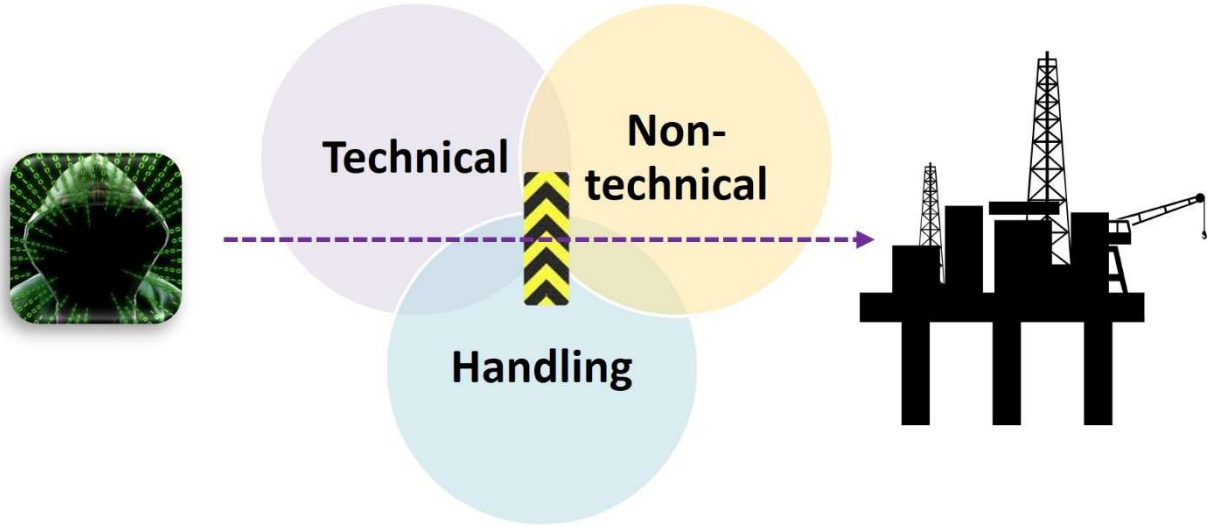


Report

Guidance on integrated safety and cybersecurity barrier management

Authors:
Knut Øien, Martin Gilje Jaatun, Christoph Thieme, Tor Olav Grøtan, Vahiny Gnanasekaran, Mary Ann Lundteigen (NTNU)

Report No:
2025:01073 - 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

Guidance on integrated safety and cybersecurity barrier management

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

VERSION
1.0

DATE
2025-10-29

AUTHORS
Knut Øien, Martin Gilje Jaatun, Christoph Thieme, Tor Olav Grøtan, Vahiny Gnanasekaran, Mary Ann Lundteigen (NTNU)

CLIENT
The Research Council of Norway

CLIENT'S REFERENCE
326717

PROJECT NO.
102020847

NO. OF PAGES
91

SUMMARY
This report on integrated safety and cybersecurity barrier management provides knowledge and guidance on identifying cybersecurity barriers and establishing corresponding performance requirements, monitoring the status of the barriers, and handling threats, vulnerabilities and barrier impairments. It covers the integration of technical and non-technical cybersecurity barrier elements, and the integration of safety and cybersecurity barrier management.

The work has been part of the PETROMAKS2 research project "Cybersecurity Barrier Management", funded by the Norwegian Research Council, Equinor and Aker BP, in close collaboration with the CDS-forum.

PREPARED BY
Knut Øien
SIGNATURE

CHECKED BY
Maria V. Ottermo, Research Manager
SIGNATURE

APPROVED BY
Geir Kjetil Hanssen, Acting Research Director
SIGNATURE

REPORT NO. 2025:01073
ISBN 978-82-14-07266-2
CLASSIFICATION Unrestricted
CLASSIFICATION THIS PAGE Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
0.5	2025-08-28	Draft version for internal commenting
0.7	2025-09-18	Draft version for commenting by external partners
0.8	2025-10-06	Draft version for commenting by CDS-forum members
1.0	2025-10-29	Final version

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

Preface

The petroleum industry has long been familiar with the concept of safety barriers and the management of these barriers to prevent major accidents. Over the past decade, the increasing convergence of information technology (IT) and operational technology (OT) has highlighted the critical need for effective cybersecurity management within the OT domain, although the concept of barriers is rarely used in cybersecurity. This development has prompted efforts to define cybersecurity barriers as a complement to existing safety barriers, and to integrate cybersecurity barrier management with traditional safety barrier management.

The purpose of this research report is to provide knowledge and guidance on establishing cybersecurity barrier management and integrating it with safety barrier management. The aim is to develop a flexible, common approach for the Norwegian petroleum industry that accommodates differences in current practices. This approach must be adapted to the specific context of each individual company. Unfortunately, there is no one-size-fits-all solution and no quick fix.

We hope the knowledge and guidance provided will support organizations that are in the process of establishing cybersecurity barrier management, while also inspiring the further development of existing approaches through the recommendations presented.

We emphasize two key aspects:

1. The distinction between cybersecurity barrier management and general cybersecurity management—specifically, identifying what constitutes a barrier versus a cybersecurity measure that is not classified as a barrier.
2. The distinction between having a cybersecurity measure in place and meeting performance requirements for such measures—with particular attention to those classified as barriers.

The report has been developed as part of the PETROMAKS2 research project *"Cybersecurity Barrier Management"*, funded by the Norwegian Research Council, Equinor and Aker BP, in close collaboration with the CDS-forum. The work has been presented and discussed in CDS-forum workshops, and the CDS-forum working committee has served as an advisory board. While the authors greatly acknowledge their contributions, the report reflects the views of the authors and may not necessarily represent the views of all CDS-forum members.

The authors also greatly acknowledge the contributions from the industry partners Equinor and Aker BP through the contact persons Jan Munkejord (Equinor) and Ragnar Heksem (Aker BP), and the external experts Pierre Kobes (Dr. Kobes Consulting) and Fredrik Gratte (Atina).

Trondheim, October 2025

Knut Øien
Project Manager, SINTEF Digital

About CDS-forum

Industry forum for cybersecurity of industrial automation and control systems.

CDS-forum is a cooperation between oil companies, engineering companies, consultants, vendors, and researchers, with a special interest in cybersecurity and the relation to Industrial Automation and Control Systems (IACS) in the petroleum industry. The participants meet twice a year for workshops, presentations, and technical discussions.

The ambition of CDS-forum is to provide a professional meeting place for knowledge development and exchange of experience, like the ambition of the equivalent PDS-forum.

Main activities include:

- Exchange of experience and ideas related to cybersecurity during the design and operation of industrial ICT systems in the petroleum industry
- Develop a user-friendly methodology for cybersecurity assessment according to IEC 62443
- Contribute to best practices within the Norwegian petroleum industry
- Contribute to the development of Norwegian guidelines for IEC 62443
- Stimulate synergies with other relevant industries within cybersecurity
- Being a driving force for increased research aimed at cybersecurity in industrial Information and Communication Technology (ICT) systems

CDS-forum members

As of 29 October 2025, CDS-forum consists of the following oil companies, engineering companies, vendors, consulting companies, service providers, research and education institutions, observers (authorities) and others:

Table of contents

Executive Summary

The Cybersecurity Barrier Management (CBM) project aims to develop new knowledge and guidance to protect industrial control and safety systems against cyberattacks. Several threat actor groups are actively targeting the petroleum sector, and the number of publicly known incidents is increasing, exposing a widening threat landscape. At the same time, ongoing digitalization has heightened system vulnerabilities. Cyberattacks on control and safety systems in the petroleum industry can result in physical damage to facilities, endanger personnel, and threaten the security of energy supply to Europe.

Digitalization can also enhance safety, for example by enabling better control of the barriers that help prevent accidents. These barriers—both technical (e.g., intrusion detection systems) and non-technical (e.g., operators in security control centers monitoring industrial control systems)—supplement normal control measures and are designed to address abnormal situations. While barrier management systems have long been applied to safeguard against accidental events, they have been used to a much lesser extent against intentional events such as cyberattacks. Establishing cybersecurity barrier management and integrating it with existing safety barrier management has therefore been a central focus of this project. The work was carried out during 2021–2025 in close collaboration with Equinor and Aker BP, the CDS-forum for cybersecurity in industrial control systems (with approximately 25 participating companies), and external experts.

Purpose of this Report

This research report on integrated safety and cybersecurity barrier management documents the knowledge developed and provides guidance on identifying cybersecurity barriers and establishing performance requirements, monitoring barrier status, and managing threats, vulnerabilities, and barrier impairments. It addresses the integration of technical and non-technical barrier elements, as well as the alignment of safety barrier management and cybersecurity barrier management.

The report offers knowledge and guidance based on current industry practices. It provides an overview of how cybersecurity barrier management has been implemented to date, includes assessments of these practices, and presents recommendations for improvement.

The report provides insight into the key decisions required to establish an effective cybersecurity barrier management system. It presents a framework designed to be adaptable and tailored to the specific needs of individual companies. Some proposals are intentionally presented as illustrative examples—such as intrusion detection and control system backup—or as partial solutions, which must be completed, interpreted, and customized in the context of each organization's operations and risk environment. There is, unfortunately, no one-size-fits-all solution and no quick fix.

Results and Key Findings

This guidance document:

- Emphasizes the importance of safety and cybersecurity barriers in preventing major accidents and highlights the emerging need to include cybersecurity barriers alongside traditional safety barriers.
- Explains the regulatory requirements for establishing cybersecurity barriers, with particular focus on the Management Regulations § 5 titled Barriers, as well as relevant authority expectations.
- Clarifies the concept of cybersecurity barriers, defining them as risk-reducing measures applied in abnormal situations, representing a subset of all cybersecurity measures.
- Defines cybersecurity barriers as measures intended to (a) detect abnormal conditions, (b) prevent abnormal conditions from developing, or (c) limit the damage caused by cyber incidents.

- Introduces a new standards-based approach for identifying cybersecurity barriers and elements, and for establishing performance requirements.
- Describes methods for status monitoring and verification of cybersecurity barrier performance.
- Details the integration of technical and non-technical barrier elements.
- Outlines a process for monitoring and handling threats, vulnerabilities, and cybersecurity barrier impairments.
- Summarizes and presents 50 recommendations for effective cybersecurity barrier management.

Two key findings affecting the integration of safety and cybersecurity barrier management in current industry practices are:

1. ***Lack of a harmonized barrier concept:*** Cybersecurity barriers are often broadly defined to include all cybersecurity measures, making it difficult to establish and verify performance requirements. This also complicates the coherent integration of cybersecurity with safety barrier management.
2. ***Differences between standards and regulatory requirements:*** Industry standards and guidelines typically mandate the implementation of cybersecurity measures, often without defining performance requirements for these measures as required by the Management Regulations § 5. This creates challenges in demonstrating compliance and ensuring effective barrier performance.

Recommendations

A selection of the recommendations is presented below, structured according to the project's three secondary objectives. The full set of recommendations is provided and further elaborated in the extended summary in Chapter 5.

1. Identification of cybersecurity barriers and verification of associated requirements

- Harmonize concepts and terminology across safety and cybersecurity barrier management
- Distinguish clearly between general cybersecurity measures and cybersecurity barriers
- Apply multiple approaches to ensure comprehensive identification of cybersecurity barriers
- Differentiate between regulatory requirements and those defined in standards and guidelines
- Formulate verifiable performance requirements for each cybersecurity barrier element
- Specify and operationalize activities for verifying cybersecurity barrier performance
- Incorporate both real-time and long-term assessment of barrier status and performance
- Use visual tools to clearly and effectively communicate the status of cybersecurity barriers

2. Integrating non-technical elements in cybersecurity barrier management

- Apply similar identification approaches for non-technical as for technical cybersecurity barriers
- Leverage OT Security Operation Centers (SOCs) as collaboration arenas for IT and OT personnel
- Avoid striving for complete convergence of IT and OT cultures and practices
- Foster mutual awareness and cross-domain understanding between IT and OT teams

3. Establishing procedures to resolve cybersecurity threats and handle barrier impairments

- Collect and integrate both external and internal information on threats, vulnerabilities, and barrier impairments
- Leverage multiple, complementary Cyber Threat Intelligence (CTI) sources
- Implement a Continuous Risk Assessment and Management Process (CRAMP)
- Establish dedicated sub-processes for managing threats, vulnerabilities, and barrier impairments

Certain choices regarding solutions or approaches are left open, as the document outlines their respective advantages and disadvantages without recommending a specific option. These decisions must be made by each individual organization based on its own context and needs.

Benefits

The advice and recommendations presented in this guidance document form part of a flexible, company-neutral framework for establishing cybersecurity barrier management and integrating it into existing safety barrier management practices. By following this guidance, organizations can initiate or strengthen their cybersecurity barrier management systems and align them with their existing safety management frameworks.

Some recommendations can be implemented directly. Others require adaptation to the specific context of each organization, while a third category may necessitate further development—ideally through collaboration between individual companies or collectively at the industry level. This need for adaptation and development stems partly from the lack of access to sensitive information—information that was not available to the project—and partly from the continuously evolving threat landscape, which demands ongoing adjustments to mitigation measures and barriers.

Adopting these recommendations facilitates alignment with regulatory requirements and the expectations of relevant authorities, contributing to more robust and integrated cybersecurity risk management.

1 Introduction

1.1 Objective

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. A cybersecurity barrier may be defined as:

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

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 are to generate new knowledge and provide guidance on:

1. Identification of cybersecurity barriers to protect ICS from cyberattacks, and development, implementation, and verification of associated requirements.
2. Integrating non-technical elements into 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], (2) a *Non-technical* Barrier Report [2], and (3) a Barrier *Handling* Report [3]. The cybersecurity barrier management guidance document [4] (this present report), is based on the three summary reports. They provide more details and also references to additional background documents.

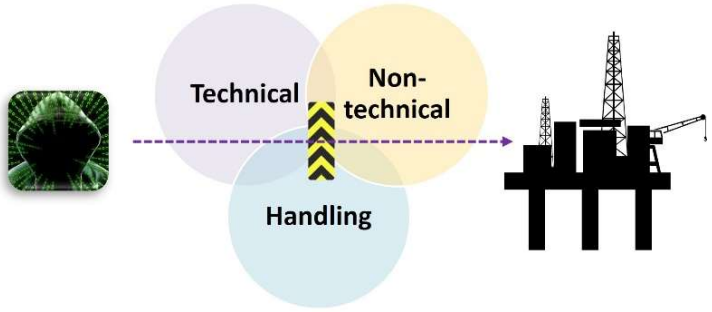


Figure 1.1 The three main parts of the CBM project

1.2 Purpose and scope

The aim of this guidance document is to provide new knowledge and guidance on integrated safety and cybersecurity barrier management, based on the following ten activities that form the foundation of the CBM project:

i) Identification of cybersecurity barriers and associated requirements
ii) Assessing the status of cybersecurity barriers
iii) Allocation and verification of security levels
iv) Integrated safety and cybersecurity barrier management
v) Integration of non-technical and technical cybersecurity barrier elements
vi) Interaction between IT and OT domains
vii) Non-technical cybersecurity barrier management
viii) Monitoring of cybersecurity barriers
ix) External threat intelligence to maintain cybersecurity barriers
x) Handling of cybersecurity barriers

The overall scope of this guidance document is defined by the ten CBM project activities and, more specifically, by the corresponding challenges associated with each:

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 the security levels of cybersecurity systems and components?
5. How to integrate safety and cybersecurity barrier management?
6. How to establish and integrate non-technical barrier elements in cybersecurity barrier management?
7. How can interaction between IT and OT domains be improved through new innovative work processes?
8. How to align practice, culture, and language between users of office IT systems and ICS?
9. How to gather information about and visualize the status of cybersecurity barriers?
10. How should information from external threat intelligence be managed to maintain cybersecurity barriers?
11. How to handle threats, vulnerabilities, and cybersecurity barrier impairments?

The answers to these questions provide new knowledge and guidance on the overall integration of safety and cybersecurity barrier management.

Detailed discussions and adaptations of the project scope have taken place throughout the duration of the project. This process began with input from partners and advisors concerning the overall project direction and scope and continued through iterative work on each of the ten specific activities listed above. Scoping considerations have been documented in internal working memos, and the resulting boundaries are partially reflected in the limitations described below.

Project discussions have also covered topics beyond the core scope, including strategies for designing out cybersecurity challenges and detailed considerations for applying various industry standards and guidelines.

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 builds upon earlier research on *safety* barrier management—particularly the work documented in [5]—which was conducted in close collaboration with the PDS Forum[1], a professional body focused on the 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 in industrial automation and control systems. The forum's Working Committee served as an advisory board to the CBM project throughout its execution.

The research employed a range of methods, including literature reviews, document analysis, observational studies, interviews, workshops, and participation in webinars, seminars, and conferences.

1.4 Limitations

The guidance presented in this document builds on prevailing industry practices in cybersecurity barrier management and their integration into established safety barrier management frameworks. However, the underlying information is based on the experiences and practices of a limited number of industry actors and may therefore not fully represent the industry as a whole.

Industry practices in cybersecurity barrier management are primarily documented in classified internal company materials—such as cybersecurity risk assessments, topology diagrams, and asset inventories—to which the research team had limited access. This limited accessibility presents a general challenge for conducting research in the field of cybersecurity.

Given the limited number of participating industry actors and the sensitive nature of cybersecurity research, this guidance document has been deliberately kept at a general level to avoid disclosing company-specific information and to maintain relevance for a broader audience.

This guidance document, together with the accompanying reports, presents a flexible framework rather than a prescriptive set of instructions. Although illustrative examples are provided, stakeholders are expected to develop tailored approaches and context-specific solutions for cybersecurity barrier management within this framework. Current industry practices in this area have evolved gradually over extended periods, and new stakeholders should be prepared for a sustained, long-term effort to establish effective cybersecurity barrier management.

1.5 Audience

The knowledge and guidance presented in this document cover a broad scope, addressing topics relevant to a diverse group of stakeholders and areas of expertise, including authorities, operating companies (asset owners), engineering companies (integration and maintenance service providers), product suppliers, vendors, consultants, Cyber Threat Intelligence (CTI) providers, Computer Security Incident Response Teams (CSIRTs), standardization bodies, and the research and education sectors.

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

1.6 Structure

The overall structure of this guidance document is inspired by the referenced report on safety barrier management [5], and the main chapters address the 11 key questions listed in Section 1.2. Although referred to as a guidance document, it encompasses both *knowledge* (e.g., what and why) and *guidance* (e.g., how). Some of this knowledge is provided as background information, but most is presented progressively throughout the report and followed by corresponding guidance, including examples.

The report consists of two introductory chapters, two main chapters (addressing the 11 key questions, shown in parentheses below), and an extended summary, as outlined below:

Chapter 1 serves as the introduction, which you are now nearly finished with—so there is no need to elaborate further here.

Chapter 2 provides background information on the barrier concept. It covers regulatory requirements, as well as perspectives and initiatives from authorities, industry stakeholders, standards and guidelines, and academic literature.

Chapter 3 addresses the identification of cybersecurity barriers (1) and their associated performance requirements (2). It also examines the integration of technical and non-technical barrier elements (6), along with the interaction between IT and OT personnel (7–8).

Chapter 4 focuses on the monitoring and follow-up of cybersecurity barriers over the short, medium, and long term (3–4). It outlines processes for monitoring and handling cybersecurity threats, vulnerabilities, and barrier impairments, structured into three sub-processes: threat landscape monitoring, vulnerability management, and cybersecurity barrier monitoring (9–11). Finally, the chapter discusses the integration of safety and cybersecurity barrier management (5).

Chapter 5 presents an extended summary of assessments and recommendations, structured around the 11 key questions that define the scope of this guidance document. This chapter is designed to be read as a stand-alone section following the introduction and therefore includes both knowledge and guidance.

Appendix A contains definitions and abbreviations.

1.7 How to read and use the guidance document

How to read the document

The structure of this guidance document is designed to accommodate varying levels of reader interest and need. Readers seeking a brief overview may refer to the *Executive Summary*. For readers seeking detailed insights without reviewing the full document, an *extended summary* is provided in Chapter 5, synthesizing the key assessments and recommendations. Readers requiring a comprehensive understanding are encouraged to read the *entire document*.

If you are looking for *specific topics or issues* within cybersecurity barrier management, you are encouraged to begin with the *Table of Contents* and navigate directly to the sections most relevant to your interests.

How to use the document

The way this document is best used depends on who you are—both in terms of the type of organization you represent (e.g., operator, supplier, regulator) and your disciplinary background (e.g., cybersecurity,

automation, safety, management). Different readers will find some sections more relevant to their interests and responsibilities.

The potential readers are indicated in Section 1.5, for which two target groups are of particular importance. They consist of operating companies (asset owners) that hold the primary responsibility for establishing and following up barriers for both safety and cybersecurity.

1. *Experienced Practitioners*
   The first target group includes operating companies that participated in the project and that have already implemented cybersecurity barrier management, though in varying forms. The descriptions of current practices in the document are largely based on insights from this group.
2. *Safety-Mature, Cybersecurity-Developing Companies*
   The second—and most important—target group consists of operating companies that have established safety barrier management but have not yet implemented cybersecurity barrier management. This group is the primary focus of the guidance, aiming to support their transition by drawing on best practices, structured recommendations, and practical integration approaches.

The first main target group benefits from insights into how other organizations have implemented cybersecurity barrier management. These insights enable them to compare external practices with their own frameworks, identify commonalities and differences, and consider opportunities for improvement. They are gained through meetings and workshops, as well as through project memos and reports, providing ongoing value to the participating companies throughout the project.

While the description of these company's own practices may not constitute new information to the company itself, the assessments made during the project and in this document offer added value. These include reflections on the strengths and weaknesses of current practices, and they form part of the new knowledge base generated. It is recognized that not all companies may fully agree with the way their practices have been described or assessed, nor may there be internal consensus within each organization on the need for improvements.

For the second target group, this document offers knowledge and guidance based on current industry practices. It provides an overview of implementation approaches to date, evaluations of existing practices, and targeted recommendations for improvement.

Readers in this group will gain insight into the key decisions required to establish an effective cybersecurity barrier management system. The document presents a framework that enables adaptation and tailoring to meet the specific needs of each individual company. Some of the guidance is intentionally presented as examples or partial solutions, requiring companies to complete, interpret, and adapt them to their own operations and risk environment.

While the recommendations in this document apply to both target groups, their implications may differ. For the first group, implementing recommendations that call for changes to existing practices may be more demanding than for companies starting from a clean slate. In contrast, the second group, which is in the process of establishing such practices, may find it easier to incorporate these recommendations from the outset, as part of a structured development effort.

Other stakeholder groups involved in cybersecurity within operational technology (OT) environments should also benefit from reading and applying this document. These groups are, as noted, described in Section 1.5.

2 The barrier concept, regulatory requirements, and background information

2.1 The barrier concept and regulatory requirements

The petroleum industry faces the risk of major accidents, which may result in multiple fatalities and large-scale oil spills. Consequently, 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 [6].

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 considered 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" [7] which depicts multiple layers of protection, also known as "defense in depth".

