more than one system. The NORSOK S-001 standard, *Technical Safety* [36], is also structured around the use of PSs.

The performance categories include functional, integrity, vulnerability, and management requirements, covering primarily technical aspects but also addressing human and organizational factors—particularly within the management category. A few cybersecurity-related requirements are included; however, to our knowledge, the TCS system has not been extended to incorporate cybersecurity to the same extent as in the TIMP approach.

5.3.3 Performance standard verification activities

In an existing performance standard for cybersecurity, the requirements are mapped to each of the barrier elements, accompanied by assurance activities designed to ensure compliance. These assurance activities include long-term verification activities, which are summarized at the end of the document. The summary outlines tasks, frequencies, and assigned responsibilities—for example, the Technical System Responsible (TSR) Telecom.

An adapted version of this summary is presented in Table 5.7.

Table 5.7 Long-term cybersecurity verification summary table

Verification task		Frequency	Responsibility
1	Review user management and firewall rules and setup to ensure that the requirements are fulfilled	Yearly	TSR Telecom
2	Review anti-virus and backup and patch management on all 3. party systems	Yearly	TSR Telecom
3	Perform a review by an external party to make sure the requirements listed in this performance standard are fulfilled	Every two years (or when needed)	TSR Telecom

This is a very useful overview, though there is room for some improvement. For example, the assurance activity *"Perform a test of the disaster recovery plan every two years,"* included in the main body of the PS, could be added to the verification summary table, as it represents a relevant long-term verification measure.

Additionally, some activities in the main body of the PS lack a clearly defined frequency. For example, the entry *"Perform regular review/audit"* does not specify what *"regularly"* entails. Clearly listing all verification activities—along with their respective frequencies—in the verification summary table could help prompt and support the determination of appropriate intervals, whether long-term, medium-term, or continuous.

Therefore, it is recommended that the table be expanded to include a broader range of verification activities, beyond those classified as long-term.

Furthermore, whereas the summary table explicitly assigns responsibility for each verification activity, this level of accountability is not consistently reflected in the main body of the performance standard, where individual assurance activities may lack clearly defined responsible roles. Developing comprehensive overviews of tailored and operationalized verification activities—with clearly assigned responsibilities—would significantly support this effort and enhance the overall effectiveness of cybersecurity barrier management.

6 Integration of safety and cybersecurity barrier management

6.1 Introduction

The overall goal of the project is to integrate safety and cybersecurity barrier management, that is to address the question: *How to integrate safety and cybersecurity barrier management?*

The regulatory background [8] mandates the establishment of barriers to prevent accidents, recognizing that such accidents may stem from both unintentional and intentional causes. Traditionally, barrier management has focused on unintentional events within the realm of safety. However, the Lysne Committee emphasized the importance of also addressing cybersecurity threats and vulnerabilities (cf. Section 3.1). Furthermore, regulatory authorities explicitly state that cybersecurity must be included as part of overall barrier management [10], cf. Section 3.2.

In the industry, some companies have established practices for integrating cybersecurity barrier management with existing safety barrier management. These integration efforts have primarily been shaped by the companies' established approaches to safety barrier management, while also being driven by the need to comply with general regulatory requirements for ICT security and cybersecurity [12]. This dual influence presents several challenges to effective integration.

We have specifically examined the practices of two companies operating on the Norwegian Continental Shelf. These companies have significantly different approaches to safety barrier management and rely on different standards and guidelines for cybersecurity requirements, as outlined in Section 3.3. As a result, their practices for cybersecurity barrier management also differ considerably. This disparity formed the basis for initiating the project: to investigate the potential for developing a flexible, common approach to barrier management in the petroleum industry that can accommodate such variations.

Both companies recognize the value of advancing cybersecurity by incorporating it into barrier management alongside safety barrier management. Their perspectives indicate a shared commitment to further developing and enhancing the integration of cybersecurity barrier management within the broader framework of safety-oriented practices.

By *integration*, we refer to the incorporation of cybersecurity barrier management into existing safety barrier management frameworks, encompassing both technical and non-technical aspects. Importantly, this integration does not imply a single, standardized solution. Instead, it allows for varying degrees of integration and requires flexibility in the choice of implementation approaches.

Examples of this flexibility include decisions such as whether to:

- Develop a dedicated cybersecurity performance standard (PS), or incorporate cybersecurity requirements into existing safety PSs,
- Establish a separate PS for non-technical barriers or combine them with technical barriers within the same PS, and
- Integrate cybersecurity barrier status into the same visualization tools as safety barriers (e.g., using barrier panels or TIMP bow-tie, cf. Chapter 5) or maintain separate dashboards for cybersecurity.

In addition, any integration effort must accommodate differences in existing safety barrier management regimes, which vary across companies. Therefore, adaptable solutions are essential to ensure practical alignment with each organization's established practices.

6.2 Integration guidance in standards, guidelines, and academic publications

6.2.1 Standards and guidelines

The most relevant standards[13] in this context are *IEC TR 63069* [22], which addresses the integration of *IEC 61508* [37] (functional safety of electrical/electronic/programmable electronic systems) with *IEC 62443* [6] (industrial cybersecurity), and *ISA-TR84.00.09* [23], which focuses on the integration of *IEC 61511* [7] (functional safety for the process industry) with *IEC 62443* [6]. In addition, the most recent editions of IEC 61508 and IEC 61511 have introduced the concept of Safety Instrumented System (SIS) security. For instance, IEC 61511 includes a dedicated subsection on SIS cybersecurity considerations.

Despite these developments, the standards primarily address the management of functional safety and cybersecurity at a general level. They do not explicitly cover *barrier management*—either for safety or cybersecurity—nor do they provide guidance on the integration of barrier management across these domains. At present, no standards exist that are specifically focused on safety or cybersecurity barrier management, whether separately or in combination.

6.2.2 Academic publications

While there is a substantial body of literature addressing the integration of safety and security in Industrial Control Systems (ICS), there is very limited focus on the specific integration of *safety and cybersecurity barrier management* [24].

A commonly used classification distinguishes between *unified* and *integrated/parallel* approaches to managing safety and security in ICS [38], [39]. Although some studies cite practical challenges as reasons for avoiding a unified approach, it is notable—and somewhat surprising—that none of the reviewed publications identifies *confidentiality* as a factor. In practice, cybersecurity risk assessments and related documentation are often classified as confidential. If these assessments were to be fully unified with safety risk assessments, the associated confidentiality requirements would then extend to safety-related assessments as well. This could complicate their dissemination and use, particularly in contexts where transparency is essential. Therefore, integration should strike a balance between unified and parallel approaches to mitigate the potential drawbacks of complete unification.

In the cases where combined safety and cybersecurity approaches are applied to identify cybersecurity barriers or measures, the focus is typically on assessing *the need* for such barriers—i.e., determining what should be established. These approaches do not generally account for the *inventory* of existing, planned, or designed cybersecurity barriers and measures.

In this project, when we refer to the *identification* of cybersecurity barriers, we do *not* include the process of determining whether barriers are needed. Instead, our scope begins *after* that decision has been made—either in the context of a new project where cybersecurity barriers have been specified, or in the evaluation of an existing facility where such barriers are already in place.

Integrated safety and cybersecurity *barrier* management is addressed only to a limited extent in the existing literature. One publication claims to have laid the groundwork for future research in this specific area [40]. In addition, two publications make brief references to the ongoing CBM project initiative [41], [42]. However, the majority of reviewed literature focuses on general approaches to *combining safety and security in ICS*, without specific attention to *barrier management* as a distinct discipline.

[13] In this context, the term *standards* is used generically and does not differentiate between *International Standards (IS)*, *Technical Reports (TR)*, and *Technical Specifications (TS)*.

6.3 Integration in industry practices

A central question addressed in this study is: *How is cybersecurity barrier management integrated with safety barrier management in industry practices?* Implicit in this question is a closely related issue: *How is cybersecurity barrier management established within the context of pre-existing safety barrier management frameworks?*

To explore these questions, we provide a brief overview of the integration approaches adopted by the two companies involved in the study, focusing on the following key aspects:

- Degree of integration between cybersecurity and safety barrier management
- Scope of security measures included in the barrier management system
- Treatment of both technical and non-technical aspects
- Use of a dedicated cybersecurity PS versus integration into existing safety PSs
- Use of a separate PS for non-technical barriers versus integration with technical barriers
- Integration of cybersecurity barriers into existing visualization tools, such as barrier panels or TIMP bow-tie, versus the use of separate dashboards

This structured comparison provides insight into how differing safety barrier management regimes influence the integration of cybersecurity, and informs the development of a flexible, industry-wide approach that can accommodate such variation.

Degree of integration between cybersecurity and safety barrier management

In both companies, the integration of cybersecurity into barrier management takes the form of an add-on to existing safety barrier management systems. These are not unified approaches, where cybersecurity and safety are treated as a single, fully integrated framework. Nor can they be classified as parallel approaches, in which both domains are developed and executed concurrently but independently.

Instead, cybersecurity barrier management is developed separately, and then adapted and appended to the company's established safety barrier management structures. This sequential and adaptive approach reflects the historical precedence and maturity of safety barrier management within both organizations, as well as the need to ensure compliance with emerging cybersecurity regulations and standards.

Scope of security measures included in the barrier management system

This issue is explored in depth in Chapters 2 and 4, where we underscore a key distinction: cybersecurity barriers are a subset of all cybersecurity measures—just as safety barriers are a subset of broader safety measures within safety barrier management.

Both companies initiate their cybersecurity barrier management practices by referencing cybersecurity requirements, which cover a wide spectrum of measures. These requirements include not only cybersecurity barriers but also more general cybersecurity measures such as policies and procedures. In contrast, safety barrier management is more narrowly scoped, focusing only on measures that qualify as safety barriers and excluding broader safety controls or performance-influencing factors from the barrier inventory itself.

This mismatch creates significant challenges for integration. In particular, there is a conceptual and practical gap between how barriers are defined and managed in the domains of safety and cybersecurity. In cybersecurity management, a broad set of measures is often treated as barriers—including administrative controls. However, within safety barrier management, only a subset of measures qualifies as barriers, based on more stringent definitions that exclude control measures and barrier performance influencing measures.

A further complication arises from differences in regulatory expectations. In safety barrier management, barrier elements must comply with verifiable performance requirements, as mandated by regulation. These include specifications for functionality, reliability, and testability. In contrast, many cybersecurity requirements focus on the presence of a security measure, rather than specifying its performance parameters or effectiveness. For example, the requirement to have a firewall or access control system may exist without accompanying criteria for its risk mitigation performance or operational reliability.

These discrepancies—both in the scope of what is considered a barrier and in the nature of requirements—pose obstacles to achieving a coherent framework. Addressing and reconciling these differences is essential for developing an integrated barrier management approach that maintains consistency across safety and cybersecurity domains, supports regulatory compliance, and ensures effective risk control.

Treatment of both technical and non-technical aspects

Both companies incorporate technical and non-technical aspects into their cybersecurity and safety barrier management practices. However, the technical components are generally addressed more comprehensively and systematically than the non-technical ones.

There are two primary entry points for the inclusion of non-technical elements:

1. Requirements derived from standards and guidelines, which explicitly address organizational and procedural aspects.
2. Systematic decomposition of barrier functions into barrier elements, including both operational/ organizational elements in safety management and people/process elements in cybersecurity management.

Standards such as IEC 62443 provide a foundation for addressing both technical controls and process-oriented security measures. These standards form the basis for medium- and long-term verification activities, as discussed in Sections 5.2 and 5.3.

The main challenge lies in the short-term monitoring and visualization of non-technical barrier elements. Tools like the barrier panel (cf. Section 5.1) are effective for displaying the real-time status of technical barriers but are less equipped to represent the status of non-technical elements. Relevant information—such as personnel competence, training, or procedural readiness—is often stored in separate source systems. Integrating such data into real-time visualization tools remains complex and presents an obstacle to full situational awareness of non-technical barrier health.

Use of a dedicated cybersecurity PS versus integration into existing safety PSs

Both companies currently maintain a separate PS for cybersecurity. However, there has been ongoing discussion within the industry about whether it may be more appropriate to incorporate cybersecurity requirements into the relevant safety PSs instead.

