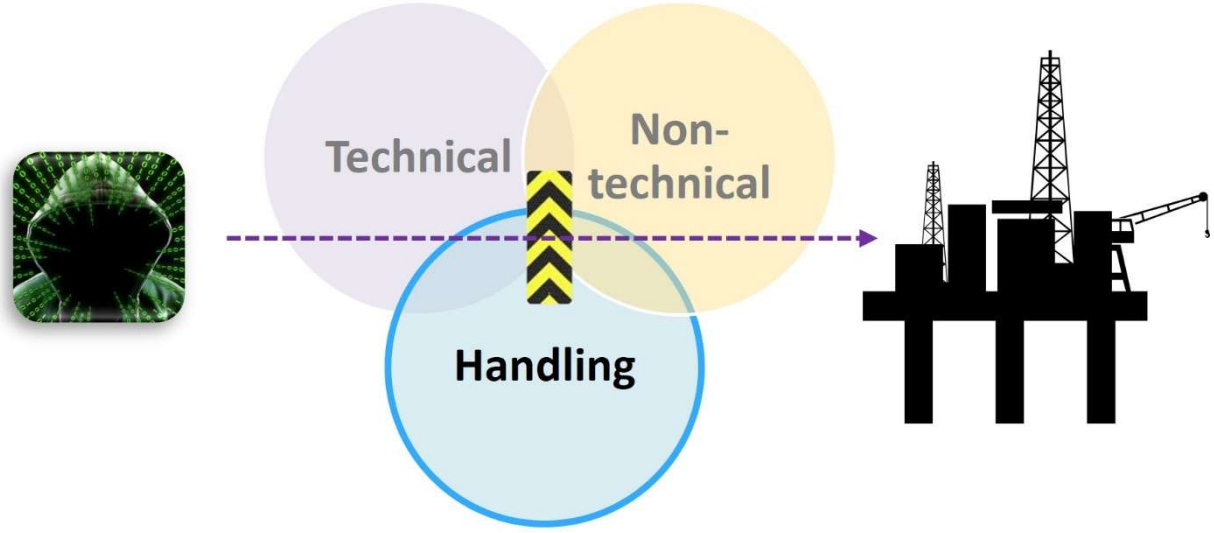

Report

Monitoring and handling cybersecurity threats, vulnerabilities and barrier impairments

Authors:
Geir K. Hanssen, Christoph Thieme, Andrea Vik Bjarkø

Report No:
2025:00702 - 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

Monitoring and handling cybersecurity threats, vulnerabilities and barrier impairments

KEYWORDS
Barriers
Barrier management
Cybersecurity barriers
Barrier impairments
Threats
Vulnerabilities
Oil and gas industry

VERSION
1.1

DATE
2025-10-29

AUTHORS
Geir K. Hanssen, Christoph Thieme, Andrea Vik Bjarkø

CLIENT
The Research Council of Norway

CLIENT'S REFERENCE
326717

PROJECT NO.
102020847

NO. OF PAGES
33

SUMMARY
This report is the third of three summary reports from the cybersecurity barrier management project. It summarizes new knowledge and guidance on the handling of cybersecurity threats, vulnerabilities and barrier impairments, covering the following activities:

i) Monitoring of cybersecurity barriers
ii) External threat intelligence to maintain cybersecurity barriers
iii) Handling of cybersecurity barriers

The other two reports cover technical and non-technical cybersecurity barriers.

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

PREPARED BY
Geir K. Hanssen
SIGNATURE

CHECKED BY
Knut Øien
SIGNATURE

APPROVED BY
Maria V. Ottermo, Research Manager
SIGNATURE

REPORT NO.
2025:00702

ISBN
978-82-14-07269-3

CLASSIFICATION
Unrestricted

CLASSIFICATION THIS PAGE
Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
0.9	2025-06-12	Draft version of WP3 report
0.95	2025-06-30	Draft version of WP3 report for commenting by project partners
1.0	2025-09-01	Final version (internal)
1.1	2025-10-29	Final version (unrestricted)

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

Table of contents

1 Introduction

1.1 Background

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

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

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

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

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

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

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

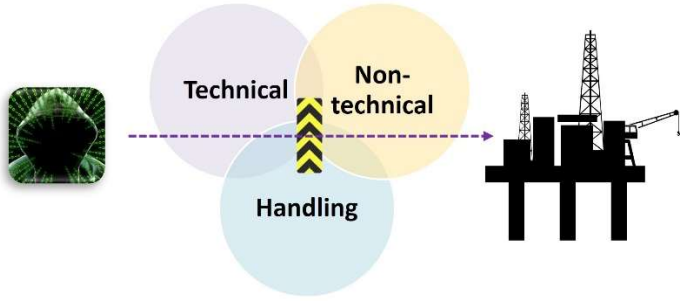

Figure 1 The three main parts of the CBM project

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

1.2 Purpose and scope

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

i) Monitoring of cybersecurity barriers
ii) External threat intelligence to maintain cybersecurity barriers
iii) Handling of cybersecurity barriers

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

1. How to gather information about and visualize the status of cybersecurity barriers?
2. How should information from external threat intelligence be managed to maintain cybersecurity barriers?
3. How to handle threats, vulnerabilities and cybersecurity barrier impairments?

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

1.3 Approach

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

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

1.4 Limitations

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

Regarding cybersecurity requirements, we mainly focus on the IEC 62443 series of standards [6], aligning with the CDS-forum statutes, which aim to bridge the gap between technical safety and cybersecurity using IEC 61511 [7] (PDS-forum) and IEC 62443 (CDS-forum).

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

This report is deliberately kept on a generic level to not disclose company-specific information and to be useful to a generic audience.

1.5 Structure

Chapter 1 introduces the document, followed by Chapter 2, the main chapter, describing current process and procedures for monitoring and handling cybersecurity threats, vulnerabilities and barrier impairments. Chapter 3 provides discussion and conclusions. Abbreviations and definitions are found in Appendix A.

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

2.1 Process overview

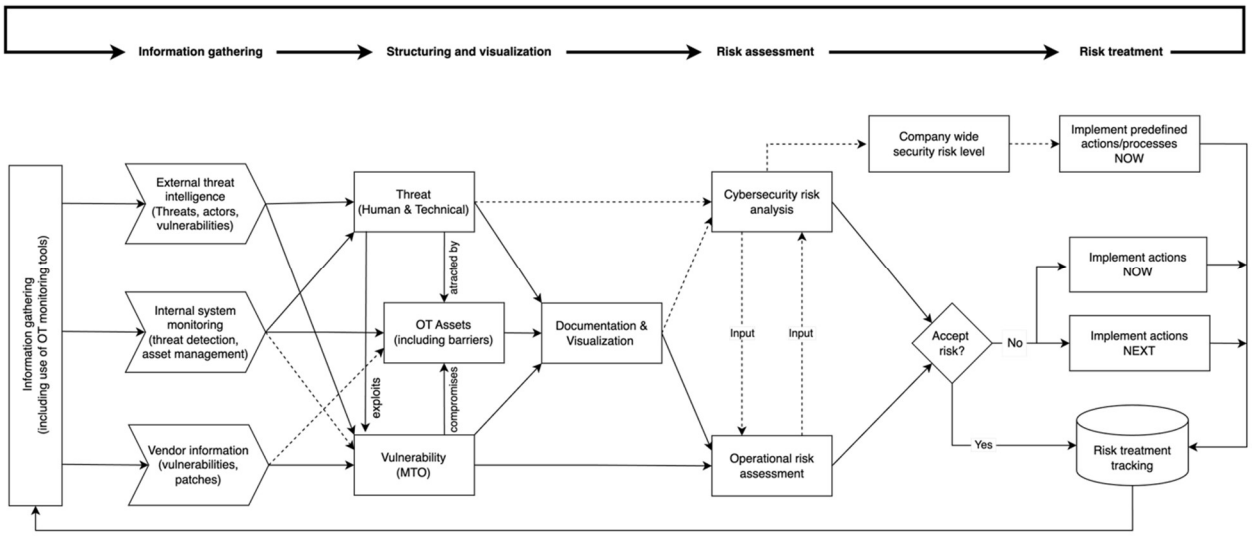

Figure 2.1 Information gathering, structuring, risk assessment, and risk treatment

The handling of cybersecurity threats, vulnerabilities and barrier impairments in OT is based on a continuous process of gathering relevant information from external and internal sources, including potential mitigations, such as patch information. This flow of information is structured to maintain an overview of the current cybersecurity situation, related to all OT assets, facilitating risk assessment and treatment.