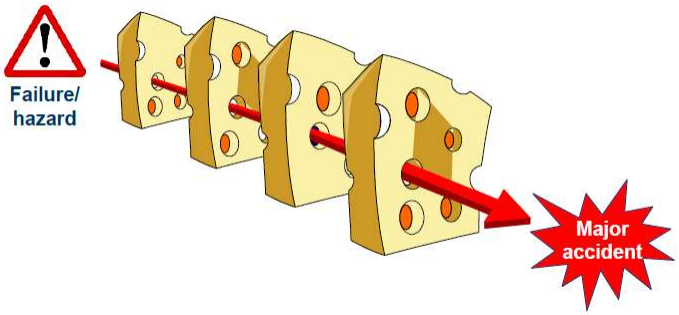


Figure 2.1 Swiss Cheese model (adapted from Reason, 1997) [7]

With multiple barriers in place, major accidents are considered "low probability, high consequence" events. However, even multiple barriers can sometimes be insufficient, potentially 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. Consequently, several requirements in MR § 5 address the capabilities and performance 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 Norwegian Ocean Industry Authority (Havtil), has clarified the difference between barriers and non-barriers in the Barrier Memorandum [8], including the provision of barrier-related definitions. Figure 2.2 illustrates the distinction between MR § 4 (safe and robust solutions) and MR § 5 (barriers).

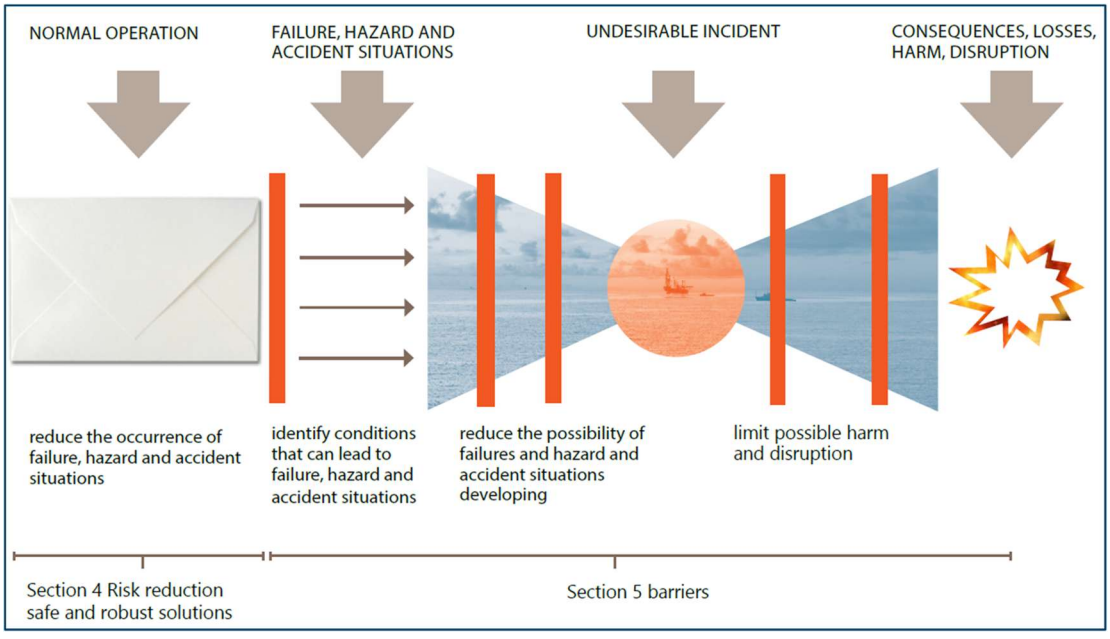


Figure 2.2 Barriers versus "safe and robust solutions" [8]

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).

Havtil further distinguishes between barriers and non-barriers by referencing performance influencing factors (PIFs). As a result, three categories of risk-reduction measures are identified: (1) safe and robust solutions or control measures applied during normal operations, (2) barriers, and (3) performance influencing factors. This classification is illustrated in Figure 2.3.

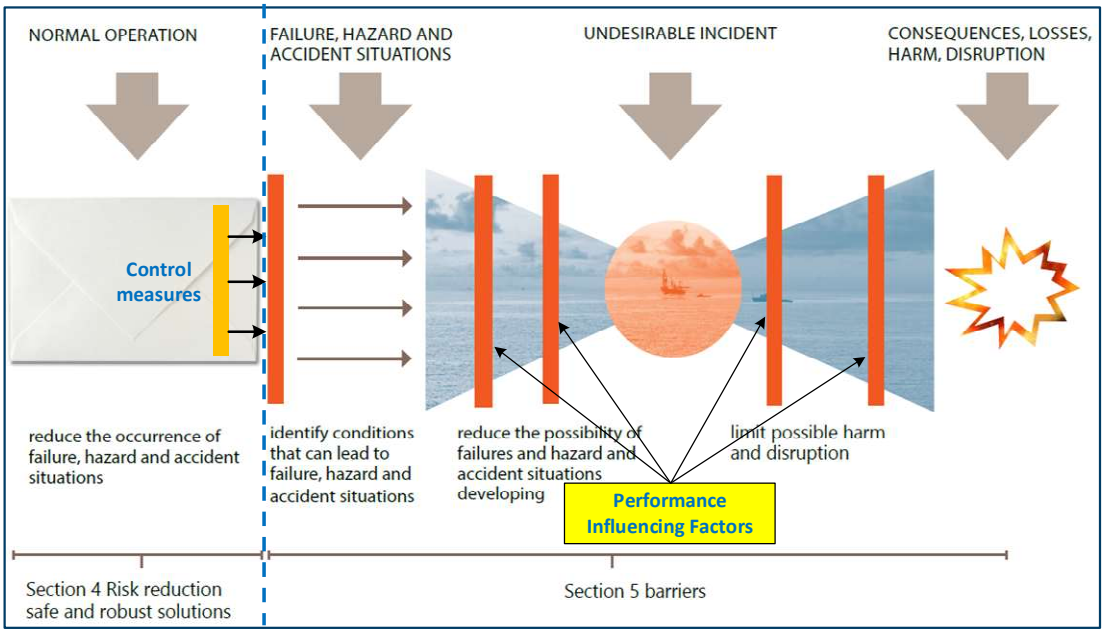


Figure 2.3 Bow-tie model distinguishing between types of measures or solutions

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 [8], where most definitions are found, are not normative. Therefore, there are somewhat divergent definitions of barriers in use in the petroleum industry.

The latest Barrier Memorandum ("Principles for Barrier Management in the Petroleum Industry") [8] explicitly includes security, stating that using barrier management principles for security incidents promotes a systematic approach to identifying, establishing, and maintaining barriers.

In addition to general requirements for barriers in the MR § 5 [6], the **Facilities Regulations** Chapter V (§§ 29-40) [9] cover requirements for physical barriers. The guideline to FR § 34a Control and monitoring system [10] 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] NOROG 104 provides information security baseline requirements (ISBRs) for security controls and measures. These are not referred to as barriers and can be

[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."

[4] Offshore Norge Guideline No. 104, previously known as NOROG 104, is referenced in this document as NOROG 104 [11].

considered *general* cybersecurity measures, managed as part of cybersecurity management, but are not necessarily part of cybersecurity *barrier* management.[5] ISBRs include requirements for cybersecurity measures that may be classified as both cybersecurity barriers and non-barriers.

A note on referencing industry standards: Havtils 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 [12], and it means that e.g., IEC 62443 may be used instead of NOROG 104.

2.2 Perspectives from public authorities

The Lysne Committee found petroleum regulations lacking specificity regarding digital threats and recommended that the Petroleum Safety Authority (PSA, now Havtil) require barriers for digital vulnerabilities (NOU 2015: 13) [13]. This recommendation aims to extend the robust safety tradition in health, safety, and environment (HSE) to the digital realm. While the safety domain (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) [14].

2.3 Perspectives and initiatives from the regulator

NOU 2015: 13 and Meld. St. 38 (2016-2017) led to four years of grants (2018-2021) for Havtil 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, Havtil focused on safety barrier management, publishing Barrier Memorandums in 2011, 2013 [15], and a major update in 2017 [8]. The 2017 update included security/cybersecurity 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 barrier 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 [16], which mentions ICT events as reportable, and § 34a of the Facilities Regulations [10], which references NOROG 104 [11]. 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.

A key finding regarding cybersecurity barrier requirements is the critical distinction between having a cybersecurity measure in place (referred to as *requirements about*) and defining how that measure must perform (referred to as *requirements to*). Many standards and guidelines tend to conflate these two aspects,

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

[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

blending the existence or presence of cybersecurity measures with the specification of their functional and performance characteristics.

It is essential to differentiate between the process of identifying cybersecurity barriers (*requirements about*) and the process of developing the associated performance requirements (*requirements to*) the barriers. The performance requirements outlined in MR § 5 relate specifically to the functionality, reliability, and maintainability of these barriers.

This distinction is fundamental for establishing a robust and effective cybersecurity barrier management system.

2.4 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 integrated cybersecurity barrier management with safety barrier management, compiled requirements for cybersecurity measures in performance standards, and established approaches for identifying cybersecurity barriers, as briefly outlined below. Certain challenges are also highlighted.

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 [17] and NOROG 104 [11], implicitly treating all cybersecurity measures as barrier measures. This contrasts with Havtil's approach, which distinguishes barrier measures from other cybersecurity measures. We advocate for this distinction to align with Havtil's reasoning and facilitate consistent integration of cybersecurity and safety barrier management.

Requirements to cybersecurity measures compiled in performance standards

The companies have established operational performance standards (PSs) for cybersecurity. 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 [17] and the NIST Cybersecurity Framework (CSF) [18], which encompass overarching security measures.

The other company's performance standard (PS) document, which is largely based on NOROG 104 [11], 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 Havtil 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.

Identification of cybersecurity barriers

Two complementary approaches to barrier identification were described in internal working memos [19], [20]: (1) an event sequence and functional top-down approach, and (2) an asset inventory bottom-up approach. When used in combination, these approaches support a 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 3.1.

2.5 Findings from cybersecurity standards and guidelines, and academic literature

Standards/guidelines like NIST CSF [18], IEC 62443 [17], IEC 63069 [21], ISA-TR.84.00.09 [22], and NOROG 104 [11] rarely define 'cybersecurity barriers,' using terms like countermeasure, security measure, and safeguard instead. We focus on IEC 62443 as an international standard, despite challenges such as some parts still being available only in draft form and the generally long timelines before final release, in favor of local guidelines like NOROG 104 [11][8]. IEC 62443 previously used 'countermeasure,' but this has changed to 'security measure'.

In a previous literature review [23], we examined publications addressing the identification of cybersecurity barriers and barrier elements, as well as the use of the term *"cybersecurity barriers."* Only a few publications used the term, and none provided a definition.

We conducted preliminary testing to identify cybersecurity barriers based on Havtil (2017) [8], distinguishing between safe and robust solutions, barriers, and performance influencing factors (PIFs), as described in Section 2.1. This testing was applied to countermeasures from ISA-TR.84.00.09 (2017) [22]. The results, documented in an internal working memo [20] and an IEEE article [23], concluded that this distinction is feasible.

[8] It should be noted that this guidance document is not intended as a general introduction to the use of IEC 62443. References to IEC 62443 are limited to two specific applications. The first is in the development of a standards-based approach for identifying cybersecurity barriers, where IEC 62443 is used as an example. The second concerns the follow-up of Security Levels (SL) in operation, a concept originating from IEC 62443.

3 Identification of cybersecurity barriers and associated performance requirements

This chapter addresses the identification of cybersecurity barriers (Sections 3.1 and 3.2) and their associated performance requirements (Section 3.3). It also covers the integration of technical and non-technical barrier elements (Section 3.4) and the interaction between IT and OT personnel (Section 3.5).

Section 3.1 outlines various approaches to identifying cybersecurity barriers, while Section 3.2 elaborates on one of these methods developed in this project as a new approach. The establishment of performance requirements in Section 3.3 is applicable to any of the approaches described in Section 3.1.

The first three sections have a primarily technical focus, which is broadened in Section 3.4 by non-technical aspects. Non-technical issues are further elaborated in Section 3.5.

3.1 Identification of cybersecurity barriers

"How can we ensure that all barrier functions, sub-functions, and elements are properly identified?" This question – corresponding to key question no. 1 in Section 1.2 – forms the foundation for the approaches presented in this chapter for the identification of cybersecurity barriers.

Note that *"identification"* of cybersecurity barriers does not encompass the initial establishment or the assessment of the need for cybersecurity measures (including barriers). Instead, it begins once the cybersecurity measures have been selected—either as part of a new project, or in relation to an existing installation with established cybersecurity measures (including barriers) [1].

Barrier identification in safety barrier management typically combines a top-down approach (I)—based on event sequences and functional breakdowns—with a bottom-up approach (II) using asset inventories. These approaches make use of methods such as barrier grids, hierarchical functional breakdowns, and barrier logic diagrams [5].

A new standards-based approach (III), developed as part of the CBM project, is introduced and further elaborated in Section 3.2. This approach begins with security measure requirements from relevant standards and guidelines and represents a different type of top-down method compared to Approach I.

Thus, we can distinguish between three approaches for the identification of cybersecurity barriers:

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

One or more approaches may be applied but combining them helps ensure a more comprehensive identification of all barrier functions, sub-functions, and elements (see Figure 3.1). Any new equipment identified as a barrier during or after implementation should also be incorporated on an ongoing basis. Although this is formally considered part of the bottom-up approach (II) (cf. Step 5C in Figure 3.1), it remains relevant regardless of which combination of approaches is used.

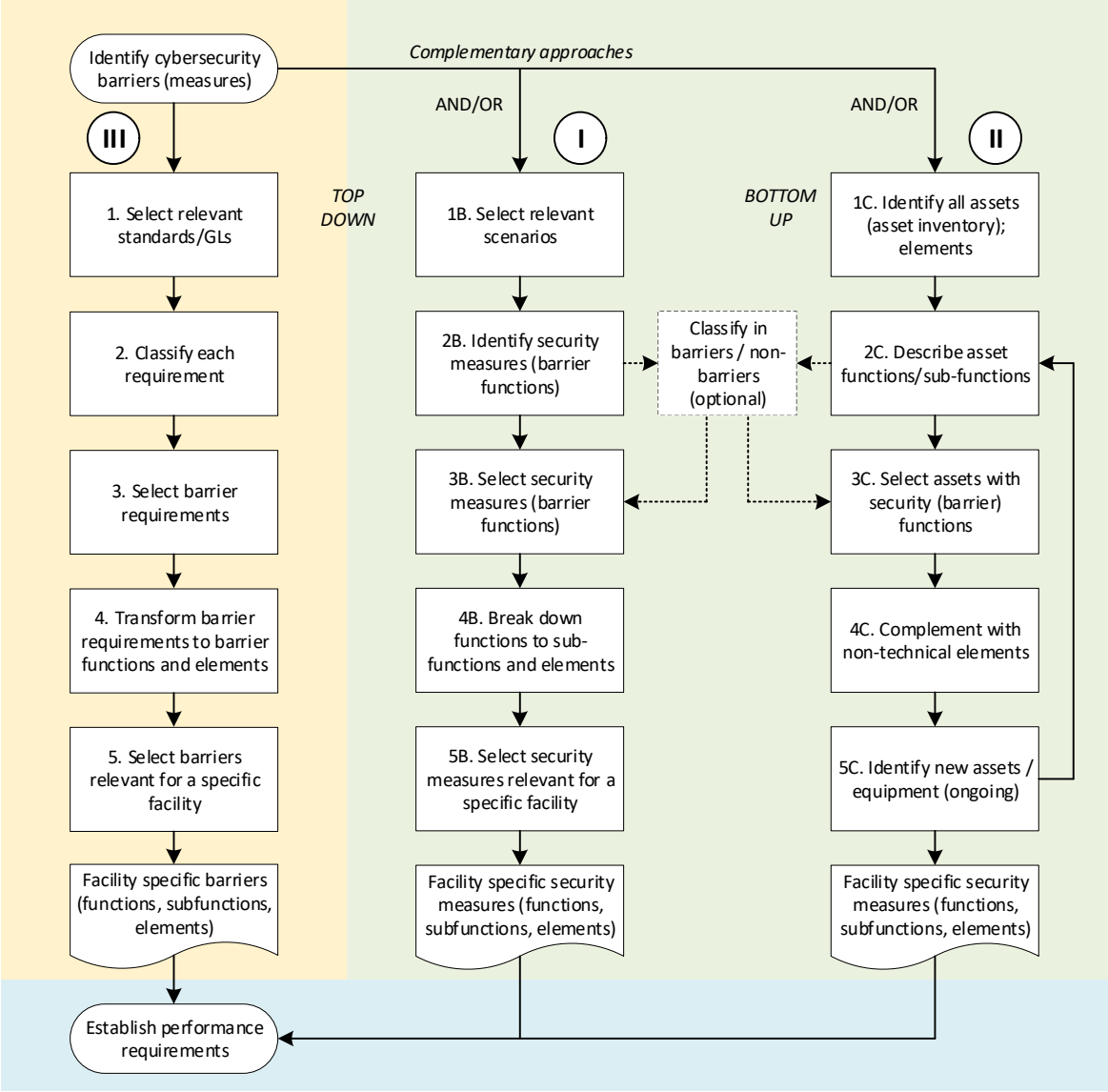


Figure 3.1 Approaches for identification of cybersecurity barriers

Approach I often begins with selected scenarios from risk assessments (e.g., network, physical, or supply chain entry points), using techniques and tools such as barrier grids or bow-ties to map barrier functions along the event chain [5]. However, because scenarios are always limited in scope, certain barrier functions, sub-functions, and elements may be overlooked.

Additionally, Approach I includes breaking down barrier functions into sub-functions and elements through a hierarchical functional breakdown, as mentioned in the Barrier Memorandum [8]. 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 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 in the Barrier Memorandum [8].

This new approach is expected to provide a more comprehensive identification of barrier functions than scenario-based methods, although gaps may still be present in the standards. Such gaps should be addressed by adding supplementary barriers. As elaborated in Section 3.2, barrier functions in this approach are by default 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.

Companies, with their access to all necessary information, can choose any approach or combination of approaches. And, as indicated in Figure 3.1 for Approach I and II, they can also decide 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—distinguishing between barriers and non-barriers—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 important for assessing consequences and risks. For more details on Approaches I and II, refer to [5] for production facilities, and [24] for drilling rigs, and the Barrier Memorandum [8] in general.

3.2 Standards-based approach

3.2.1 Principles

The development of the standards-based approach for identifying cybersecurity barriers and establishing performance requirements—along with the overarching flexible framework for cybersecurity barrier management—is based on the following five core principles:

1. *Company neutrality* – It should be applicable across organizations, without being tailored to any specific company.
2. *Independence from existing frameworks* – It should remain independent of selected requirements, standards, and/or guidelines.
3. *Regulatory alignment* – It should adhere to the regulations, definitions, and reasoning established by relevant authorities (e.g., Havtil).
4. *Compatibility with safety barrier management* – It should be suitable for integration with various regimes of safety barrier management.
5. *Inclusion of non-barrier security measures* – It should also account for security measures that are not formally defined as barriers.

The approach distinguishes between barriers and non-barriers in accordance with the Barrier Memorandum [8]. However, non-barriers are also addressed in line with the fifth principle, which supports compliance with general cybersecurity requirements—encompassing both barriers and non-barriers—as outlined in the guidelines to FR § 34a [10]. Asset owners are responsible for deciding whether to manage non-barriers in a manner similar to barriers, bearing in mind that stricter regulatory requirements apply to barriers.

The standards-based approach to identify cybersecurity barriers and associated performance requirements has been grounded in the five core principles. It applies a top-down approach based on a preferred cybersecurity standard or guideline [25].

3.2.2 Overview of the standards-based approach

The nine-step method consists of two main parts: the first five steps focus on identifying cybersecurity barrier functions and elements, while the remaining four steps address the establishment of performance requirements to the barriers and the verification of 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 the flowchart in Figure 3.2, and the method is described in detail in the technical barrier report [1]. Each step includes a description, a justification or explanation, and relevant examples or elaborations. For exemplification, we focus on the international standard IEC 62443, specifically Parts 2-1 [26] and 3-3 [27]. The Security Program Elements (SPEs) in Part 2-1 are particularly important 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).

Two examples applied throughout the method description are *intrusion detection* for continuous monitoring and *control system backup*. As outlined in the introduction, a cybersecurity barrier is defined as a measure intended to (a) detect abnormal conditions, (b) prevent abnormal conditions from developing, or (c) limit the damage caused by cyber incidents. Intrusion detection aligns with the first function—detecting abnormal conditions—while backup supports the third function by enabling restoration to normal operation and thereby limiting damage.

Steps 1–7 are illustrated in Figure 3.3 using the examples of intrusion detection and control system backup from IEC 62443-3-3. The execution of these steps is documented using spreadsheets. The final two steps (8–9) aim to fulfill the performance requirements for the barrier elements and for all cybersecurity measures, respectively.