The primary rationale for keeping a separate cybersecurity PS is that it ensures dedicated attention and visibility for cybersecurity concerns, which might otherwise be underemphasized within broader safety documentation. Moreover, as cybersecurity is a comparatively less mature discipline, it requires focused treatment.

Conversely, integrating cybersecurity requirements into existing safety PSs could enhance awareness of the interdependencies between safety and cybersecurity. This approach would help highlight the potential safety consequences of compromised cybersecurity barriers or controls, reinforcing the understanding that

cybersecurity is not merely a technical or compliance issue, but also a critical component of overall safety management. However, such integration may lead to redundancy, as the same cybersecurity requirements could be repeated across multiple safety PSs, potentially complicating maintenance and consistency.

In addition, safety and cybersecurity are disciplines that typically fall under separate areas of responsibility. Merging them into the same PS could create challenges in clearly defining and allocating responsibilities.

In current practice, this integration is partially achieved through cross-communication mechanisms. For example, if weaknesses are identified in the cybersecurity PS—such as during a TIMP assessment—these findings are communicated to the responsible parties for the affected safety PSs. In this way, although the standards are maintained separately, there is a functional linkage that supports integrated risk understanding and management across domains.

Use of a separate PS for non-technical barriers versus integration with technical barriers

In both companies, technical and non-technical aspects of cybersecurity are integrated within a single cybersecurity PS. This reflects a unified treatment of cybersecurity as a domain that inherently involves both technical controls (e.g., firewalls, intrusion detection systems) and non-technical aspects (e.g., organizational procedures, training, and awareness).

However, this is different from how non-technical aspects are treated within safety barrier management. For example, one of the companies maintains a separate PS for competence and training, which applies to safety-related barriers. In contrast, cybersecurity-related competence and training are incorporated directly into this company's cybersecurity PS, rather than being managed under a separate standard—reflecting the unified approach described above.

Establishing a separate PS for non-technical aspects may provide clearer focus on these elements and support better harmonization with safety barrier management practices.

Integration of cybersecurity barriers into existing visualization tools

Both companies have taken steps to integrate cybersecurity barriers into the existing visualization tools originally developed for safety barrier management.

This integration offers several key benefits. First, it enables easy access to specific and critical information related to cybersecurity barriers, presented in formats already familiar to both operational and management personnel. Second, by displaying cybersecurity barriers within the same visual context as safety barriers, it increases the visibility of cybersecurity issues and promotes greater organizational awareness and attention to cybersecurity risks.

These visualization practices contribute to the broader objective of establishing a unified situational awareness framework, in which both safety and cybersecurity barriers are monitored and assessed in a cohesive manner—despite underlying differences in their structure, purpose, and origin.

7 Discussion and conclusions

The discussion is structured around the following five questions constituting the scope of this report:

1) How to identify barriers and barrier elements?
2) How to develop, implement and verify cybersecurity barrier requirements?
3) How to assess the cybersecurity barrier status?
4) How to verify security levels of cybersecurity systems and components?
5) How to integrate safety and cybersecurity barrier management?

1. How to identify barriers and barrier elements?

Top-down approach in safety barrier management

In safety barrier management, it is common to use a top-down approach for the identification of barriers and barrier elements. The starting point for identifying barrier functions is scenarios based on Defined Situations of Hazard and Accident (DSHAs) for major accidents included in risk assessments. The scenarios can be presented in various ways, such as barrier grids [43] or bow-ties.

The breakdown from barrier functions to barrier elements occurs in layers through a number of sub-functions, sub-sub-functions, etc. until the functions can be materialized through one or more specific barrier elements. Sub-functions and associated lower-level functions include safety instrumented functions (SIFs), safety functions (SFs), and safety-critical tasks (SCTs). The barrier elements, in safety barrier management, are of three types: technical, operational, and organizational.

Bottom-up approach in safety barrier management

Experience from safety barrier management shows that such a systematic top-down breakdown is not necessarily comprehensive; in other words, not all barrier elements are uncovered. A complementary method that increases the coverage is to go the opposite way – from the bottom up – by illustrating the logical relationships between all the barrier elements at each functional level (sub-functions, sub-sub-functions, SIFs, etc.) for each barrier function. This approach can identify additional equipment and actions necessary to achieve the barrier function. It requires access to all "inventory" and system drawings, such as P&IDs (Piping and Instrumentation Diagrams).

Even when using both approaches, experience shows that additional barrier elements are also uncovered during operation—partly as entirely “new” elements, and partly because certain elements are chosen to be categorized as barrier elements that were not previously classified as such.

Top-down approach in cybersecurity barrier management

In cybersecurity barrier management, the practice has been to use one of the approaches—either top-down or bottom-up. The top-down approach has started with a number of cyber incident scenarios and the use of bow-tie diagrams as a tool for identifying and illustrating barrier functions related to a "top event." The breakdown from barrier functions to barrier elements has been coarse, with only one level of barrier functions and one level of barrier elements. No levels of sub-functions or sub-sub-functions, etc., have been used.

There are several challenges (or areas for improvement) with this practice. The first concerns the scenarios. In safety barrier management (as well as in safety risk analyses and emergency preparedness analyses), there is a commonly agreed set of DSHAs (Defined Situations of Hazard and Accident), whereas for cyber incidents, there are various types and numbers of scenarios. The second challenge is that the bow-tie tool

can be misleading in that it presents only one event (the "top event") within what is actually an event chain. Which event in the chain is defined as the top event influences what is regarded as probability-reducing versus consequence-reducing measures. This, in turn, affects the understanding of what constitutes a control measure (maintaining control – normal operation) versus a barrier measure (regaining control). The third challenge is the coarse breakdown from one level of barrier functions to one level of barrier elements, without any intermediate sub-functions. The result can be an incomplete breakdown, meaning that the barrier elements are described as sub-functions rather than final barrier elements. This also impacts the categorization into different types of barrier elements (or security measures), which in cybersecurity are technical, human, and process-based. A sub-function can contain more than one type of barrier element.

The practice described here has been influenced by adaptation to the existing safety barrier management practices within the same company, including the number of levels in the breakdown of barrier functions.

The challenge of achieving a comprehensive, yet not overly extensive, set of scenarios for cyber incidents is something the industry should collaborate on, as it is relevant for both projects and operations. This begins with (cyber)security risk analyses, and the scenarios included in them. The work on scenarios may also include links to safety incidents, i.e., the safety DSHAs (Defined Situations of Hazard and Accident).

An alternative, or complement, to the bow-tie is the barrier grid [43], which makes all the events in the event chain visible and can include links to safety DSHAs.

The number of levels in the breakdown of barrier functions should be flexible and not limited to only one level of barrier elements without any levels of sub-functions.

Bottom-up approach in cybersecurity barrier management

The practice of the bottom-up approach starts with identifying relevant ICT systems and equipment from, among other sources, topology diagrams within the disciplines that use such systems and equipment. The focus has been on systems rather than on barrier functions and elements. The aggregation upward has followed the phases of the NIST Cybersecurity Framework (CSF) to the overall Performance Standard (PS), which is considered the "cyber barrier" and compared to the safety barriers aggregated at the PS level. One of the challenges—or particularities—of this approach is the limited linkage to barrier functions and elements. A general challenge with a bottom-up approach is the lack of a complete asset inventory, especially for existing installations.

The assessment, starting with the relevant ICT systems and equipment, is based on cybersecurity requirements from sources such as the IEC 62443 standard series and the NIST Cybersecurity Framework (CSF), which are by default regarded as barrier requirements. A selection of these requirements has been reformulated into questions used to evaluate the medium-term status of the relevant ICT systems.

A new standard-based top-down approach in cybersecurity barrier management

A third approach for identifying barrier functions and barrier elements, established in this project, also starts with the general cybersecurity requirements set out in standards and guidelines but filters out those requirements that are relevant to barriers. This approach aligns with the authorities' definition of barriers, while the development of the method has not depended on access to confidential information such as cyber risk analyses, a complete asset inventory, or topology diagrams. The method is described in detail in Chapter 4, where the first five of nine steps deal with the identification of barrier functions and barrier elements. Standards with cybersecurity requirements for OT systems, such as IEC 62443, generally cover all types of

situations—i.e., all scenarios, whether these involve network-based attacks, physical intrusion, insiders, or the supply chain.

Combination of methods

None of the methods provide a guarantee that all barrier functions and barrier elements are identified, and the coverage improves by combining several of the three methods. In addition, it will be necessary to include barrier elements that are uncovered during operations.

Which methods are used is up to each individual company. This will be influenced by existing approaches to safety barrier management.

2. How to develop, implement and verify cybersecurity barrier requirements?

Barrier requirements, according to the Management Regulations (MR) § 5, concern setting verifiable performance requirements for the barrier elements—that is, for the measures defined as barriers. How effective should they be? How well should they perform? This is not about which measures should be in place—that is the answer to Question 1 above.

Fulfilment of general cybersecurity requirements, according to the Facilities Regulations (FR) § 34a, is neither sufficient nor necessary to fulfil the requirements of the Management Regulations (MR) § 5. The reason it is not sufficient is that the requirements in standards and guidelines such as IEC 62443, NOROG 104, NIST CSF, etc., are largely about having cybersecurity measures in place, and only to a limited extent about the performance of those measures. Furthermore, the requirements are general, such as "regular monitoring," regardless of context. What does "regular" mean? The requirements must be specified and adapted to the context—i.e., the specific facility, zone, system, etc. The requirements are also not comprehensive, as a requirement to have a cybersecurity measure in place is not always followed by a requirement regarding the performance of that measure. In such cases, performance requirements must be derived and established for the specific measure. The reason these requirements are also, in many cases, not necessary to fulfil MR § 5 is that they are not barrier requirements, but rather general cybersecurity requirements.

In order to fulfil not only MR § 5 but also FR § 34a—i.e., the "dual objective"—this has been accounted for in the method described in Chapter 4 (through Step 9). It is up to the companies to have corresponding performance requirements and verification of these for general cybersecurity measures, just as for barriers. This becomes a consequence of defining control measures as barrier measures.

The current practice is to regard all cybersecurity requirements in standards and guidelines as barrier requirements, in order to fulfil the "dual objective." However, the connection between these requirements and barrier elements is questionable—among other reasons, because many of the general requirements are difficult to assign to a specific barrier element. Furthermore, verification becomes challenging unless the requirements are tailored and adapted to the individual operator and installation, and unless the requirements are sufficiently specified and operationalized. How verification can be improved is described in Chapter 5. The actual implementation of the requirements is the responsibility of the operating companies.

3. How to assess the cybersecurity barrier status?

The assessment of the status of barriers is two-fold. One part is the ongoing status regarding whether they currently have any impairments. This is a requirement under MR § 5, which states that "personnel shall be aware of which barriers and barrier elements are not functioning or have been impaired." We refer to this

as “short-term” follow-up, where barrier panels have traditionally been used as a tool in daily operations—including in cybersecurity barrier management—by adapting the panel used for safety barrier management.

One of the challenges is determining which indications of barrier impairments should be included and flagged in the barrier panel (as red, yellow, or green according to a traffic light system). These status indicators typically cover actual (physical) faults, disconnections (functional failures), and the probability of failure based on the status of preventive maintenance and testing within safety barrier management. In cybersecurity barrier management, vulnerabilities are also a relevant category and may serve as a potential status indicator. However, the recommendation from industry partners is to handle specific vulnerabilities (CVEs) as part of the ongoing vulnerability assessment process, without including them in the barrier panel. In general, it must be possible to automatically collect the information that goes into the barrier panel, since the status presented is real-time or near real-time. A menu of relevant status indicators that can serve as a starting point is presented in Chapter 5.

The second form of status assessment concerns the verification of the performance requirements of the barriers, typically through performance indicators, audits, or reviews—or a combination of these. This can occur relatively frequently (weeks to months) or more infrequently (annually or less), and we generally distinguish between “medium-term” and “long-term” follow-up of whether the barrier requirements are being met. In the first category, the TIMP method has been used—originally for safety barrier management, but also for cybersecurity barrier management, albeit in a somewhat adapted form. This verification is typically carried out quarterly, with the results for the cybersecurity barriers compiled together with the results for the safety barriers. Both automatically harvested information and manual assessments are used. There has been a stated desire from some parties for a greater degree of automation. TIMP is based on information from, among other sources, the Technical Condition Safety (TCS) method and is also partially built on this method used for long-term follow-up of safety barriers. The TCS method has not been implemented for cybersecurity barrier management, as far as we know.