This process comes in addition to IT-level cybersecurity processes, which prevents most cybersecurity attacks on higher Purdue levels, e.g., above level 3.5, which could also potentially cause harm at the lower OT-levels, but where the assumption is that, e.g., attacks are blocked before any OT assets are influenced. Hence, the process described in this report ensures additional prevention against remaining threats, either attacks that potentially could slip through despite of IT-security measures or attacks directly aimed at the OT-levels, e.g., through insiders. Hence, it is a complement to dedicated IT cybersecurity processes.

One part of the OT asset landscape consists of cybersecurity defences that protect and defend the other, more critical part—commonly referred to as the "crown jewels"—which are responsible for direct control of physical processes. Some of these OT-level cyber defences function as ***cybersecurity barriers***, offering an additional layer of protection beyond IT-level cybersecurity measures. Their role is particularly important in managing post-compromise or abnormal situations. This aligns with the definition of a cybersecurity barrier as a measure intended to a) detect abnormal conditions, b) prevent abnormal conditions from developing, and c) limit the damage caused by cyber incidents (cf. the technical barrier report [1]).

After providing this overview of the process, each of the parts will now be described in more detail. First, each of the **main phases** of the process will be described, namely:

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

Then the implementation of the process for each main type of information will be described, from gathering to execution and documentation of the risk treatment, i.e., the **subprocesses**:

- Threat landscape monitoring
- Vulnerability management
- Cybersecurity barrier monitoring

The description of these subprocesses—the main pathways through the overall process—is followed by a section on organization, which covers all three subprocesses and outlines who is involved in each.

2.2 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 CERTs. 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 forms 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 may be identified. This information may reach several roles in the organization, but for this report we focus on typical OT cybersecurity roles.

Figure 2.2 illustrates the external information (upper part) and internal information (lower part) provided on threats, vulnerabilities, and barrier impairments.

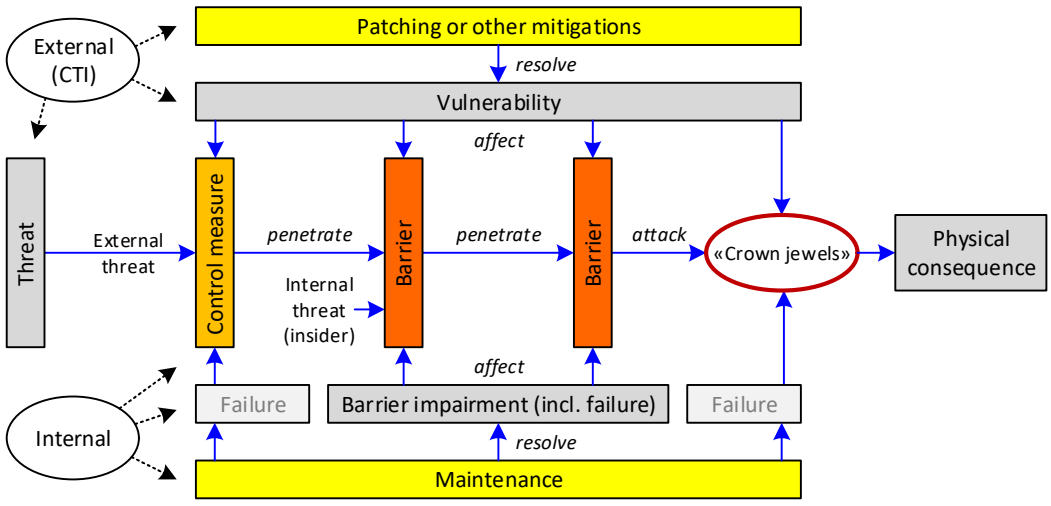

Figure 2.2 Information gathering in relation to cybersecurity barriers

As stated in Section 1.1, barriers complement preventive controls, which are illustrated in Figure 2.2 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 [8] is a relevant resource with an extensive knowledge-base of known adversary tactics and techniques, offering examples, mitigations, and strategies for detection.

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.

Regulatory requirements emphasize the importance of tracking such impairments. For example, [9] states: *"Personnel shall be aware of which barriers and barrier elements are not functioning or have been impaired."*

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 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*. (See Chapter 5 in the technical barrier report [1].)

Additionally, the distinction between vulnerabilities and impairments is not always clear-cut. For instance, a misconfiguration during operation (e.g., of a firewall ruleset) may be classified as a vulnerability, yet it can lead to reduced defensive capability even in the absence of deliberate exploitation. In such cases, it may be more appropriate to consider it an impairment, also because the source of detection is typically internal.

Another important internal information source pertains to generalized weaknesses in barriers—such as when barriers are outdated, insufficient, or no longer effective in the current threat landscape. These issues do not necessarily manifest as conventional vulnerabilities that can be addressed through patching or routine maintenance. Instead, the appropriate remedy may involve design modifications or the introduction of additional barriers. These generalized weaknesses are not considered impairments.

This nuance is not explicitly captured in Figure 2.2, which does not reflect cases where the resolution lies beyond standard maintenance and involves a broader barrier strategy update.

A final remark regarding Figure 2.2 concerns the role of patching and maintenance (represented by the yellow boxes). While patching is crucial for resolving vulnerabilities in cybersecurity barriers, and

maintenance is essential for sustaining both cybersecurity and safety barriers, it is important to note that these activities are not barriers themselves. Rather, they serve to influence the performance of barriers, and are therefore categorized as *Performance Influencing Factors* (PIFs). PIFs represent a third category of measures, distinct from:

- Control measures—which are used during normal operational conditions, and
- Barriers—which are activated or become critical during abnormal or failure scenarios.

This categorization follows the reasoning presented by Havtil [10], and is further elaborated in the technical barrier report [1]. See section 2.6.3 for details on monitoring of cybersecurity barriers and whether they have the right performance.

A variety of external information sources and providers distribute information about potentially relevant threats and vulnerabilities. The preferred sources may vary over time and from company to company, but some commonly used sources are included in Table 2.1, while techniques for acquiring such information are presented in Table 2.2.

Table 2.1 Examples of external information sources for threats and vulnerabilities

Source	Description
CTI vendors	These are companies that specialize in providing cyber threat intelligence services. They collect, analyse, and distribute threat data to help organizations stay ahead of potential threats. Examples include (the list is not complete): **CrowdStrike**[3] (Endpoint threat intelligence and adversary tracking. Offers IOC feeds and reports relevant to both IT and OT environments. Tracks threat actor groups including nation-state activity relevant to critical infrastructure.) **IBM X-Force**[4] (Enterprise and industrial threat intelligence and research. Provides curated vulnerability and exploit data, malware analysis, and incident support for ICS. Maintains the IBM X-Force Exchange, a rich CTI sharing platform.) **Recorded Future**[5] (Broad threat intelligence platform using machine learning and massive data sources. Provides strategic, operational, and tactical CTI, with industry-specific threat insights. Offers real-time alerts and integrations with security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools.) **Dragos Inc.**[6] (Specialized in ICS/OT cybersecurity. Offers highly tailored threat intelligence, detection content, and response services for oil & gas, energy, and industrial operations. Publishes the Dragos Year in Review (widely cited in critical infrastructure security)).
CERT's (Computer Emergency Response Team)	KraftCERT[7] (Eng. InfraCERT) is the sector Computer Emergency Response Team (CERT) and Incident Response Team (IRT) for the Norwegian Energy Sector. KraftCERT provides cyber threat intelligence services tailored to the energy (and petroleum) sector. Their offerings include threat analysis, vulnerability monitoring, early warning of malicious activity, and incident response support. Other CERT's may also be used, such as Thailand Computer Emergency Response Team (ThaiCERT), which may provide cyber threat intelligence earlier than KraftCERT due to the geographical time-difference.
NSM/NCSC	Norwegian National Security Authority (NSM) and its National Cybersecurity Center (NCSC)[8] provide national coordination and operational capabilities for cybersecurity. NCSC monitors

[3] https://www.crowdstrike.com/en-us/
[4] https://exchange.xforce.ibmcloud.com/
[5] https://www.recordedfuture.com/
[6] https://www.dragos.com/dragos-worldview/
[7] https://www.kraftcert.no/no/
[8] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

Source	Description
	and analyses cyber threats, supports incident response, and protects critical infrastructure through a 24/7 threat centre and national sensor network.
CISA (US Cybersecurity and Infrastructure Security Agency)	Similar, and complimentary, to NCSC, but for the U.S., the Cybersecurity and Infrastructure Security Agency (CISA)[9] provides threat intelligence, incident response support, and cybersecurity guidance to public and private sector organizations.
ICS suppliers	ICS suppliers provide information regarding vulnerabilities on their systems. Experience shows that the major IACS vendors is more proactive, distributing frequent and relevant cyber threat information. Information about vulnerabilities for specific assets may also be followed by information on how to patch the vulnerability.
Vulnerability databases	These databases store information about known software and hardware vulnerabilities. They help organizations identify and patch security flaws before they can be exploited. Examples include the National Vulnerability Database (NVD)[10] and the Common Vulnerabilities and Exposures (CVE)[11] database by Mitre. It is however important to notice that a CVE is not an exploit or an incident, but a catalogued weakness that *could* be exploited by attackers - if not mitigated.
Other stakeholders	In the context of CTI, stakeholders include anyone within the organization who has an interest in cybersecurity. This can range from executive leadership (e.g., CISOs, CIOs) to IT and security teams (including dedicated OT cybersecurity teams). They help set intelligence requirements and use the gathered intelligence to make informed decisions.
Other types of feeds	These include various data streams that provide real-time information about cyber threats. They can be open-source (free) or commercial (paid) and cover different aspects such as malware signatures, IP addresses, and domain names. An example is URLhaus[12] for malware URLs.