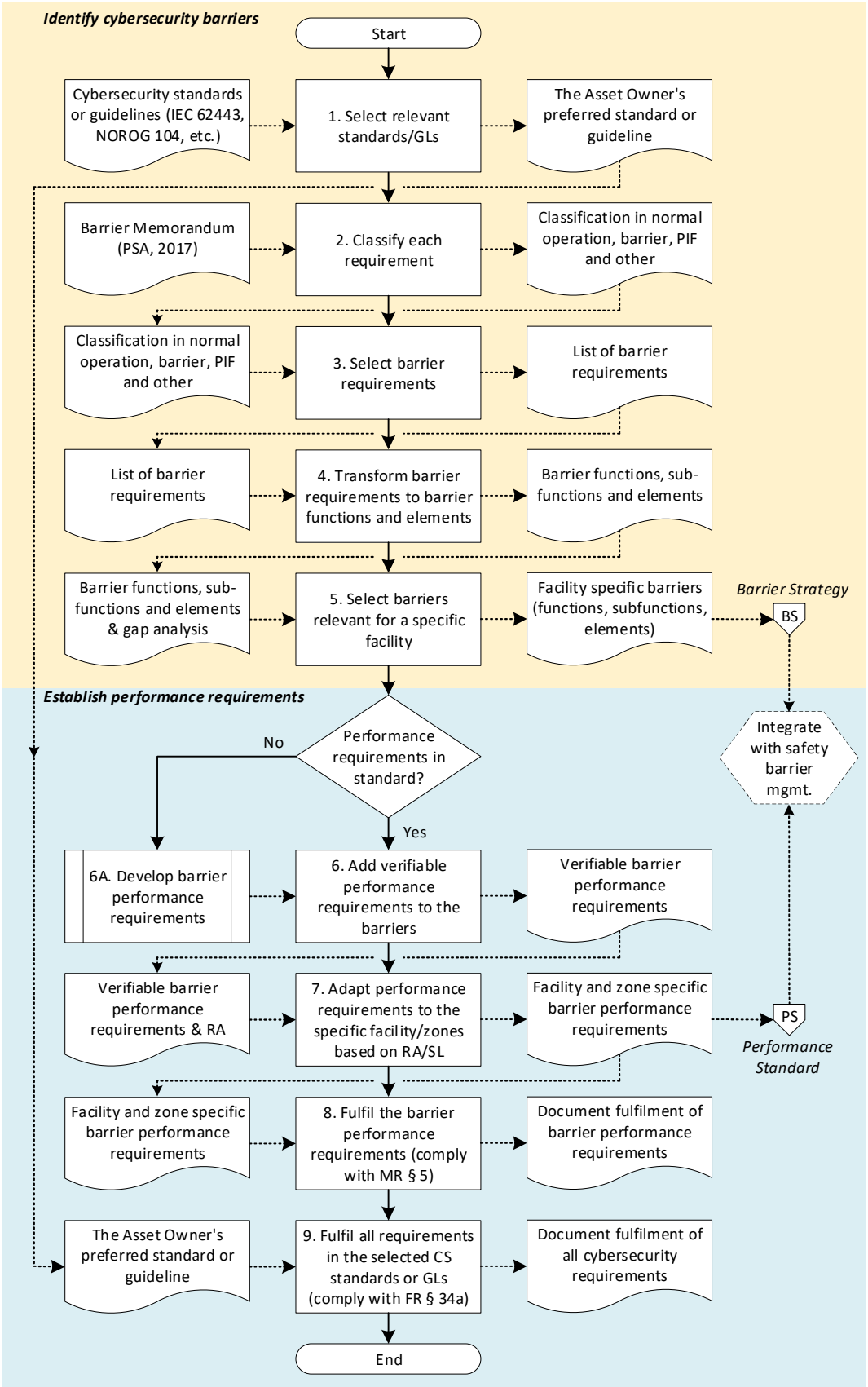
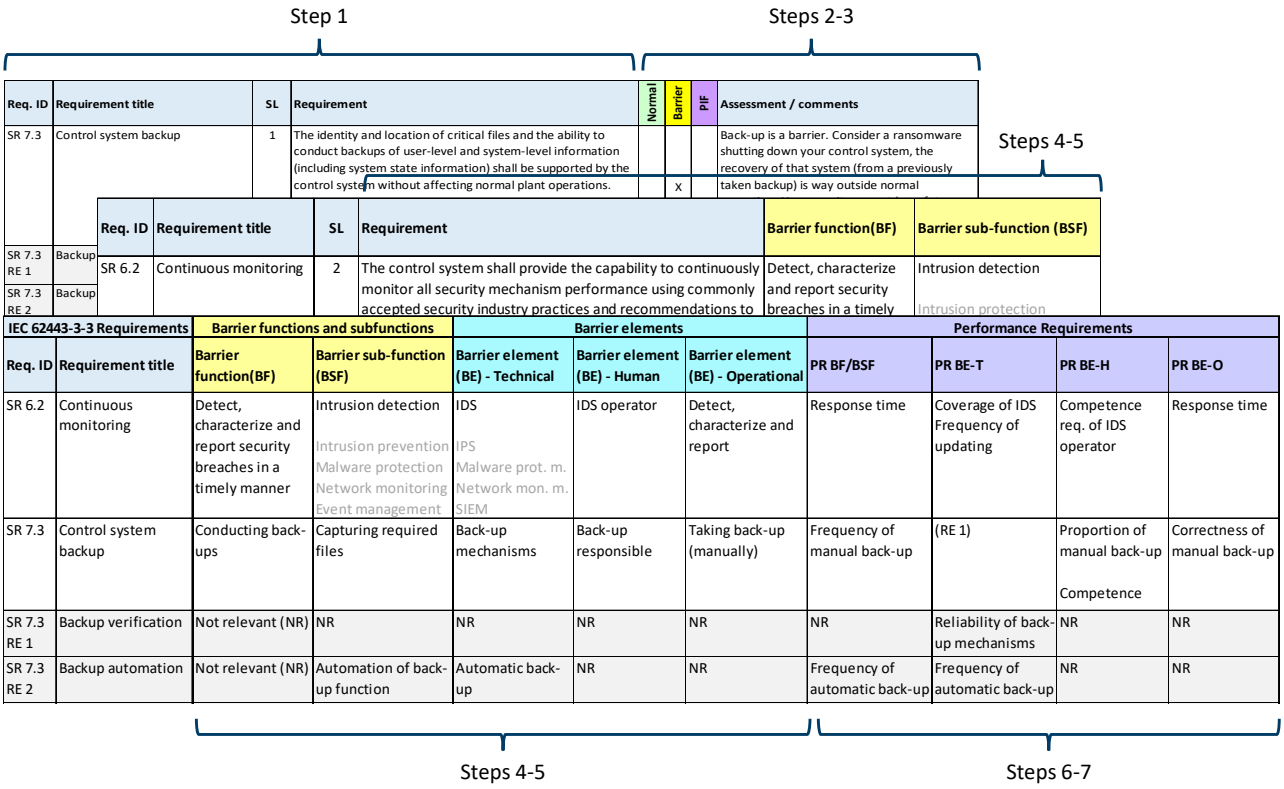


Figure 3.2 Flowchart of the standards-based method



Req. ID	Requirement title	SL	Requirement	Normal	Barrier	PIF	Assessment / comments
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

	Req. ID	Requirement title	SL	Requirement	Barrier function(BF)	Barrier sub-function (BSF)
SR 7.3 RE 1	Backup	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	Intrusion detection
SR 7.3 RE 2	Backup						Intrusion protection

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

Figure 3.3 Examples of documenting the assessments using the standards-based method

In *Step 1*, requirements from preferred standards are extracted and listed in a spreadsheet.

In *Step 2*, each requirement is classified as either part of normal operation, related to a barrier, or a factor influencing barrier performance, i.e., a PIF, using a decision tree. This step also includes documenting the basis for the classification.

In *Step 3*, only those requirements classified as related to barrier functions are retained for further assessments.

In *Step 4*, the barrier-related requirements are translated into barrier functions, which are then further decomposed into barrier sub-functions and barrier elements—categorized as technical, human, or operational. The breakdown utilizes a barrier hierarchy, cf. [8], and the rationale and supplemental guidance in IEC 62443-3-3.

In *Step 5*, only the barrier functions and elements relevant to a specific facility are selected. For example, Intrusion Detection Systems (IDS) may be used at the facility, whereas Intrusion Prevention Systems (IPS) may not. This is provided with a gap analysis between a generic analysis/facility and a specific facility.

In *Step 6*, verifiable performance requirements are assigned to the barrier functions and elements. This is elaborated in the next section, including examples.

In *Step 7*, these performance requirements are adapted as needed to the specific facility, zone, and system context.

3.3 Performance requirements

Sections 3.1 and 3.2 focus on ensuring that all barrier functions, sub-functions, and elements are properly identified. This section addresses the subsequent challenge: establishing verifiable performance requirements for the barrier elements, corresponding to key question no. 2 in Section 1.2 and mandated by MR § 5 [6]: *"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 organizational barrier elements necessary for the individual barrier to be effective."

A performance requirement is defined as a *"verifiable requirement for the properties of the barrier elements in order to ensure the barrier is effective."* [8]

Standards and guidelines often require that specific cybersecurity measures be in place. However, the performance requirements outlined in MR § 5 pertain to how well barriers—typically at the level of individual barrier elements—must perform with respect to properties such as functionality, integrity, and robustness [8]. If the selected standard or guideline includes relevant performance requirements, these can be adopted directly. If such requirements are missing or insufficient, they must be developed and supplemented.

This process is represented as Step 6A in Figure 3.2—a subprocess in which performance requirements are derived from the characteristics of the barrier elements to ensure coverage of relevant properties. In this step, both direct and indirect performance requirements are considered. The latter are established through the use of Performance Influencing Factors (PIFs).

Although Step 6A and the description provided in this section are related to Approach III, it should be noted that the establishment of performance requirements applies regardless of which approach to identifying cybersecurity barriers is used, as illustrated in the lower part of Figure 3.1.

Steps 6 and 7 focus on assigning performance requirements to barriers and adapting these requirements to the specific context of the facility, zone, and system. This is illustrated in Figure 3.3, which provides examples of performance requirements (PR) for each barrier element (BE) across the three categories: Technical (T), Human (H), and Operational (O). Alternatively, performance requirements may also be defined at the level of barrier functions (BF) or barrier sub-functions (BSF), as shown in the first PR column of the figure. In addition, PIFs—such as competence—can serve as indirect performance requirements. For example, competence requirements as illustrated in the PR BE-H column.

Step 8 involves ensuring that the barrier performance requirements identified in Step 7 are fulfilled, in accordance with MR § 5 [6]. This is an ongoing process that requires regular monitoring and verification to confirm that the performance requirements continue to be met over time. Effective verification necessitates that each performance requirement is clearly defined and accompanied by an operationalized method of measurement. Only when both the requirement and its evaluation method are explicitly specified can compliance and performance be reliably assessed.

This is further elaborated and illustrated in the following examples, using control system backup to demonstrate the operationalization of performance requirement verification for both a technical barrier element (Example 1) and a non-technical barrier element (Example 2).

Example 1 – verification of performance requirements – technical barrier elements

As shown in Figure 3.3, the requirement ID SR 7.3 from IEC 62443-3-3 specifies *backup mechanisms* as a technical barrier element, with reliability defined as the direct performance requirement (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 both immediately after the backup process and at regular intervals thereafter.

As with all performance requirements, this must be clearly specified and operationalized. Key questions include: *What constitutes integrity verification? How frequently should it be carried out? 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 3.1. 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.

Table 3.1 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/

Barrier status follow-up is categorized into short-, medium-, and long-term monitoring. In Table 3.1, the frequency range of *weekly–monthly* corresponds to medium-term follow-up, while *yearly* reflects long-term monitoring. These indicative timeframes are linked to the verification of performance requirements, as further described in Sections 4.2 and 4.3.

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 (cf., Section 4.1).

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, most of the activities listed in Table 3.1—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—randomly selected—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 3.2.

Table 3.2 Example of operationalizing backup performance verification

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, as described by the next example.

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 4.

Example 2 – verification of performance requirements – non-technical barrier elements

The performance requirement defined for the technical barrier element in the example above is *"reliability of backup,"* operationalized as achieving 90% reliability based on daily backups. This requirement addresses the error-free aspect of the verification activity but does not explicitly account for whether backups are performed according to schedule—particularly when executed manually. This scheduling aspect can be linked to the performance requirement *"correctness of manual backup,"* which is assigned to the operational barrier element in Figure 3.3. The human barrier element is the backup responsible.

Verification that backups are performed as scheduled can be operationalized as shown in Table 3.3, where daily manual backups are assumed. The corresponding performance requirement specifies that 90% of the backups must occur on schedule.

Table 3.3 Example of operationalizing manual backup performance verification

Frequency of manual back-up	Daily
Direct performance requirement	90% on schedule
Verification	Check all back-up log files from last two weeks
Rules (status)	0-1 backups not performed on schedule: Green
	2-3 backups not performed on schedule: Yellow
	4-14 backups not performed on schedule: Red

3.4 Integration of technical and non-technical barrier elements

The first three sections (Sections 3.1–3.3) had a primarily technical focus. This section broadens the perspective by addressing the integration of non-technical barrier elements, corresponding to key question no. 6 in Section 1.2: *"How to establish and integrate non-technical barrier elements in cybersecurity barrier management?"*

The method for identifying barrier functions and elements, and establishing performance requirements, as described in Sections 3.1–3.3 apply to both technical and non-technical cybersecurity barrier elements.

The identification of these elements typically begins with a top-down approach—whether using Approach I or Approach III—in which barrier functions are identified first. Alternatively, a bottom-up approach may be applied, where barrier elements are identified directly.

Top-down decomposition from barrier functions to barrier elements, through one or more levels of sub-functions, is illustrated in Figure 3.4. On the left, the breakdown and general barrier terminology used in Havtil's guidance on barrier management [8] is presented. On the right, the corresponding cybersecurity-specific barrier elements used in the CBM project are shown.

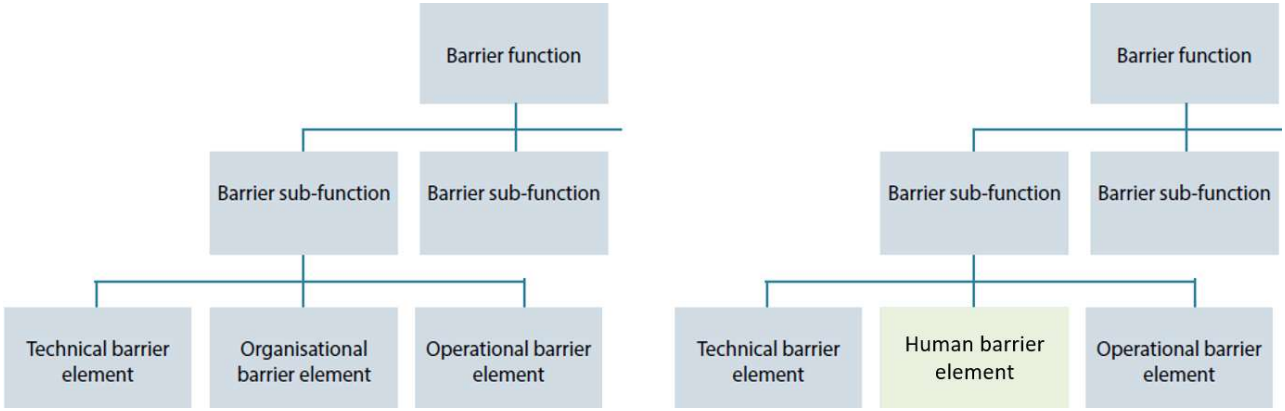


Figure 3.4 Barrier hierarchy with barrier elements according to Havtil (left) and CBM (right)

Following the notation used in the CBM project, barrier elements (BE) that execute a barrier function are classified as either technical (BE-T), human (BE-H), or operational (BE-O). The latter two—human and operational—are collectively referred to as non-technical barrier elements.

According to the definitions and notations provided by Havtil [8], *organizational* barrier elements (BEs) refer specifically to sharp-end personnel—those responsible for activating and operating a technical BE, or for

performing a barrier function in the absence of a technical BE. In contrast, *operational* BEs refer to the specific actions or activities that personnel must carry out to realize a barrier function.

However, the term *organizational BE* can lead to confusion, as it may be interpreted more broadly in the context of the MTO (Man–Technology–Organization) framework. Within that framework, *organization* typically encompasses blunt-end personnel, such as management or support staff, who are not directly involved in the activation or operation of barrier functions.

A second reason for changing the notation from *organizational barrier element* to *human barrier element* is to align with the cybersecurity "triangle", which consists of technology, people, and process. In this context, the term *people* correspond more directly to *human*. Furthermore, the term *operational* is widely used in safety barrier management within the petroleum industry, making it more appropriate than *process* in the safety domain. These considerations are discussed in greater detail in the technical barrier report [1].

Examples of non-technical barrier elements include those related to intrusion detection and control system backups. The associated human barrier elements are the individuals responsible for managing the intrusion detection system (IDS) and for performing regular system backups, respectively. The corresponding operational barrier elements involve actions such as detecting, characterizing, and reporting security breaches, as well as conducting routine backups. Additional non-technical barrier elements can be identified using the methods described in the technical barrier report.

The intrusion detection and backup examples—illustrated in Figure 3.3—are further detailed for their non-technical elements in Table 3.4, as presented in the non-technical barrier report [2].

Table 3.4 Examples of generic performance requirements related to continuous monitoring (e.g., IDS) and control system backup, adapted from the non-technical barrier report [2]

Req. ID	Req. title	Barrier function	Barrier subfunction	Barrier Elements		Performance Requirements	
				BE-Human	BE-Operational	BE-Human requirement	BE-Operational requirement
SR6.2	Continuous monitoring	Detect, characterize and report security breaches in a timely manner	Intrusion detection	IDS operator (e.g., IT/OT responsible, OT security technician, SOC)	Detect	Availability of personnel Regular rotation of personnel Competency in using the IDS	Response time
			Characterize intrusion	IDS operator (e.g., IT/OT responsible, OT security technician, SOC)	Analyze and characterize	Availability of personnel	Response time
			Report security breach	IDS operator (e.g., IT/OT responsible, OT security technician, SOC)	Report	Availability of personnel	Response time Reporting routine based on severity of breach shall be available
SR7.3	Control system backup	Conducting backups (manual)	Backing up required files	Back-up responsible role (e.g., OT technician, TSR instrumentation)	Taking back-up (manually)	Availability of personnel Competency to take manual back-ups	Correctness of manual back-up Correctness of procedure for manual back-up

The examples provided are not exhaustive and should be reviewed or reassessed by the asset owner or the party responsible for identifying barrier functions and barrier elements. In the examples shown in Table 3.4, the continuous monitoring function has been expanded from a single subfunction in Figure 3.3 to three distinct sub-functions. Similarly, backups can be viewed as part of a broader restore function, which consists of the following sub-functions: 1) take backup, 2) verify backup, and 3) restore using the backup.

The complementary bottom-up approach (Approach II) for identifying technical barrier elements—as described in the technical barrier report—begins with asset inventories.

A corresponding bottom-up approach for identifying non-technical barrier elements involves examining the roles and actions associated with handling cybersecurity incidents, starting from the detection of abnormal conditions, in line with the previously stated definition of cybersecurity barriers. This means assessing whether individuals serve as human barrier elements and determining which of their actions qualify as operational barrier elements.

Some of the relevant roles involved in handling cybersecurity incidents—and potentially contributing as human barrier elements—include:

- Offshore Installation Manager (OIM) / Emergency Response Leader (ERL)
- Control Room Operator (CRO)
- Field Operator (FO)
- Discipline Lead (DL) / Technical System Responsible (TSR)
- Emergency Management Team 1. Line (EMT offshore)
- Emergency Management Team 2. Line (EMT onshore)
- IT/OT responsible
- IT/OT security team
- OT security technician
- Security Operations Centre (SOC)
- Computer Security Incident Response Team (CSIRT)

It is important to note that the roles involved in detecting abnormal conditions, preventing their escalation, and limiting damage are not necessarily directly responsible for activating barriers. Some roles primarily perform support functions that influence the effectiveness of barrier elements without constituting barrier elements themselves, e.g., an IT/OT responsible providing communication and "translation" between the SOC and the offshore facility. As such, their actions or activities may be classified as Performance Influencing Factors (PIFs) rather than barrier functions or elements.

3.5 IT/OT interaction

In this section, non-technical issues are further elaborated by addressing key questions no. 7 and 8 in Section 1.2: *"How can interaction between IT and OT domains be improved through new innovative work processes?"* and *"How can practice, culture, and language be aligned between users of office IT systems and ICS?"*

Two key roles in the handling of cyber incidents—where effective interaction between IT and OT is critical—are the Security Operations Center (SOC) and the operating company's IT/OT security team. SOC services may be provided by a Managed Security Service Provider (MSSP) or operated in-house. Close cooperation between the SOC and the IT/OT security team is essential to ensure that incident response efforts are context-aware and tailored to the operational environment.

The concept of an Operational Technology Security Operations Center (OT SOC) builds on the well-established IT SOC model, adapting it to OT environments with the primary goal of strengthening real-time monitoring and threat detection across OT systems. However, an OT SOC is often perceived as an extension—or proxy—of IT, which may inadvertently reinforce existing cultural divides between the two domains.

As part of the incident response workflow, the SOC is responsible for notifying offshore management and the first-line emergency management team (EMT) offshore—including the Offshore Installation Manager (OIM)—when a cyber incident is detected from onshore. Intrusions may be identified through the SOC's monitoring tools and network sensors, which are designed to detect Indicators of Compromise (IOCs). In addition, the SOC may receive threat intelligence from external sources, such as Computer Security Incident Response Teams (CSIRTs) and Cyber Threat Intelligence (CTI) providers.

A central focus of collaboration between IT (SOC) and OT personnel is to address the unique challenges of monitoring operational technology (OT) environments. Since SOC practices originate in the IT domain, developing an effective OT SOC requires close cooperation between IT and OT staff. Such collaboration fosters mutual understanding: IT personnel gain deeper insight into the structure, constraints, and operational dynamics of OT systems, while OT personnel become more familiar with IT security tools and monitoring methodologies, and how these can be effectively adapted to OT contexts.

The introduction of an OT SOC can serve as a constructive platform for fostering collaboration, providing a joint operational space that promotes integration and mutual understanding between IT and OT stakeholders. Findings indicate a shared recognition of the need for cooperation and adaptive practices across both domains [28]. Joint work processes not only facilitate the effective deployment and operation of OT SOCs but also act as key enablers for sustained IT/OT integration and the advancement of cross-domain cybersecurity maturity.

Another approach to strengthening an operating company's IT/OT interaction is to establish structured meeting arenas where IT and OT personnel regularly collaborate and exchange knowledge. These dedicated forums provide opportunities for IT staff to gain deeper insight into OT equipment, its operational characteristics, and contextual constraints. At the same time, they enable both IT and OT personnel to build a shared understanding of IT security tools, their capabilities, limitations, and appropriate applications within OT environments.

IT/OT interaction can evolve and mature when actively supported by management through the allocation of adequate resources and sustained organizational commitment. Meeting arenas should be established as structured, recurring forums where personnel can:

- Share domain-specific knowledge
- Exchange ideas and perspectives
- Collaboratively address IT/OT challenges with flexibility
- Learn from both individual and shared experiences
- Participate in cybersecurity training and exercises tailored to managers as well as IT/OT personnel

Deliberate efforts to identify common ground and build mutual trust are essential for enabling effective cross-domain interaction. Collaborative environments promote shared understanding and problem-solving, facilitating effective IT/OT interaction without requiring complete cultural alignment. Instead, they support integration through dialogue, adaptability, and continuous learning.

Participation in these collaborative activities should be recognized as an integral part of routine responsibilities, rather than deprioritized in favor of immediate operational demands. Fostering a mindful and collaborative work environment further strengthens cross-domain understanding and supports the development of sustained cooperation between IT and OT personnel.

With respect to language and culture, full cultural alignment between IT and OT domains is not a prerequisite for effective collaboration [28]. Instead, fostering mutual awareness and understanding of each domain's cultural norms and specialized terminology provides a sufficient foundation for successful interaction—both in day-to-day operations and during irregular or unexpected events. Each domain operates within a distinct context and is guided by different priorities, which naturally shape their respective approaches to cybersecurity.

For example, IT security practices are typically guided by the principles of confidentiality, integrity, and availability (CIA). In contrast, OT security practices emphasize safety, availability, and integrity, with a strong focus on maintaining continuous and stable operations.

Recognizing and respecting these fundamental differences fosters more effective collaboration between IT and OT personnel without imposing artificial or counterproductive alignment of practices. Instead of forcing convergence, promoting mutual understanding and complementary interaction enables each domain to contribute its unique strengths toward achieving shared cybersecurity objectives.

4 Monitoring and follow-up of cybersecurity barriers

This chapter addresses the monitoring and follow-up of cybersecurity barriers over the short, medium, and long term (Sections 4.1–4.3). It outlines processes for monitoring and managing cybersecurity threats, vulnerabilities, and barrier impairments, structured into three sub-processes: threat landscape monitoring, vulnerability management, and cybersecurity barrier monitoring (Section 4.4). Finally, the chapter discusses the integration of safety and cybersecurity barrier management (Section 4.5).

Sections 4.1–4.3 describe methods and tools for monitoring and following up cybersecurity barriers, while Section 4.4 presents processes and procedures for such monitoring—particularly for short-term and, to some extent, medium-term follow-up. Section 4.4 also broadens the scope by including processes for managing threats and vulnerabilities, in addition to monitoring and handling cybersecurity barrier impairments.

Section 4.5 addresses the overarching goal of integrating safety and cybersecurity barrier management and incorporates insights from current industry practices on key aspects of such integration.

Although methods, tools, processes, and procedures exist for monitoring and following up cybersecurity barriers, making this truly operational remains one of the main challenges in cybersecurity barrier management—i.e., *"to do what we say we will do."*

Chapter 3 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?*" In addition, it provided guidance on how to develop, implement, and verify cybersecurity barrier requirements.

In this chapter, we take a deeper look into the verification of these requirements and explore two additional questions: "*How can the status of cybersecurity barriers be assessed?*" and "*How can the security levels of cybersecurity systems and components be verified?*" Cf. key question no. 3 and 4 in Section 1.2.

The identified cybersecurity barriers and their corresponding performance requirements are typically documented in a *barrier strategy* and an associated *performance standard*, as illustrated in Figure 4.1.

