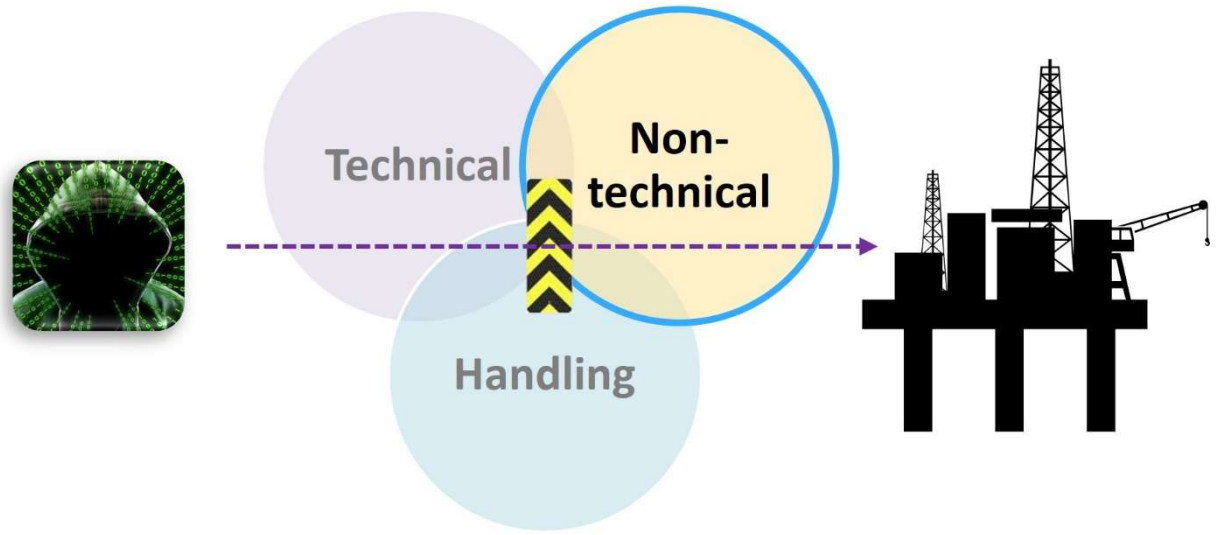

Report

Non-technical cybersecurity barrier management

Authors:
Christoph Thieme, Vahiny Gnanasekaran, Tor Olav Grøtan

Report No:
2025:00701 - 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

Non-technical cybersecurity barrier management

KEYWORDS
Barriers
Barrier management
Cybersecurity barriers
Human barriers
Operational barriers
Oil and gas industry

VERSION
1.1

DATE
2025-10-29

AUTHORS
Christoph Thieme, Vahiny Gnanasekaran, Tor Olav Grøtan

CLIENT
The Research Council of Norway

CLIENT'S REFERENCE
326717

PROJECT NO.
102020847

NO. OF PAGES
36

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

i) Integration of non-technical and technical cybersecurity barrier elements
ii) Interaction between IT and OT domains

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

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

PREPARED BY
Christoph Thieme
SIGNATURE

CHECKED BY
Martin Gilje Jaatun, Acting Research Manager
SIGNATURE

APPROVED BY
Geir K. Hanssen, Acting Research Director
SIGNATURE

REPORT NO. 2025:00701
ISBN 978-82-14-07268-6
CLASSIFICATION Unrestricted
CLASSIFICATION THIS PAGE Unrestricted

Document history

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

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

Table of contents

1 Introduction

1.1 Background

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

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

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

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

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

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

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

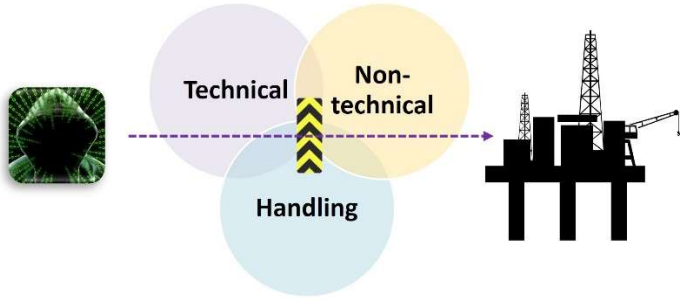

Figure 1.1 The three main parts of the CBM project

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

1.2 Purpose and scope

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

i) Integration of non-technical and technical cybersecurity barrier elements
ii) Interaction between Information Technology (IT) and Operational Technology (OT) domains