Suppliers do also provide information about threats that they are aware of for their particular equipment, which also may be followed-up by recommendations for patching. Typically, the large providers, e.g. SAS vendors, are those that offer the most relevant information, often in connection with a contractual responsibility of maintaining a Configuration Management DataBase (CMDB). Smaller vendors may not be able to maintain and provide an updated overview of threats and vulnerabilities, and there have been cases where the asset owner has had to contact the vendor for information. This underlines the importance of having multiple sources to ensure that relevant information is received and acted upon as soon as possible.

Table 2.2 Examples of techniques for acquiring information on threats and vulnerabilities

Source	Description
Penetration testing	These are simulated cyberattacks conducted to identify and exploit vulnerabilities in an organization's systems. They help in assessing the effectiveness of security measures and improving defences. Types of pen tests include internal, external, and web application pen tests. Given the OT-context, pen-test tools and methods must be used with caution to avoid disturbing or disrupting sensitive, safety-critical systems, as well as normal operation.
Dark web crawlers	These are tools used to scan and collect data from the dark web. They help in identifying threats such as stolen data, hacker activities, and emerging cyber threats. Dark web crawlers can track activities on hidden forums and marketplaces to provide actionable intelligence.
Honeypots	Honeypots are decoy systems designed to attract cyber attackers. They mimic real systems to lure attackers and gather information about their TTPs. Types of honeypots include low-interaction, high-interaction, and pure honeypots.

[9] https://www.cisa.gov
[10] https://nvd.nist.gov/
[11] https://cve.mitre.org/
[12] https://urlhaus.abuse.ch/

The information an operating company gathers about threats and vulnerabilities is both overlapping and complementary, and there is no clear-cut distinction between the two external information categories shown in Figure 2.1. For instance, patch-related information may not only come directly from the equipment vendor responsible for developing and distributing the patch but also from CERTs—such as KraftCERT—or specialized security firms like Dragos.

The information is complementary in terms of both timeliness and informational richness—both of which can be critical. For example, some operating companies rely on CERTs in other time zones, such as ThaiCERT, to benefit from early warnings relative to their own local time and working hours. Conversely, later reports on a vulnerability—such as a CVE—may offer more comprehensive guidance on recommended mitigation measures, including patching. Therefore, obtaining "the same" information from multiple sources can be highly valuable. However, this must be balanced against the risk of information overload, as well as the associated costs and resource requirements.

Not everyone within an operating company requires the same information. Data that is critical for certain roles may be irrelevant—or even distracting—for others. This is especially true for high-level information regarding threats and threat actors, which we will revisit later in the discussion.

In addition to the two main categories of external information, internal data is also collected. As previously noted, **internal system monitoring** can be divided into two types: monitoring as a barrier function (e.g., intrusion detection systems) – part of threat detection (cf. Figure 2.1), and monitoring of the barrier itself, i.e., assessing whether it is degraded – part of asset management (cf. Figure 2.1). Examples of commonly used technologies/tools related to the first type is provided in Table 2.3.

Table 2.3 Examples of company internal monitoring technologies/tools

Source	Description
Intrusion Detection Systems (IDS)	IDS monitor the interface between IT and OT levels and downwards to the middle OT-level. Below this, there are simply too many systems to be able to monitor effectively. Some OT systems may also be complicated to monitor for intrusion detection, and one should also be cautions to not interfere with OT-systems at the lower levels as this may introduce a risk of disturbing operation or safety-critical systems (according to FR §34a). Hence, it is important to assume that lower-level systems are well protected by the layers above. There are mainly three providers, Dragos, Clarity and Nozomi that are in use in the industry, but where experience shows that there may be an insufficient understanding of the protocols that these systems use. External service providers, such as Mnemonic, may oversee activity and security logs outside the OT teams working hours to ensure coverage 24/7.
Firewall monitoring	Firewalls govern and restrict communication between assets and layers/zones (ref. IEC 62443-3-2) and should be monitored to ensure that they operate as intended, and that firewall rules and configuration is correct and active.
Microsoft Defender[13]	Microsoft operating systems are frequently in use at the OT levels and hence Microsoft Defender is used to gain insight into endpoints where it can be used to maintain an asset inventory without scanning or interfering with systems (which is a challenge for IDS). It can also be used for threat detections for known attack patterns or zero-day anomalies. Furthermore, it can assist in mapping known vulnerabilities (such as CVE's) to specific assets.
SPLUNK[14]	Information about and from a variety of OT systems, typically logs, can be gathered, systematized, visualized, and analysed in a joint overview. Examples are firewalls, routers, switches, zone controllers, engineering workstations, historians, and dedicated security

[13] https://www.microsoft.com/en-us/security/business/microsoft-defender
[14] https://www.splunk.com/

Source	Description
	systems such as IDS. It can be used to detect anomalies in, e.g., network traffic in the OT layers, log-in's, injection of malware, etc.

Internal system monitoring related to the second part – the status of the barrier itself – includes failures, such as barrier impairments, and is typically found in various systems, including maintenance records within CMMS and health status indicators for all components of control systems in SAS.

Because maintaining an overview of barrier status is fundamental to effective cybersecurity barrier management, internal monitoring is positioned at the center of Figure 2.1—between the two types of external information.

In addition, internal monitoring of OT assets provides information that is also essential for vulnerability management. This includes details such as software and patch versions, system configurations, and related data. 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 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.

2.3 Structuring and visualisation

The information gathered from external and internal sources is structured in threats, vulnerabilities and status of OT assets – especially the status of the cybersecurity barriers in terms of impairments. This information facilitates the three main subprocesses: Threat landscape monitoring, vulnerability management, and cybersecurity barrier monitoring[15].

The relationships between the terms 'threat', 'vulnerability' and 'barrier impairment' are not straight forward, especially the concept of 'barrier impairment' since neither 'barrier' or 'impairment' have been part of the cybersecurity vocabulary. The relationships are illustrated in Figure 2.2, and the distinction between barrier impairments and vulnerabilities has been discussed in detail in the technical barrier report [1], including relations to the ISA/IEC 62443 ontology [11].

Here, we start out with a focus on the concepts of 'threat' and 'vulnerability' which are central to cybersecurity risk management in an OT context. And while they are distinct terms, they are also closely related. We follow the ISA/IEC 62443 ontology to define how **threat** and **vulnerability** relate, by together being functions of the likelihood of a **risk** as illustrated in Figure 2.3.

With reference to the overall cybersecurity process that is described in Section 2.1, we relate **threat** and **vulnerability** and how they impose a risk of **compromising** an **asset** (cf. Figure 2.4). Threat actors are attracted by the opportunity to compromise an **asset** (here: OT assets). In the context of the CBM project, this mainly relates to human threats that are enabled by skills, resources and motivation. There are also technical threats such as hardware or software failures; however, as described in the technical barrier report [1], we relate failures and impairments directly to the OT assets (see also Figure 2.2).

[15] In the CBM project we focus on impairments of cybersecurity barriers, although – as shown by Figure 2.2 – failures affect control measures and crown jewels in addition to the barriers.