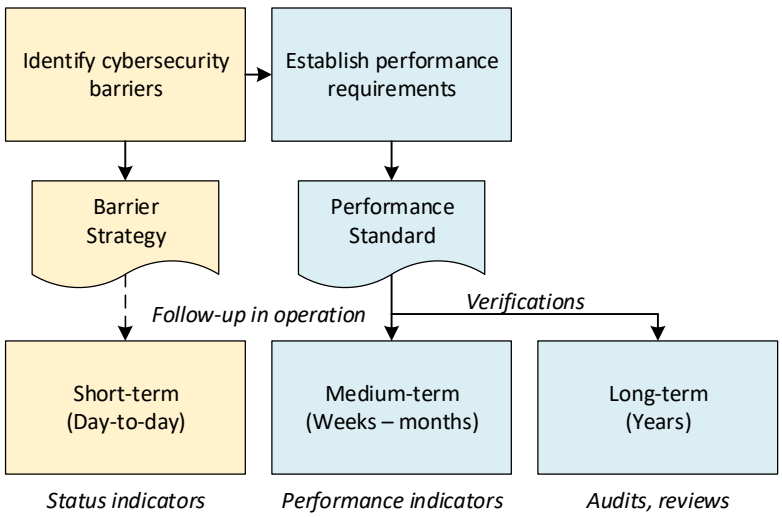


Figure 4.1 Monitoring and follow-up of cybersecurity barriers and performance requirements

This figure also emphasizes the importance of following up on cybersecurity barriers and requirements during the operational phase—specifically by monitoring the status of the barriers and verifying that their performance requirements continue to be met.

It is also worth noting that the colour scheme in Figure 4.1 corresponds to the flowchart presented in Figure 3.2, where yellow represents Steps 1–5 and blue represent Steps 6–9.

The identification of cybersecurity barriers is mandated by MR § 5, Subsection 3 (cf. Section 2.1), 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 method outlined in Chapter 3 (Section 3.2) includes non-barrier cyber-security measures (steps 1 and 9), follow-up in operation may encompass both cybersecurity barriers and general cybersecurity measures, the latter in order to fulfil FR § 34a.

4.1 Short-term follow-up

This section addresses the short-term follow-up of cybersecurity barriers, focusing on the barrier panel tool (Section 4.1.1) and short-term status indicators for use in tools such as the barrier panel (Section 4.1.2). It responds to key question no. 3 in Section 1.2: *"How to assess the cybersecurity barrier status?"*

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.

4.1.1 Status panel

Regulatory requirements do not specify how personnel should be made aware of the status of cybersecurity barriers. In safety barrier management, however, a common approach is to present the status through a *barrier panel*, typically using a *traffic light system* to visually indicate the condition of each barrier. An example of such a panel is shown in Figure 4.2 and has also been applied in cybersecurity barrier management.

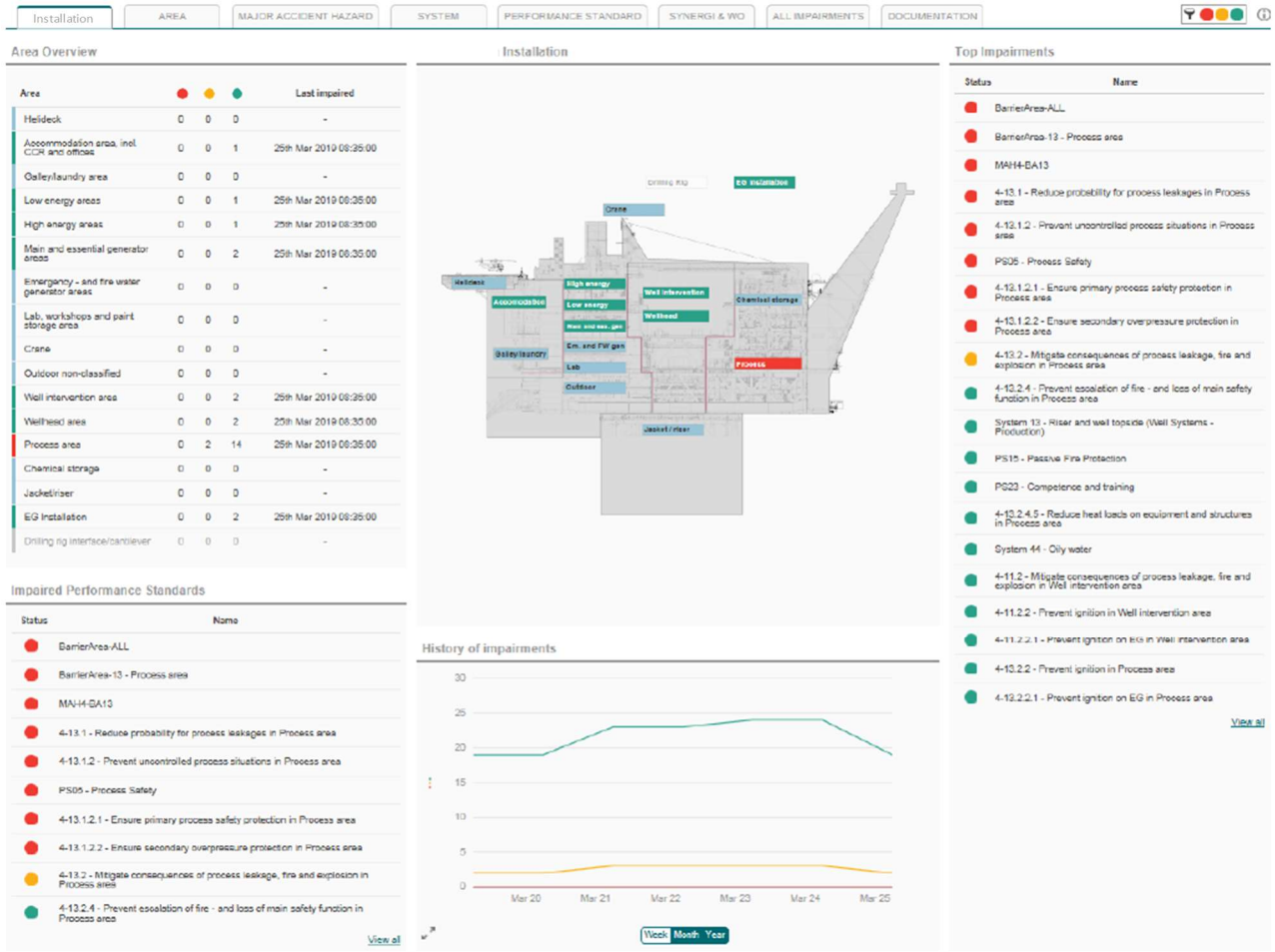


Figure 4.2 Example of barrier panel (front page)

The status displayed in the barrier panel is derived from information automatically collected from various primary sources such as the incident reporting system—which captures non-conformances—and the maintenance system, which tracks status information from 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[9] 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.

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 integration of cybersecurity barriers in an existing safety barrier panel raises some issues, one concerning *confidentiality* and another concerning the treatment of *vulnerabilities*.

[9] A tag is a unique code that defines the functional location and function of a physical component in a facility, e.g., 87ID221 for a specific backup server or 87IQ226 for a given firewall.

Confidentiality

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.

Vulnerabilities

How should vulnerabilities be treated in assessing the status of cybersecurity barriers?

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*.

IEC 63069 [21] 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 [22] states that *"threats exploiting vulnerabilities lead to failure."*

Given this, an important question arises: *How should vulnerabilities be treated when assessing and reporting the status of cybersecurity barriers? Should they be considered impairments by default, or only when certain conditions are met—such as active exploitation or a high severity rating?* To address these questions, it is useful to distinguish between two types of vulnerabilities: *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 Section 4.4.5 and in the third summary report on handling barriers [3].[10]

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. Engineering phases are mostly focused on general vulnerabilities, and through various assessments identify any missing cybersecurity measures (which may lead to modifications).

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*[11], 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.

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. In addition, visualizing vulnerabilities in such panels raises confidentiality concerns, particularly related to access control, as discussed earlier.

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.

4.1.2 Short-term status indicators

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 barrier 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*.

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.

[10] It should be noted that while vulnerability management is a continuous process during the operational phase, patching is typically performed only occasionally during the engineering phases—most often during testing activities (such as FAT, SAT, and commissioning)—since the equipment is powered down and stored or preserved at yards.

[11] 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).

Examples of status indicators—conditions or impairments—corresponding to red, yellow or green status of a barrier tag are provided in Table 4.1 for technical barrier elements, and in Table 4.2 for non-technical barrier elements. These are intended to offer insights into the types of indicators that may be relevant for assessing the status of barrier elements.

Additionally, there are rules for adjusting the status during barrier impairment handling (cf. Section 4.4.5) and rules or algorithms for aggregating status from the barrier tag level up to the area and facility levels.

Table 4.1 Example of status rule set for technical barrier elements

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.

Table 4.2 Example of status rule set for non-technical cybersecurity barrier elements

Rule set – non-technical cybersecurity barrier elements	Signal	Source
The following conditions give a **RED** status light on non-technical cybersecurity barrier elements		
If required/mandatory courses, training or experience are missing	UQ	HRM
If required certificates are missing	CE	HRM
If incomplete emergency preparedness training (< 50% last 12 months)	EPT	ETC
If required personnel unavailable	UP	HRM
The following conditions give a **YELLOW** status light on non-technical cybersecurity barrier elements		
If required/mandatory courses, training or experience is overdue	DQ	HRM
If incomplete emergency preparedness training (≥ 50% and < 100% last 12 months)	EPT	ETC
If backup personnel unavailable	UBP	HRM
If workload too high	WL	Synergi
If checklists/procedures incorrect or unsuitable *	IP	Synergi
If checklists/procedures unavailable at required locations *	UPR	Synergi
If none of the above, the barrier element shows as **GREEN** in the barrier panel		

* These are related to operational barrier elements, whereas the rest are related to human barrier elements.

Information that signals a *critical functional failure*—triggering a *red status indication* on the barrier panel—includes the following conditions:

- *Unqualified Personnel (UQ):* Mandatory courses, training, or required experience are missing. This information is sourced from the Human Resource Management (HRM) system.
- *Missing Certificates (CE):* Required certifications have not been obtained, based on data from the HRM system.
- *Incomplete Emergency Preparedness Training (EPT-C):* A significant shortfall in completed training sessions—less than 50% of planned emergency preparedness training completed. This is based on data from the Emergency Training Compliance (ETC) system.
- *Unavailable Personnel (UP):* Required personnel are not available, as reported by the HRM system.

Information that indicates a *degraded functional failure*—triggering a *yellow status indication* on the barrier panel—includes the following conditions:

- *Degraded Qualifications (DQ):* Mandatory courses, training, or experience are overdue. Data sourced from the Human Resource Management (HRM) system.
- *Incomplete Emergency Preparedness Training (EPT):* Between 50% and 100% of planned training activities have been completed. Based on data from the Emergency Training Compliance (ETC) system.
- *Unavailability of Backup Personnel (UBP):* Required backup personnel are not available, as reported by the HRM system.
- *High Workload (WL):* Excessive workload reported, potentially affecting performance. Data obtained from Synergi or another incident/deviation reporting system.
- *Incorrect or Unsuitable Procedures (IP):* Procedures or checklists are inappropriate or not aligned with operational needs. Identified through systems such as Synergi.
- *Unavailable Procedures (UPR):* Required procedures or checklists are missing at designated locations. Also reported through systems such as Synergi.

Note: The last three indicators—displayed in grey font—may be classified as *Performance Influencing Factors (PIFs)*. These do not reflect barrier status directly but provide indirect insights into the overall condition and effectiveness of the barrier elements.

Tables 4.1 and 4.2 are partly based on existing practices in safety barrier management. Using the same practices for cybersecurity barrier management as for safety barrier management will facilitate the integration between cybersecurity and safety barrier management (cf. Section 4.5).

4.2 Medium-term follow-up

This section addresses the medium-term follow-up of cybersecurity barriers, presenting an existing tool in Section 4.2.1 and a new method in Section 4.2.2.

A tool used for medium-term follow-up of cybersecurity barriers is the Technical Integrity Management Program (TIMP), which—like the barrier panel—was originally developed for safety barrier management and later adapted for cybersecurity barrier management.

Unlike the barrier panel, TIMP is not intended for visualizing current impairments of barriers. Instead, it is primarily linked to MR § 5, Subsection 4, which concerns the definition of performance requirements and the implicit regulatory expectation of verifying barrier performance. TIMP is briefly introduced in Section 4.2.1 and is further detailed in the Technical Barrier Report [1].

When examining the verification of cybersecurity barrier performance on a medium-term basis—i.e., weekly to monthly—the focus shifts to the question: *"How can the security levels of cybersecurity systems and components be verified?"* This corresponds to key question no. 4 in Section 1.2 and is closely linked to the IEC 62443 concept of security levels, particularly the monitoring of the Operational Security Level (SL-O). This topic is further discussed in Section 4.2.2.

The follow-up of verification activities—such as those outlined in verification strategies like the one for control system backup shown in Table 3.1—will be presented in Section 4.3 on long-term follow-up. These strategies typically encompass both medium-term and long-term verification activities, ensuring that performance requirements are consistently met over time.

4.2.1 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[12] (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 4.3. A TIMP assessment for each performance standard is conducted every third month.

[12] See Section 5.3.2 in the Technical Barrier Report [1] for a description of TCS.

Figure 4.3 TIMP visualization of technical barrier status [5]

For cybersecurity, the company utilizing this tool has introduced an additional performance standard, which is visualized alongside the safety performance standards within the TIMP bow-tie diagram. A more detailed description of this approach is provided in Section 5.2.2 of the Technical Barrier Report [1].

4.2.2 Monitoring of Operational Security Level (SL-O)

As described above, the question *"How can the security levels of cybersecurity systems and components be verified?"* is closely linked to the IEC 62443 concept of Security Levels (SL) and the monitoring of the Operational Security Level (SL-O). In other words, it must be ensured that the security levels maintained during operation (SL-O) are aligned with the approved security levels that were established during design and implemented during construction—referred to as the Implemented Security Level (SL-I).

This approach is analogous to the concept of Safety Integrity Level (SIL) in functional safety, particularly the practice of monitoring "SIL in operation." The terms SL-O and SL-I are newly introduced in IEC 62443-1-1 [29], whereas the previously used term Achieved Security Level (SL-A) is now deprecated.

In addition, two related terms—Maturity Level (ML) and Security Protection Rating (SPR)—are also relevant. The SPR is a function of both SL and ML, and these concepts are important for the evaluation of cybersecurity barriers, as they provide a more comprehensive view of both technical capability and organizational readiness. The ML concept is derived from the Capability Maturity Model Integration (CMMI), which defines five maturity levels (1–5), whereas IEC 62443 defines four maturity levels (ML 1–4). An ML of 3 or higher indicates that human activities are documented and that responsible individuals consistently perform these activities in accordance with the documented procedures.

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.

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 4.3 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 4.3 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. 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 4.3.

In the examples presented in Table 4.3, 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 62443-1-1 [29] 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 signal 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?* 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 related 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 [30]. 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, since there are no configuration functions inside these “pipes”.

As a result of this conceptual distinction, conduits have not been included in the analysis presented above—for example, in Table 4.3—which focuses exclusively on zones and their associated SL-I and SL-O values.

It should be noted that SL-O (and Security Levels in general) is a concept introduced in the IEC 62443 standard and is not limited to cybersecurity barriers. Instead, it encompasses all cybersecurity measures that contribute to the overall Security Level (SL), as defined within the IEC 62443 framework.

4.3 Long-term follow-up

As noted in the previous section, verification activities outlined in strategies such as the one for control system backup (Table 3.1) encompass both medium-term (weekly to monthly) and long-term (annual) verification activities. These are addressed collectively in Section 4.3.1.

Section 4.3.2 provides a review of current industry practices related to verification activities.

4.3.1 Verification strategies and activities

Tailored and operationalized cybersecurity verification activities should be readily available to support both medium-term and long-term follow-up. Examples of such verification strategies—for control system backup and intrusion detection—are presented in the Technical Barrier Report [1], consisting of six and seven

verification activities, respectively. These strategies include a mix of medium- and long-term verification actions.

The verification strategy for control system backup is also reproduced in Table 3.1 for reference. In addition, examples of verification activities applicable to non-technical barrier elements are provided in Section 2.3.2 of the Non-technical Barrier Report [2].

Tailored means that the barriers or measures should be relevant to the specific operator and facility, and that the frequency of verification activities should be appropriately adapted to the operational context.

Operationalized means that the verification process must be clearly defined—specifying how the verification is to be conducted and what constitutes an acceptable outcome. This is exemplified in Section 3.4.

MR § 5, Subsection 3, states: *"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."* This clause underscores the requirement for clearly defined barrier strategies.

Accordingly, *verification strategies* may be incorporated into the overall barrier strategy in one of two ways:

- Direct inclusion within the barrier strategy document itself, with all details specified; or
- Indirect referencing external systems, such as maintenance management systems or other relevant systems.

Alternatively—or additionally—these links to verification activities may be provided through the *performance standards*, ensuring traceability and integration across documentation. This is further discussed in the next section.

4.3.2 Performance standard verification activities

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

An adapted version of this summary is presented in Table 4.4.

Table 4.4 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 3rd 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 provides a very useful overview, though there is room for 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 clearly defined frequencies. For example, the entry *"Perform regular review/audit"* does not specify what "regularly" entails. Clearly listing all verification activities—together 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.

4.4 Process and procedures for monitoring and handling cybersecurity threats, vulnerabilities and barrier impairments

Sections 4.1–4.3 described methods and tools for monitoring and following up cybersecurity barriers over the short, medium, and long term. This section presents processes and procedures for such monitoring, with particular emphasis on short-term and, to some extent, medium-term follow-up. It also broadens the scope beyond Sections 4.1–4.3 by including processes for managing threats and vulnerabilities, in addition to monitoring and addressing cybersecurity barrier impairments.

The handling of cybersecurity threats, vulnerabilities, and barrier impairments in operational technology (OT) environments is based on a continuous process of gathering and processing relevant information from both external and internal sources. This includes data on potential mitigations, such as patch availability and advisories. The information flow is structured to provide a comprehensive overview of the current cybersecurity posture across all OT assets, thereby facilitating timely risk assessment and treatment [31].

An overview of this process, the Continuous Risk Assessment and Mitigation Process (CRAMP), is illustrated in Figure 4.4.

A part of the OT asset landscape comprises cybersecurity defences designed to protect and defend the more critical systems—commonly referred to as the *"crown jewels"*—which are responsible for the direct control of physical processes. Some of these OT-level cybersecurity defences serve as *cybersecurity barriers*, providing an additional layer of protection beyond traditional IT-level cybersecurity measures. Their role is particularly important in managing post-compromise or abnormal situations.

This perspective aligns with the definition of a cybersecurity barrier presented in Section 1.1, where such barriers are defined as measures intended to (a) detect abnormal conditions, (b) prevent abnormal conditions from developing, or (c) limit the damage caused by cyber incidents.

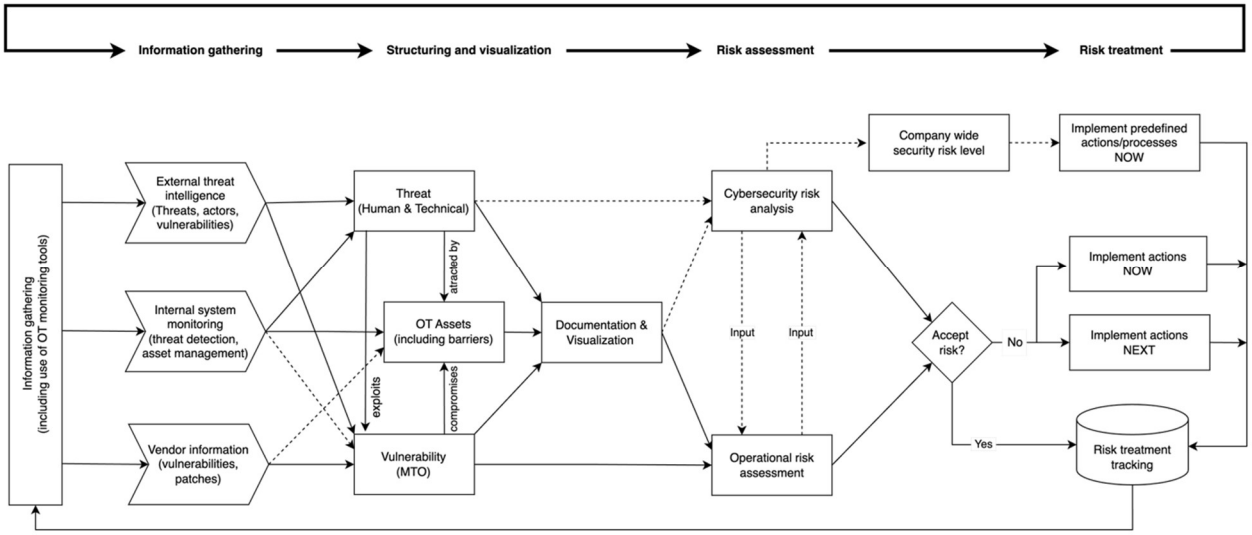


Figure 4.4 Information gathering, structuring, risk assessment, and risk treatment process

The different parts of the process are described in the following sections, beginning with the *main phases* outlined in Sections 4.4.1–4.4.4, namely:

1. Information gathering
2. Structuring and visualization
3. Risk assessment
4. Risk treatment

This is followed by the *subprocesses* described in Section 4.4.5:

- Threat landscape monitoring
- Vulnerability management
- Cybersecurity barrier monitoring

4.4.1 Information gathering

Information about threats, specific vulnerabilities, and associated recommendations for mitigation measures—such as patching—comes from a variety of *external sources*. These sources can be categorized into two main types. The first includes external threat intelligence information on threats and vulnerabilities, typically provided by specialized service providers such as threat hunting firms and CSIRTs. The second type consists of guidance on mitigation measures, such as vulnerability patching, which generally originates from the vendors of the affected equipment, i.e., vendor information.

In addition to the two main categories of external information, internal data is also collected through *internal system monitoring*, including any impairments of the cybersecurity barriers.

Together, these form a continuous flow of information that must be handled, also on a continuous basis because the threat landscape is constantly evolving, and because new vulnerabilities and weaknesses may be identified. This information may reach several roles in the organization, but for this report we focus on typical OT cybersecurity roles.

Figure 4.5 illustrates the external information (upper part) and internal information (lower part) provided on threats, vulnerabilities, and barrier impairments.

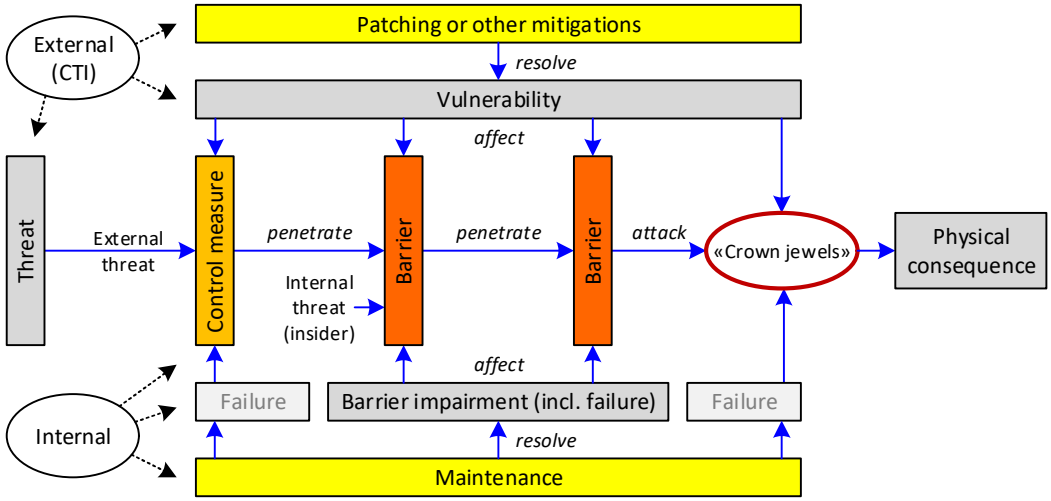


Figure 4.5 Information gathering in relation to cybersecurity barriers

As stated in Section 1.1, barriers complement preventive controls, which are illustrated in Figure 4.5 as control measures such as perimeter firewalls and data encryption. In this context, cybersecurity barriers—including intrusion detection systems (IDS), and backups—serve to protect crown jewels, such as programmable logic controllers (PLCs), engineering workstations (EWSs), and safety instrumented systems (SISs), to avoid physical consequences of a cyber-attack.