4. How to verify security levels of cybersecurity systems and components?

In the project, we have demonstrated how security levels can be verified by monitoring security levels during operations (SL-O), in a way somewhat similar to “SIL in operation” within functional safety. The starting point is to verify the security level requirements established through SL-I (and originally through SL-T). This status thus also forms part of the answer to Question 3. The security level requirements are tied to each specific zone and are based on an IEC 62443–based approach. This means, firstly, that the scope is not limited to barriers only but encompasses cybersecurity measures in general. Secondly, it relies on the IEC 62443 methodology for determining/calculating security levels, which presents certain practical challenges—including the understanding of zones and conduits, and calculations with or without the use of vectors. This is elaborated in Chapter 5.2.3. “SL in operation” constitutes a “medium-term” or “long-term” follow-up, and as mentioned, it is part of the response to Question 3. A general challenge—or limitation—is that the follow-up and verification of SL-O is based on the use of IEC 62443, which is not applied by all companies.

5. How to integrate safety and cybersecurity barrier management?

The integration of safety and cybersecurity barrier management is addressed to a very limited extent in standards, guidelines, and academic literature. What is discussed typically concerns the integration of safety and cybersecurity in general.

The current practice is that cybersecurity has been an add-on to and adapted within the already existing safety barrier management framework, but without harmonizing the terminology. There is no definition of cybersecurity barriers, and the practice has been to define all cybersecurity measures as barriers, cf. the

discussion under Question 1. This has led to challenges in follow-up, partly because cybersecurity requirements are not synonymous with performance requirements, cf. the discussion under Question 2.

The visualization of cybersecurity (barrier) status has also been adapted to the existing systems and tools used for safety barrier management, such as the barrier panel and TIMP.

An adaptation to the already existing safety barrier management is natural, both because there is an established methodology to build upon, and to increase visibility and awareness. However, for current practices, it is more accurate to say that cybersecurity management (in general) has been integrated with safety barrier management.

How can or should this be done? As a starting point, it is sensible and practical to adapt to the way safety barrier management is practiced in the specific company. Since this practice varies, any general recommendation must be flexible, as we have described in this project. There are many considerations and decisions that must be made within such a flexible framework, including clearly distinguishing between general cybersecurity management (cf. FR § 34a) and cybersecurity barrier management (cf. MR § 5), for example by harmonizing the barrier concept and definition between cybersecurity and safety. Other considerations and decisions that need to be made are discussed in Chapter 6.

Conclusions

1. How to identify barriers and barrier elements?

Comprehensive identification of cybersecurity barriers and barrier elements is achieved through a combination of multiple methods, including top-down and bottom-up approaches, along with a standards-based approach developed as part of this project. Additionally, newly identified barrier elements discovered during operations should be continuously incorporated.

2. How to develop, implement and verify cybersecurity barrier requirements?

Developing cybersecurity barrier requirements implies establishing verifiable performance requirements—specific and operationalized—for the barrier elements. Verification strategies must align with these requirements, while implementation responsibilities rest with the operating companies.

3. How to assess the cybersecurity barrier status?

The status of cybersecurity barriers is assessed through two main components: (i) the ongoing condition, focusing on any current impairments (short-term), and (ii) the verification of performance requirements, typically conducted through indicators, audits, or reviews (medium- to long-term).

4. How to verify security levels of cybersecurity systems and components?

Verification of security levels can be conducted in a manner analogous to “SIL in operation” from the field of functional safety, by monitoring the operational Security Level (SL-O) against the implemented Security Level (SL-I). It is important to note that this represents a medium- to long-term follow-up of cybersecurity measures more broadly and is not limited to barrier performance alone.

5. How to integrate safety and cybersecurity barrier management?

Integration of cybersecurity into safety barrier management is practiced by incorporating and adapting cybersecurity management—currently extending beyond barrier-specific elements—into existing safety barrier management frameworks. Several key aspects influencing the integration process require deliberate choices, as outlined in the report.

References

[1] K. Øien, C. Thieme, and M. G. Jaatun, 'ICS cybersecurity barriers and associated requirements', SINTEF Digital, 2025:00700, 2025.

[2] C. Thieme, V. Gnanasekaran, and T. O. Grøtan, 'Non-technical cybersecurity barrier management', SINTEF Digital, 2025:00701, 2025.

[3] G. K. Hanssen, C. Thieme, A. Vik Bjarkø, and K. Øien, 'Monitoring and handling cybersecurity threats, vulnerabilities and barrier impairments', SINTEF Digital, 2025:00702, 2025.

[4] K. Øien *et al.*, 'Guidance on integrated safety and cybersecurity barrier management', SINTEF Digital, 2025.

[5] S. Hauge and K. Øien, 'Guidance for barrier management in the petroleum industry', 2016, Accessed: Oct. 15, 2023. [Online]. Available: https://sintef.brage.unit.no/sintef-xmlui/handle/11250/3048555

[6] IEC, 'IEC 62443: Industrial communication networks - Network and system security'. IEC. [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443

[7] IEC, *IEC 61511-1 Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, 2017. Accessed: Oct. 15, 2023. [Online]. Available: https://webstore.iec.ch/publication/61289

[8] *Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities (The Management Regulations)*. 2022. Accessed: Feb. 02, 2023. [Online]. Available: https://www.ptil.no/en/regulations/all-acts/?forskrift=611

[9] J. Reason, *Managing the Risks of Organizational Accidents*. London: Routledge, 1997. doi: 10.4324/9781315543543.

[10] A. Eltervåg *et al.*, 'Principles for barrier management in the petroleum industry', Mar. 2017. Accessed: Dec. 01, 2022. [Online]. Available: https://www.havtil.no/contentassets/43fc402b97e64a7cbabdf91c64b349cb/barriers-memorandum-2017-eng.pdf

[11] *Regulations relating to design and outfitting of facilities, etc. in the petroleum activities (The Facilities Regulations)*. 2022. [Online]. Available: https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/innretningsforskriften_e.pdf

[12] PSA, *Guidelines regarding the facilities regulations*. 2023. Accessed: Feb. 08, 2025. [Online]. Available: https://www.havtil.no/en/regulations/all-acts/?forskrift=634

[13] 'Recommended guidelines on information security baseline requirements for process control, safety and support ICT systems', Guideline NOROG 104, Dec. 2016. Accessed: Feb. 02, 2023. [Online]. Available: https://www.offshorenorge.no/retningslinjer/arkiv/integrerte-operasjoner/104-anbefalte-retningslinjer-krav-til-informasjonssikkerhetsniva-i-ikt-baserte-prosesskontroll--sikkerhets--og-stottesystemer-ny-revisjon-pr-05.12.2016/

[14] *Regulations relating to health, safety, and the environment in the petroleum activities and at certain onshore facilities (The Framework Regulations)*. 2019. Accessed: Oct. 06, 2023. [Online]. Available: https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/rammeforskriften20_e.pdf

[15] O. Lysne, 'NOU 2015: 13 - Digital sårbarhet - sikkert samfunn - Beskytte enkeltmennesker og samfunn i en digitalisert verden'. Regjeringen, Nov. 30, 2015. Accessed: Dec. 01, 2022. [Online]. Available: https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

[16] The Ministry of Justice and Public Security, *Meld. St. 38 (2016–2017) Cyber Security — A joint responsibility*. 2017.

[17] G. Frafjord, V. Kristensen, and Ø. Lauridsen, 'Principles for barrier management in the petroleum industry'. Petroleum Safety Authority Norway, Jan. 29, 2013.

[18] PSA, *Guidelines regarding the management regulations*. 2022. Accessed: Nov. 04, 2023. [Online]. Available: https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/styringsforskriften_veiledning_e.pdf

[19] 'Framework for Improving Critical Infrastructure Cybersecurity', Feb. 2018. Accessed: Feb. 02, 2023. [Online]. Available: https://www.nist.gov/cyberframework/framework

[20] K. Øien, S. Hauge, M. G. Jaatun, L. Flå, and L. Bodsberg, 'Cybersecurity Barrier Management (CBM) project baseline WP1', SINTEF Digital, Internal memo 102020847, 2022.

[21] K. Øien, M. G. Jaatun, L. Flå, and C. A. Thieme, 'Cybersecurity Barrier Management (CBM) – Identification of Cybersecurity Barriers (T1.1) version 1', SINTEF Digital, Internal memo 102020847–1, 2023.

[22] IEC, *IEC TR 63069 Industrial-process measurement, control and automation- Framework for functional safety and security*, May 20, 2019. [Online]. Available: https://webstore.iec.ch/publication/31421

[23] ISA, *ISA-TR84.00.09-2017, Cybersecurity Related to the Functional Safety Lifecycle*, Apr. 10, 2017. [Online]. Available: https://www.isa.org/products/isa-tr84-00-09-2017-cybersecurity-related-to-the-f
[24] K. Øien, S. Hauge, M. G. Jaatun, L. Flå, and L. Bodsberg, '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.
[25] S. Øie, A. Wahlstrøm, H. Flataker, and S. Rørkjær, 'Barrier Management in Operation for the Rig Industry - Good Practices', DNV-GL, 2013–1622, Mar. 2014.
[26] IEC, *IEC 62443-2-1 ED 2: 2024 Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners*, 2023.
[27] IEC, *IEC 62443-3-3:2013 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*, 2013. [Online]. Available: https://webstore.iec.ch/preview/info_iec62443-3-3%7Bed1.0%7Den.pdf
[28] IEC, *CD:2025-01 - IEC 62443-1-1-ED1 Security for automation and control systems - Part 1-1: Overview and guidance for the IEC 62443 series*, IEC Technical Specification, 2025.
[29] N. C. Guzman, D. K. M. Kufoalor, I. Kozine, and M. A. Lundteigen, 'Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel', in *Proceedings of the 29th European Safety and Reliability Conference, Lower Saxony, Germany*, 2019, pp. 22–26.
[30] IEC, *IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security Risk assessment for system design*, 2020. [Online]. Available: https://webstore.iec.ch/publication/30727
[31] 'DNV-RP-G108 Guideline for the use of IEC 62443 in the oil and gas industry', DNV. Accessed: Feb. 02, 2023. [Online]. Available: https://www.dnv.com/Default
[32] F. Gratte, 'IEC 62443 Profiles for Oil & Gas projects', 2020.
[33] ISA/IEC, 'ISA/IEC 62443 Ontologies'. ISA, Aug. 30, 2022.
[34] C. A. Thieme and K. Øien, 'Cybersecurity Barrier Management (CBM) – Assessing the Status of Cybersecurity Barriers (T1.2) v2.0', SINTEF Digital, Internal memo 102020847–2, 2024.
[35] M. G. Jaatun, C. Thieme, M. A. Lundteigen, and F. Gratte, 'Cybersecurity Barrier Management (CBM) – Security levels (T1.3) - version 1.1', SINTEF Digital, Internal memo 102020847–3, 2025.
[36] 'NORSOK S-001:2018. Technical safety', Standards Norway, Standard, 2018. Accessed: Oct. 06, 2023. [Online]. Available: https://release.standard.no/en/webshop/ProductCatalog/ProductPresentation/?ProductID=981001
[37] IEC, *IEC 61508-1:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety- Related Systems*. Accessed: Jul. 11, 2022. [Online]. Available: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=429346
[38] E. Lisova, I. Šljivo, and A. Čaušević, 'Safety and security co-analyses: A systematic literature review', *IEEE Syst. J.*, vol. 13, no. 3, pp. 2189–2200, 2018.
[39] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, 'A survey of approaches combining safety and security for industrial control systems', *Reliab. Eng. Syst. Saf.*, vol. 139, pp. 156–178, 2015.
[40] B. Z. Téglásy, B. A. Gran, S. Katsikas, V. Gkioulos, and M. A. Lundteigen, 'Clarification of the Cybersecurity and Functional Safety Interrelationship in Industrial Control Systems: Barrier Concepts and Essential Functions', in *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*, 2020.
[41] T. Onshus *et al.*, 'Security and Independence of Process Safety and Control Systems in the Petroleum Industry', *J. Cybersecurity Priv.*, vol. 2, no. 1, pp. 20–41, 2022, doi: 10.3390/jcp2010003.
[42] T. O. Grøtan, S. Petersen, T. Myklebust, and G. K. Hanssen, 'SecureSafety; state-of-the-art and remaining challenges', in *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*, 2020.
[43] N. J. Edwin, L. Fornes, and K. Øien, 'Improved Safety in the Arctic through Digitalization', 2019, Accessed: Oct. 18, 2023. [Online]. Available: http://rpsonline.com.sg/proceedings/9789811127243/pdf/0252.pdf
[44] K. Øien, M. G. Jaatun, and C. A. Thieme, 'Cybersecurity Barrier Management (CBM) – Identification of Cybersecurity Barriers (T1.1) Final', SINTEF Digital, Internal memo 102020847–1, 2025.