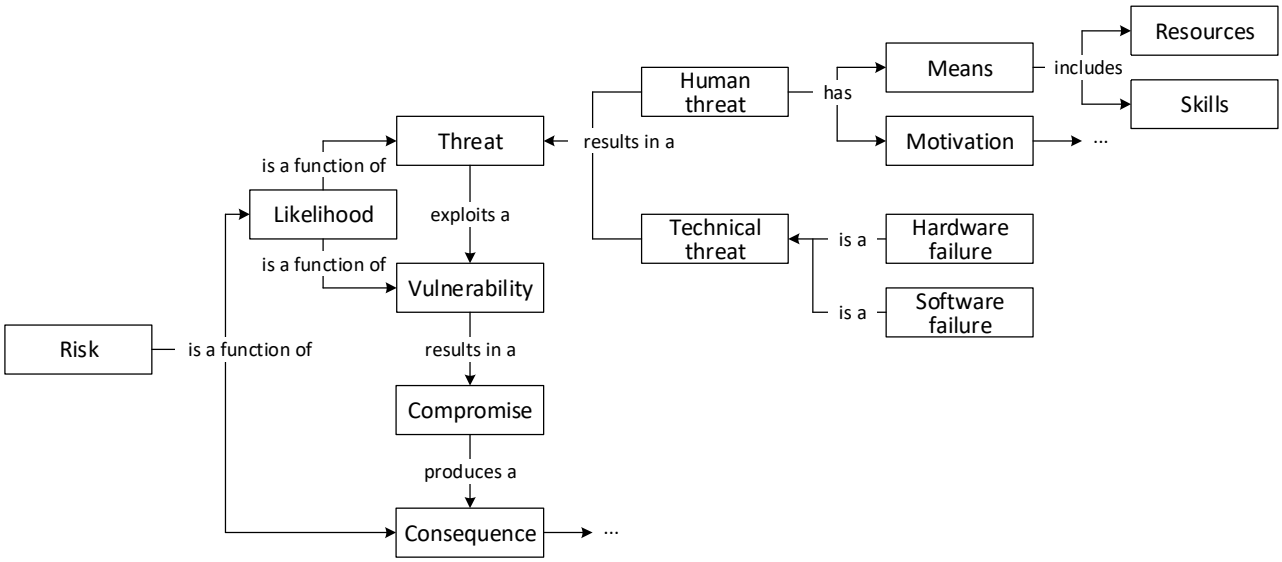

Figure 2.3 Ontology diagram of risk (adapted from [11])

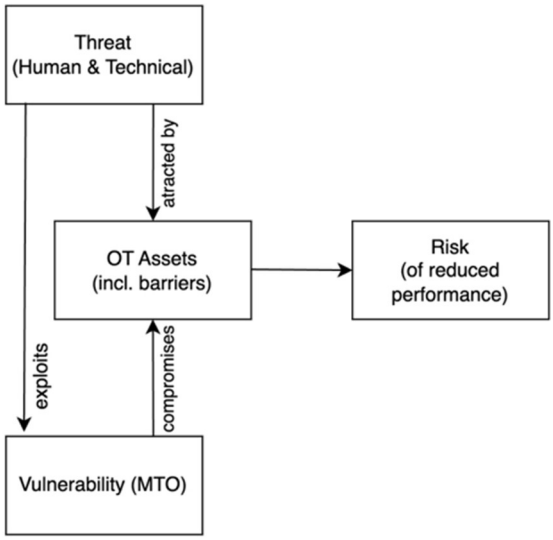

Figure 2.4 Risk as a function of threat, vulnerability and consequence on OT assets

A threat is a potential cause of an unwanted incident that may result in harm to a system, asset, or operation, while a vulnerability is a weakness or flaw in a system that can be exploited by a threat. Hence, a threat is an intent or event, e.g., misuse by an insider, that that could trigger an attack given that it is possible by a vulnerability, e.g., unpatched software, an inactive firewall etc. Then the risk is given by the likelihood of a threat exploiting a vulnerability and the consequence it may have for an asset.

Threats are reported, e.g., in weekly reports describing the threat landscape. This may cover different types of security threats, including cybersecurity threats. Vulnerabilities are continuously documented as 'service tickets' in a vulnerability management system for further handling including risk assessment. However, both threats and vulnerabilities may be "fast tracked", if immediate action is required.

Visualisation of cybersecurity barrier status, including the use of barrier panels, is described in the technical barrier report (Chapter 5) [1].

2.4 Risk assessment

2.4.1 System level

Risk assessments are carried out in the design phase of a facility, and reused when upgrading and modifying a facility with new OT assets. System level risk assessments may be used to inform considerations about a companywide security risk level and provide input to continuous component level assessments in the operations phase.

For example, weekly security updates can be done where the general threat status in different parts of the world is evaluated, covering cyber threats and actors, and cyber threats particular for IACS. This represents the general threat level towards the organization. Based on this assessment, the company wide security risk level is determined. For each facility predefined physical and cybersecurity actions are implemented and decided on by the respective offshore installation manager.

2.4.2 Component (continuous) level

For day-to-day operations, a simpler process is used, where previously unknown threats and vulnerabilities are assessed, mainly based on networking diagrams and OT asset inventories (or similar databases on equipment being used in the facility). A general component-level risk assessment process may have the following steps:

1. **Check relevance:** Check whether a potentially affected OT asset is installed in the facility by checking the OT asset inventory and the configuration management database (CMDB).
2. **Initial assessment:** Conduct an initial severity assessment based on network location and potential impact. Check how the vulnerability may affect IACS. In general, locating a vulnerability to the affected Purdue level can be used as a guide:

   Level 3: The possible consequences arising from an attack or vulnerability on this equipment are often unacceptable and patching should be started quickly. Patching on Purdue level 3 is seen as less complicated as many components used are standard IT, or very similar to standard IT components and the patches can be applied without problems.

   Level 2: The risk evaluation is focusing on possible consequences, vulnerabilities and issues leading to bypassing of administrative accounts that need to be handled. Equipment on level 2 is often only modifiable through administrative user accounts, which are not active during normal production. Therefore, resources are often better used on other threats and vulnerabilities. In addition, patching is seen as a possible source to disturb other equipment. Much equipment on level 2 is based on Windows PCs and other equipment suppliers need to assure that a patch will not affect their equipment.

   Level 1: Patches are normally not prioritized, as there is a small attack surface. The most important part is to monitor and assess the information exchange to level 1. Communication that is not recognized or unauthorized will be assessed and measures taken to prevent it in the future. Updating/patching of equipment on level 1 is seen as difficult, as it may lead to production stops and problems, due to downtime. Testing of the patches is necessary to minimize downtime.
3. **Register vulnerability:** Register the vulnerability as a service ticket that requires an action. In critical situations (risk is considered to be unacceptable on the short term) a case is opened (e.g., in a system like Synergi etc.), escalating the handling of the vulnerability and mobilizing additional resources and management to resolve it as soon as possible.
4. **Inform:** Inform the OT asset owner of the vulnerability (ideally, such notifications should be automated).

5. **Detailed assessment:** Assess risk of the vulnerability together with the OT asset owner (risk of patching versus the risk of not patching). Suppliers may also be contacted for more information.
6. **Decide measures:** Decide on and implement measures with OT asset owner, e.g.,
    a. Patching
        i. Immediately (NOW)
        ii. During the next opportunity (i.e. production shutdown) (NEXT)
        iii. Do not patch (NEVER)
    b. Compensating measures
    c. Nothing

When assessing the impact of a vulnerability, some key considerations may be:

1. What OT assets are affected by the vulnerability?
2. What is required to exploit the vulnerability? E.g., does it require internet or physical access? Does it require logging into a server/system?
3. How often is the OT asset connected to the internet/network?
4. Is a specific toolkit required?
5. How "deep" into the network is the OT asset, i.e., what protections are implemented to protect the specific OT asset?
6. What other OT assets are protected by the OT asset (if vulnerability applies to a cybersecurity barrier)?
7. What other protective measures are "behind" the OT asset (if vulnerability applies to a cybersecurity barrier)?
8. Will the vulnerability/patch affect the production process? How long will production be affected?
9. Is the vulnerability affecting the OT Demilitarized zone (DMZ)?
10. What are the consequences of not patching the OT asset? What are potential consequences of patching the OT asset?
11. Who will carry out the patching? Are there service agreements in place?
12. Does patching require the OT asset to be recommissioned?

The CVE-score provided in CVE notifications may give an indication of the risk, however, considering the concerns above, it is not a direct measurement of the vulnerability severity. Generally, the risk assessment gets more complicated if the vulnerability is in OT specific devices. For standard software (Anti-Virus, Virtual Private network (VPN), Microsoft based network components) the assessment is simpler and more straight forward to carry out.

Entering vulnerability information as tickets enables regular follow-up by the assigned OT cybersecurity personnel. It serves as a reminder to check if the vulnerability may require attention or can be resolved soon. More critical vulnerabilities (and threats) that cannot be resolved should be documented in a risk register, which should be reviewed on a regular basis at the management level.

In order to enter a vulnerability in a risk register, the OT asset owner, i.e., the asset operations manager, and offshore installation manager, needs to understand the significance of the vulnerability, which may be difficult to achieve. An additional register should be used by the OT personnel to document critical vulnerabilities, exchange information between facilities, and to use it in discussions with the facility management.

Typically questions when reviewing a risk register are:

- Has anything changed [regarding the vulnerability] in the context of the OT asset?

- Can anything be done to remove or mitigate the vulnerability in the new context/with the changes?
- Can the vulnerability be abused in the future? What conditions need to be met for this abuse?