Cyber Threat Intelligence (CTI) provides information not only about threats and threat actors, but also about vulnerabilities and potential mitigations, such as patching. CTI also encompasses insights gained from previous attacks, including detailed information on Tactics, Techniques, and Procedures (TTPs) used by adversaries. MITRE ATT&CK is a relevant source for TTPs [32].

A significant portion of this intelligence originates from *external sources*, particularly when vulnerabilities are defined in terms of specific identifiers, such as Common Vulnerabilities and Exposures (CVEs). Specific vulnerabilities (CVEs) can affect both IT and OT assets. If exploited, these vulnerabilities may lead to functional failures of the affected assets. However, as long as the vulnerabilities remain unexploited, the assets typically continue to function as intended.

In addition to such vulnerabilities, assets may also experience failures that result in an immediate degradation of function—either a complete failure (non-functioning) or a partial reduction in performance, commonly referred to as an *impairment*. This distinction is particularly important in the context of cybersecurity barriers, where asset functionality directly influences protective capabilities.

Whereas information on threats and specific vulnerabilities (e.g., CVEs) primarily originates from external sources, information on barrier impairments is derived from *internal monitoring and diagnostics*. It is important to distinguish between two types of internal monitoring:

1. *Monitoring as a barrier function*—for example, an Intrusion Detection System (IDS) monitoring for intrusions, which relates to the *cybersecurity status of the OT system*.
2. *Monitoring of the barrier itself*—i.e., determining whether the IDS is functioning as intended, which relates to the *cybersecurity barrier status*.

A key remark regarding Figure 4.5 concerns the role of patching and maintenance, represented by the yellow boxes. While patching is vital for addressing vulnerabilities in cybersecurity barriers, and maintenance is critical for sustaining both cybersecurity and safety barriers, it is important to emphasize that these activities are not barriers themselves. Instead, they influence the performance of barriers and are therefore categorized as *Performance Influencing Factors* (PIFs).

PIFs constitute a third category of risk-reduction measures, distinct from:

- Control measures (orange bar): applied during normal operational conditions, and
- Barriers (red bars): activated or relied upon during abnormal or failure scenarios.

This categorization is introduced in Section 2.1 and further elaborated in the Technical Barrier Report [1].

The information an operating company gathers about threats and vulnerabilities is often both overlapping and complementary, and there is no clear-cut distinction between the two external information categories depicted in Figure 4.4. For example, patch-related information may originate not only from the equipment vendor responsible for developing and distributing the patch, but also from external sources such as CSIRTs—e.g., KraftCERT/InfraCERT[13]—or specialized cybersecurity service providers such as Dragos[14].

The information gathered from various sources is often complementary in terms of both timeliness and informational richness—factors that can be critical for effective cybersecurity response. For instance, some operating companies utilize international CSIRTs located in different time zones, such as ThaiCERT[15], to receive early warnings relative to their own local time and working hours. Conversely, later reports on a vulnerability—such as a CVE—may provide more detailed and actionable guidance on recommended mitigation measures, including patching.

As a result, obtaining what appears to be *"the same"* information from multiple sources can be highly valuable. However, this must be balanced against the risks of information overload and the associated costs and resource demands involved in processing and validating overlapping inputs.

Not all personnel within an operating company require access to the same information. Data that is critical for certain roles may be irrelevant—or even distracting—for others. This is particularly true for high-level intelligence on threats and threat actors, which may be essential for strategic decision-makers but of limited practical use to frontline technical staff.

Maintaining an overview of barrier status is fundamental to effective cybersecurity barrier management. For this reason, internal monitoring is positioned at the center of Figure 4.4—situated between the two categories of external information—to reflect its central role in integrating and contextualizing threat and vulnerability data.

In addition, internal monitoring of OT assets provides information that is essential for effective vulnerability management. This includes data such as software and patch versions, system configurations, and other asset-related details. While much of this information is typically stored in systems such as a Configuration Management Database (CMDB), it is not always consolidated in a single, unified source—creating challenges

[13] InfraCERT
[14] www.dragos.com
[15] Homepage - Thailand Computer Emergency Response Team (ThaiCERT)

for timely and accurate vulnerability assessments. Therefore, the use of an automated OT asset inventory system that integrates with the ticketing system should be considered.

4.4.2 Structuring and visualization

The information collected from external and internal sources is structured into three key categories: threats, vulnerabilities, and the status of OT assets—with particular emphasis on the condition of cybersecurity barriers and any impairments (cf. Section 4.1). This structured information supports the execution of three main subprocesses: threat landscape monitoring, vulnerability management, and cybersecurity barrier monitoring[16].

These subprocesses are outlined in Section 4.4.5.

Threats are typically reported through periodic updates—such as weekly threat landscape reports—which may cover various types of security threats, including those related to cybersecurity. Vulnerabilities, on the other hand, are continuously documented as *service tickets* within a dedicated vulnerability management system. These tickets are then processed for further handling, including risk assessment and treatment. However, both threats and vulnerabilities may be "*fast-tracked*" if they require immediate attention.

The visualization of cybersecurity barrier status—including the use of barrier panels—is described in Section 4.1.

4.4.3 Risk assessment

The process described in Figure 4.4 broadly distinguishes between overall cybersecurity risk analysis and operational risk assessment, both of which may employ various methods. The overall cybersecurity risk analysis is generally more comprehensive than the operational risk assessment, which is conducted more frequently and often within shorter timeframes. This distinction can also be framed as a differentiation between "system-level" and "component-level" risk assessments.

Overall cybersecurity risk analysis

Risk assessments are conducted during the design phase of a facility and are reused during upgrades or modifications involving new OT assets. These system-level risk assessments—or other overarching risk analyses—can inform evaluations of the company-wide security risk level and serve as input to component-level operational risk assessments.

For example, weekly security updates may be conducted to evaluate the general threat landscape across different regions of the world. These updates typically cover cyber threats and threat actors, including those specifically targeting industrial control systems. Such assessments represent the general threat level facing the organization. Based on this overall cybersecurity risk analysis, the company-wide security risk level is determined. For each facility, predefined physical and cybersecurity measures are implemented, with final decisions made by the respective Offshore Installation Manager (OIM).

Operational risk assessment

For day-to-day operations, a simplified process is used to assess previously unknown threats and vulnerabilities. This assessment is primarily based on network diagrams and OT asset inventories, or similar

[16] In the CBM project we focus on impairments of cybersecurity barriers, although – as shown by Figure 4.5 – failures affect control measures and crown jewels in addition to the barriers.

databases documenting the equipment used within the facility. A general operational risk assessment process at the component level may include the following steps:

1. *Asset identification:* Verify whether the potentially affected OT asset is installed in the facility by consulting the OT asset inventory and the Configuration Management Database (CMDB).
2. *Initial severity assessment:* Conduct a preliminary assessment of severity based on the asset's network location and its potential impact on operations or safety.
3. *Registration:* Register the vulnerability as a service ticket[17] to initiate formal handling and tracking.
4. *Notification:* Inform the OT asset owner about the identified vulnerability.
5. *Risk assessment:* Collaboratively assess the risk of the vulnerability with the OT asset owner, considering asset criticality and exposure.
6. *Decision and implementation of measures:* In coordination with the OT asset owner, decide on and implement appropriate risk treatment measures, such as:
    a. Patching
        i. Immediately (NOW)
        ii. During the next opportunity (e.g., a production shutdown) (NEXT)
        iii. Do not patch (NEVER)
    b. Compensating measures
    c. Nothing

Further considerations related to impact assessment are detailed in the Barrier Handling Report [3].

The CVE score included in vulnerability notifications can provide an indication of associated risk. However, it should not be interpreted as a direct measure of the vulnerability's severity. Risk assessments become more complex when vulnerabilities are found in OT-specific devices. In contrast, for standard IT software—such as antivirus programs, virtual private network (VPN) solutions, or Microsoft-based network components—the assessment process is generally more straightforward and easier to carry out.

Documenting vulnerability information as service tickets allows assigned OT cybersecurity personnel to systematically follow up on them. This approach serves as a proactive reminder to evaluate whether each vulnerability requires immediate attention or can soon be resolved. For more critical vulnerabilities—and threats—that cannot be promptly addressed, it is important to record them in a risk register. This register should be regularly reviewed at the management level to ensure appropriate oversight and risk mitigation.

To enter a vulnerability into the risk register, the OT asset owner—typically the Asset Operations Manager or Offshore Installation Manager—must first understand the significance of the vulnerability. However, this can be challenging in practice. To support this process, OT personnel should maintain a supplementary register for documenting critical vulnerabilities. This register can also facilitate information sharing between facilities and serve as a basis for discussions with facility management.

For vulnerabilities that cannot be resolved but are deemed acceptable, the corresponding service ticket may be closed. To ensure traceability, explanatory comments must be added to justify why mitigation measures were or were not implemented. Before the ticket is closed, this decision must undergo a quality control process to confirm that the associated risk has been appropriately addressed.

[17] A service ticket is used to verify whether the relevant product is in use within the company and to determine whether patching should be performed “now, next, or never”. If patching is required, a work order (and work permit) is prepared when the OT system is located offshore. For onshore OT systems, a different case-handling system may be used, such as ServiceNow (following an ITIL change process).

4.4.4 Risk treatment and tracking

General actions

Actions are taken based on the criticality of the identified threat or vulnerability. In particularly severe cases, the situation is managed as a cybersecurity incident, prompting the mobilization of internal resources across the organization. When necessary, external support—such as from KraftCERT—may also be engaged. In such cases, the time and effort invested are considered worthwhile to resolve the issue effectively.

However, these efforts often represent short-term measures aimed at improving monitoring and enabling a faster response should the threat materialize. Typically, such situations lead to the patching of critical systems or the implementation of mitigation measures, such as disconnecting affected systems or reconfiguring firewalls.

The most invasive mitigation measure is a complete shutdown of the facility. This action carries significant risks, including those associated with an unscheduled shutdown, the complexity of a subsequent restart, and the resulting loss of production.

An alternative action, when a threat or vulnerability is imminent, is to transition the facility into so-called *island mode*. In this state, the facility is disconnected from central onshore systems—and critically, from the internet. While this enhances cybersecurity isolation, it also introduces limitations: remote support and patch deployment are no longer possible, and the central onshore facility loses visibility into operations on the offshore site.

The decision to enter island mode is made by the Offshore Installation Manager. The island mode procedure has been formalized, verified, and is now incorporated into training scenarios.

Patching

For a vulnerability to be considered critical and associated with high risk, it typically must have a high CVE score and affect an OT asset that, when exposed, has the potential to communicate with other OT systems and the internet.

In contrast, non-critical vulnerabilities—those assessed as low risk—do not require immediate patching. In such cases, updates are usually deferred and grouped together for implementation during the next scheduled maintenance period. This may coincide with a full system overhaul or planned maintenance of specific parts of the facility.

In cases where patches are unavailable or cannot be applied, compensating measures must be implemented. These may include restricting the system's functionality or disconnecting it from the network or the internet to reduce exposure and potential risk.

Further guidance on patching strategies and procedures can be found in the Barrier Handling Report [3].

Identified challenges in handling threats, vulnerabilities and patches

Overview of OT assets

One of the main challenges in managing OT cybersecurity is maintaining a comprehensive and up-to-date overview of OT assets and their physical and logical locations—typically recorded in a Configuration Management Database (CMDB). This is particularly difficult for assets that are rarely interacted with or are unique to a specific facility. While this information exists, it is often fragmented across multiple systems, making it difficult to consolidate and assess effectively.

Automating the identification of OT assets used within a facility, along with highlighting their physical placement and position in the network, would significantly streamline the vulnerability criticality and risk assessment process. However, the connection between physical devices and the logical network architecture is not always clearly documented or easy to assess. Here digital twins may be a solution.

A closely related challenge is the creation and maintenance of a reliable OT asset inventory. Not all devices are automatically detected or registered, which undermines completeness. Improved processes and supporting tools are necessary to establish accurate inventories for both new and existing facilities, and to ensure their upkeep throughout the facility's operational lifetime.

Manual effort

Additionally, the patching process is currently perceived as highly manual and resource-intensive. This is particularly true for common OT systems such as PCs, servers, and network devices, where greater automation is both needed and desirable. Automation should support the identification of available updates and facilitate their deployment once they have successfully passed necessary testing and validation procedures.

A distributed process

Managing OT cybersecurity threats, vulnerabilities, and barrier impairments involves multiple roles and processes. Experience has shown a clear need for integrated systems that can consolidate information from various sources and provide facility-specific assessments of vulnerability criticality. Such systems would significantly simplify and accelerate decision-making and the implementation of appropriate actions.

Currently, risk treatment activities—including the tracking of identified risks, compensating measures, and deferred patches—are distributed across multiple unconnected systems. This fragmentation hampers efficiency and consistency. Enhanced automation and integration of these processes would improve oversight, reduce response time, and support more effective long-term risk management.

OT cybersecurity knowledge

In general, foundational knowledge of OT cybersecurity can be strengthened at the management level and among operational roles working closely with OT environments. Additionally, the specific expertise of OT cybersecurity specialists—particularly regarding vulnerabilities, threats, and patch management—is not currently formalized. This lack of structured competence may hinder the efficient handling and mitigation of cybersecurity issues.

4.4.5 Subprocesses

The monitoring and handling of cybersecurity threats, vulnerabilities, and barrier impairments can be divided into three main subprocesses:

1. *Threat Landscape Monitoring*
   Continuous observation and analysis of emerging cyber threats relevant to the OT environment, including trends, adversary tactics, and threat intelligence sources.
2. *Vulnerability Management*
   Identification, assessment, prioritization, and remediation of vulnerabilities in OT systems, based on risk and asset criticality.
3. *Cybersecurity Barrier Monitoring*
   Surveillance of technical and non-technical cybersecurity barriers to detect impairments or weaknesses that could reduce cybersecurity posture.

These subprocesses are briefly introduced here. More detailed descriptions can be found in the Barrier Handling Report [3].

Information regarding the organizational responsibilities for monitoring and managing cybersecurity threats, vulnerabilities, and barrier impairments is also available in the Barrier Handling Report.

Threat landscape monitoring

This subprocess is illustrated in Figure 4.6.

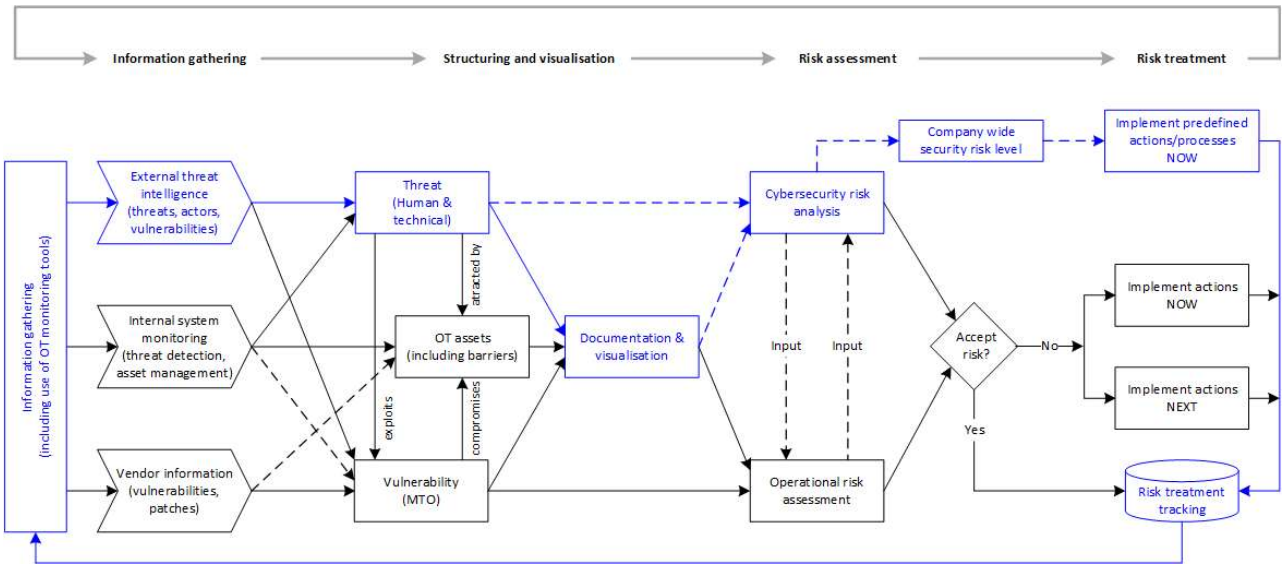


Figure 4.6 Subprocess: Threat landscape monitoring

Information about threats and threat actors is typically collected from multiple sources. This intelligence is often consolidated into weekly reports that support the assessment of the company's overall security risk level.

The security risk model generally consists of four predefined levels; each associated with a specific set of actions. These actions are implemented according to the assessed risk level and are tracked to ensure proper execution and accountability.

In addition, various threat reports and advisories can be leveraged to strengthen cybersecurity measures, including the reinforcement of existing cybersecurity barriers. Detailed insights into threat actor tactics, techniques, and procedures (TTPs) support the prioritization of security actions specifically tailored to defend against known attack patterns.

Vulnerability management

This subprocess is illustrated in Figure 4.7.

Information about vulnerabilities can be sourced from many of the same Cyber Threat Intelligence (CTI) providers that supply data on threats and threat actors, as well as directly from the vendors of affected assets.

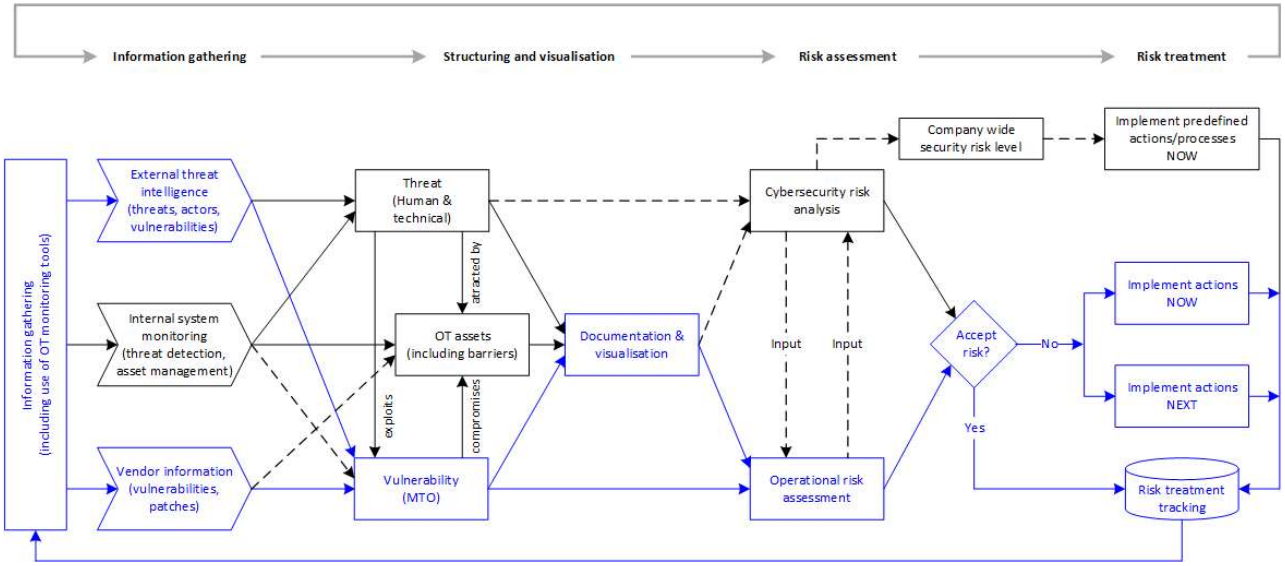


Figure 4.7 Subprocess: Vulnerability management

This subprocess primarily addresses specific technical vulnerabilities—namely CVEs. However, broader vulnerabilities, including those linked to human and organizational factors—commonly framed within the MTO (Man, Technology, Organization) model—are equally important. These general vulnerabilities are typically identified through internal assessments, audits, or feedback from operational activities.

The distinction between specific technical vulnerabilities and general vulnerabilities was introduced in Section 4.1.1, and is further elaborated in the Technical Barrier Report [1].

CVEs are managed internally through operational risk assessment and treatment processes, as outlined in Sections 4.4.3 and 4.4.4, and further detailed in the Barrier Handling Report [3].

CVEs can apply to any OT asset, including control measures, cybersecurity barriers, and high-value assets (crown jewels), as illustrated in Figure 4.5. This suggests that, within the context of cybersecurity barrier monitoring, vulnerabilities could potentially be considered alongside impairments (see Figure 4.4).

However, as outlined in Section 4.1.1, industry partners recommend that specific technical vulnerabilities—such as CVEs—be managed through the established vulnerability management process rather than being integrated into the barrier status panel. An exception to this approach may be considered if the CVEs are first screened to remove “noise”; in that case, it could be reasonable to include them in the barrier panel.

Cybersecurity barrier monitoring

This subprocess is illustrated in Figure 4.8.

Information on the status of cybersecurity barriers is obtained through internal system monitoring of OT assets classified as cybersecurity barriers, cf. Sections 2.1 and 3.2.2.

Cybersecurity barrier impairments can be visualized in barrier panels alongside safety barrier impairments (see Section 5.1 in [1]). These impairments may be addressed in a manner similar to vulnerabilities—through operational risk assessment and treatment processes guided by criticality considerations (cf. Figure 4.7).

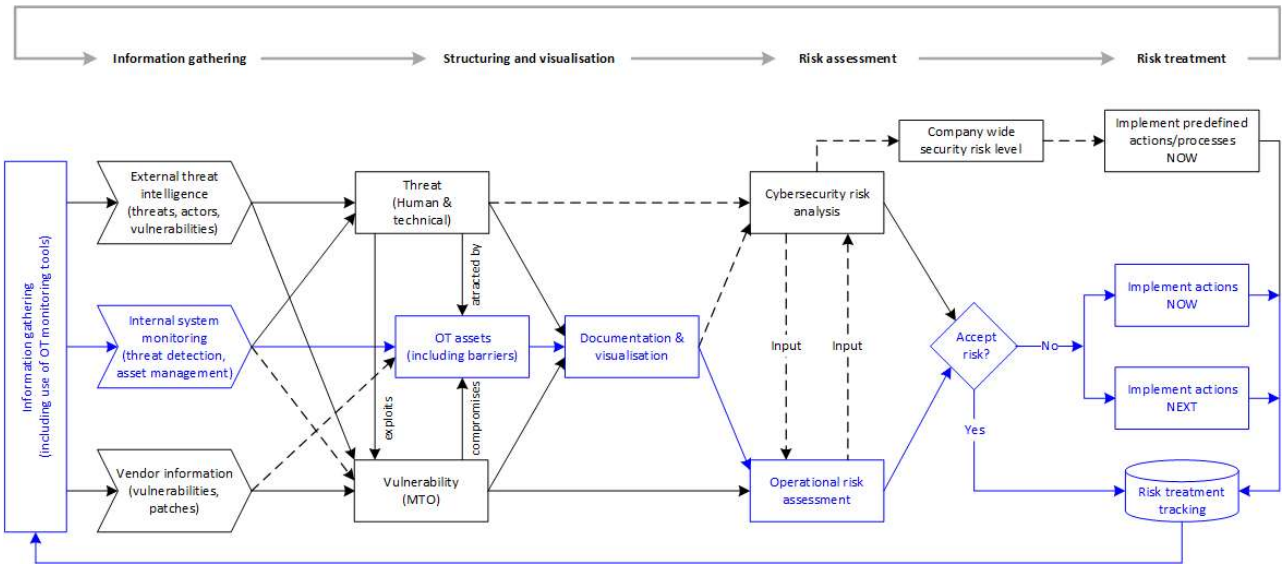


Figure 4.8 Subprocess: Cybersecurity barrier monitoring

Additionally, cybersecurity barriers are followed up through the verification of defined performance requirements, as described in Sections 3.3 and 4.2–4.3. These performance requirements, which are derived from recognized standards such as IEC 62443, encompass both technical and non-technical cybersecurity measures. They form the foundation for medium- and long-term verification activities aimed at ensuring the sustained effectiveness of cybersecurity barriers.