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

1. How to establish and integrate non-technical barrier elements in cybersecurity barrier management?
2. How can interaction between IT and OT domains be improved through new innovative work processes?
3. How to align practice, culture and language between users of office IT systems and ICS?

The first challenge is related to the first activity, and the two last are related to the second activity.

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 non-technical barrier management part, and continuing through iterative work on the two 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 on 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, topology diagrams, and asset inventories. Thus, the guidance provided is high-level and generic. Some examples are given, but without covering all topics in detail.

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

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

Some of the findings and recommendations presented in this report are based on empirical studies, including observational studies and interviews with industry actors. Only a few industry actors participated in these studies; as such, the findings and recommendations may not fully represent the industry as a whole. Nevertheless, key aspects have been carefully included in the descriptions to ensure that critical roles and perspectives are appropriately covered.

1.5 Structure

Chapter 1 introduces the document, followed by Chapter 2 describing the integration of technical and non-technical cybersecurity barrier elements. Chapter 3 addresses interaction between IT and OT domains, whereas Chapter 4 provides discussion and conclusions. Abbreviations and definitions are found in Appendix A.

2 Integration of technical and non-technical cybersecurity barrier elements

The methodologies for identifying barrier functions and elements, establishing performance requirements for these elements, and conducting short-, medium-, and long-term follow-up—as outlined in the technical barrier report [1]—apply to both technical and non-technical cybersecurity barrier elements. This report takes a closer look at these aspects specifically for non-technical cybersecurity barrier elements, including: The identification of non-technical barrier elements (Section 2.1), the definition of performance requirements (Section 2.2), and the approaches for follow-up (Section 2.3). The chapter concludes with examples of non-technical cybersecurity barrier elements (Section 2.4).

2.1 Identification of non-technical barrier elements

The identification of both technical and non-technical barrier elements typically begins with a top-down approach, in which barrier functions are first identified. Alternatively, a bottom-up approach may be used, wherein barrier elements are identified directly. These methodologies are described in detail in the technical barrier report [1].

A top-down breakdown from barrier functions to barrier elements—traversing multiple levels of sub-functions—is illustrated in Figure 2.1. On the left, the breakdown and general barrier terminology used in the Norwegian Petroleum Safety Authority (PSA)'s guidance on barrier management [8] is presented; note that the PSA is now known as the Norwegian Ocean Industry Authority (Havtil). On the right, the cybersecurity-specific barrier elements used in the CBM project are shown.