For vulnerabilities that cannot be resolved, but are deemed acceptable, the corresponding service ticket is closed. For traceability, comments are added to describe why measures have (not) been taken and add traceability. This decision needs to be quality controlled before the ticket can be closed to assure that the risk has been handled.

2.5 Risk treatment and tracking

2.5.1 General actions

Actions are taken based on the criticality of the threat or vulnerability. In very serious cases, the situation is handled similar to a cybersecurity incident, when required resources are mobilized from within the company. In addition, external resources, such as KraftCERT may be involved. Here, the time and effort spent is seen worth to invest to solve the issue. However, this is only a short-term solution for improved monitoring and quicker response, in case the threat should manifest. Such a situation will normally result in patching of the critical systems or mitigation measures, such as, disconnecting systems, or reconfiguring firewalls, etc.

The most invasive action would be to shut down an entire facility, but this includes risk associated with a non-scheduled shutdown and later start-up in addition to loss of production. Another action, when a threat or vulnerability is imminent is to put the facility into so called island-mode. In island-mode the facility is disconnected from central onshore facilities and more importantly from the internet. One disadvantage with this is that remote support and patching cannot be executed, and the central onshore facility is “blind” to what is happening on the facility. This decision is made by the offshore installation manager. The island mode procedure is now a training scenario and has been verified.

2.5.2 Patching

For a vulnerability to be seen as critical, having a high risk, normally there must be a high CVE score, and the affected OT asset must when exposed be able to communicate with other OT assets and the internet. If a non-critical vulnerability (i.e., low risk) needs patching, patches are not applied immediately. Normally these types of updates are collected and carried out collectively during the next maintenance period. This may be a total system overhaul, or planned maintenance of (parts of) the facility.

In cases where no patches are available or can be applied, compensating measures are applied. This could be that the system cannot be used or connected to the network or internet.

A management of change process is used when a patch is applied. The first step is an engineering query, which is a request from offshore personnel to the engineering department onshore to suggest a solution to a problem (in this case of a vulnerability or installing a patch). This will result in a change of the system. The change is then added to the turn-around-plan (if not a critical patch) or to the Synergi-case (for very time-critical situations). The turn-around-plan describes maintenance actions and changes to be conducted when the system is overhauled. Offshore facilities are regularly shut down, to carry out maintenance, inspections, modifications and changes that cannot be carried out during normal operation.

Before patches on level 1 can be applied, a consequence analysis should be done, assessing the need for manual operation or backup operators. For some systems, i.e., PLCs, it is enough to monitor them during and after patching, others may need more supervision and manual control. Before a patch is applied the cybersecurity responsible for a facility and the responsible for facility integrity need to agree to the procedure for patching. The level of detail needs to be so high that the patches easily can be reversed.

For some OT assets the patch needs to be tested on a test system or have clearance for patching by the system supplier. Patches are then applied according to the decided procedure when possible (during turn around or immediately).

2.5.3 Identified challenges for handling of threats, vulnerabilities and patches

Overview of OT assets: One of the main challenges is to hold a sufficient overview over OT assets and their location (in an CMDB). Especially for OT assets that are normally not interacted with or that are unique for a facility. This information is available but spread out over different systems. An automation of the identification of OT assets being used in one facility and highlighting its position (physically and in the network) would greatly simplify the criticality/risk assessment process of vulnerabilities. The connection between physical devices and the logical architecture is not always easily assessable - here digital twins may be a solution. Another challenge closely associated with the assessment process is the OT asset inventory. Not all devices are automatically added or recognized. Better processes and tools are needed to create the inventory (for new and existing facilities) and maintain it through the facility's lifetime.

Manual effort: In addition, patching itself is seen as a very manual job. Especially for the most common OT systems such as PCs, servers, network devices, etc., more automation is desirable. Automation is required for identification of available updates and roll-out of these, once they have passed tests.

A distributed process: There are several roles and processes in play for managing OT cybersecurity threats, vulnerabilities and barrier impairments. Experience shows that there is a need for systems that connect the information from different sources and provide an assessment of criticality of vulnerabilities for the different facilities, simplifying and accelerating the process to take actions. Also risk treatment and tracking of risks, compensating measures and deferred patches is currently spread out over different systems, which could be improved through automation.

OT cybersecurity knowledge: Basic knowledge on OT cybersecurity can in general be improved at the management level and for relevant roles close to OT. Specific knowledge of the OT cybersecurity specialists is not formalized for vulnerabilities, threats and patches, which could hinder an efficient handling and mitigation.

2.6 Subprocesses

We can distinguish between the following three main subprocesses for monitoring and handling of cyber-security threats, vulnerabilities and barrier impairments:

i) Threat landscape monitoring
ii) Vulnerability management
iii) Cybersecurity barrier monitoring

2.6.1 Threat landscape monitoring

This subprocess is illustrated in Figure 2.5.

Information about threats and threat actors is typically gathered from multiple sources, examples of which are provided in Table 2.1. This information can be compiled into weekly reports that contribute to assessing the company's overall security risk level. The different security risk levels—typically four—have predefined actions associated with them. These actions are implemented based on the designated level and are tracked to ensure proper execution.

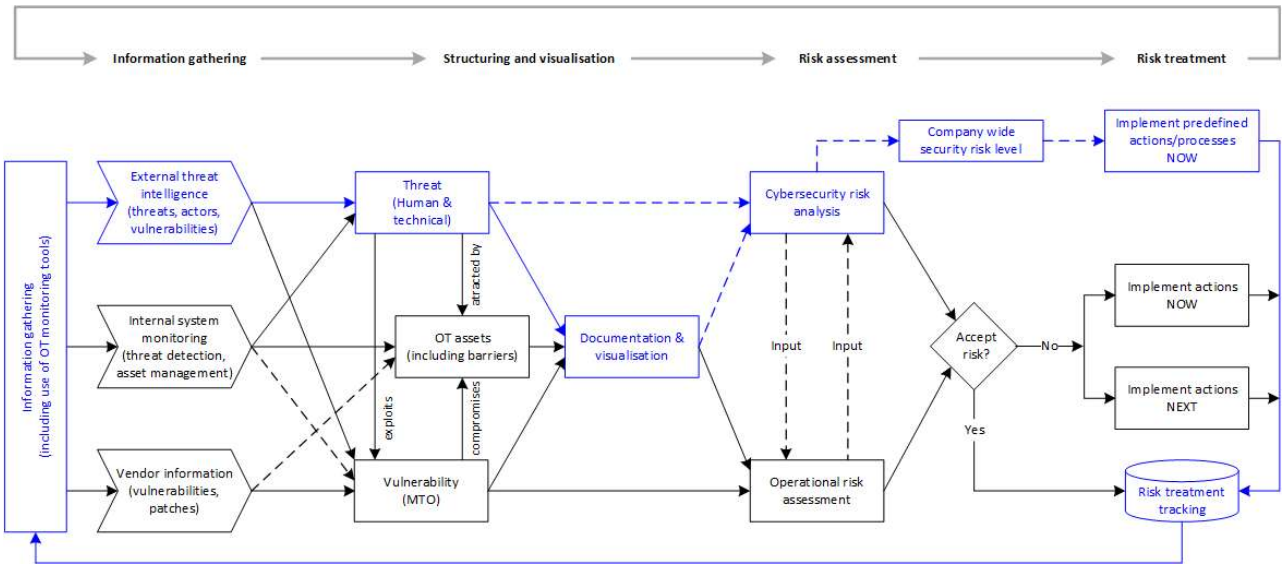

Figure 2.5 Subprocess: Threat landscape monitoring

In addition, various threat reports and advisories can be used to enhance cybersecurity measures, including reinforcement of cybersecurity barriers. Detailed information on threat actor tactics, techniques, and procedures (TTPs) can help prioritize security measures tailored to defend against known attack patterns.

2.6.2 Vulnerability management

This subprocess is illustrated in Figure 2.6.