Appendix A Abbreviations and definitions

Abbreviations

Abbreviation	Description
ACS	Automation and Control System
AVAIL	System integrity and availability
BE	Barrier Element
BE-H	Human Barrier Element
BE-O	Operational Barrier Element
BE-T	Technical Barrier Element
BF	Barrier Function
BPCS	Basic Process Control System
BS	Barrier Strategy
BSF	Barrier Sub-Function
CBM	Cybersecurity Barrier Management
CISA	Cybersecurity and Infrastructure Security Agency
CM	Corrective Maintenance
CM-C	Corrective Maintenance – Critical
CMMS	Computerized Maintenance Management System
COMP	Component Security
CVE	Common Vulnerabilities and Exposures
CVE-E	Common Vulnerabilities and Exposures – Exploited
DC	Data Confidentiality
DNV	Det Norske Veritas
DoS	Denial of Service
DSHA	Defined Situations of Hazard and Accident
DPR	Direct Performance Requirement
EG	Edvard Grieg (an offshore facility)
EuC	Equipment under Control
FDIS	Final Draft International Standard
FR	Facilities Regulations
FR	Foundational Requirement
GL	Guideline
Havtil	Norwegian Ocean Industry Authority
HIDS	Host-based IDS
HMI	Human Machine Interface
HSA	Health Status Alarm
HSE	Health, Safety and Environment
IAC	Identification and Authentication Control
IACS	Industrial Automation and Control System
ICS	Industrial Control System
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronics Engineers
INH	Inhibited
IPR	Indirect Performance Requirement
IPS	Intrusion Prevention System

ISA	International Society of Automation
IT	Information Technology
ML	Maturity Level
MR	Management Regulations
NC	Non-Conformance
NIDS	Network-based IDS
NIST CSF	National Institute of Standards and Technology – Cybersecurity Framework
NOROG	Norsk Olje og Gass (now Offshore Norge)
NORSOK	NORsk SOkkels Konkurranseposisjon (acronym in Norwegian) – set of standards
NOU	Norges Offentlige Utredninger (Norwegian Public Reports)
NR	Not Relevant
NSA	Norwegian Shipowners' Association
NVD	National Vulnerability Database
OT	Operational Technology
PDS	Reliability of Safety Instrumented Systems (abbr. in Norwegian)
P&ID	Piping and Instrumentation Diagram
PIF	Performance Influencing Factor
PM	Preventive Maintenance
PM-C	Preventive Maintenance – Critical
PR	Performance Requirement
PS	Performance Standard
PSA/PTIL	Petroleum Safety Authority (now Havtil)
RA	Risk Analysis
RA	Resource Availability
RDF	Restricted Data Flow
RE	Requirement Enhancement
RP	Recommended Practice
SAS	Safety and Automation System
SCAI	Safety Control Alarms and Interlocks
SCE	Safety Critical Element
SCT	Safety Critical Task
SF	Safety Function
SI	System Integrity
SIEM	Security Information and Event Management
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SL	Security Level
SL-A	Achieved Security Level
SL-I	Implemented Security Level
SL-O	Operational Security Level
SL-T	Target Security Level
SPE	Security Program Element
SPR	Security Protection Rating
SR	System Requirement
SuC	System under Consideration
TCC	Technical Condition Cybersecurity
TCS	Technical Condition Safety
THO	Technical, Human and Operational

TIMP	Technical Integrity Management Program
TR	Technical Report
TRE	Timely Response to Events
TSR	Technical System Responsible
UC	Use Control
WD	Working Draft
WP	Work package

Definitions

Term [reference]	Description/definition
Automation and control solution [28]	Collection of people, processes, and automation and control systems with the purpose of monitoring, controlling, and managing the operation of the equipment under control. Note 1 to entry: An automation and control solution includes the instantiation of one or more automation and control systems.
Automation and control system (ACS) [28]	Interacting collection of related components that provide functions for monitoring and controlling the operation of equipment under control. Note 1 to entry: The automation and control system includes, but is not limited to: actuating function, control function, data flow control function, history function, hosting function, manipulating function, safety function, sensing function, view function, utility function (security, management), and view function.
Availability [28]	Property of ensuring timely and reliable access to and use of control system information and functionality.
Barrier [10]	A measure intended to identify conditions that may lead to failure, hazard and accident situations, prevent an actual sequence of events occurring or developing, influence a sequence of events in a deliberate way, or limit damage and/or loss.
Barrier function [10]	The task or role of a barrier.
Barrier element [10]	Technical, operational and organizational measures or solutions involved in the realization of a barrier function.
Barrier management [10]	Coordinated activities for establishing and maintaining barriers so that they fulfil their functions at all times.
Barrier strategy [10]	Plan for how barrier functions, on the basis of the risk picture, are implemented in order to reduce risk.
Capability security level (SL-C) [28]	Security level inherent in a product or technology. Note 1 to entry: Capability security level is determined during the product development phase of the security lifecycle.
Compensating security measure [28]	Security measure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.
Conduit [28]	See security conduit.
Confidentiality [28]	Assurance that information is not disclosed to unauthorized individuals, processes, or devices.
Control system [28]	A type of automation and control system that provides the control function. EXAMPLE: Distributed Control System (DCS), Industrial Control System (ICS), Supervisory Control and Data Acquisition (SCADA) system.
Countermeasure [28]	See security measure.
Cyber asset [23]	Device contained within the system under consideration (SuC), e.g., controller, server, engineering work station, etc.
Cyber incident [23]	Communication with an E/E/PE device within a control system that negatively impacts process safety, the environment, operations, confidentiality, SCAI integrity, or IACS availability.
Cybersecurity [28]	Actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, or damage to systems or informational assets. Note 1 to entry: Cybersecurity includes the concepts of identification, authentication, accountability, authorization, availability, privacy, and confidentiality.

Term [reference]	Description/definition
Cybersecurity barrier [44]	A measure intended to a) detect abnormal conditions, b) prevent abnormal conditions from developing, and c) limit the damage caused by cyber incidents.
Defense-in-depth [28]	Provision of multiple security measures, especially in layers, with the intent to prevent or delay an attack.
Equipment under control (EuC) [28]	Equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other activities. [SOURCE: IEC 61508-4:2010]
Error [7]	Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition. [SOURCE: IEC 60050-192:2015, 192-03-02]
Failure [7]	Loss of ability to perform as required. Note 1 to entry: A failure of a device is an event that results in a fault state of that device. Note 2 to entry: When the loss of ability is caused by a latent fault, the failure occurs when a particular set of circumstances is encountered. Note 3 to entry: Performance of required functions necessarily excludes certain behavior, and some functions may be specified in terms of behavior to be avoided. The occurrence of such behavior is a failure. Note 4 to entry: Failures are either random or systematic (see 3.2.59 and 3.2.81). [SOURCE: IEC 60050-192:2015, 192-03-01, modified – Notes to entry have been changed]
Failure mode [7]	Manner in which failure occurs. Note 1 to entry: A failure mode may be defined by the function lost or the state transition that occurred. [SOURCE: IEC 60050-192:2015, 192-03-17]
Fault [7]	Inability to perform as required, due to an internal state. Note 1 to entry: A fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the life-cycle, such as specification, design, manufacture or maintenance. Note 2 to entry: A fault of a device results in a failure when a particular set of circumstances is encountered. [SOURCE: IEC 60050-192:2015, 192-04-01, modified – Some notes to entry have been changed, others have been deleted]
Foundational requirement (FR) [28]	Requirement that provides a basis for technical requirements in all standards in the IEC 62443 series.
Functional safety [7]	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.
Hazard [7]	Potential source of harm. Note 1 to entry: The term includes danger to persons arising within a short time scale (e.g., fire and explosion) and also those that have a long-term effect on a person's health (e.g., release of a toxic substance or radioactivity). [SOURCE: ISO/IEC Guide 51:2014, 3.2, modified – Note 1 to entry has been added]
Human error [7]	Intended or unintended human action or inaction that produces an inappropriate result. Note 1 to entry: Mistakes, slips, and lapses are examples of human errors. Note 2 to entry: This excludes malicious action.
Implemented security level (SL-I) [28]	Security level of an automation solution that is designed and implemented based on the security requirements specified by the asset owner. Note 1 to entry: Implemented security level is determined during the integration phase of the security lifecycle.
Integrity [28]	State that connectivity, control, or safety have not been changed, destroyed or lost in an unauthorized or accidental manner.
Intrusion [28]	Unauthorized act of compromising a system. Note 1 to entry: See “attack.”
Intrusion detection [28]	security service that monitors and analyses system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner
Maturity level (ML) [28]	Qualitative indicator for characterizing the efficiency of an organization to implement requirements according to documented policies and procedures.

Term [reference]	Description/definition
Monitoring system [28]	Type of automation and control system that consolidates sensor measurements and displays them to an operator of the equipment under control.
Operational barrier element [10]	The actions or activities which personnel must perform in order to realize a barrier function.
Operational security level (SL-O) [28]	Security level of an ACS that is operated and maintained based on the security requirements specification. Note 1 to entry: Operational security level is determined during the operation and maintenance phases of the security lifecycle.
Organizational barrier element [10]	Personnel with defined roles or functions and specific competence involved in the realization of a barrier function.
Patch [28]	Update that corrects a specific defect. Note 1 to entry: A defect can cause a security vulnerability, reliability issue or operability issue. Note 2 to entry: An adjective may be used to describe the type of patch (e.g., security patch, reliability patch, operability patch).
Performance-influencing factors [10]	Factors identified as having significance for barrier functions and the ability of barrier elements to function as intended.
Performance requirement [10]	Verifiable requirement for the properties of the barrier elements in order to ensure that the barrier is effective.
Protection layer [7]	Any independent mechanism that reduces risk by control, prevention or mitigation. Note 1 to entry: It can be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical mechanism such as a relief valve, a SIS or an administrative procedure such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions (see Figure 9). [Not included]
Redundancy [7]	The existence of more than one means for performing a required function or for representing information. Note 1 to entry: Examples are the use of duplicate devices and the addition of parity bits. Note 2 to entry: Redundancy is used primarily to improve reliability or availability. [SOURCE: IEC 61508-4:2010, 3.4.6]
Reliability [28]	Ability of a system to perform a required function under stated conditions for a specified period. Note 1 to entry: Reliability is also defined as the probability that a system or component will perform its specified function under given conditions upon demand or for a prescribed period of time.
Risk [28]	Expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence.
Safety [28]	Freedom from unacceptable risk.
Safety function [28]	Control function with the purpose of protecting health, safety, environment, and the equipment under control. Note 1 to entry: Components with safety functions are developed, installed and maintained using the processes defined in IEC 61508 and IEC 61511.
Safety functions [11] FR § 3	Technical barrier elements that are intended to reduce the possibility of a concrete fault, hazard and accident situation occurring, or that limit or prevent damage or inconveniences.
Safety functions [11] FR § 8	Facilities shall be equipped with necessary safety functions that can at all times a) detect abnormal conditions, b) prevent abnormal conditions from developing into hazard and accident situations, c) limit the damage caused by accidents.
Safety integrity level (SIL) [28]	Discrete level (one out of four) for specifying the safety integrity requirements of the safety functions to be allocated to the safety systems. Note 1 to entry: Safety integrity level 4 has the highest level of safety integrity. safety integrity level 1 has the lowest.
Safety system [11]	Technical barrier elements that are realized in a common system.
Safety system [28]	A type of automation and control system that provides safety functions. EXAMPLE: Safety instrumented systems, fire alarm systems, fire and gas systems, automatic train protection systems, protective relays.
Security [28]	Condition of automation and control solution being free from unauthorized access and from unauthorized or accidental change, destruction or loss.