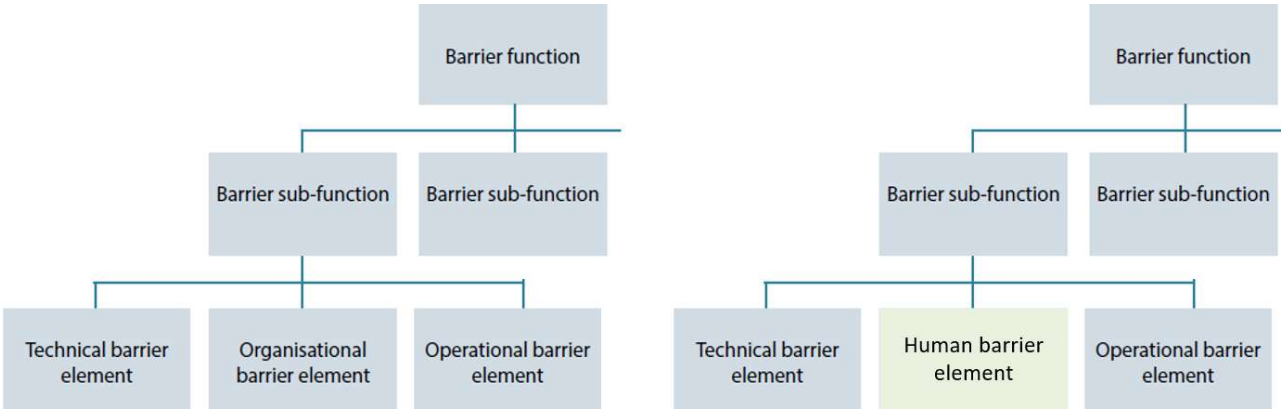

Figure 2.1 Barrier hierarchy with barrier elements according to PSA (left) and CBM (right)

Following the notation used in the CBM project, barrier elements (BE) that execute a barrier function can be classified as technical (BE-T), human (BE-H), or operational (BE-O). The latter two categories—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 to sharp-end personnel who activate and operate a technical BE. Operational BEs, on the other hand, are the actions or activities that personnel must carry out in order to realize a barrier function. The use of the term *organizational BE* can create confusion, as it may be interpreted more broadly in the context of organizational aspects within the MTO (Man-Technology-Organization) framework. In that context,

organization typically includes blunt-end management personnel who are not directly involved in the activation of barriers.

A second reason for changing the notation from *organizational barrier element* to *human barrier element* is alignment with the cybersecurity "triangle," which consists of technology, people, and process. In this context, the term *people* corresponds more directly to *human*. Additionally, the term *operational* is widely used in safety barrier management within the petroleum industry, making it preferable to *process* in this domain. These considerations are further elaborated in the technical barrier report [1].

Examples of non-technical barrier elements identified in the technical barrier report [1] include those related to intrusion detection and control system backups. The associated human barrier elements are the individuals responsible for the intrusion detection system (IDS) and for performing system backups, respectively. Corresponding operational barrier elements involve actions such as detecting, characterizing, and reporting security breaches, as well as conducting regular backups. Additional non-technical barrier elements can be identified using the methodologies outlined in the technical barrier report. The intrusion detection and control system backup examples are further detailed in Section 2.4.

As stated in the technical barrier report, a cybersecurity barrier is defined as a measure intended to a) detect abnormal conditions, b) prevent abnormal conditions from developing, and c) limit the damage caused by cyber incidents. Intrusion detection corresponds to the first function—detecting abnormal conditions—while backup contributes to limiting the damage by enabling restoration of the system to normal operation.

The complementary bottom-up approach for identifying technical barrier elements—described in the technical barrier report—begins with asset inventories. A corresponding bottom-up approach for identifying non-technical barrier elements is presented in the following two subsections. This approach examines the roles and actions involved in handling cybersecurity incidents, starting from the detection of abnormal conditions, in line with the previously stated definition.

The broader picture—including all relevant roles related to incident and accident handling —is presented first, followed by the specific roles used in the Norwegian petroleum industry. The second subsection focuses on specific roles used in the Norwegian petroleum industry and their interactions. 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 perform support functions that influence the effectiveness of barrier elements without being barrier elements themselves. These roles are referred to as *Performance Influencing Factors* (PIFs). Generally, many of the roles described in the first subsection serve support functions and are therefore classified as PIFs, whereas most roles in the second subsection are directly involved as human barrier elements.

2.1.1 Roles and actions involved in the handling of cybersecurity incidents

Incident response roles, responsibilities, and decision authority have been examined from both safety and cybersecurity perspectives in Gnanasekaran et al. [9]. The proposed role taxonomy consists of two layers: the upper *ecosystem* layer and the lower *joint incident response team* layer, as illustrated in Figure 2.2. The described roles can serve as a foundation for identifying the human BE and human Performance Influencing Factors (PIFs) relevant to incident handling.