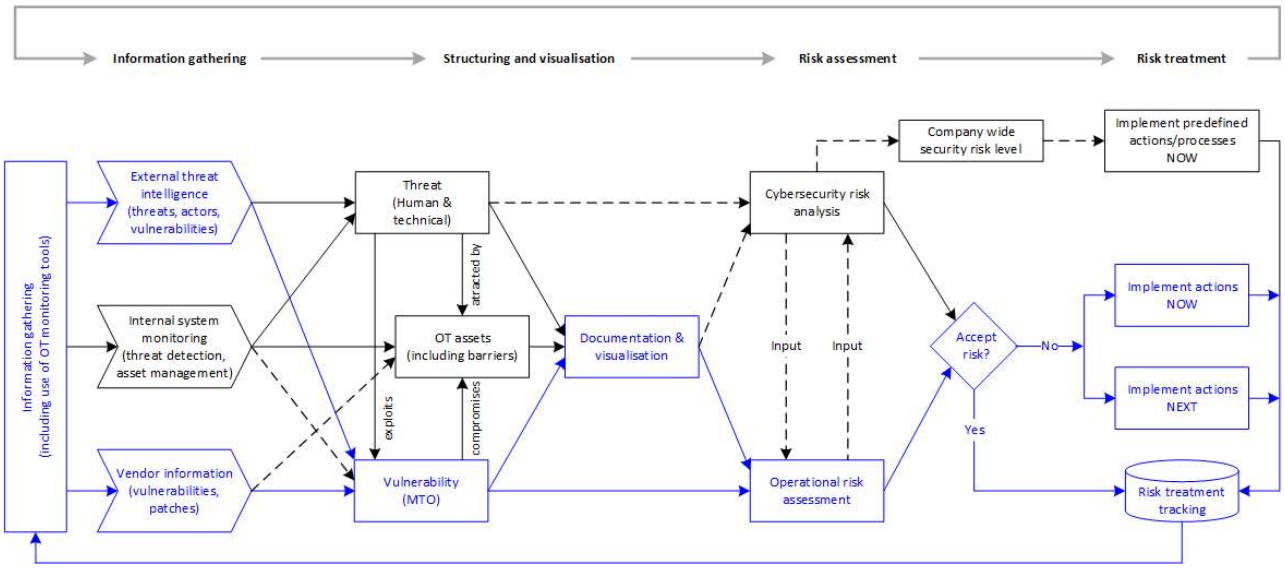

Figure 2.6 Subprocess: Vulnerability management

Information about vulnerabilities can be obtained from many of the same cyber threat intelligence (CTI) providers as those used for threats and threat actors (cf. Table 2.1), as well as from the vendors of the affected assets. This section focuses on specific technical vulnerabilities, i.e., CVEs, though general vulnerabilities related to human and organizational factors (i.e., MTO: Man, Technology, Organization) are also important and are often identified through internal sources. The distinction between specific and general vulnerabilities is further discussed in the Technical Barrier Report [1].

CVEs are managed internally through operational risk assessment and treatment, as described in Sections 2.4.2 and 2.5.

CVEs can apply to any OT asset, including control measures, cybersecurity barriers, and crown jewels, as illustrated in Figure 2.2. This implies that, in cybersecurity barrier monitoring, vulnerabilities could be considered alongside impairments (cf. Figure 2.2).

However, as discussed in the Technical Barrier Report [1], the recommendation from industry partners is to manage specific vulnerabilities (CVEs) through the ongoing vulnerability management process, rather than including them in the barrier 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.

2.6.3 Cybersecurity barrier monitoring

This subprocess is illustrated in Figure 2.7.

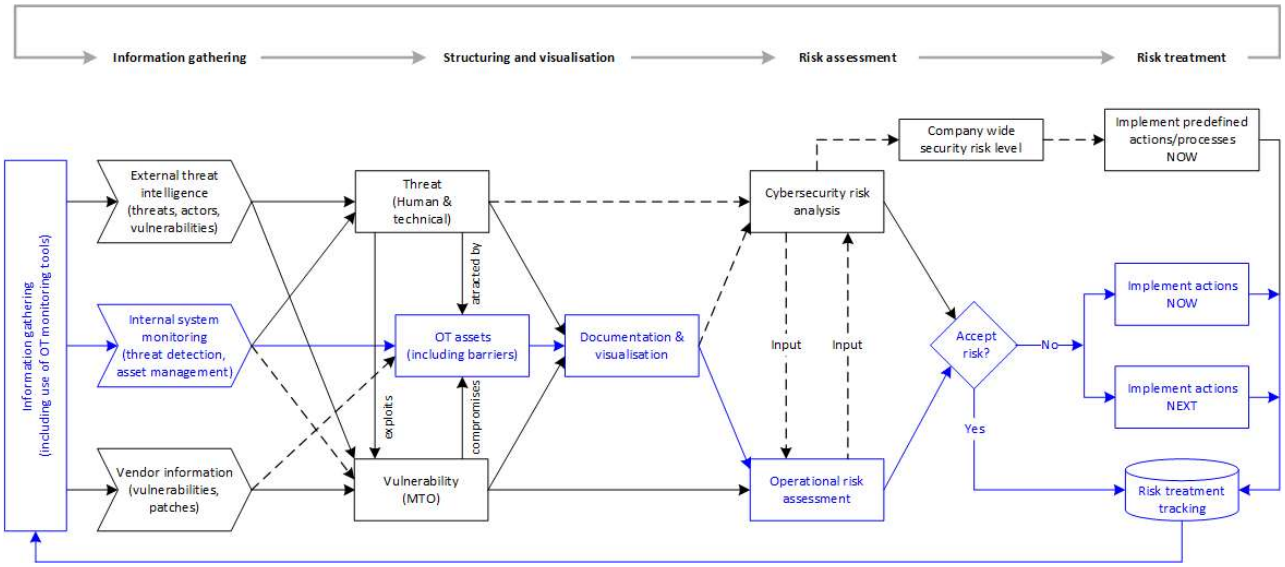

Figure 2.7 Subprocess: Cybersecurity barrier monitoring

Information about the status of cybersecurity barriers is obtained through internal system monitoring of OT assets that are classified as cybersecurity barriers, based on the criteria outlined in the Technical Barrier Report [1]. Cybersecurity barrier impairments can be visualized in barrier panels alongside safety barrier impairments (cf. Section 5.1 in [1]) and may be addressed in a manner similar to vulnerabilities (cf. Figure 2.6), through operational risk assessment and treatment based on criticality.

Additionally, cybersecurity barriers are followed up through verification of performance requirements, as described in the Technical Barrier Report (Chapter 5) [1]. These performance requirements, derived from standards such as IEC 62443, address both technical and non-technical security measures. They serve as the foundation for medium- and long-term verification activities.

The main challenge lies in the short-term monitoring and visualization of non-technical barrier elements. Tools such as the barrier panel are effective for displaying the real-time status of technical barriers but are less suited to representing the status of non-technical elements. Relevant information—such as personnel

competence, training, and procedural readiness—is often stored in separate source systems. Integrating this data into real-time visualization tools remains complex and poses a significant obstacle to achieving full situational awareness of non-technical barrier health. (See further elaboration in the Non-technical Barrier Report [2].)

The threat detection component of internal system monitoring refers to systems such as IDS, as exemplified in Table 2.3. This pertains to the use of systems—including cybersecurity barriers—for detecting threats, rather than monitoring the status or performance of cybersecurity barriers, which is the focus of this subprocess.

Further details on the various phases of the cybersecurity barrier monitoring subprocess—with an 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 visualisation

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 the Technical Barrier Report (Section 5.1.4) [1], and in the Non-technical Barrier Report (Section 2.3.1) [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 [9]: *"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) [16] 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.

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

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 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.

2.7 Organisation

The organisation that is responsible for monitoring and handling cybersecurity threats, vulnerabilities and barrier impairments spans the strategic, operational, and execution (field) levels.

2.7.1 Strategic level

At the strategic level, the responsibility for OT cybersecurity lies with the corporate cybersecurity leadership, typically represented by the Chief Information Security Officer (CISO) and a cybersecurity governance body or steering group. This level is responsible for defining the overall cybersecurity strategy for the company, aligning it with business objectives, regulatory requirements, and safety principles.

The strategic level ensures that cybersecurity is embedded as a part of enterprise risk management and that there is sufficient governance, oversight, and resource allocation to manage cyber risks in OT environments. It defines key policies, risk acceptance criteria, and performance indicators, including the management of cybersecurity barriers as integral components of risk reduction.

Strategic leadership also provides the mandate and framework for cross-functional collaboration between IT, OT, and safety functions. It is responsible for approving high-level decisions involving risk trade-offs, such as accepting the temporary impairment of a cybersecurity barrier or delaying patch deployment when operational continuity is critical. The latter should be done in close dialogue with the operational level which have access to the specific details of a risk situation.

Additionally, this level oversees compliance with internal and external requirements (e.g., IEC 62443 [6], PSA/Havtil Management Regulations § 5 [9], and the EU NIS2 directive [12]), and maintains engagement with external stakeholders such as sector-specific CERTs, regulators, and threat intelligence providers.

The strategic level defines the expectations and structure that the operational and execution levels follow to ensure effective and coordinated cybersecurity risk management.

2.7.2 Operational level

The operational level is responsible for the day-to-day execution of cybersecurity processes in the OT environment. This includes the continuous monitoring, analysis, coordination, and decision-making required to handle cybersecurity threats, assess vulnerabilities, and maintain the functionality of cybersecurity barriers. This level also ensures that all cybersecurity-related actions and decisions are properly documented and tracked using tools such as the CMMS, Synergi, and risk registers. This supports both traceability and continuous improvement.