The primary challenge lies in the short-term monitoring and visualization of non-technical barrier elements. While tools such as the barrier panel are effective for displaying the real-time status of technical cybersecurity barriers, they are less suitable for representing non-technical barriers.

Key information related to non-technical barriers—such as personnel competence, training status, and procedural readiness—is typically maintained in separate source systems. Integrating this data into real-time visualization tools remains technically complex and presents a significant obstacle to achieving full situational awareness of non-technical barrier health. Further discussion on this topic is provided in the Non-technical Barrier Report [2].

The threat detection component of internal system monitoring refers to systems such as IDS. These systems are used to identify and detect cybersecurity threats in real time and may themselves be considered part of the overall cybersecurity barrier framework.

However, this subprocess focuses on monitoring the *status* and *performance* of cybersecurity barriers—not on threat detection. The distinction lies in the objective: detecting external threats versus assessing the ongoing integrity and effectiveness of the barriers in place to defend against them.

Further details on the various phases of the cybersecurity barrier monitoring subprocess—with particular emphasis on short-term monitoring—are provided below, beginning with some foundational context.

Foundational context

The barrier strategy, performance standards, or associated documentation or sources (e.g., asset inventories) should provide information on, for example:

- Barrier functions and elements (technical, human, and operational)
- Coverage and mapping to specific areas, zones and assets
- Performance requirements, such as response time and uptime
- Performance influencing factors (PIFs) affecting the barrier elements
- Dependencies, including power supply, upstream barriers, or other supporting systems
- Verification and maintenance activities, including responsible personnel

Information gathering

Internal system monitoring includes information on barrier impairments from sources such as:

- Computerized Maintenance Management Systems (CMMS), e.g., SAP
- Incident and non-conformance reporting systems, e.g., Synergi
- Built-in diagnostics of OT assets and barrier elements, e.g., from SAS
- Status of inhibited or bypassed equipment, e.g., from SAS
- Human Resource (HR) systems, covering personnel competence and training

Information on impairments for short-term monitoring should ideally be collected automatically. In addition, manual reviews and audits are conducted as part of medium- and long-term follow-up, including the performance of non-technical barriers.

Structuring and visualization

The structuring of information on barrier impairments involves classifying the impairments based on the degree to which the barriers are affected. A common classification used in CMMS distinguishes between critical failures, degraded failures, and incipient failures.

A common tool for visualizing the degree of barrier impairments is the barrier panel. Barrier panels typically employ a traffic light system, where:

- Red indicates a critical functional failure (complete impairment)
- Yellow indicates a degraded condition (partial impairment)
- Green indicates normal functioning (no or insignificant impairment)

Examples of status indicators—reflecting conditions or impairments corresponding to red, yellow, or green status—based on the information sources listed above, are provided in Section 4.1.2.

A barrier panel or dashboard should include/present:

- Status on various aggregation levels; highlighting red and yellow statuses
- Impairment handling status
- Overview of last impaired barrier tags
- Overview of top criticalities (of impaired barrier tags)
- Trend, i.e., history of impairments
- Trend in handling impairments
- Link to service tickets, cases, work orders, deviations/non-conformances, etc.
- Link to support documents
- Timestamp of last update

Aggregation levels can follow structures such as:

Barrier tag → Barrier element → Barrier subfunction → Barrier function → Area → Overall installation, and/or *Barrier tag → System → Performance standard → Overall installation.*

A barrier panel is a decision support and risk communication tool used by both offshore operational personnel and onshore support staff. The main objectives of installing a barrier status panel are:

- To provide all users with up-to-date, easily accessible information about the health status of barriers, thereby offering critical insight into the current risk picture.
- To support operational personnel during the planning and preparation of maintenance activities by giving an overview of barriers that are unavailable or degraded in specific areas or zones.
- To assist maintenance personnel by displaying overviews of degraded or failed barrier elements, helping them prioritize maintenance tasks effectively.
- To show trends in barrier status over time, providing valuable input for assessing potential modifications to equipment, its usage, and/or its maintenance routines.

A barrier panel is a practical means of fulfilling the requirement set out in subsection 5 of the Management Regulations § 5 [6]: *"Personnel shall be aware of which barriers and barrier elements are not functioning or have been impaired."*

While full integration of relevant information into a single system—such as a barrier panel—is the goal, current practices often depend on fragmented systems and expert judgment. Future efforts should prioritize the development of unified and automated OT cybersecurity overviews.

Risk assessment

The operational risk assessment of barrier impairments is somewhat similar to the assessment of vulnerabilities. However, a key difference is that relevance does not need to be verified, as all notifications pertain to existing assets (barrier tags) [18] on a specific facility. Another distinction is that parts of the assessment may be pre-prepared. This enables partial automation of the risk assessment process within a barrier panel.

The risk assessment of barrier impairments involves several steps, including:

- Determining the degree of impairment, i.e., assigning a red or yellow status—similar to the classification used for safety barriers.
- Assessing the severity in advance, based on both the level of protection (e.g., Purdue model layer) and the potential impact. For safety barriers, this typically relates to tag criticality, which is based on factors such as redundancy and consequence (in terms of the tag's risk reduction potential).
- Automatically combining status and tag criticality to calculate a tag impairment score. A higher score is assigned to red statuses than to yellow ones for tags with the same criticality. These scores are also used to determine aggregated status at different levels from tags to the overall installation.
- Manually checking whether the impairment affects the barrier function, or whether the associated risk increase is considered insignificant. In such cases, the status may be manually adjusted to green.

Risk treatment

The risk treatment of barrier impairments is similar to the treatment of vulnerabilities. Actions are typically categorized as either immediate (NOW), deferred (NEXT), or none (NEVER)—the latter applying when the risk is accepted. In the case of specific vulnerabilities, the remedy is often patching, whereas for barrier

[18] This requires that cybersecurity measures have been correctly tagged as barrier (or safety critical) elements.

impairments, the typical corrective action is maintenance. In both scenarios, compensating measures can be implemented as temporary risk mitigation.

In safety barrier management, risk assessment and consideration of compensating measures are integral to the impairment handling process. When a barrier panel is used to visualize current status, the implementation of compensating measures prompts a reassessment. Typically, a red status can be credited and downgraded to yellow, while a yellow status may be credited and further reduced to green, reflecting the reduced risk level.

Once barrier impairments have been addressed through maintenance and repair, the corresponding tag status is reset to green.

All actions should be tracked and documented, preferably within a centralized system that ensures traceability and oversight.

4.5 Integration of safety and cybersecurity barrier management

The overarching goal of the project is to integrate safety and cybersecurity barrier management—addressing the central question: "*How to integrate safety and cybersecurity barrier management?*" corresponding to key question no. 5 in Section 1.2. Section 4.5 provides knowledge and guidance to support this integration, beginning with background knowledge in Section 4.5.1 and followed by insights from current industry practices on key aspects of such integration in Section 4.5.2.

4.5.1 Background knowledge

The regulatory background [6] 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 2.2). Furthermore, regulatory authorities explicitly state that cybersecurity must be included as part of overall barrier management [8] (cf. Section 2.3).

In the petroleum industry, some companies have established practices for integrating cybersecurity barrier management with their existing safety barrier management frameworks. 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 [10]. This dual influence—regulatory compliance to both barrier management and ICT security in general—presents several challenges to effective and coherent integration.

The CBM project 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 2.4. As a result, their practices for cybersecurity barrier management also differ considerably.

This disparity served as the primary motivation for initiating the CBM project—to explore the potential for developing a flexible, common framework for cybersecurity barrier management in the petroleum industry that can accommodate such variations across organizations.

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

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 the adoption of a single, standardized solution. Rather, it supports varying degrees of integration and requires flexibility in the selection of implementation approaches to accommodate different organizational contexts and needs.

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 a unified PS, and
- Integrate cybersecurity barrier status into the same visualization tools used for safety barriers (e.g., barrier panels or TIMP bow-tie, cf. Chapter 4) or maintain separate dashboards for cybersecurity monitoring.

In addition, any integration effort must accommodate differences in existing safety barrier management regimes, which can vary significantly between companies. As a result, adaptable solutions are essential to ensure practical alignment with each organization's established practices and operational context.

4.5.2 Integration in industry practices

A central question addressed in this study is: *How is cybersecurity barrier management integrated with safety barrier management in current 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 cybersecurity measures* included in the barrier management system
- *Treatment of technical and non-technical aspects* within the barrier framework
- *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* (e.g., barrier panels or TIMP bow-tie) versus use of separate dashboards

This structured comparison provides valuable insight into how variations in safety barrier management regimes influence the integration of cybersecurity. It also supports the development of a flexible, industry-wide approach that can accommodate such differences across organizations.

Degree of integration between cybersecurity and safety barrier management

In both companies, the integration of cybersecurity into barrier management is implemented as an add-on to existing safety barrier management systems. These are not unified approaches in which cybersecurity and

safety are treated within a single, fully integrated framework. Nor can they be classified as parallel approaches, where both domains are developed and managed concurrently but operate independently of one another.

Instead, cybersecurity barrier management is developed as a separate effort and subsequently adapted and appended to each company's existing safety barrier management structures. This sequential and adaptive approach reflects the historical precedence and greater maturity of safety barrier management within both organizations. It also underscores the growing need to align with evolving cybersecurity regulations and standards.

Scope of cybersecurity measures included in the barrier management system

This issue is examined in detail in Chapters 2 and 3, where a key distinction is emphasized: *cybersecurity barriers* represent a subset of the broader set of cybersecurity measures—just as *safety barriers* constitute a subset of overall safety measures within the context of safety barrier management.

Both companies initiate their cybersecurity barrier management practices by referencing a broad set of cybersecurity requirements. These requirements encompass not only defined cybersecurity barriers, but also more general measures such as policies, procedures, and administrative controls.

In contrast, safety barrier management is more narrowly scoped. It focuses exclusively on measures that qualify as safety barriers, explicitly excluding broader safety controls and performance-influencing factors from the formal barrier inventory.

This mismatch presents significant challenges for integration. Specifically, there is both a conceptual and practical gap between how barriers are defined and managed within the domains of safety and cybersecurity.

A further complication arises from differing regulatory expectations between safety and cybersecurity domains. In safety barrier management, barrier elements are required—by regulation—to comply with clearly defined and verifiable performance requirements. These include specifications for functionality, reliability, and testability, ensuring that safety barriers consistently perform as intended under defined conditions.

In contrast, many cybersecurity requirements focus primarily on the *existence* of security measures, rather than on their *performance parameters* or effectiveness. For instance, a requirement may mandate the implementation of a firewall or access control system, without specifying how its performance should be evaluated in terms of risk mitigation capability or operational reliability.

These discrepancies—both in the scope of what qualifies as a barrier and in the nature of associated requirements—pose obstacles to establishing a coherent and unified framework. Reconciling these differences is essential for developing an integrated barrier management approach that ensures consistency across safety and cybersecurity domains, supports regulatory compliance, and promotes effective risk control.

Treatment of technical and non-technical aspects within the barrier framework

Both companies incorporate technical and non-technical aspects into their cybersecurity and safety barrier management practices. However, the technical aspects are typically addressed in a more comprehensive and systematic manner compared to the non-technical aspects, which often receive less formalized attention.

There are two primary entry points for incorporating non-technical aspects into barrier management practices:

1. *Requirements derived from standards and guidelines*
   These requirements explicitly address organizational and procedural aspects, ensuring that non-technical considerations are formally integrated into barrier definitions and expectations.
2. *Systematic decomposition of barrier functions into barrier elements*
   This approach involves breaking down barrier functions to include both operational and organizational components in safety management, as well as people- and process-related 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 4.2 and 4.3.

The main challenge lies in the short-term monitoring and visualization of non-technical barrier elements, as discussed in Section 4.4.5.

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

Both companies currently maintain a separate PS for cybersecurity. However, there is ongoing discussion within the industry regarding whether it may be more appropriate to integrate cybersecurity requirements into the corresponding safety PSs, rather than maintaining them as standalone documents.

The primary rationale for maintaining a separate cybersecurity PS is to ensure dedicated attention and visibility for cybersecurity concerns, which might otherwise be underemphasized if embedded 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, partial integration is achieved through cross-communication mechanisms between cybersecurity and safety domains. 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 relevant safety PSs. Thus, although the standards are maintained separately, this exchange of information creates a functional linkage that supports integrated risk understanding and coordinated management across both 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 approach reflects a unified treatment of cybersecurity as a domain that inherently

encompasses both technical controls—such as firewalls and intrusion detection systems—and non-technical measures, including organizational procedures, training, and awareness initiatives.

However, this approach differs from how non-technical aspects are addressed within safety barrier management. For instance, one of the companies maintains a separate PS specifically for competence and training related to safety 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 existing visualization tools that were 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.

5 Extended summary of assessments and recommendations

This research is summarized through assessments and recommendations structured around eleven key questions that define the scope of this guidance document. The responses to these questions provide knowledge and guidance on the integration of safety and cybersecurity barrier management, supporting a holistic and coordinated approach to risk control in industrial environments.

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?
6) How to establish and integrate non-technical barrier elements in cybersecurity barrier management?
7) How can interaction between IT and OT domains be improved through new innovative work processes?
8) How to align practice, culture and language between users of office IT systems and ICS?
9) How to gather information about and visualize the status of cybersecurity barriers?
10) How should information from external threat intelligence be managed to maintain cybersecurity barriers?
11) How to handle threats, vulnerabilities and cybersecurity barrier impairments?

The extended summary is primarily based on the discussions and conclusions presented in the three summary reports [1], [2], and [3]. In addition, selected assessments and findings from Chapters 3 and 4 are reiterated to provide context for the recommendations and to allow the summary to be read as a stand-alone section. Recommendations are included in the text as *italicized subheadings* with numbering in parentheses.

This chapter is fairly comprehensive, and an alternative is to proceed directly to the tables listing the recommendations. Further explanation of each recommendation can be found in the text preceding the corresponding tables.

1. How to identify barriers and barrier elements?

This is a fundamental question, as identifying the relevant barriers forms the basis for addressing many of the subsequent issues. Various methods exist for this purpose, with top-down and bottom-up approaches being the most commonly applied. These methods were initially developed within the domain of safety barrier management and were later adapted for cybersecurity barrier management—primarily because the latter builds upon the established frameworks and practices of the former.

Additionally, a new standards-based approach has been developed as part of the CBM project. Furthermore, operational experience indicates that it is essential to account for barrier elements that may be uncovered during operations. The completeness of barrier identification improves when multiple methods are applied in combination. Therefore, the following sections discuss the various approaches—both established and emerging—including common practices within safety barrier management.

Top-down approach in safety barrier management

In safety barrier management, a top-down approach is commonly used to identify barriers and their associated elements. This process typically begins with scenarios derived from Defined Situations of Hazard and Accident (DSHAs), which are developed for major accident risks as part of formal risk assessments. These

scenarios provide the foundation for identifying specific barrier functions. They may be visualized through structured representations such as barrier grids or bow-tie diagrams.

The breakdown from barrier functions to barrier elements occurs in hierarchical layers, progressing through sub-functions, sub-sub-functions, and so on, until each function can be realized by one or more concrete barrier elements. These intermediate functional layers often include Safety Instrumented Functions (SIFs), Safety Functions (SFs), and Safety-Critical Tasks (SCTs). In safety barrier management, the barrier elements are typically categorized into three types: technical, operational, and organizational.

Bottom-up approach in safety barrier management

Experience from safety barrier management demonstrates that a systematic top-down decomposition is not always comprehensive—some barrier elements may remain unidentified. To improve coverage, a complementary bottom-up approach can be employed. This method works by illustrating the logical relationships among barrier elements across all functional levels (e.g., sub-functions, sub-sub-functions, Safety Instrumented Functions (SIFs), etc.) for each barrier function. By doing so, it can reveal additional equipment, tasks, or actions necessary to achieve the barrier function. Implementing this approach depends on having access to detailed system documentation and inventories, including Piping and Instrumentation Diagrams (P&IDs).

Remain open to emerging barrier elements during operations (1.1)

Even when both top-down and bottom-up approaches are applied, operational experience shows that additional barrier elements are often identified during actual system operation. These may include entirely new elements that were not previously considered, as well as existing elements that are retrospectively classified as barrier elements—often because their functional importance becomes evident in practice.

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 central "top event." However, the breakdown from barrier functions to barrier elements has been coarse, with only one level of barrier functions and one level of barrier elements. Intermediate functional layers—such as sub-functions or sub-sub-functions—have not been incorporated into the methodology.

Several challenges—or areas for improvement—have been identified with this practice:

First, the use of scenarios poses a fundamental issue. In safety barrier management, as well as in safety risk and emergency preparedness analyses, there is typically a well-defined and commonly accepted set of Defined Situations of Hazard and Accident (DSHAs). In contrast, cybersecurity lacks a standardized set of incident scenarios, leading to significant variability in both the types and number of scenarios considered. This variability complicates consistent barrier identification and comparison across companies. It also drives up costs in engineering projects, as limited standardization reduces the potential for re-use across projects.

Second, the application of bow-tie diagrams can be misleading. A bow-tie typically illustrates only a single "top event" within what is, in reality, a broader event chain. The choice of which event is defined as the top event directly influences whether associated measures are interpreted as probability-reducing (preventive) or consequence-reducing (mitigative). This distinction affects the understanding of whether a given measure serves as a *control measure* (for maintaining control and normal operations) or as a *barrier measure* (for regaining control after a loss of control). Misinterpretation here can lead to flawed categorization of barriers.

Third, the simplified breakdown structure—consisting of only one level of barrier functions and one level of barrier elements—results in a lack of intermediate sub-functions. This often leads to an incomplete decomposition of barrier functionality, where elements described may actually be sub-functions rather than final, actionable barrier elements. Such ambiguity also complicates the categorization of barrier elements. In cybersecurity, barriers are typically grouped into technical, human, and process-based types; however, a sub-function may encompass more than one of these categories, thereby obscuring clear allocation and responsibility.

It is important to note that the practice described here has been shaped by the adaptation of existing safety barrier management practices within the same organization. This includes, in particular, the adoption of the same number of hierarchical levels in the breakdown of barrier functions.

Recommended improvements to the challenges above include:

Promote industry collaboration on cyber incident scenarios (1.2)
First challenge: The challenge of establishing a comprehensive—yet manageable—set of cyber incident scenarios is one that warrants industry-wide collaboration. This issue is relevant across both project development and operational phases. Scenario development should begin with cybersecurity risk analyses, where the selection and framing of scenarios play a critical role.

Integrate cybersecurity and safety scenarios (1.3)
First challenge, cont.: Moreover, this work may benefit from explicit links to existing safety scenarios, particularly the Defined Situations of Hazard and Accident (DSHAs), thereby enabling a more integrated view of safety and cybersecurity risk landscapes.

Use complete event sequence diagrams (1.4)
Second challenge: An alternative—or complementary—tool to the bow-tie diagram is the barrier grid. Unlike the bow-tie, the barrier grid presents the full sequence of events within the event chain, offering a more comprehensive view. It also allows for explicit linkage to safety DSHAs thereby supporting integrated safety and cyber-security analyses.

Support flexible hierarchical decomposition of barrier functions (1.5)
Third challenge: The breakdown of barrier functions should allow for flexibility in the number of hierarchical levels and should not be restricted to a single layer of barrier elements without intermediate sub-functions. A multi-level structure enables a more accurate and complete representation of the relationships between barrier functions and their implementing elements.

Bottom-up approach in cybersecurity barrier management
The bottom-up approach in cybersecurity barrier management typically begins by identifying relevant ICT systems and equipment—drawing on sources such as topology diagrams from engineering disciplines that operate these systems. The focus has been placed on the systems themselves, rather than on the associated barrier functions and elements.

Upward aggregation has followed the phases of the NIST Cybersecurity Framework (CSF), ultimately leading to the overall Performance Standard (PS), which is viewed as *the* "cyber barrier." This “cyber barrier” is then compared to the safety barriers aggregated at the PS level.

One of the challenges—or particularities—of this approach is the limited connection to barrier functions and elements, which can hinder consistency and complementarity with top-down methods. More generally, a known limitation of bottom-up methodologies is the frequent absence of a complete and up-to-date asset inventory—especially in the context of legacy or existing installations.

The assessment process—beginning with the identification of relevant ICT systems and equipment—is guided by cybersecurity requirements drawn from established sources such as the IEC 62443 standard series and the NIST Cybersecurity Framework (CSF). These requirements are, by default, treated as barrier requirements. A selected subset of them has been reformulated into structured evaluation questions, which are used to assess the medium-term cybersecurity status of the identified ICT systems.

A new standards-based approach in cybersecurity barrier management

Distinguish clearly between general cybersecurity measures and cybersecurity barriers (1.6)

A third approach for identifying barrier functions and barrier elements—developed as part of this project—also begins with the general cybersecurity requirements outlined in recognized standards and guidelines.

However, it distinguishes itself by filtering these requirements to retain only those that are relevant to barriers. This approach is consistent with regulatory definitions of barriers and has the added advantage of not requiring access to sensitive or confidential information, such as detailed cybersecurity risk analyses, comprehensive asset inventories, or system topology diagrams. However, in the final step of identifying cybersecurity barriers (Step 5; see Section 3.2.2), it is necessary to select the specific barriers applicable to the facility in question. This requires access to information about the actual cybersecurity measures implemented at that facility.

The standards-based approach is described in Section 3.2, where the first five of nine steps are dedicated to the identification of barrier functions and elements. Cybersecurity standards for operational technology (OT) systems, such as IEC 62443, typically encompass all categories of threat scenarios—including network-based attacks, physical intrusion, insider threats, and supply chain vulnerabilities—thereby ensuring broad applicability.

Combination of approaches

Apply multiple approaches to ensure comprehensive identification of cybersecurity barriers (1.7)

None of the three approaches (cf. Section 3.1) offers a guarantee that all barrier functions and barrier elements will be identified. However, the overall coverage improves significantly when the approaches are used in combination. Furthermore, it is essential to account for additional barrier elements that may be uncovered during system operation.

The choice of approaches remains the responsibility of each individual company and will typically be influenced by the organization's existing approach to safety barrier management.

Recommendations on identifying barrier functions and elements:

No.	Recommendation
1.1	***Remain open to emerging barrier elements during operations:*** Recognize that new or overlooked barrier elements may be discovered during system deployment or operation. Maintain processes for updating the barrier model accordingly.
1.2	***Promote industry collaboration on cyber incident scenarios:*** Engage in cross-industry cooperation to define cyber incident scenarios. This promotes consistency and harmonization across stakeholders.