Term [reference]	Description/definition
	Note 1 to entry: Types of security are cyber security and physical security.
Security conduit [28]	Set of data flows between security zones that share common security requirements.
Security control [28]	See security measure. Note 1 to entry: "control" or "security control" are typically used for information systems security, but could be confused with "control system" or "control function."
Security event [28]	Occurrence in a system that is relevant to the security of the system.
Security incident [28]	Violation or imminent threat of violation of ACS security policies, acceptable use policies, or standard security practices.
Security level (SL) [28]	Set of security measures that supports a degree of risk reduction. Note 1 to entry: Security levels (SLs) are SL-1 – Low, SL-2 – Medium, SL-3 – High, and SL-4 - Very high. Note 2 to entry: Security level types are capability security level (SL-C), target security level (SL-T), implemented security level (SL-O), and operational security level (SL-O).
Security measure [28]	Measures taken to protect the safety, integrity, availability, and confidentiality of an automation and control solution and its equipment under control. Note 1 to entry: Security measures are implemented to meet security requirements. Note 2 to entry: Types of security measures are physical security measures, process security measures, or technical security measures.
Security protection rating (SPR) [28] *	Values that represent the outcome of the assessment of the fulfilment of security requirements of the CRS by the security measures of the security protection scheme.
Security zone [28]	Set of systems or components that share common security requirements. Note 1 to entry: Security zones can be physical or logical.
System under consideration (SuC) [28]	Defined collection of automation and control solutions and related assets for the purpose of performing a security risk assessment.
Target security level (SL-T)	Desired security level based on a risk assessment. Note 1 to entry: Target security level is determined during the design phase of the security lifecycle.
Technical barrier element [10]	Equipment and systems involved in the realization of a barrier function.
Threat [28]	Circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
Vulnerability [28]	Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy.
Zone [28]	See security zone.

* [28] uses the term "security program rating" in the list of definition. This is assumed to be a mistake. "Security protection rating" is used in the text.

Appendix B: Classification of requirements in IEC 62443-2-1

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
SPE 1 – Organizational security measures (ORG)						
ORG 1 – Security related organization and policies						
ORG 1.1: Information security management system (ISMS)	If the asset owner has an ISMS, the asset owner shall coordinate the IACS SP with the ISMS. If the asset owner does not have an ISMS, the asset owner shall incorporate the appropriate management processes into the IACS SP.				X	A general cybersecurity aspect that is not specifically linked to barriers.
ORG 1.2: Background checks	The asset owner shall have policies and procedures about performing background checks on all personnel who require access to the IACS (including employees, contractors, subcontractors, consultants, product suppliers and service providers) prior to granting them access to the IACS. Where feasible and allowed by applicable law, such background checks shall include identity verification and criminal records checks.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations through insiders.
ORG 1.3: Security roles and responsibilities	The asset owner shall have policies and procedures around defining and assigning security roles and responsibilities to qualified personnel, including employees, contractors, subcontractors and consultants.				X	A general cybersecurity aspect that is not specifically linked to barriers.
ORG 1.4: Security awareness training	The asset owner shall have policies and procedures requiring all personnel (including employees, contractors, subcontractors, consultants, product suppliers and service providers) who interact with the IACS receive formal cybersecurity awareness training that is updated on a regular basis.			X		Training is considered a PIF for people / organizational barrier elements.
ORG 1.5: Security responsibilities training	The asset owner shall have policies and procedures requiring all personnel (including employees, contractors, subcontractors, consultants, product suppliers and service providers) who interact with the IACS receive formal cybersecurity training that is relevant to their IACS cybersecurity responsibilities. Such training shall either be accepted or provided by the asset owner.			X		Training is considered a PIF for people / organizational barrier elements.
ORG 1.6: Supply chain security	The asset owner shall have policies and procedures that specify requirements for suppliers of products and services addressing cybersecurity risks to the IACS. The asset owner policies and procedures shall consider recursive requirements on the suppliers, where feasible.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations through the supply chain.
ORG 2 – Security assessments and reviews						
ORG 2.1: Security risk mitigation	The asset owner shall have policies and procedures around identifying, documenting, and mitigating or otherwise managing IACS cybersecurity risks, including determining a tolerable risk level and responding to risks outside that tolerable risk level.	X				Safe and robust practice. Accepting the risk of getting into failure, hazard and accident situations.

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
ORG 2.2: Processes for discovery of security anomalies	The asset owner shall have policies and procedures related to periodically discovering and addressing, through manual or automated processes: a) undocumented and unauthorized components/software connected to or communicating within the IACS, b) undocumented and/or unauthorized network traffic, c) new and/or known but undocumented vulnerabilities in the IACS, and d) other security anomalies and non-conformities.	X	**X**			Processes intended to identify conditions outside normal operation. The "first barrier". However, c) new vulnerabilities in the IACS are "normal operation", as this is the nature of software. (Patching is the remedy and should also be considered part of "normal operation".)
ORG 2.3: Secure development and support	The asset owner shall have policies and procedures addressing the use of a secure development lifecycle process for the development and support of systems and components used in the IACS.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations during development and support (cf. Part 4-1).
ORG 2.4: SP reviews	The asset owner shall have policies and procedures related to periodically reviewing the SP to: a) verify that it is being properly applied, b) validate that the technical and process security measures continue to meet the system security requirements, c) address changes in the organization and its processes, technical changes in the Automation Solution and changes in the threat environment, and d) make improvements, as appropriate.				X	A general cybersecurity aspect that is not specifically linked to barriers (although it includes barriers).
ORG 3 – Security of physical access						
ORG 3.1: Physical access control	The asset owner shall have policies and procedures around physical access to the IACS, including access to facilities, equipment and cabling, is controlled to meet risk targets.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations through unauthorized physical access.
SPE 2 – Configuration management (CM)						
CM 1 – Inventory management of IACS hardware/ software components and network communications						
CM 1.1: Asset inventory baseline	The asset owner shall have policies and procedures to document, verify and maintain, throughout the full life cycle of the IACS, the inventory baseline of all devices, hardware components, software components, communications protocols and open communications ports used in the IACS to include, but are not limited to: a) organizational responsibilities, b) manufacturer, c) model, d) version numbers, e) serial numbers, f) network interfaces, g) communication addresses, h) revision/patch levels, and i) history.	**X**		X		Safe and robust solution. Avoid getting into failure, hazard and accident situations by having an overview of the assets ("knowing what you have"). It will also be of help in a failure, hazard or accident situation, i.e., it will be of significant help to manage an attack. (This is a PIF for the barrier functions deduced from the requirements that addresses the management of an attack. This mapping has so far not been performed.)

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
CM 1.2: Infrastructure drawings/documentation	The asset owner shall have policies and procedures to verify and maintain the current baseline of drawings/documentation showing the physical and logical connectivity of all IACS devices and software components.	X		X		Safe and robust solution. Avoid getting into failure, hazard and accident situations by having an overview of connectivity. It will also be of help in a failure, hazard or accident situation, i.e., it will be of significant help to manage an attack.
CM 1.3: Configuration settings	The asset owner shall have policies and procedures to document the configuration settings of all IACS devices and software applications and to verify their operational compliance with the documented configuration.	**X**		X		Safe and robust solution. Avoid getting into failure, hazard and accident situations by having correct configuration settings. This also applies to technical barrier elements, and verification of compliance is a PIF.
CM 1.4: Change control	The asset owner shall have policies and procedures to authorize, validate and approve changes to the current configuration baseline and infrastructure drawings/documentation, including revision and patch levels.	**X**		X		Safe and robust solution. Avoid getting into failure, hazard and accident situations by change management. This also applies to technical barrier elements, and changes may affect the performance, i.e. it may be a PIF.
SPE 3 – Network and communications security (NET)						
NET 1 – System segmentation						
NET 1.1: Segmentation from non-IACS zones	The asset owner shall have policies and procedures segmenting IACS from non-IACS zones and limiting any interconnections to the minimum necessary for IACS operations and within tolerable risk.		**X**			It is a barrier preventing events developing and limit damage or loss. (The segregation and containment functionality is not relevant to normal operation.)
NET 1.2: Documentation of zones and network zone interconnections	The asset owner shall have policies and procedures about documenting and maintaining a baseline of all IACS zones and network zone interconnections and/or conduits, the security risks associated with each, their designation as trusted or untrusted, the SL-T and the SPR for each.	X		X		Safe and robust solution. Avoid getting into failure, hazard and accident situations by having an overview of zones and interconnections. It will also be of help in a failure, hazard or accident situation, i.e., it will be of significant help to manage an attack.
NET 1.3: Network segmentation from safety systems	If the IACS contains a safety system network, the asset owner shall have policies and procedures related to protecting the safety system from interference by non-safety system networks and their devices.		X			It is a barrier preventing events developing and limit damage or loss.
NET 1.4: Network autonomy	If external network connections are not necessary for essential functions, the asset owner shall have policies and procedures around the ability to operate the IACS as designed when disconnected from external networks (for example, fail-safe operation, safe shut down, restricted operation and normal operation).		X	(X)		Disconnecting the asset from external networks is not part of normal operation. It is a barrier. (It also affects the possibility of staying within normal operation, or at some degraded / abnormal situation/operation, not directly the performance, but whether a barrier is activated or not.)

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
NET 1.5: Network disconnection from external networks	If external network connections are not necessary for essential functions, the asset owner shall have policies and procedures around the ability to disconnect the IACS from external networks to protect itself or the external networks from actual or suspected threats.		X			This is a barrier function, to prevent an actual sequence of events occurring or developing, influence a sequence of events in a deliberate way, or limit damage and/or loss.
NET 1.6: Internal network access control	The asset owner shall have policies and procedures around identifying, documenting, and mitigating or otherwise managing security risks associated with communications between internal IACS network segments, including determining a tolerable risk level and responding to risks outside that tolerable risk level.		**X**			It is a barrier preventing events developing and limit damage or loss. (Protecting against unintended flow of information).
NET 1.7: Network accessible services	The asset owner shall have policies and procedures around protecting network accessible services from unauthorized network access.	**X**				It is a safe and robust solution, avoiding getting outside of normal operation.
NET 1.8: User messaging	The asset owner shall have policies and procedures around restricting the capability of user-to-user messages transferred on IACS networks from containing payloads, such as attachments, network links or scripts, that can be used to support attacks against the IACS.	X				It is a safe and robust solution to prevent getting malware into the network.
NET 1.9: Network time distribution	The asset owner shall have policies and procedures around securely distributing and synchronizing time within the IACS.	**X**		X		It is a safe and robust solution, which also should include some protection against tampering.
NET 2 – Secure wireless access						
NET 2.1: Wireless protocols	The asset owner shall have policies and procedures about the use of wireless communications within the IACS and which industry accepted protocols are authorized for use, if any. Any wireless protocol(s) shall be documented, and this documentation maintained to include: a) a current baseline configuration of each, b) data exchanges with other network segments, and c) security capabilities and features employed by each wireless network.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by having an overview of the wireless networks and protocols.
NET 2.2: Wireless network segmentation	If wireless communications are authorized for use in the IACS, the asset owner shall have policies and procedures around segmenting wireless networks from other IACS network segments.		**X**			It is a barrier preventing events developing and limit damage or loss.
NET 2.3: Wireless properties and addresses	If wireless communications are authorized for use in the IACS, the asset owner shall have policies and procedures around configuring wireless networks with properties and network addresses that minimize information useful to attackers.		X			It is a barrier preventing events developing and limit damage or loss.
NET 3 – Secure remote access						
NET 3.1: Remote access applications	If remote access is authorized for use in the IACS, the asset owner shall have policies and procedures around the use of commonly accepted remote access applications in the IACS.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by having commonly accepted remote access applications.