The operational level functions effectively when roles are clearly defined, communication between disciplines is strong, and all stakeholders share a common understanding of cyber and operational risk. The OT cybersecurity team plays a key role in facilitating this integration and ensuring that the organization can respond to cybersecurity challenges in a timely, coordinated, and risk-informed manner.

OT cybersecurity team: At the center of this level is the OT cybersecurity team, a cross-functional group that brings together personnel with responsibilities for cybersecurity monitoring, risk assessment, and system coordination in OT environments. This team is led by the **OT cybersecurity lead or coordinator**, who ensures structured handling of cyber risks and serves as the key interface between IT security, engineering, operations, and vendors.

SOC: The OT Security Operations Center (OT-SOC) works in close collaboration with the OT cybersecurity team. While the SOC is typically responsible for monitoring security events via Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and IDS tools, the OT cybersecurity team evaluates the operational relevance of these events, performs risk contextualization, and coordinates appropriate actions with other stakeholders.

Control system engineers and automation teams: Support the evaluation and implementation of technical measures such as patching, firewall configuration, segmentation, or system hardening. They ensure that any changes are safe, tested, and compatible with OT operational constraints.

Technical experts: This role is highly organization-dependent and is typically divided into multiple specialized roles—each corresponding to a specific application system (e.g., MySQL databases, SAP enterprise platforms, Honeywell safety and automation systems) or domain area (e.g., IT layer, OT layer, control room environments).

The role serves two primary objectives. First, technical experts provide in-depth knowledge of the affected systems, enabling them to support and enhance the effectiveness of other incident response team members. They are responsible for advising on the implementation of system-specific measures, mitigation strategies, and technical recovery steps. Second, they are tasked with responding to joint incidents that require high-criticality authorizations—such as root-level access or privileged administrative credentials—making their involvement essential in high-impact scenarios.

OT asset owners and Offshore Installation Managers (OIMs): Responsible for operational risk decisions. They determine whether a vulnerability or barrier impairment warrants immediate action, delayed treatment, or documented risk acceptance. In critical situations, they may authorize isolation of systems, including the use of island mode, to mitigate threats.

2.7.3 Execution (field) level

The execution level is where cybersecurity-related decisions and planned actions are carried out in practice. It involves personnel and external partners responsible for implementing technical changes, reporting system conditions, and supporting recovery and maintenance of cybersecurity barriers across field locations and offshore installations. All execution-level activities are based on decisions made at the operational level and follow established change management and safety procedures. The field teams often rely on support from engineering, the OT cybersecurity team, and operations leadership to validate the safety and timing of their actions.

This level plays a vital role in maintaining the functional integrity of cybersecurity barriers and ensuring that field actions are carried out in a consistent, safe, and documented manner. Proper coordination and communication between field staff and the operational level are essential to avoid unintended impacts on safety, production, or system stability.

Field personnel (internal): Key roles at this level include maintenance personnel and field technicians. These actors ensure that vulnerabilities are remediated, systems are patched or reconfigured, and impaired barriers are restored, either as part of routine maintenance or through immediate interventions.

Maintenance and field personnel execute actions, which often has to be done on-site, such as applying approved patches, updating firmware, restarting services, or physically inspecting and restoring affected components. They are also responsible for reporting anomalies and confirming the completion of tasks through systems such as the CMMS or other operational tools.

External roles: Vendors and service providers support this process by providing timely vulnerability disclosures, validated software updates, configuration guidance, and troubleshooting assistance. In some cases, they also participate in on-site activities or remote diagnostics under controlled conditions. Their input is critical for assessing the feasibility and risk of implementing technical changes, particularly for legacy or proprietary systems.

The main roles across the barrier management lifecycle are summarized in Table 2.4.

Table 2.4 Roles and responsibilities

Role	Threat Monitoring	Vulnerability Management	Barrier Monitoring
CISO / Governance Body	Approves strategy, risk levels	Defines risk acceptance criteria	Sets oversight for barrier performance

OT Cybersecurity Lead and team	Coordinates input & reporting	Oversees triage & asset mapping	Leads impairment evaluation & tracking
SOC Analysts	Monitor alerts (SIEM, IDS)	Feed CVE alerts to OT cybersecurity team	Raise alerts if barriers are impaired (does not have the intended performance)
Control System Engineers	Validate threat impact on assets	Assess and test patches	Maintain functionality of barriers
OT Asset Owners / OIM	Make operational decisions	Accept or defer patching	Approve compensating measures
Field Technicians	(none)	Implement patches	Restore impaired barriers
Vendors / Integrators	Provide CTI	Issue patches & advisories	Assist diagnostics & updates

3 Discussion and conclusions

The discussion, including its conclusions, is organized around the following three questions, which define the scope of this report:

1) How to gather information about and visualize the status of cybersecurity barriers?
2) How should information from external threat intelligence be managed to maintain cybersecurity barriers?
3) How to handle threats, vulnerabilities and cybersecurity barrier impairments?

First, it is important to clarify the scope, as the questions are somewhat narrower in focus than the broader research objectives and task descriptions. While the first two questions address cybersecurity barriers—central to the project—the monitoring component also encompasses threats and vulnerabilities, as well as impairments to cybersecurity barriers, as outlined in the handling aspect discussed in the third question.

1. How to gather information about and visualize the status of cybersecurity barriers?
Effective cybersecurity barrier management relies on the continuous collection and integration of both external and internal information. To understand the status of cybersecurity barriers, it is essential to monitor for both impairments (degradations in performance or outright failures) and vulnerabilities that may compromise barrier effectiveness.

Externally, relevant data is sourced from cyber threat intelligence (CTI) providers, ICS suppliers, national and international CERTs, and vulnerability databases (e.g., CVE or NVD). These sources provide timely information on threats and vulnerabilities, often accompanied by patch advisories or recommendations for mitigation. Internally, monitoring systems such as IDS, firewall logs, Microsoft Defender, and CMMS platforms collect operational data on the performance and health of OT assets, including those classified as cybersecurity barriers.

To make this information actionable, it should be structured and visualized. A key tool for this is a barrier panel which is a dashboard-style interface that aggregates barrier status data, e.g., using a traffic-light system (red for critical impairments, yellow for degraded conditions, and green for normal operation). These panels allow users at both offshore and onshore levels to assess real-time risk, plan maintenance, and prioritize actions. Barrier panels should also support historical trend analysis and link to underlying service tickets, diagnostic logs, or maintenance records, enabling traceability and assisting decision support.

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

2. How should information from external threat intelligence be managed to maintain cybersecurity barriers?
Managing cybersecurity barriers requires timely and structured use of external threat intelligence to anticipate, detect, and respond to evolving threats. External sources, including CTI vendors, CERTs, ICS suppliers, and national security authorities, offer crucial insights into current threats, emerging vulnerabilities, and mitigation strategies. These inputs are particularly valuable when they provide contextualized intelligence on tactics, techniques, and procedures (TTPs) used by threat actors targeting industrial control systems.

To maintain cybersecurity barriers, this information must be continuously collected, assessed, and integrated into operational decision-making processes. Weekly threat landscape reports, for example, help organizations assess their overall exposure and determine a suitable risk level. This in turn guides predefined actions such as reinforcing barriers, increased monitoring, or applying relevant patches. In critical situations, external intelligence can trigger immediate response measures, including isolation of systems or activation of compensating controls.

However, the value of external intelligence depends on its relevance, timeliness, and ability to be acted upon. Organizations can use multiple complementary sources to ensure coverage and early warning, for example leveraging CERTs in other time zones. At the same time, mechanisms (and personnel) must be in place to filter, prioritize, and inform appropriate roles, avoiding information overload. OT cybersecurity teams play a central role in contextualizing external alerts, mapping them to asset inventories, and assessing their implications for barrier performance.

Ultimately, external threat intelligence should not only inform tactical or operational responses but also guide strategic updates to the cybersecurity barrier strategy. This includes reviewing barrier design, refining detection capabilities, and planning for new defences aligned with the evolving threat landscape.

3. How to handle threats, vulnerabilities and cybersecurity barrier impairments?

Handling threats, vulnerabilities, and impairments to cybersecurity barriers requires a structured, risk-informed approach that balances operational continuity with timely mitigation. While these elements differ in origin, threats often come from external intelligence, vulnerabilities from identified weaknesses in systems, and impairments from degraded or non-functioning barriers, they converge in requiring coordinated assessment and treatment.