1.3	***Integrate cybersecurity and safety scenarios:*** Align cyber incident scenarios with safety-related scenarios, particularly those involving Defined Situations of Hazard and Accident (DSHA). This highlights dependencies and effects of cybersecurity on safety.
1.4	***Use complete event sequence diagrams:*** Develop event sequence diagrams that illustrate the full progression of an incident—not just the top event. This supports better understanding of barrier placement, interaction, and timing, as well as differentiation between control measures and barrier functions.
1.5	***Support flexible hierarchical decomposition of barrier functions:*** Allow adaptability in defining the number and granularity of sub-function levels when decomposing barrier functions into elements. This flexibility supports a more accurate breakdown.
1.6	***Distinguish clearly between general cybersecurity measures and cybersecurity barriers:*** Consider using the new standards-based approach to differentiate generic cybersecurity controls from those that fulfil the specific role of barriers.
1.7	***Apply multiple approaches to ensure comprehensive identification of cybersecurity barriers:*** Employ a combination of approaches/methods to identify cybersecurity barrier functions and elements. This multi-method approach enhances completeness and reduces the risk of omission.

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

Differentiate between regulatory requirements and those defined in standards and guidelines (2.1)

According to the Management Regulations (MR) § 5, barrier requirements pertain to establishing verifiable performance requirements for the identified barrier elements—that is, for the measures defined as barriers. These requirements address questions such as: *How effective must the barrier be?* and *What level of performance is required?* This does not concern which measures should be in place—that was the focus of Question 1. Instead, it is about defining how well each barrier must function to be considered adequate for its intended role.

Fulfilment of general cybersecurity requirements—such as those stipulated in the Facilities Regulations (FR) § 34a—is neither sufficient nor necessary to meet the requirements of MR § 5. The reason it is not sufficient is that cybersecurity standards and guidelines (e.g., IEC 62443, NOROG 104, NIST CSF) primarily emphasize the presence of cybersecurity measures, but only to a limited extent address the performance of those measures. These standards often prescribe general practices—such as “regular monitoring”—without defining what "regular" means in a specific operational context. To serve as barrier requirements under MR § 5, these measures must be further specified and tailored to the context of a particular facility, zone, or system.

Avoid over-classifying cybersecurity measures as barriers (2.2)

The reason these general cybersecurity requirements are also not necessary for fulfilling MR § 5 is that they do not, by default, qualify as barrier requirements. While valuable for establishing baseline cybersecurity practices, only those applicable for barriers are required for fulfilling MR § 5.

To meet both the requirements of MR § 5 and FR § 34a—i.e., to achieve the “dual objective”—this need has been addressed in the standards-based method described in Section 3.2 (specifically through Step 9). The method facilitates that performance requirements and verification mechanisms are considered not only for designated barriers but also for general cybersecurity measures.

It remains the responsibility of each company to establish corresponding performance requirements and verification processes for general cybersecurity measures, in the same way as for identified barriers. This becomes a necessary consequence when control measures—originally intended to maintain normal operations—are formally defined and managed as barrier measures. In such cases, these control measures

must meet the same level of rigour in terms of performance specification and validation as traditional barriers.

Ensure strong traceability in standard-to-barrier mappings (2.3)
Current practice often treats all cybersecurity requirements found in standards and guidelines as barrier requirements in an effort to satisfy the dual objective—compliance with both MR § 5 and FR § 34a. However, this practice raises important concerns. One key issue is the weak connection between many of these general requirements and clearly defined barrier elements. Many requirements are formulated at a high level and cannot be directly linked to specific technical, operational, or organizational barrier elements.

Formulate verifiable requirements for each cybersecurity barrier element (2.4)
Moreover, effective verification of these requirements becomes challenging unless they are carefully tailored and adapted to the specific context of each operator and installation. Without sufficient specification and operationalization, the requirements remain too abstract to serve as the basis for verifiable performance requirements, as mandated by MR § 5.

Specify and operationalize activities for verifying cybersecurity barrier performance (2.5)
Similarly, activities for verifying the performance of cybersecurity barriers must be clearly defined and operationalized. For each verification activity, the methods, frequency, responsible parties, and success criteria should be explicitly specified. These activities must be actionable, practical, and aligned with the organization's operational capabilities.

Recommendations on development and verification of cybersecurity barrier performance requirements:

No.	Recommendation
2.1	***Differentiate between regulatory requirements and those defined in standards and guidelines:*** Do not confuse performance requirements as defined under the Management Regulations § 5 with requirements found in cybersecurity standards emphasizing presence or design features.
2.2	***Avoid over-classifying cybersecurity measures as barriers:*** To reduce verification overhead, refrain from treating every cybersecurity measure as a barrier. Instead, apply the new standards-based approach to define barriers more selectively and meaningfully. See Recommendation 1.1.
2.3	***Ensure strong traceability in standard-to-barrier mappings:*** When deriving performance requirements from standards, ensure each mapping to barrier elements is based on well-substantiated and relevant links. This enhances validity and auditability.
2.4	***Formulate verifiable requirements for each cybersecurity barrier element:*** Each cybersecurity barrier element should have its own set of deduced performance requirements that are specific, measurable, and testable.
2.5	***Specify and operationalize activities for verifying cybersecurity barrier performance:*** Clearly define the methods, frequency, responsibilities, and success criteria for each verification activity. These should be actionable, realistic, and aligned with operational capabilities.

3. How to assess the cybersecurity barrier status?
Incorporate both real-time and long-term assessment of barrier status and performance (3.1)
The assessment of barrier status consists of two key dimensions. The first is the ongoing, real-time status of whether any barriers or barrier elements are currently impaired or non-functional, and the second is verification of performance requirements. The first is directly linked to a requirement under the Management Regulations (MR) § 5, which states that *"personnel shall be aware of which barriers and barrier elements are not functioning or have been impaired."* This type of monitoring is referred to as short-term follow-up.

Use visual tools to clearly and effectively communicate the status of cybersecurity barriers (3.2)
In practice, this short-term follow-up is often supported by the use of barrier panels—visual tools designed to communicate the status of safety-critical barriers in daily operations.

Consolidate cybersecurity and safety barrier monitoring (3.3)
In the context of cybersecurity, existing safety barrier panels have been adapted to support cybersecurity barrier management as well, providing operators with a consolidated view of the status of both safety and cybersecurity barriers.

Establish relevant status indicators for impairments (3.4)
One of the key challenges in short-term barrier follow-up is determining which indicators of barrier impairments should be included and visualized in the barrier panel—typically using a traffic light system (red, yellow, green). In safety barrier management, these indicators commonly reflect actual faults, disconnections or functional failures, and the probability of failure, which may be inferred from the status of preventive maintenance and testing activities.

Include vulnerability indicators thoughtfully (3.5)
In the context of cybersecurity barrier management, vulnerabilities represent an additional category of potential status indicators. However, based on recommendations from several industry partners, specific vulnerabilities—such as those listed in the Common Vulnerabilities and Exposures (CVE) database—should be managed through dedicated vulnerability management processes rather than included in the barrier panel display, unless they have been thoroughly evaluated for relevance and criticality prior to inclusion.

Automate real-time status data collection (3.6)
Given that the barrier panel provides a real-time or near real-time overview, it is essential that the input data for status indicators can be automatically collected from operational systems. A preliminary menu of relevant status indicators, that can be considered for implementation, is provided in Chapter 4.

The second key dimension of barrier status assessment involves verification of performance requirements, typically conducted through the use of performance indicators, audits, reviews, or a combination thereof. These activities may be performed at varying intervals—ranging from relatively frequent (e.g., weekly or monthly) to more infrequent (e.g., annually or less). As such, it is useful to distinguish between medium-term and long-term follow-up of whether the barrier requirements are being met.

Leverage existing verification systems (3.7)
In the medium-term category, the TIMP method (Technical Integrity Management Program) has been employed—originally developed for safety barrier management but also adapted for use in cybersecurity barrier management. This verification is typically conducted on a quarterly basis, and the results for cybersecurity barriers are often compiled alongside those for safety barriers.

Enhance automation in long-term performance verification (3.8)
The assessment process involves a combination of automatically harvested data and manual assessments. Some stakeholders have expressed a clear interest in increasing the degree of automation in this process.

TIMP draws upon various sources of information, including elements from the Technical Condition Safety (TCS) method, which serves as a foundation for long-term follow-up in safety barrier management. However, as of now, the TCS method has not been implemented for cybersecurity barrier management.

Recommendations on assessing the status of cybersecurity barriers:

No.	Recommendation
3.1	***Incorporate both real-time and long-term assessment of barrier status and performance:*** Cybersecurity barrier status assessments must address both immediate, real-time impairments and longer-term evaluations of barrier effectiveness and performance. This ensures timely responses as well as strategic oversight.
3.2	***Use visual tools to clearly and effectively communicate the status of cybersecurity barriers:*** Implement a clear and intuitive visualization mechanism—such as a barrier panel—to communicate the current status of cybersecurity barriers. Visual tools enhance situational awareness and support decision-making.
3.3	***Consolidate cybersecurity and safety barrier monitoring:*** Where feasible, use the same tool for monitoring both cybersecurity and safety barriers. This enables an integrated view of the overall barrier landscape and streamline operational workflows.
3.4	***Establish relevant status indicators for impairments:*** Define and implement status indicators tailored to your organizational needs. These should be grounded in relevant source systems and reflect meaningful states of barrier degradation or failure.
3.5	***Include vulnerability indicators thoughtfully:*** Specific vulnerabilities (CVEs) may serve as useful status indicators for certain barriers. However, they can also be managed through dedicated vulnerability management processes. The most effective and context-appropriate treatment should be considered.
3.6	***Automate real-time status data collection:*** Ensure that data feeding into barrier status indicators is collected automatically to support real-time or near real-time updates. This minimizes manual effort and increases responsiveness.
3.7	***Leverage existing verification systems:*** Consider adapting existing systems for the long-term verification of safety barrier performance to also cover cybersecurity barriers, ensuring consistency in assurance practices.
3.8	***Enhance automation in long-term performance verification:*** Explore opportunities to automate the collection and analysis of data used in periodic verification activities. Increased automation supports scalability and reduces resource burden over time.

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

Utilize the SL-O concept from IEC 62443 for operational follow-up (4.1)

The project has demonstrated how security levels can be verified during operations—referred to as Security Level in Operation (SL-O)—in a manner conceptually similar to the practice of monitoring SIL (Safety Integrity Level) in operation within functional safety. The starting point for SL-O is the verification of security level requirements originally defined through SL-T (Target Security Level) and SL-I (Implemented Security Level). As such, SL-O monitoring forms an integral part of the response to Question 3, concerning the follow-up and verification of cybersecurity performance.

The security level requirements are assigned to specific zones, as defined by the IEC 62443 standard series. This has two key implications. First, the scope of SL-O extends beyond barriers and includes general cybersecurity measures, reflecting a broader system security perspective. Second, the approach is based on the IEC 62443 methodology for determining and verifying security levels—an approach that introduces certain practical challenges. These include the correct interpretation and application of concepts such as zones and conduits, and the complexities of security level calculation, whether or not the use of security requirement vectors is applied.

SL-O constitutes a form of medium-term or long-term follow-up, depending on how frequently the verification is performed. However, a general limitation of this approach is that it relies on IEC 62443, which is not applied by all companies. Some companies have preferences for other cybersecurity standards or guidelines.

Incorporate the Security Protection Rating – Operational (SPR-O) (4.2)
In addition, two related terms—Maturity Level (ML) and Security Protection Rating (SPR)—are also relevant. The SPR is a function of both SL and ML, and these concepts are important for the evaluation of cybersecurity barriers, as they provide a more comprehensive view of both technical capability and organizational readiness.

Promote cross-industry collaboration on SL-O and SPR-O (4.3)
The implementation of IEC 62443 concepts—namely Security Levels (SL), Maturity Levels (ML), and Security Protection Rating (SPR)—during operational phases is complex and not straightforward. To ensure effective application, further development and practical operationalization are necessary. This should be pursued through broad, industry-wide collaboration.

Recommendations on the verification of Security Levels (SL):

No.	Recommendation
4.1	***Utilize the SL-O concept from IEC 62443 for operational follow-up:*** It is recommended to monitor and verify Security Levels during system operation using the SL-O (Security Level – Operational) concept as defined in IEC 62443. Although this approach is specific to the IEC 62443 standard and not exclusively focused on cybersecurity barriers, it provides a structured method for assessing operational security effectiveness.
4.2	***Incorporate the Security Protection Rating – Operational (SPR-O):*** Similarly, apply the SPR-O (Security Protection Rating – Operational) approach to capture both the operational Security Level (SL) and the organizational Maturity Level (ML). This supports a more holistic view of cybersecurity capability and implementation quality over time.
4.3	***Promote cross-industry collaboration on SL-O and SPR-O:*** Continued development and operationalization of the SL-O and SPR-O concepts should be pursued through industry-wide cooperation. Such collaboration can help standardize methodologies, align expectations across stakeholders, and facilitate benchmarking and best practice sharing.

5. How to integrate safety and cybersecurity barrier management?
The integration of safety and cybersecurity barrier management is addressed only to a limited extent in existing standards, industry guidelines, and academic literature. Where the topic is mentioned, the focus is typically on the general integration of safety and cybersecurity—for example, in risk assessments, governance models, or system design considerations—rather than on the specific and systematic integration of barrier functions and elements across both domains.

Harmonize concepts and terminology across safety and cybersecurity barrier management (5.1)
Current practice shows that cybersecurity has largely been integrated as an add-on within the existing safety barrier management framework. However, this integration has taken place without a harmonized terminology or a clear conceptual alignment between the two domains. Notably, there is no formal definition of cybersecurity barriers, and the prevailing approach—discussed under Question 1—has been to treat all cybersecurity measures as barriers by default.

Avoid broad classification of cybersecurity measures as barriers (5.2)
This has created challenges in follow-up and verification, particularly because general cybersecurity requirements are not equivalent to verifiable performance requirements, as highlighted in the discussion under Question 2.

The visualization of the status of cybersecurity barriers—or more broadly, general cybersecurity measures—has likewise been adapted to existing systems and tools originally developed for safety barrier management.

This includes the use of tools such as the barrier panel for real-time status monitoring and TIMP for periodic performance verification.

Leverage alignment of cybersecurity barrier management with safety barrier management (5.3)
Adapting cybersecurity barrier management to the existing safety barrier management framework is a natural step, both because it builds on an established methodology and because it helps increase visibility and awareness for cybersecurity. However, in practice, it is more accurate to state that general cybersecurity management—rather than a structured cybersecurity barrier management approach—has been integrated into safety barrier management. This reflects the current state, where general cybersecurity requirements by default are considered as barrier requirements.

Adopt a company-specific integration strategy (5.4)
How can—or should—this integration be achieved? As a starting point, it is both sensible and practical to align with the way safety barrier management is already practiced within the specific company. Since these practices vary across organizations, any general recommendation must be flexible and adaptable, as outlined in this project.

Within such a flexible framework, several important considerations and decisions must be addressed. A key step is to clearly distinguish between general cybersecurity management (cf. FR § 34a) and cybersecurity barrier management (cf. MR § 5). One practical approach is to work toward a harmonized concept and definition of barriers that applies across both cybersecurity and safety domains.

Consider and decide on key dimensions (5.5)
Additional considerations and decisions that need to be made are discussed in Section 4.5 in this report.

Recommendations on the integration of safety and cybersecurity barrier management:

No.	Recommendation
5.1	***Harmonize concepts and terminology across safety and cybersecurity barrier management:*** Strive for conceptual and terminological alignment between cybersecurity and safety barrier management, to the extent feasible. This harmonization fosters coherence in risk communication, reduces ambiguity, and facilitates cross-disciplinary collaboration.
5.2	***Avoid broad classification of cybersecurity measures as barriers:*** Not all cybersecurity measures prescribed in industry standards and guidelines should be classified as cybersecurity barriers by default. Overextending the barrier concept can hinder harmonization with safety practices and dilute the functional clarity of true barriers. See Recommendations 1.1 and 2.2.
5.3	***Leverage alignment of cybersecurity barrier management with safety barrier management:*** Build upon existing safety barrier management methodologies when aligning cybersecurity practices. This approach increases visibility and awareness for cybersecurity.
5.4	***Adopt a company-specific integration strategy:*** Recognize that safety barrier management frameworks vary across organizations. Tailor the integration approach to fit the specific structure, maturity, and risk profile of your organization.
5.5	***Guide the integration of safety and cybersecurity barrier management using a deliberate and documented approach. Consider and decide on the following key dimensions:*** Degree of integration, scope of cybersecurity measures, treatment of technical vs. non-technical barriers, use of dedicated cybersecurity Performance Standards (PSs) vs. integration into existing safety PSs, use of separate vs. integrated PSs for non-technical cybersecurity barriers and safety barriers, and integration of cybersecurity barriers into existing visualization tools versus use of separate dashboards (cf. Section 4.5.2).

6. How to establish and integrate non-technical barrier elements in cybersecurity barrier management?

Apply similar identification approaches for non-technical as for technical cybersecurity barriers (6.1)

The process of establishing both technical and non-technical barrier elements generally follows a top-down approach. In this method, cybersecurity barrier functions are first defined, and specific elements—*both technical and non-technical*—are subsequently linked to these functions in an integrated and systematic manner. This ensures that all relevant components contributing to the function's reliability are identified and managed cohesively.

Additionally, a bottom-up approach may be applied, where individual barrier elements are identified directly from observed operational practices, existing workflows, or system configurations. This approach is particularly useful for uncovering *non-technical elements* that may not be explicitly documented but are embedded in the organization's day-to-day operations.

Non-technical barrier elements encompass both human and operational components. *Operational barrier elements* refer to specific actions that operators must carry out to support or fulfil a cybersecurity barrier function. These actions frequently involve the activation or utilization of *technical barrier elements* by a human operator—commonly referred to as the *human barrier element*. As system automation decreases, the operator's role becomes increasingly critical to maintaining the effectiveness of the barrier function.

Top-down identification of non-technical cybersecurity barrier elements

Apply a top-down functional breakdown to include non-technical elements (6.2)

There are two primary top-down approaches for identifying non-technical cybersecurity barrier elements (cf. Question 1 above):

1. Standards-Based Approach
   This approach starts with cybersecurity requirements specified in applicable standards. These requirements typically address organizational and procedural aspects of cybersecurity. However, they are often defined at a high level. As a result, further interpretation and operationalization are usually necessary to effectively integrate them into a structured barrier management framework.
2. Functional Breakdown Approach
   This method involves systematically decomposing each cybersecurity barrier function into its constituent elements, including both *human barrier elements* and *operational barrier elements*. Such a breakdown facilitates a clearer allocation of responsibilities and a more precise definition of the actions needed to support the intended barrier function.

Bottom-up identification of non-technical cybersecurity barrier elements

Complement the top-down approach with a bottom-up analysis (6.3)

Reviewing an organization's incident response plans for cybersecurity incidents provides valuable input for identifying relevant roles and personnel who may serve as *human barrier elements*. These documents often outline the practical distribution of responsibilities and actions during incident scenarios, offering insight into how human and operational components contribute to the overall effectiveness of cybersecurity barrier functions. This report briefly presents some relevant roles involved in incident response in Section 3.4.

Differentiate between active barrier roles/actions and Performance Influencing Factors (PIFs) (6.4)

It is essential to distinguish between roles and actions that directly enable the reliable execution of a cybersecurity barrier function and those that serve as *Performance Influencing Factors* (PIFs). PIFs are contextual elements that may affect the performance of a barrier function—either positively or negatively—but are not integral to its core operation. Accurate classification and documentation of both *human* and

operational barrier elements are critical for maintaining clarity in barrier management and for preventing the conflation of supporting influences with essential functional components.

Performance requirements to non-technical cybersecurity barrier elements

Define performance requirements for non-technical elements in a similar structured way as for technical barrier elements (6.5)

Performance requirements must be defined for all non-technical barrier elements and subsequently operationalized to enable systematic follow-up and verification. These requirements are essential to ensure that both *human* and *operational barrier elements* can reliably and consistently fulfil their intended cybersecurity functions.

For *human barrier elements*, performance requirements may include:

- Specific competence
- Clearly defined criteria for action
- Required response time
- Availability
- Integrity of the human role in performing the barrier function

For *operational barrier elements*, performance requirements may address:

- Reliability
- Correctness

Additional performance requirements may be identified for both human and operational barrier elements, depending on the specific cybersecurity barrier functions they support and the contextual demands of their application.

Monitoring and follow-up of non-technical cybersecurity barrier elements

Ensure effective monitoring and follow-up mechanisms (6.6)

To effectively operationalize and monitor non-technical barrier elements, data must be collected from multiple sources and integrated into the organization's overall barrier follow-up system. In the case of non-technical cybersecurity barrier elements, this may necessitate the use of systems and tools that differ from those commonly employed for monitoring technical barriers.

For example, data relevant to *human barrier elements*—such as competence records, role assignments, and training status—are often maintained within the organization's Human Resource Management (HRM) system. To support effective barrier oversight, these data sources must be aligned with barrier management objectives to enable accurate tracking, verification, and continuous improvement of barrier performance.

A key challenge in managing non-technical cybersecurity barriers is the short-term monitoring and visualization of their status. While real-time monitoring tools—such as barrier panels—are effective for displaying the status of *technical* barriers, they are considerably less suited to capturing and representing the dynamic, context-dependent nature of *non-technical* elements. Integrating relevant data into real-time visualization tools remains a complex task and continues to impede the development of full situational awareness regarding the health and effectiveness of non-technical cybersecurity barriers.

Formalize roles, responsibilities, and tasks (6.7)

Technical barrier elements are generally addressed more comprehensively and systematically than their non-technical counterparts. In many cases, *non-technical barrier elements* remain implicit within operational

practices—meaning they are not consistently documented, monitored, or managed in a structured manner. Formalizing the roles, responsibilities, and tasks associated with non-technical barrier elements reinforces their importance and enables systematic management, traceability, and performance monitoring within the organization's overall barrier management system.

Recommendations on establishing and integrating non-technical barrier elements in cybersecurity barrier management:

No.	Recommendation
6.1	***Apply similar identification approaches for non-technical as for technical cybersecurity barriers:*** Non-technical barrier elements should be identified or established using approaches comparable to those applied for technical barriers. This supports a consistent and integrated barrier management framework across domains.
6.2	***Apply a top-down functional breakdown to include non-technical elements:*** When decomposing barrier functions into elements, ensure both technical and non-technical components are captured. For each sub-function, systematically examine roles (human barrier elements) and actions (operational barrier elements). In some cases, a sub-function may rely solely on non-technical barriers.
6.3	***Complement the top-down approach with a bottom-up analysis:*** Conduct a bottom-up review of the organization's incident response plans to identify non-technical roles, responsibilities, and actions that contribute to cybersecurity barrier functions.
6.4	***Differentiate between active barrier roles/actions and Performance Influencing Factors (PIFs):*** Clearly distinguish between roles and actions that directly implement barrier functions and those that act as PIFs. Avoid conflating supportive influences with elements that perform essential barrier actions, to maintain clarity in barrier accountability and performance assessment.
6.5	***Define performance requirements for non-technical elements in a similar structured way as for technical barrier elements:*** Non-technical barrier elements must have defined performance requirements, covering properties like competence, training, availability, criteria for action, and response times. Such requirements ensure human and operational barrier elements can reliably fulfil their cybersecurity barrier functions.
6.6	***Ensure effective monitoring and follow-up mechanisms:*** Like technical elements, non-technical barrier elements require ongoing monitoring. This involves collecting and integrating relevant data from multiple sources—including HRM systems—into the organization's barrier follow-up tools or systems.
6.7	***Formalize roles, responsibilities, and tasks:*** Clearly formalize the roles, responsibilities, and associated tasks for all non-technical barrier elements. This will reinforce their importance, enabling systematic management, traceability, and performance monitoring.