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
NET 3.2: Remote access connections	If remote access is authorized for use in the IACS, the asset owner shall have policies and procedures around authorizing, authenticating, encrypting, documenting, logging and monitoring all interactive remote access connections. Documentation for each connection shall include, but not be limited to: a) its purpose, b) the remote access application to be used, c) encryption and authentication technologies used, d) how the connection will be established (for example, via the Internet through a virtual private network (VPN) through a DMZ) with instructions, as necessary, e) the circumstances requiring the connection, f) the length of time the connection needs to be open, including expected inactivity periods, g) the location and identity of the remote client device, application and user, and h) any compliance requirements that need to be met prior to establishing the connection.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by having overview of remote access connections.
NET 3.3: Remote access termination	If remote access is authorized for use in the IACS, the asset owner shall have policies and procedures around terminating all interactive remote access connections after a configured inactivity period.		**X**			Restricting remote access across zone boundaries. (Reduce potential for unauthorized access). This is a barrier. Normal operation would be that the user logs out (but we sometimes forget...). It is a barrier protecting the system from human errors.
SPE 4 – Component security (COMP)						
COMP 1 – Components and portable media						
COMP 1.1: Component hardening	The asset owner shall have policies and procedures to harden components prior to their use in the IACS to protect their software and hardware features, to maintain the hardened state during the lifetime of the components and to maintain the documentation of hardening items, means and procedures of the components.	**X**				Safe and robust solution. Avoid getting into failure, hazard and accident situations by removing or disabling unnecessary features.
COMP 1.2: Dedicated portable media	The asset owner shall have policies and procedures related to the approved or disapproved use or functions of portable media within the IACS.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by the use of dedicated portable media.
COMP 2 – Malware protection						
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				Safe and robust solution. Avoid getting into failure, hazard and accident situations by ensuring malware are not present prior to use.
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**			It is a barrier preventing events developing by detecting malware and preventing them from executing.
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		Testing affects the performance of the anti-malware (the barrier); thus, it is a PIF (it has a significant impact). It is a PIF for COMP 2.2.

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
COMP 3 – Patch management						
COMP 3.1: Security patch authenticity/integrity	The asset owner shall have policies and procedures related to verifying the authenticity and integrity of all patches prior to installation.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by ensuring that patches have not been tampered with prior to installation.
COMP 3.2: Security patch validation and installation	The asset owner shall have policies and procedures related to the testing for compatibility, approval and installation of security patches applicable to components in a timely manner after their release.	X		(X)		Safe and robust solution. Avoid getting into failure, hazard and accident situations by ensuring that patches are compatible (in a timely manner) prior to installation. For patches of barrier elements, this affects the performance of the barriers, i.e., it may also be a PIF (for any barrier elements).
COMP 3.3: Security patch status	The asset owner shall have policies and procedures related to the documentation and maintenance of the security patch status of all components.	X		(X)		Safe and robust solution. Avoid getting into failure, hazard and accident situations by having an overview of the patch status. It will also be of help in a failure, hazard or accident situation, i.e., it will be of significant help to manage a vulnerability or an attack.
COMP 3.4: Security patching retention of security	The asset owner shall have policies and procedures to verify that security patch installation does not cause a reduction in the security of the component.	X		(X)		Safe and robust solution. Avoid getting into failure, hazard and accident situations by ensuring that patches do not affect the functioning of the component. For patches of barrier elements, this affects the performance of the barriers, i.e., it may also be a PIF.
COMP 3.5: Security patch mitigation	The asset owner shall have policies and procedures related to assessing the risk of not installing any applicable security patches, and if the risk is not tolerable, addressing the risk and documenting the resolution.	X		(X)		Safe and robust solution. Avoid getting into failure, hazard and accident situations by risk assessing and compensating for non-installed patches. For patches of barrier elements, this affects the performance of the barriers, i.e., it may also be a PIF.
SPE 5 – Protection of data (DATA)						
DATA 1 – Protection of data						
DATA 1.1: Data classification	The asset owner shall have policies and procedures related to identifying and classifying all IACS data requiring safeguarding according to their protection requirements.	**X**		(X)		Safe and robust solution. Avoid getting into failure, hazard and accident situations by protecting relevant data. For data of barrier elements, this affects the performance of the barriers, i.e., it may also be a PIF. This is a PIF

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
						for barrier functions/elements derived from technical backup/recovery requirements.
DATA 1.2: Data confidentiality	The asset owner shall have policies and procedures related to the confidentiality of IACS data taking into account risks to compromise of the data according to their classification.		**X**			Protecting information (flow) has similarities with containment of energy flow, which is considered a barrier. In practice, this means encryption.
DATA 1.3: Safety system configuration mode	If safety systems are authorized for use in the IACS, the asset owner shall have policies and procedures related to: a) updating the safety system configuration only when configuration mode is enabled, and b) only enabling configuration mode when configuration changes are necessary.		X	X		Configuration mode of safety systems (barriers) affects the performance of the barriers, i.e., it can be considered a PIF. It may also be considered a barrier in that it may reduce or slow an intruder's possibility to change the configuration settings.
DATA 1.4: Data retention policy	The asset owner shall have policies and procedures related to data retention during the entire IACS lifecycle, including purging.		**X**			This is containment (to avoid unauthorized/ unintended flow of information) therefore it is a barrier
DATA 1.5: Cryptographic mechanisms	The asset owner shall have policies and procedures related to utilizing commonly accepted cryptographic mechanisms in the IACS.		**X**			Encryption is about containment of information, which is considered a barrier. The encryption itself does not change the flow of information during normal operation, but it does prevent against unintended flow of information (eavesdropping etc.)
DATA 1.6: Key management	If cryptographic mechanisms utilizing keys are approved for use in the IACS, the asset owner shall have policies and procedures around using, protecting and enforcing the lifetime of cryptographic keys follow practices and recommendations commonly accepted by both the industrial and security communities.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by proper key management (if keys are allowed).
DATA 1.7: Data integrity	The asset owner shall have policies and procedures related to data integrity protection from compromise, whether at rest or in motion (electronically or physically), that takes into account applicable risks.		X			Protection of information. Protection against transmission errors.
SPE 6 – User access control (USER)						
USER 1 – Identification and authentication						
USER 1.1: User identity assignment	The asset owner shall have policies and procedures for assigning IACS-specific identifiers, authenticators and roles to users (human users, software processes and devices).	**X**				Safe and robust solution. Avoid getting into failure, hazard and accident situations by assigning user identity for legitimate users.
USER 1.2: User identity removal	The asset owner shall have policies and procedures for removing/disabling IACS-specific identifiers, authenticators, roles and access rights for human users, software processes and devices that do not or no longer need access.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by removing unnecessary access paths.

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
USER 1.3: User identity persistence	The asset owner shall have policies and procedures to verify that IACS-specific user identifiers, authenticators, roles and their associated access rights that are used to support essential IACS operations, including operator accounts, are configured so they are not disabled automatically.	X		(X)		Safe and robust solution. Avoid getting into failure, hazard and accident situations by not allowing automatic removal of users. This can lead to DoS of essential operations; thus, it may affect the performance of a barrier (being an essential operation).
USER 1.4: Access rights assignment	The asset owner shall have policies and procedures for assigning, reviewing and removing access rights to/from IACS-specific roles and users.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by giving explicit access rights (to users/roles).
USER 1.5: Least privilege	The asset owner shall have policies and procedures to verify that IACS users are only granted the access rights that they require to perform their assigned tasks.	**X**				Safe and robust solution. Avoid getting into failure, hazard and accident situations by giving only needed access rights, which also limits potential attack surface.
USER 1.6: Software service authentication	The asset owner shall have policies and procedures related to identifying and authenticating software services prior to their execution.	**X**				Safe and robust solution. Avoid getting into failure, hazard and accident situations by not allowing to start the software before identifying and authenticating it.
USER 1.7: Software services interactive login rights	The asset owner shall have policies and procedures related to denying software services interactive login capabilities.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by setting interactive login capabilities to disallowed.
USER 1.8: Human user authentication	The asset owner shall have policies and procedures related to identifying and authenticating all human users on all IACS interfaces that can be used by human users to access the IACS. This includes but is not limited to: a) device interactive human user login interfaces, b) application interfaces such as web services, file transfers and OPC servers, and c) remote desktop interfaces that provide human users login access to IACS devices over the network. NOTE Some OSs manage the conveyance of the authenticated user identity transparently to the application and make the user identity available to the application.	**X**				Safe and robust solution. Avoid getting into failure, hazard and accident situations by not allowing e.g. guest and anonymous accounts used in the IACS. Part of normal operation (of flow of information).
USER 1.9: Multifactor authentication (MFA)	The asset owner shall have policies and procedures related to using MFA by devices that support interactive human user login for remote access or when they are located in public access areas.		X			Presumably, MFA exists only to protect against situations where the user/password information has leaked to other unauthorized parties (unintended flow of information) and is being used for exploitation. I.e., it is a barrier.
USER 1.10: Mutual authentication	The asset owner shall have policies and procedures related to using mutual authentication for access to all server applications hosted on IACS devices, including web technology-based servers.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by reducing the possibility of spoofing through mutual authentication.

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
USER 1.11: Password protection	When passwords are used in the IACS, the asset owner shall have policies and procedures to increase the degree of difficulty to compromise passwords, including complexity, lifetime and reuse.	**X**				Safe and robust solution. Avoid getting into failure, hazard and accident situations by using password policies making it difficult to compromise the password.
USER 1.12: Shared and disclosed/compromised passwords	The asset owner shall have policies and procedures for managing shared and disclosed/compromised passwords.		X			Compromised passwords imply unintended flow of information; thus, it is a barrier.
USER 1.13: User login display information	The asset owner shall have policies and procedures to display login information to the user to assist in the detection of fraudulent logins.		**X**			It is a barrier assisting in the detection of fraudulent logins.
USER 1.14: User login failure displays	The asset owner shall have policies and procedures related to displaying information following a login failure to limit the information useful to attackers.		**X**			To protect the information from possible exploitation by unauthorized individuals.
USER 1.15: Consecutive login failures	The asset owner shall have policies and procedures related to denying login access to user accounts for a specified length of time or until unlocked by an authorized administrator after the configured number of consecutive unsuccessful login attempts have occurred.		**X**			To protect against unauthorized access. This is not considered normal operation since repeated, failed login attempts is not a normal flow of information.
USER 1.16: Session integrity	The asset owner shall have policies and procedures related to protecting sessions from unauthorized access and modification.		**X**			To avoid man-in-the-middle attack. Prevents unauthorized access.
USER 1.17: Concurrent sessions	The asset owner shall have policies and procedures related to limiting the number of concurrent sessions per interface for any given human user, software process or device.	**X**				Safe and robust solution. Avoid getting into failure, hazard and accident situations by limiting the number of concurrent sessions.
USER 1.18: Screen lock	The asset owner shall have policies and procedures related to locking user screens upon user request or automatically after a configured period of inactivity unless failure to access the screen can result in a greater risk to the IACS. Re-authentication shall be required of an authorized user to unlock it.	**X**				Safe and robust solution. Avoid getting into failure, hazard and accident situations by using screen locks when appropriate.
USER 1.19: Component authentication	The asset owner shall have policies and procedures related to identifying and authenticating all components connected to the IACS.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by requiring component's ability to be authenticated.
USER 2 – Authorization and access control						
USER 2.1: Authorization	The asset owner shall have policies and procedures related to enforcing assigned access rights for all users.	**X**				Safe and robust solution. Avoid getting into failure, hazard and accident situations by enforcing assigned access rights to prevent by-passing.
USER 2.2: Separation of duties	The asset owner shall have policies and procedures related to separation of duties, reducing the privileges assigned to IACS users to the minimum needed.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by separation of duties using the least privilege principle.