The first step is identification and relevance assessment. For vulnerabilities, this involves checking if affected assets are actually present in the facility and evaluating the potential impact based on, for example, asset location, network exposure, and function. Barrier impairments, in contrast, are directly linked to known assets and often have pre-established criticality ratings. Threats may trigger broader assessments of the facility's exposure, particularly if they align with known system configurations or vulnerabilities.

Once identified, risks are categorized and tracked through ticketing systems, risk registers, and barrier panels. Actions are typically classified as immediate (NOW), deferred (NEXT), or not required (NEVER), depending on severity, asset criticality, and feasibility of mitigation. Mitigation may include patching, maintenance, compensating controls, or (in critical scenarios) facility isolation through island mode. A management of change process ensures that all actions are documented, reviewed, and approved before implementation.

Integration of fragmented data is a challenge. Vulnerability tracking, patch scheduling, and barrier status monitoring often reside in separate systems, requiring coordination across multiple roles, disciplines, and organizational levels. OT cybersecurity teams play a central role in bridging potential silos, supported by control system engineers, offshore installation managers, and external vendors.

Ultimately, effective handling demands not only reactive capabilities but also forward-looking actions, such as asset inventories (automated if possible), pre-configured response plans, and performance monitoring, to support rapid, safe, and consistent decision-making across the cybersecurity barrier lifecycle.

References

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

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

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

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

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

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

[8] O. Alexander, 'MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy', MITRE, MP01055863, 2020.

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

[10] A. Eltervåg *et al.*, 'Principles for barrier management in the petroleum industry', Mar. 2017. Accessed: Dec. 01, 2022. [Online]. Available: https://www.ptil.no/en/technical-competence/explore-technical-subjects/news/2017/barrier-memorandum/

[11] ISA/IEC, 'ISA/IEC 62443 Ontologies'. ISA, Aug. 30, 2022.

[12] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)*, vol. 333. 2022. Accessed: Feb. 02, 2023. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj/eng

[13] IEC, 'IEC 62443-1-1-ED1:2025 Security for automation and control systems - Part 1-1: Overview and guidance for the IEC 62443 series', IEC, IEC Technical Specification, 2025.

[14] ISA, 'ISA-TR84.00.09-2017, Cybersecurity Related to the Functional Safety Lifecycle'. Apr. 2017. [Online]. Available: https://www.isa.org/products/isa-tr84-00-09-2017-cybersecurity-related-to-the-f

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

Appendix A Abbreviations and definitions

Abbreviations

Abbreviation	Description
CBM	Cybersecurity Barrier Management
CDS	Cybersecurity of Industrial Automation and Control Systems (Industry Forum)
CERT	Cybersecurity Emergency Response Team
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMDB	Configuration Management DataBase
CMMS	Computerized Maintenance Management System
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
DMZ	Demilitarized Zone
EWS	Engineering workstation
Havtil	Norwegian Ocean Industry Authority
HR	Human Resource
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IRT	Incident Response Team
ISA	International Society of Automation
IT	Information Technology
MTO	Man-Technology-Organization
NCSC	National Cyber Security Centre
NIS2	Network and Information Security 2
NSM	Norwegian National Security Authority (Nasjonal Sikkerhetsmyndighet)
NVD	National Vulnerability Database
OIM	Offshore Installation Manager
OT	Operational Technology
PC	Personal Computer
PDS	Reliability of Safety Instrumented Systems (Industry Forum)
PLC	Programmable Logic Controller
PIF	Performance Influencing Factor
PLC	Programmable Logic Controller
PSA/PTIL	Petroleum Safety Authority (now Havtil)
SAS	Safety and Automation System
SIEM	Security Information and Event Management
SIS	Safety Instrumented Systems
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
TTP	Tactics, Techniques and Procedures
URL	Uniform Resource Locator
VPN	Virtual Private Network
WP	Work package

Definitions

Term [reference]	Description/definition
Automation and control solution [13]	Collection of people, processes, and automation and control systems with the purpose of monitoring, controlling, and managing the operation of the equipment under control. Note 1 to entry: An automation and control solution includes the instantiation of one or more automation and control systems.
Automation and control system (ACS) [13]	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 [13]	Property of ensuring timely and reliable access to and use of control system information and functionality.
Barrier [10]	A measure intended to identify conditions that may lead to failure, hazard and accident situations, prevent an actual sequence of events occurring or developing, influence a sequence of events in a deliberate way, or limit damage and/or loss.
Barrier function [10]	The task or role of a barrier.
Barrier element [10]	Technical, operational and organizational measures or solutions involved in the realization of a barrier function.
Barrier management [10]	Coordinated activities for establishing and maintaining barriers so that they fulfil their functions at all times.
Barrier strategy [10]	Plan for how barrier functions, on the basis of the risk picture, are implemented in order to reduce risk.
Capability security level (SL-C) [13]	Security level inherent in a product or technology. Note 1 to entry: Capability security level is determined during the product development phase of the security lifecycle.
Compensating security measure [13]	Security measure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements.
Confidentiality [13]	Assurance that information is not disclosed to unauthorized individuals, processes, or devices.
Control system [13]	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.
Cyber incident [14]	Communication with an E/E/PE device within a control system that negatively impacts process safety, the environment, operations, confidentiality, SCAI integrity, or IACS availability.
Cybersecurity [13]	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 [15]	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 [13]	Provision of multiple security measures, especially in layers, with the intent to prevent or delay an attack.
Equipment under control (EuC) [13]	Equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other activities. [SOURCE: IEC 61508-4:2010]
Failure [7]	Loss of ability to perform as required. Note 1 to entry: A failure of a device is an event that results in a fault state of that device. Note 2 to entry: When the loss of ability is caused by a latent fault, the failure occurs when a particular set of circumstances is encountered. Note 3 to entry: Performance of required functions necessarily excludes certain behavior, and some functions may be specified in terms of behavior to be avoided. The occurrence of such behavior is a failure.

Term [reference]	Description/definition
	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]
Fault [7]	Inability to perform as required, due to an internal state. Note 1 to entry: A fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the life-cycle, such as specification, design, manufacture or maintenance. Note 2 to entry: A fault of a device results in a failure when a particular set of circumstances is encountered. [SOURCE: IEC 60050-192:2015, 192-04-01, modified – Some notes to entry have been changed, others have been deleted]
Functional safety [7]	Part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers.
Hazard [7]	Potential source of harm. Note 1 to entry: The term includes danger to persons arising within a short time scale (e.g., fire and explosion) and also those that have a long-term effect on a person's health (e.g., release of a toxic substance or radioactivity). [SOURCE: ISO/IEC Guide 51:2014, 3.2, modified – Note 1 to entry has been added]
Integrity [13]	State that connectivity, control, or safety have not been changed, destroyed or lost in an unauthorized or accidental manner.
Intrusion [13]	Unauthorized act of compromising a system. Note 1 to entry: See “attack.”
Intrusion detection [13]	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
Monitoring system [13]	Type of automation and control system that consolidates sensor measurements and displays them to an operator of the equipment under control.
Patch [13]	Update that corrects a specific defect. Note 1 to entry: A defect can cause a security vulnerability, reliability issue or operability issue. Note 2 to entry: An adjective may be used to describe the type of patch (e.g., security patch, reliability patch, operability patch).
Performance-influencing factors [10]	Factors identified as having significance for barrier functions and the ability of barrier elements to function as intended.
Performance requirement [10]	Verifiable requirement for the properties of the barrier elements in order to ensure that the barrier is effective.
Protection layer [7]	Any independent mechanism that reduces risk by control, prevention or mitigation. Note 1 to entry: It can be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical mechanism such as a relief valve, a SIS or an administrative procedure such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions (see Figure 9). [Not included]
Redundancy [7]	The existence of more than one means for performing a required function or for representing information. Note 1 to entry: Examples are the use of duplicate devices and the addition of parity bits. Note 2 to entry: Redundancy is used primarily to improve reliability or availability. [SOURCE: IEC 61508-4:2010, 3.4.6]
Reliability [13]	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 [13]	Expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence.
Safety [13]	Freedom from unacceptable risk.
Safety function [13]	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.

Term [reference]	Description/definition
Safety functions [10] FR § 3	Technical barrier elements that are intended to reduce the possibility of a concrete fault, hazard and accident situation occurring, or that limit or prevent damage or inconveniences.
Safety functions [10] 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.
Security [13]	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 event [13]	Occurrence in a system that is relevant to the security of the system.
Security incident [13]	Violation or imminent threat of violation of ACS security policies, acceptable use policies, or standard security practices.
Security measure [13]	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 zone [13]	Set of systems or components that share common security requirements. Note 1 to entry: Security zones can be physical or logical.
Technical barrier element [10]	Equipment and systems involved in the realization of a barrier function.
Threat [13]	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 [13]	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 [13]	See security zone.