7. How can interaction between IT and OT domains be improved through new innovative work processes?

One innovative work process that can significantly enhance interaction between the IT and OT domains is the establishment and integration of Operational Technology Security Operations Centers (OT SOCs). These centres may be developed in-house or outsourced through a Managed Security Service Provider (MSSP), depending on organizational needs and resources.

Leverage OT SOC as a collaboration arena (7.1)

Since Security Operations Center (SOC) practices originate in the IT domain, developing an effective OT SOC requires close collaboration between IT and OT personnel. This collaboration fosters mutual understanding: IT personnel gain deeper insight into the structure, constraints, and operational dynamics of OT systems, while OT personnel become more familiar with IT security tools, monitoring methodologies, and how these can be effectively adapted to OT contexts.

These joint work processes are essential not only for the successful deployment and operation of OT SOCs but also as key enablers of long-term IT/OT integration and the advancement of cross-domain cybersecurity maturity.

Establish structured forums for ongoing IT/OT collaboration (7.2)
In parallel, structured meeting arenas can further strengthen IT/OT interaction. By establishing regular forums where IT and OT personnel collaborate and exchange knowledge, organizations create a foundation for continuous learning and trust-building. These forums provide IT staff with valuable exposure to OT equipment, operational characteristics, and contextual constraints. Simultaneously, they enable both IT and OT personnel to develop a shared understanding of cybersecurity tools—including their capabilities, limitations, and appropriate applications within OT environments.

Secure active management support and resource commitment (7.3)
Establishing and maintaining structured forums for IT/OT collaboration requires active managerial support, including the allocation of sufficient time, resources, and sustained organizational commitment. To enable effective cross-domain interaction, deliberate efforts must be made to identify common ground and to foster mutual understanding and trust between IT and OT personnel.

Recommendations on improved interactions between IT and OT domains:

No.	Recommendation
7.1	***Leverage OT Security Operation Centers (SOCs) as collaboration arenas for IT and OT personnel:*** Utilize OT SOCs as strategic platforms for fostering closer interaction between IT and OT domains. These centers serve as practical touchpoints for shared situational awareness, joint monitoring, and collaborative response to cybersecurity threats affecting both domains.
7.2	***Establish structured forums for ongoing IT/OT collaboration:*** Create regular and structured meeting arenas where IT and OT personnel can meet, collaborate, and exchange knowledge. These forums—whether operational coordination meetings, joint planning workshops, or incident review sessions—build a foundation of mutual understanding, trust, and learning across technical and organizational boundaries.
7.3	***Secure active management support and resource commitment:*** The establishment and sustainability of effective IT/OT collaboration require active and visible management support. This includes allocation of sufficient time, resources, and sustained organizational commitment. Promoting a culture of mutual respect and mindfulness, which reinforces collaborative behavior, enhances cross-domain understanding, and strengthens long-term cooperation between IT and OT professionals.

8. How to align practice, culture and language between users of office IT systems and ICS?
Avoid striving for complete convergence of IT and OT cultures and practices (8.1)
Full alignment between IT and OT domains—across practices, culture, and language—may not be necessary, nor always desirable. Each domain operates within a distinct operational context and is guided by different priorities, such as data confidentiality and availability in IT versus process safety and continuity in OT. These contextual differences naturally shape divergent approaches to cybersecurity, risk management, and day-to-day operations.

Foster mutual awareness and cross-domain understanding between IT and OT teams (8.2)
Recognizing and respecting these differences is key to fostering productive collaboration. Instead of pursuing complete convergence, organizations should aim to establish interoperable practices, develop a shared baseline vocabulary, and promote mutual cultural awareness. This approach supports more effective communication and decision-making across domains without compromising the specific needs of either environment.

Enable effective interaction during both routine and non-routine situations (8.3)
Fostering mutual awareness and understanding of each domain's cultural norms and specialized language provides a sufficient foundation for successful interaction—both in day-to-day operations and during irregular or unexpected events.

Recommendations on alignment of practices, culture and language between users of office IT systems and Industrial Control Systems (ICS):

No.	Recommendation
8.1	***Avoid striving for complete convergence of IT and OT cultures and practices:*** Full alignment of practices, cultural norms, and language between IT and OT domains is neither necessary nor always practical. These domains operate under different priorities, constraints, and operational contexts that require domain-specific approaches.
8.2	***Foster mutual awareness and cross-domain understanding between IT and OT teams:*** Instead of full convergence, aim to cultivate a shared understanding of each domain's distinct culture, terminology, and operational logic. Building this mutual awareness enables more effective communication and collaboration, especially in joint processes and integrated responses. This can be obtained through Recommendations 7.1 to 7.3.
8.3	***Enable effective interaction during both routine and non-routine situations:*** A foundational understanding of each other's practices and language is sufficient to support successful interaction—not only in daily operations, but also during irregular or emergency events when effective coordination is critical.

9. How to gather information about and visualize the status of cybersecurity barriers?
It should first be noted that this question—along with Question 10—has a somewhat narrower focus than the broader research objectives and task descriptions. While both questions address cybersecurity barriers, which are central to the project, the monitoring component also extends to the identification and assessment of threats and vulnerabilities.

Collect and integrate external and internal information (9.1)
Effective cybersecurity barrier management depends on the continuous collection and integration of both external and internal information. To accurately assess the status of cybersecurity barriers, it is essential to monitor for both impairments—such as performance degradations or outright failures—and vulnerabilities that could compromise barrier effectiveness.

Externally, relevant data is obtained from sources such as cyber threat intelligence (CTI) providers, industrial control system (ICS) suppliers, national and international Computer Security Incident Response Teams (CSIRTs), and established vulnerability databases (e.g., CVE, NVD). These sources offer timely information on emerging threats and vulnerabilities, often accompanied by patch advisories or mitigation recommendations.

Internally, data is collected through monitoring systems such as intrusion detection systems (IDS), firewall logs, Microsoft Defender, and Computerized Maintenance Management Systems (CMMS). These platforms provide operational insights into the performance and health of OT assets, including those designated as cybersecurity barriers.

Structure and visualize the collected information (9.2)
To make this information actionable, it must be structured and visualized in a way that supports timely decision-making. A key tool for this purpose is the barrier panel—a dashboard-style interface that aggregates barrier status data, often using a traffic-light system (e.g., red for critical impairments, yellow for degraded conditions, and green for normal operation).

Present status, trends, and access to underlying data (9.3)
These panels enable personnel both offshore and onshore to assess real-time risk, plan maintenance activities, and prioritize corrective actions. In addition to real-time monitoring, effective barrier panels should support historical trend analysis and provide links to underlying service tickets, diagnostic logs, or maintenance records. This enhances traceability and strengthens decision support across the barrier management lifecycle.

Visualizing the status of cybersecurity barriers in this manner not only supports compliance with regulatory requirements (e.g., § 5 of the Management Regulations) but also enhances organizational situational awareness, ensuring that impairments are identified, understood, and addressed in a timely and risk-informed manner.

Recommendations on gathering and visualizing the status on threats, vulnerabilities and cybersecurity barriers:

No.	Recommendation
9.1	***Collect and integrate both external and internal information on threats, vulnerabilities, and barrier impairments:*** Effective cybersecurity barrier management depends on the continuous collection and integration of both external and internal data sources. To accurately assess the status of cybersecurity barriers, organizations must monitor threats, vulnerabilities, and impairments—such as performance degradation or complete failure—that may compromise barrier effectiveness.
9.2	***Structure and visualize the collected information:*** To make information actionable, it must be structured and visualized in a way that enables timely and informed decision-making. A key tool for this purpose is the barrier panel—a dashboard-style interface that consolidates and displays barrier status data.
9.3	***Present status, trends, and access to underlying data:*** Barrier panels support both offshore and onshore personnel in assessing real-time risk, planning maintenance, and prioritizing corrective actions. In addition to current status indicators, effective panels should offer historical trend analysis and provide direct access to supporting data—such as service tickets, diagnostic logs, and maintenance records—to improve traceability and strengthen operational decision support.

10. How should information from external threat intelligence be managed to maintain cybersecurity barriers?
Effective management of cybersecurity barriers requires the timely and structured utilization of external threat intelligence to anticipate, detect, and respond to evolving threats. External sources—including cyber threat intelligence (CTI) vendors, CSIRTs, ICS suppliers, and national security authorities—provide critical insights into current threat landscapes, emerging vulnerabilities, and recommended mitigation strategies.

These inputs are especially valuable when they include contextualized intelligence on the tactics, techniques, and procedures (TTPs) employed by threat actors targeting industrial control systems (ICS).

To maintain effective cybersecurity barriers, threat intelligence must be continuously collected, assessed, and integrated into operational decision-making processes. Tools such as weekly threat landscape reports enable organizations to evaluate their current exposure and determine an appropriate risk level. This assessment, in turn, guides predefined actions—such as reinforcing barriers, increasing monitoring efforts, or applying relevant patches.

In critical situations, timely external intelligence may trigger immediate response measures, including the isolation of affected systems or the activation of mitigation measures, to mitigate potential impacts and preserve system integrity.

Leverage multiple, complementary CTI sources (10.1)
However, the value of external threat intelligence ultimately depends on its relevance, timeliness, and actionability. To ensure comprehensive coverage and early warning, organizations should draw on multiple complementary sources, such as leveraging CSIRTs operating in other time zones for around-the-clock situational awareness.

Implement effective filtering and prioritization (10.2)
At the same time, effective filtering and prioritization mechanisms—along with designated personnel—must be in place to process incoming information, inform the appropriate roles, and prevent information overload. Within this framework, OT cybersecurity teams play a central role in contextualizing external alerts, mapping them to asset inventories, and assessing their implications for cybersecurity barrier performance.

Integrate CTI into barrier strategy and design (10.3)
Ultimately, external threat intelligence should inform not only tactical and operational responses but also drive strategic updates to the organization's cybersecurity barrier strategy. This includes reviewing barrier designs, refining detection capabilities, and planning new defensive measures aligned with the evolving threat landscape.

Recommendations on managing external threat intelligence to maintain cybersecurity barriers:

No.	Recommendation
10.1	***Leverage multiple, complementary Cyber Threat Intelligence (CTI) sources:*** To ensure comprehensive threat coverage and timely alerts, organizations should utilize a range of CTI sources. This includes leveraging national and international CSIRTs, particularly those operating in different time zones, to maintain continuous situational awareness. Further, cascading or combining insights from various sources can increase the richness, context, and relevance of the information.
10.2	***Implement effective filtering and prioritization:*** Robust filtering and prioritization mechanisms are essential to manage the flow of incoming intelligence. These mechanisms—supported by dedicated personnel—help ensure that relevant information is routed to the appropriate roles while minimizing the risk of information overload and alert fatigue.
10.3	***Integrate CTI into barrier strategy and design:*** External threat intelligence should inform not only immediate tactical and operational responses but also strategic decisions regarding the organization's cybersecurity barrier framework. This includes revisiting barrier architectures, enhancing detection capabilities, and planning new defensive measures that are aligned with the evolving threat landscape.

11. How to handle threats, vulnerabilities and cybersecurity barrier impairments?
Implement a Continuous Risk Assessment and Management Process (CRAMP) (11.1)
Handling threats, vulnerabilities, and impairments to cybersecurity barriers requires a structured, risk-informed approach that balances operational continuity with the need for timely mitigation. Although these elements differ in origin—threats typically stem from external intelligence sources, vulnerabilities arise from identified weaknesses in systems, and impairments result from degraded or non-functioning barriers—they converge in requiring coordinated assessment and treatment.

The first step in handling threats, vulnerabilities, and impairments is identification and relevance assessment. For *vulnerabilities*, this involves verifying whether the affected assets are present within the facility and evaluating potential impact based on factors such as asset location, network exposure, and operational function. In contrast, *barrier impairments* are typically tied to known assets and are often accompanied by pre-established criticality ratings, which support immediate prioritization. *Threats* may

prompt broader assessments of facility exposure—particularly when they align with known system configurations, existing vulnerabilities, or high-value target assets.

Once identified, risks are categorized and tracked using tools such as service ticketing systems, risk registers, and barrier panels. The implementation of mitigation measures is typically prioritized using classifications such as NOW (immediate action), NEXT (deferred action), or NEVER (no action required), based on the severity of the issue, the criticality of the affected asset, and the feasibility of mitigation.

Mitigation measures may include patching, maintenance, the deployment of compensating measures, or, in critical scenarios, facility isolation through the activation of island mode. A formal Management of Change (MoC) process ensures that all actions are properly documented, reviewed, and approved prior to implementation, thereby maintaining traceability and reinforcing governance throughout the intervention.

Establish dedicated sub-processes and coordinate them (11.2)
The integration of fragmented data remains a significant challenge in cybersecurity barrier management. Functions such as vulnerability tracking, patch scheduling, and barrier status monitoring are often managed through separate systems, necessitating coordination across multiple roles, disciplines, and organizational levels. OT cybersecurity teams play a central role in bridging these potential silos, working in close collaboration with control system engineers, offshore installation managers, and external vendors.

Adopt proactive, forward-looking measures (11.3)
Ultimately, effective handling of threats, vulnerabilities and cybersecurity barrier impairments requires not only reactive capabilities, but also proactive, forward-looking measures. These include maintaining up-to-date asset inventories (automated where feasible), implementing pre-configured response plans, and conducting continuous performance monitoring. Together, these practices support rapid, safe, and consistent decision-making across the entire cybersecurity barrier lifecycle.

Recommendations on handling threats, vulnerabilities and cybersecurity barrier impairments:

No.	Recommendation
11.1	***Implement a Continuous Risk Assessment and Management Process (CRAMP):*** Addressing threats, vulnerabilities, and impairments to cybersecurity barriers require a structured, risk-informed approach that balances operational continuity with the need for timely mitigation. Although these elements differ in origin—threats typically arise from external intelligence, vulnerabilities from weaknesses in systems, and impairments from degraded or failed barriers—they converge in demanding coordinated assessment and treatment through a continuous risk management framework.
11.2	***Establish dedicated sub-processes for managing threats, vulnerabilities, and barrier impairments:*** While the handling of threats, vulnerabilities, and barrier impairments follows similar overarching steps—information gathering, structuring, risk assessment, and risk treatment—effectiveness is enhanced by implementing structured sub-processes for each element. These include threat landscape monitoring, vulnerability management, and cybersecurity barrier monitoring. Clear delineation of responsibilities and workflows within each sub-process supports consistency and improves responsiveness.
11.3	***Adopt proactive, forward-looking measures:*** Robust handling requires not only reactive capabilities but also proactive strategies. These include maintaining accurate and up-to-date asset inventories (preferably automated), developing pre-configured response and mitigation plans, and conducting ongoing performance monitoring. Together, these practices enable timely, safe, and consistent decision-making throughout the cybersecurity barrier lifecycle.

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] Havtil, *Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities (The Management Regulations)*. 2022. Accessed: Sept. 15, 2025. [Online]. Available: https://www.havtil.no/en/regulations/all-acts/?forskrift=611

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

[8] 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

[9] Havtil, *Regulations relating to design and outfitting of facilities, etc. in the petroleum activities (The Facilities Regulations)*. 2022. Accessed: Sept. 15, 2025. [Online]. Available: https://www.havtil.no/en/regulations/all-acts/?forskrift=634

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

[11] '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/

[12] Havtil, *Regulations relating to health, safety, and the environment in the petroleum activities and at certain onshore facilities (The Framework Regulations)*. 2019. Accessed: Sept. 15, 2025. [Online]. Available: https://www.havtil.no/en/regulations/all-acts/?forskrift=158

[13] 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/

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

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

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

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

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

[19] 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.

[20] 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.

[21] 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

[22] 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

[23] 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.
[24] 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.
[25] K. Øien, M. G. Jaatun, and C. Thieme, 'Cybersecurity Barriers and Performance Requirements', presented at the ESREL SRA-E 2025, Stavanger: Research Publishing, Singapore. doi: 10.3850/978-981-94-3281-3.
[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] S. Pettersen, V. Gnanasekaran, and T. O. Grøtan, 'Understanding techno-cultural shaping of cyber resilience in the nexus of safety, security, IT and OT', *Submitt. Saf. Sci. Spec. Issue Risk Resil. Crisis Emerg. Manag.*, 2025.
[29] 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.
[30] 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.
[31] G. K. Hanssen, C. A. Thieme, A. V. Bjarkø, M. A. Lundteigen, K. Bernsmed, and M. G. Jaatun, 'A Continuous OT Cybersecurity Risk Analysis and Mitigation Process', in *Proceeding of the 33rd European Safety and Reliability Conference*, Singapore: Research Publishing Services, 2023, pp. 3190–3197. doi: 10.3850/978-981-18-8071-1_p413-cd.
[32] MITRE Corporation, 'MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy', The MITRE Corporation, Dec. 2020. [Online]. Available: https://attack.mitre.org/docs/ATTACK_for_ICS_Design_and_Philosophy_March_2020.pdf
[33] 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.
[34] 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

Appendix A Definitions and abbreviations

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
CDS	Cybersecurity of Industrial Automation and Control Systems
CE	Certificates missing
CERT	Cybersecurity Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CISA	Cybersecurity and Infrastructure Security Agency
CM	Corrective Maintenance
CM-C	Corrective Maintenance – Critical
CMDB	Configuration Management Database
CMMI	Capability Maturity Model Integration
CMMS	Computerized Maintenance Management System
CRAMP	Continuous Risk Assessment and Mitigation Process
CRO	Control Room Operator
CS	Cybersecurity
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVE-E	Common Vulnerabilities and Exposures – Exploited
DC	Data Confidentiality
DL	Discipline Lead
DSHA	Defined Situations of Hazard and Accident
DQ	Degraded Qualifications
EMT	Emergency Management Team
EPT	Emergency Preparedness Training incomplete
ERL	Emergency Response Leader
ETC	Emergency Training Compliance (system)
EWS	Engineering Work Station
FAT	Factory Acceptance Test
FDIS	Final Draft International Standard
FO	Field Operator
FR	Facilities Regulations
FR	Foundational Requirement
GL	Guideline
Havtil	Norwegian Ocean Industry Authority

HRM	Human Resource Management
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
ID	Identifier
IDS	Intrusion Detection System
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronics Engineers
INH	Inhibited
IP	Incorrect (or unsuitable) Procedures
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISBR	Information Security Baseline Requirements
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ML	Maturity Level
MoC	Management of Change
MR	Management Regulations
MSSP	Managed Security Service Provider
MTO	Man – Technology – Organization
NC	Non-Conformance
NIST CSF	National Institute of Standards and Technology – Cybersecurity Framework
NOROG	Norsk Olje og Gass (now Offshore Norge)
NOU	Norges Offentlige Utredninger (Norwegian Public Reports)
NR	Not Relevant
NSA	Norwegian Shipowners' Association
NVD	National Vulnerability Database
OIM	Offshore Installation Manager
OT	Operational Technology
PC	Personal Computer
PDS	Reliability of Safety Instrumented Systems (abbr. in Norwegian)
P&ID	Piping and Instrumentation Diagram
PIF	Performance Influencing Factor
PLC	Programmable Logic Controller
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
SAP	Systems, Applications and Products (in data processing)
SAS	Safety and Automation System
SAT	Site Acceptance Test

SCAI	Safety Control Alarms and Interlocks
SCT	Safety Critical Task
SF	Safety Function
SI	System Integrity
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
SOC	Security Operations Center
SPE	Security Program Element
SPR	Security Protection Rating
SR	System Requirement
TA	Technical Authority/Responsible
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
TTP	Tactics, Techniques, and Procedures
UBP	Unavailable Backup Personnel
UC	Use Control
UP	Unavailable Personnel
UPR	Unavailable Procedures
UQ	Unqualified Personnel
VPN	Virtual Private Network
WC	Working Committee
WL	Workload
WP	Work package

Definitions

Term [reference]	Description/definition
Automation and control system (ACS) [29]	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 [29]	Property of ensuring timely and reliable access to and use of control system information and functionality.
Barrier [8]	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 [8]	The task or role of a barrier.

Term [reference]	Description/definition
Barrier element [8]	Technical, operational and organizational measures or solutions involved in the realization of a barrier function.
Barrier management [8]	Coordinated activities for establishing and maintaining barriers so that they fulfil their functions at all times.
Barrier strategy [8]	Plan for how barrier functions, on the basis of the risk picture, are implemented in order to reduce risk.
Conduit [29]	See security conduit.
Confidentiality [29]	Assurance that information is not disclosed to unauthorized individuals, processes, or devices.
Control system [29]	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 [29]	See security measure.
Cyber asset [22]	Device contained within the system under consideration (SuC), e.g., controller, server, engineering work station, etc.
Cyber incident [22]	Communication with an E/E/PE device within a control system that negatively impacts process safety, the environment, operations, confidentiality, Safety Control Alarms and Interlocks (SCAI) integrity, or IACS availability.
Cybersecurity [29]	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.
Cybersecurity barrier [33]	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 [29]	Provision of multiple security measures, especially in layers, with the intent to prevent or delay an attack.
Error [34]	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 [34]	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 [34]	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 [34]	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) [29]	Requirement that provides a basis for technical requirements in all standards in the IEC 62443 series.
Functional safety [34]	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 [34]	Potential source of harm.

Term [reference]	Description/definition
	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]
Implemented security level (SL-I) [29]	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 [29]	State that connectivity, control, or safety have not been changed, destroyed or lost in an unauthorized or accidental manner.
Intrusion [29]	Unauthorized act of compromising a system. Note 1 to entry: See "attack."
Intrusion detection [29]	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) [29]	Qualitative indicator for characterizing the efficiency of an organization to implement requirements according to documented policies and procedures.
Monitoring system [29]	Type of automation and control system that consolidates sensor measurements and displays them to an operator of the equipment under control.
Operational barrier element [8]	The actions or activities which personnel must perform in order to realize a barrier function.
Operational security level (SL-O) [29]	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 [8]	Personnel with defined roles or functions and specific competence involved in the realization of a barrier function.
Patch [29]	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 [8]	Factors identified as having significance for barrier functions and the ability of barrier elements to function as intended.
Performance requirement [8]	Verifiable requirement for the properties of the barrier elements in order to ensure that the barrier is effective.
Redundancy [34]	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 [29]	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 [29]	Expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence.
Safety [29]	Freedom from unacceptable risk.
Safety function [29]	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 [9] 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.

Term [reference]	Description/definition
Safety functions [9] 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) [29]	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 [9]	Technical barrier elements that are realized in a common system.
Safety system [29]	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 [29]	Condition of automation and control solution being free from unauthorized access and from unauthorized or accidental change, destruction or loss. Note 1 to entry: Types of security are cyber security and physical security.
Security conduit [29]	Set of data flows between security zones that share common security requirements.
Security control [29]	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 incident [29]	Violation or imminent threat of violation of ACS security policies, acceptable use policies, or standard security practices.
Security level (SL) [29]	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 [29]	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) [29] *	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 [29]	Set of systems or components that share common security requirements. Note 1 to entry: Security zones can be physical or logical.
Target security level (SL-T) [29]	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 [8]	Equipment and systems involved in the realization of a barrier function.
Threat [29]	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 [29]	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 [29]	See security zone.

* [29] uses the term “security program rating” in the list of definitions. This is assumed to be a mistake. “Security protection rating” is used in the text.