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
USER 2.3: Multiple approvals	The asset owner shall have policies and procedures to verify that approval by two or more users are required for actions that can result in serious impact to the industrial process, unless failure to perform the action can result in a greater impact to the industrial process.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by requiring multiple approvals for critical actions.
USER 2.4: Manual elevation of privileges	The asset owner shall have policies and procedures related to requiring explicit elevation of privileges, including supervisor overrides, for all operations that require elevated privileges.	X				Safe and robust solution. Avoid getting into failure, hazard and accident situations by manual elevation of privilege and authorization of the operation.
SPE 7 – Event and incident management (EVENT)						
EVENT 1 – Event and incident management						
EVENT 1.1: Event detection	The asset owner shall have policies and procedures related to the reporting, logging, analysis and response (immediate or delayed) of IACS security-related events that are detected to support security management activities.		**X**			Event detection is a barrier function.
EVENT 1.2: Event reporting	The asset owner shall have policies and procedures related to reporting IACS security-related events in a timely manner.		**X**			Event "reporting" (warning/notification) as a basis for deciding on actions is a barrier function.
EVENT 1.3: Event reporting interfaces	The asset owner shall have policies and procedures around utilizing interfaces commonly accepted by the industrial and security communities for reporting IACS security-related events.		**X**			Event reporting interfaces contribute to better understanding and appropriate response; thus, it is a barrier system/function.
EVENT 1.4: Logging	The asset owner shall have policies and procedures related to writing IACS security-related events to one or more protected event/audit logs and retaining them for an adequate time period.		**X**			Event logging contributes to detection and support event response; thus, it is a barrier function.
EVENT 1.5: Log entries	The asset owner shall have policies and procedures about the information contained in IACS security-related audit and event log entries to support non-repudiation and time-correlated analysis of events.			**X**		Information contained in the event log entries supports review and analysis, i.e., it affects detection and decision of actions (barrier functions). Thus, it is a PIF.
EVENT 1.6: Log access	The asset owner shall have policies and procedures around utilizing interfaces commonly accepted by the industrial and security communities to access IACS security-related audit and event logs.	**X**				For after-the-fact investigation. Will not stop the event sequence there and then.
EVENT 1.7: Event analysis	The asset owner shall have policies and procedures around the analysis of IACS security related events to identify and characterize attacks, security compromises and security incidents in a timely manner.		X			Event analysis is, in addition to detection and response, a necessary part of the handling of events. Event analysis for immediate response is a barrier (sub)function.

Sub-elements	Requirements	Normal operation	Barrier	PIF	Other	Assessment
EVENT 1.8: Incident handling and response	The asset owner shall have policies and procedures for employing and keeping current a process for evaluating and responding to IACS security-related incidents.		X			The immediate handling of, and response to, a security incident is the "final" barrier (sub)function in managing events/incidents.
EVENT 1.9: Vulnerability handling	The asset owner shall have policies and procedures related to identifying, addressing and resolving existing and newly identified IACS vulnerabilities in a timely manner.		X			The handling of newly identified vulnerabilities is a barrier function. The situation is outside normal operation.
SPE 8 – System integrity and availability (AVAIL)						
AVAIL 1 – System availability and intended functionality						
AVAIL 1.1: Continuity management	The asset owner shall have policies and procedures related to employing and keeping current a site disaster recovery plan (DRP), business continuity plan (BCP) or both, that includes disaster scenarios, failure handling procedures and processes for maintaining the required level of operational continuity.		X			Recovery and continuity are barrier functions. The situation is outside normal operation and needs to be "normalized". DRPs and BCPs can be considered operational barrier elements.
AVAIL 1.2: Resource availability management	The asset owner shall have policies and procedures related to protecting the IACS from resource/equipment failures due to power disruptions, unintentional capacity/processing overloads, hardware failures and intentional DoS attacks. These policies and procedures shall also consider remediation actions, such as device replacement.		**X**			Resource availability management, such as handling capacity overloads, is mainly a barrier function. It covers techniques such as redundancy, alarms, segmentation, filtering and firewalls.
AVAIL 1.3: Failure-state	The asset owner shall have policies and procedures related to bringing the IACS to a predetermined state if normal operation cannot be maintained as a result of a detected security compromise.		**X**			A manual or automated process of bringing the IACS to a predetermined "fail-secure" state is a barrier function (like ESD).
AVAIL 2 – Backup/restore/archive						
AVAIL 2.1: Backup	The asset owner shall have policies and procedures related to backing up the IACS at regular intervals to support recovery to a stable state.		**X**			Backing-up the IACS at regular intervals support recovery also from an attack (cf. SR 7.3 in Appendix C).
AVAIL 2.2: Backup non-interference	The asset owner shall have policies and procedures validating that backup processes do not adversely affect normal operations of the IACS.	**X**				Validating that the backup process does not interfere with normal operations is a safe and robust solution.
AVAIL 2.3: Backup verification	The asset owner shall have policies and procedures to verify the integrity of backup data at the completion of the backup and periodically after the backup.			**X**		Verification of the integrity of backup data is related to AVAIL 2.1 (and SR 7.3 RE 1).
AVAIL 2.4: Backup media	The asset owner shall have policies and procedures around handling and storing backup media in a safe and secure manner to ensure its integrity, authenticity and availability when needed and the confidentiality of the data is maintained.	X				Storage and protection of backup media is a safe and robust solution.
AVAIL 2.5: Backup restoration	The asset owner shall have policies and procedures related to restoring the IACS from a backup to a stable state in a timely manner.		**X**	X		Backup restoration in itself is a barrier function, whereas periodically tests to ensure that the backup works as intended is a PIF.

The bold cross marks indicate some degree of overlap with IEC 62443-3-3. This is based on the cross-references provided in IEC 62443-2-1 Annex A.2 (Table 91). This means that similar requirements are found in IEC 62443-3-3 documented in Appendix C below. It should be noted that the cross-references are sometimes not directly comparable, or only partly overlapping, which means that the classification may be different between Part 2-1 (Appendix B) and Part 3-3 (Appendix C).

33 of the 87 requirements (38 %) are related to barriers. 27 are only related to barriers, whereas 3 are related to both barriers and PIFs, and 1 is also related to normal operation.

The distribution of the various categories (with some requirements relevant for more than one category) is:

- Normal operation: 47
- Barrier: 33
- PIF: 20
- Other: 3

Appendix C: Classification of requirements in IEC 62443-3-3

FR	Req. ID	Requirement title	SL	Requirement	Normal operation	Barrier	PIF	Other	Comments
FR 1 – Identification and authentication control (IAC)									
FR 1 - IAC	SR 1.1	Human user identification and authentication	1	The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	X				Part of normal operation (of flow of information). (Normal) control of information flow requires (normal) control of human users.
FR 1 - IAC	SR 1.1 RE 1	Unique identification and authentication	2						
FR 1 - IAC	SR 1.1 RE 2	Multifactor authentication for untrusted networks	3						
FR 1 - IAC	SR 1.1 RE 3	Multifactor authentication for all networks	4						
FR 1 - IAC	SR 1.2	Software process and device identification and authentication	2	The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.	X				Part of normal operation (of flow of information). (Normal) control of information flow requires (normal) control of software processes and devices.
FR 1 - IAC	SR 1.2 RE 1	Unique identification and authentication	3						
FR 1 - IAC	SR 1.3	Account management	1	The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.	X				Part of normal operation (of flow of information) through the control of user accounts.
FR 1 - IAC	SR 1.3 RE 1	Unified account management	3						
FR 1 - IAC	SR 1.4	Identifier management	1	The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.	X				Part of normal operation (of flow of information) through identifier management.
FR 1 - IAC	SR 1.5	Authenticator management	1	The control system shall provide the capability to: a) initialize authenticator content; b) change all default authenticators upon control system installation; c) change/refresh all authenticators; and d) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	X				Part of normal operation (of flow of information) through authenticator management.
FR 1 - IAC	SR 1.5 RE 1	Hardware security for software process identity credentials	3						

FR	Req. ID	Requirement title	SL	Requirement	Normal operation	Barrier	PIF	Other	Comments
FR 1 - IAC	SR 1.6	Wireless access management	1	The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	X				Part of normal operation (of flow of information). (Normal) control of information flow requires (normal) control of all users engaged in wireless communication.
FR 1 - IAC	SR 1.6 RE 1	Unique identification and authentication	2						
FR 1 - IAC	SR 1.7	Strength of password-based authentication	1	For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.	X				Part of normal operation (of flow of information). (Normal) control of information flow requires (normal) control of human users' password-based authentication.
FR 1 - IAC	SR 1.7 RE 1	Password generation and lifetime restrictions for human users	3						
FR 1 - IAC	SR 1.7 RE 2	Password lifetime restrictions for all users	4						
FR 1 - IAC	SR 1.8	Public key infrastructure certificates	2	Where PKI is utilized, the control system shall provide the capability to operate a KPI according to commonly accepted best practices or obtain public key certificates from an existing PKI.	X				Controlling/regulating flow of information to avoid getting into a failure, hazard or accident situation, i.e., part of normal operation.
FR 1 - IAC	SR 1.9	Strength of public key authentication	2	For control systems utilizing public key authentication, the control system shall provide the capability to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate certificates by constructing a certification path to an accepted CA or in case of self-signed certificates by deploying leaf certificates to all hosts which communicate with subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software or device) control of the corresponding private key; and e) map the authenticated identity to a user (human, software process or device).	X				Controlling/regulating flow of information to avoid getting into a failure, hazard or accident situation, i.e., part of normal operation.
FR 1 - IAC	SR 1.9 RE 1	Hardware security for public key authentication	3						
FR 1 - IAC	SR 1.10	Authenticator feedback	1	The control system shall provide the capability to obscure feedback of authentication information during the authentication process.	?	X			To protect the information from possible exploitation by unauthorized individuals. This requirement prevents uncontrolled flow of information, which is not part of normal operation, since the requirement does not relate to normal flow of information (which would be the flow from a keyboard into the

FR	Req. ID	Requirement title	SL	Requirement	Normal operation	Barrier	PIF	Other	Comments
									system being logged into - use-case: login-prompt).
FR 1 - IAC	SR 1.11	Unsuccessful login attempts	1	The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time until unlocked by an administrator when this limit has been exceeded. For system accounts on behalf of which critical services or servers are run, the control system shall provide the capability to disallow interactive logons.		**X**			To protect against unauthorized access. This is not considered normal operation since repeated, failed login attempts is not a normal flow of information. And it is considered a barrier, since a mechanism which protects against brute-force attacks is not relevant to the normal operation of the system.
FR 1 - IAC	SR 1.12	System use notification	1	The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	**X**				It "does not improve IACS security" (cf. guidance).
FR 1 - IAC	SR 1.13	Access via untrusted networks	1	The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.		X			Monitoring of flow of information in the context of this requirement is conducted with the implicit purpose of detecting abnormal access, which is detection, and thus a barrier.
FR 1 - IAC	SR 1.13 RE 1	Explicit access request approval	2						
FR 2 – Use control (UC)									
FR 2 - UC	SR 2.1	Authorization enforcement	1	On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.	**X**				Controlling the normal use of the control system. (applies to all, including own personnel).
FR 2 - UC	SR 2.1 RE 1	Authorization enforcement for all users	2						
FR 2 - UC	SR 2.1 RE 2	Permission mapping to roles	2						
FR 2 - UC	SR 2.1 RE 3	Supervisor override	3						
FR 2 - UC	SR 2.1 RE 4	Dual approval	4						
FR 2 - UC	SR 2.2	Wireless use control	1	The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.	**X**	**X**			Controlling the normal use of the control system. The monitoring part is detection and therefore a barrier (cf. SR 1.13).
FR 2 - UC	SR 2.2 RE 1	Identify and report unauthorized wireless devices	3						

FR	Req. ID	Requirement title	SL	Requirement	Normal operation	Barrier	PIF	Other	Comments
FR 2 - UC	SR 2.3	Use control for portable and mobile devices	1	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			Restricting the use/access to the control system. (Prevent potential undesired network traffic, malware and/or information exposure). This is part of normal operation since it is controlling normal use of the control system (ref. "requiring context specific authorization"), similarly to SR 2.2 (use-case: periodically using a portable device to obtain measurements from sensors). It is a barrier since use of mobile devices, and flow of information to/from mobile devices, is otherwise (excluding the use-case above) not normal operation (best-case it is maintenance, worst-case it is an attack).
FR 2 - UC	SR 2.3 RE 1	Enforcement of security status of portable and mobile devices	3						
FR 2 - UC	SR 2.4	Mobile code	1	The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system that include a) preventing the execution of mobile code; b) requiring proper authentication and authorization for origin of the code; c) restricting mobile code transfer to/from the control system; and d) monitoring the use of mobile code.	X	X			Usage restrictions (to avoid potential damage to the control system). This is normal operation since mobile code transfer may be part of normal operation (e.g. opening a web-interface from a browser on a separate computer, but both hosts are inside the control system). This is also a barrier since the system shall prevent mobile code from being transferred from outside the control system into the control system (someone attempting to use a browser on a control system computer to access a web-interface outside the control system, which is not normal operation).
FR 2 - UC	SR 2.4 RE 1	Mobile code integrity check	3						
FR 2 - UC	SR 2.5	Session lock	1	The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session, or another authorized human user re-establishes access using appropriate identification and authentication procedures.		X			Restricting access to specified workstations or nodes. (Reduce potential for unauthorized access). This is a barrier. Normal operation would be that the user logs out (but we sometimes forget...). It is a barrier protecting the system from human errors.

FR	Req. ID	Requirement title	SL	Requirement	Normal operation	Barrier	PIF	Other	Comments
FR 2 - UC	SR 2.6	Remote session termination	2	The control system shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.		**X**			Restricting remote access across zone boundaries. (Reduce potential for unauthorized access). This is a barrier. Normal operation would be that the user logs out (but we sometimes forget...). It is a barrier protecting the system from human errors.
FR 2 - UC	SR 2.7	Concurrent session control	3	The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software or device) to a configurable number of sessions.	X				Usage control (and limit potential of resource starvation DoS).
FR 2 - UC	SR 2.8	Auditable events	1	The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.	X	**X**			Only parts of this is a barrier; messages such as "Operating system events" can be disk failures, fan-failures, power-supply failures, network link failure etc. Meaning normal wear and tear for a control system, which is related to security since they affect "availability". To detect and handle these events is normal operation. For other messages such as access control, configuration changes, backup/restore events etc., these are very much audit log events and used to detect / investigate abnormal behavior. Monitoring these types of events is a barrier (the audit log messages have no value / interest as long as the system is only exposed to normal operation).
FR 2 - UC	SR 2.8 RE 1	Centrally managed, system-wide audit trail	3						
FR 2 - UC	SR 2.9	Audit storage capacity	1	The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.	**X**				Normal "secure and robust" solution.
FR 2 - UC	SR 2.9 RE 1	Warn when audit record storage capacity threshold reached	3						

FR	Req. ID	Requirement title	SL	Requirement	Normal operation	Barrier	PIF	Other	Comments
FR 2 - UC	SR 2.10	Response to audit processing failures	1	The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	**X**				Audit processing after the fact.
FR 2 - UC	SR 2.11	Timestamps	2	The control system shall provide timestamps for use in audit record generation.	X				Necessary for audit record generation.
FR 2 - UC	SR 2.11 RE 1	Internal time synchronization	3						
FR 2 - UC	SR 2.11 RE 2	Protection of time source integrity	4						
FR 2 - UC	SR 2.12	Non-repudiation	3	The control system shall provide the capability to determine whether a given human user took a particular action.		**X**			Avoids denial of responsibility for actions. This avoidance is a barrier (cf. SR 3.9).
FR 2 - UC	SR 2.12 RE 1	Non-repudiation for all users	4						
FR 3 – System integrity (SI)									
FR 3 - SI	SR 3.1	Communication integrity	1	The control system shall provide the capability to protect the integrity of transmitted information.	X	**X**			Protection of information. Protection against transmission errors. Basic integrity mechanisms are part of robust normal operation, but sophisticated integrity mechanisms are considered barriers.
FR 3 - SI	SR 3.1 RE 1	Cryptographic integrity protection	3						
FR 3 - SI	SR 3.2	Malicious code protection	1	The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.		**X**			Prevention, detection and/or mitigation of malware. (Nothing to do with normal operation).
FR 3 - SI	SR 3.2 RE 1	Malicious code protection on entry and exit points	2						
FR 3 - SI	SR 3.2 RE 2	Central management and reporting for malicious code protection	3						
FR 3 - SI	SR 3.3	Security functionality verification	1	The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.			**X**		Scheduled maintenance is a PIF (or provide information about the performance, i.e., supporting verification). It affects several functions and requirements.
FR 3 - SI	SR 3.3 RE 1	Automated mechanisms for security functionality verification	3						

FR	Req. ID	Requirement title	SL	Requirement	Normal operation	Barrier	PIF	Other	Comments
FR 3 - SI	SR 3.3 RE 2	Security functionality verification during normal operation	4						
FR 3 - SI	SR 3.4	Software and information integrity	2	The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.		**X**			Detection and protection are barrier functions.
FR 3 - SI	SR 3.4 RE 1	Automated notification about integrity violations	3						
FR 3 - SI	SR 3.5	Input validation	1	The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.	X				To verify that input information has not been tampered with (e.g., set points). This is robust normal design protecting against states outside the design limits of the assets.
FR 3 - SI	SR 3.6	Deterministic output	1	The control system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.		**X**			To ensure integrity of normal operation. If not, the control system will be outside of normal operation.
FR 3 - SI	SR 3.7	Error handling	2	The control system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.	X	X			Error information needs to be available for error handling but should not be available to be exploited by adversaries. Error handling must be part of normal operation. Containment of information is a barrier, so only parts of this requirement are a barrier.
FR 3 - SI	SR 3.8	Session integrity	2	The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.		**X**			To avoid man-in-the-middle attack. Prevents unauthorized access.
FR 3 - SI	SR 3.8 RE 1	Invalidation of session IDs after session termination	3						
FR 3 - SI	SR 3.8 RE 2	Unique session ID generation	3						
FR 3 - SI	SR 3.8 RE 3	Randomness of session IDs	4						
FR 3 - SI	SR 3.9	Protection of audit information	2	The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.		X			To protect audit information from unauthorized access. This is a barrier. It is not normal operation that one needs to protect the audit information from modification / deletion, this is to protect against someone covering their tracks.
FR 3 - SI	SR 3.9 RE 1	Audit records on write-once media	4						
FR 4 – Data confidentiality (DC)									
FR 4 - DC	SR 4.1	Information confidentiality	1	The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.		**X**			Protecting information (flow) has similarities with containment of energy flow, which is considered a barrier. In practice, this means

FR	Req. ID	Requirement title	SL	Requirement	Normal operation	Barrier	PIF	Other	Comments
									encryption. It is a barrier in a confidentiality context (against violations of GDPR, or leakage of competitive information, or leakage of information which may damage reputation, ...) and confidentiality breach can also indirectly affect safety.
FR 4 - DC	SR 4.1 RE 1	Protection of confidentiality at rest or in transit via untrusted networks	2						
FR 4 - DC	SR 4.1 RE 2	Protection of confidentiality across zone boundaries	4						
FR 4 - DC	SR 4.2	Information persistence	2	The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.		X			This is containment (to avoid unauthorized/ unintended flow of information) therefore it is a barrier (cf. SR 3.9 and SR 4.1).
FR 4 - DC	SR 4.2 RE 1	Purging of shared memory resources	3						
FR 4 - DC	SR 4.3	Use of cryptography	1	If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.		X			Encryption is about containment of information, which is considered a barrier. The encryption itself does not change the flow of information during normal operation, but it does prevent against unintended flow of information (eavesdropping etc.).
FR 5 – Restricted data flow (RDF)									
FR 5 - RDF	SR 5.1	Network segmentation	1	The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.		X			Segregation and containment are about protecting against unintended flow of information. The segregation and containment functionality is not relevant to normal operation.
FR 5 - RDF	SR 5.1 RE 1	Physical network segmentation	2						
FR 5 - RDF	SR 5.1 RE 2	Independence from non-control system networks	3						
FR 5 - RDF	SR 5.1 RE 3	Logical and physical isolation of critical networks	4						
FR 5 - RDF	SR 5.2	Zone boundary protection	1	The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.		X			Zone protection is about protecting against unintended flow of information. Zone protection functionality is not relevant to normal operation.
FR 5 - RDF	SR 5.2 RE 1	Deny by default, allow by exception	2						

FR	Req. ID	Requirement title	SL	Requirement	Normal operation	Barrier	PIF	Other	Comments
FR 5 - RDF	SR 5.2 RE 2	Island mode	3						
FR 5 - RDF	SR 5.2 RE 3	Fail close	3						
FR 5 - RDF	SR 5.3	General purpose person-to-person communication restrictions	1	The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.	X				Normal "secure" behavior.
FR 5 - RDF	SR 5.3 RE 1	Prohibit all general-purpose person-to-person communications	3						
FR 5 - RDF	SR 5.4	Application partitioning	1	The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.			X		Facilitate implementing a zoning model. It is a PIF for SR 5.1 and SR 5.2.
FR 6 – Timely response to events (TRE)									
FR 6 - TRE	SR 6.1	Audit log accessibility	1	The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	X				For after-the-fact investigation. (Will not stop the event sequence there and then).
FR 6 - TRE	SR 6.1 RE 1	Programmatic access to audit logs	3						
FR 6 - TRE	SR 6.2	Continuous monitoring	2	The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner. (NOTE: Response time is a local matter outside the scope of this standard.)		X			To detect security breaches.
FR 7 – Resource availability (RA)									
FR 7 - RA	SR 7.1	Denial of service protection	1	The control system shall provide the capability to operate in a degraded mode during a DoS event.		X			Protection of safety systems in DoS situations.
FR 7 - RA	SR 7.1 RE 1	Manage communication loads	2						
FR 7 - RA	SR 7.1 RE 2	Limit DoS effects to other systems or networks	3						
FR 7 - RA	SR 7.2	Resource management	1	The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.			X		Resource exhaustion which is not caused by DoS attacks (addressed in SR 7.1) is caused by unintended intensity in flow of information or unintended intensity in processing of information. This influences the performance (response times, capacity) of the control system; thus, this is a PIF (e.g., of SR 6.2).

FR	Req. ID	Requirement title	SL	Requirement	Normal operation	Barrier	PIF	Other	Comments
FR 7 - RA	SR 7.3	Control system backup	1	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**			Back-up is a barrier. Consider a ransomware shutting down your control system, the recovery of that system (from a previously taken backup) is way outside normal operation. However, it may not be safety critical (e.g., only affecting production), thus it depends on the consequence classes included.
FR 7 - RA	SR 7.3 RE 1	Backup verification	2						
FR 7 - RA	SR 7.3 RE 2	Backup automation	3						
FR 7 - RA	SR 7.4	Control system recovery and reconstitution	1	The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.		**X**			Recovery is a barrier. However, it may not be safety critical (e.g., only affecting production), thus it depends on the consequence classes included.
FR 7 - RA	SR 7.5	Emergency power	1	The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.		**X**			To prevent loss of function of security mechanisms. Switching to emergency power is outside normal operation.
FR 7 - RA	SR 7.6	Network and security configuration settings	1	The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.	**X**				This is part of normal operation. Recommended network and security configurations are "robust and secure" design.
FR 7 - RA	SR 7.6 RE 1	Machine-readable reporting of current security settings	3						
FR 7 - RA	SR 7.7	Least functionality	1	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.	**X**				Hardening prior to operation. Normally sound secure solutions.
FR 7 - RA	SR 7.8	Control system component inventory	2	The control system shall provide the capability to report the current list of installed components and their associated properties.	**X**	**X**			This is part of normal operation, but it can also be used to detect unintended/ unauthorized installation of software, similarly to SR 3.2, in such a use-case this would be a barrier.

The bold cross marks indicate some degree of overlap with IEC 62443-2-1. This is based on the cross-references provided in IEC 62443-2-1 Annex A.2 (Table 91). This means that similar requirements are found in IEC 62443-2-1 documented in Appendix B above.

28 of the 51 requirements (55 %) are related to barriers. 19 are only related to barriers, whereas 9 are related to both normal operation and barriers.

The distribution of the various categories (with some requirements relevant for more than one category) is:

- Normal operation: 29
- Barrier: 28
- PIF: 3
- Other: 0