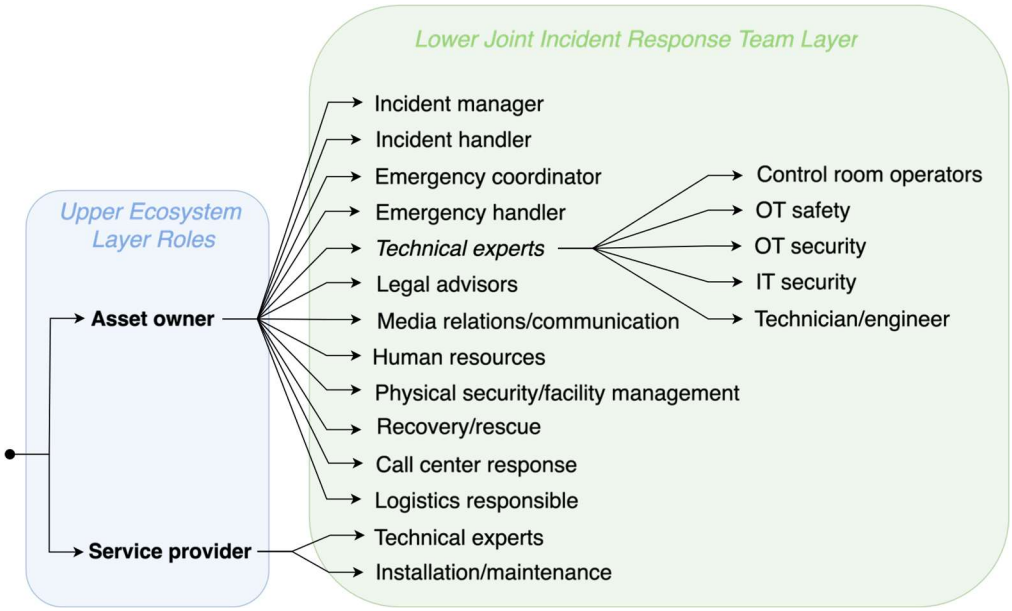

Figure 2.2 Overview of the role taxonomy in joint incident response

The **Upper Ecosystem Layer roles** encompass broader aspects of joint incident response, including the involvement of actors across the supply chain [10], as primarily outlined in the IEC 62443 standard. They comprise the following roles:

Asset Owner: This role encompasses the responsibilities of the *Incident Handler* and most of its associated or inheriting roles, as the Asset Owner represents the organization that hosts and operates the incident response team. In this capacity, the Asset Owner holds overarching authority over incident management within their organizational domain and is ultimately accountable for the systems, data, and infrastructure affected by the incident.

Service Provider: This role represents external companies or entities that deliver services to the *Asset Owner*. In this context, *services* may include physical components, subsystems, stand-alone systems, or specialized support in responding to faults, failures, or cyberattacks. Service Providers typically have less access to the facility, such as read-only access to log files from on-site instances of security products and permission to communicate with the incident response team through designated channels. Their involvement is essential for diagnosing system interactions and facilitating coordinated response efforts.

The **Lower Joint Incident Response Team Layer** describes roles that are confined to a single organization, typically involving small groups or individual members, and focuses on tasks that require immediate attention.

External actors—such as those not directly involved in the affected systems or those performing tasks that are not directly related to the system operation, e.g., regulators, first responders, governmental agencies are not included in the role taxonomy. The number of personnel assigned to each role varies depending on the size of the response team and the organizational priorities in the given context.

Incident Manager: The primary responsibility of the Incident Manager is to oversee the incident response process and the handling of the incident, which primarily involves high-level decision-making. Depending on the size and composition of the incident response team, some critical decision may be partially or fully

delegated to the *Technical Experts* role. Functionally, the role often serves as a coordinator or "second pair of eyes," rather than a direct, hands-on decision-maker.

Two role variations are outlined in the ENISA guide [11]:

1. **Triage Officer**: This role may be appointed to evaluate and prioritize response actions, particularly in situations involving limited resources or high operational workload.
2. **Team Manager**: This role may be introduced to assume responsibility for team coordination and management, thereby allowing the Incident Manager to focus exclusively on high-criticality decision-making.

Incident Handler: Serving as the foundation for all other roles within the team, the Incident Handler is performing the incident handling. Typical responsibilities include incident detection, initial analysis, containment, eradication, and communication with other team members. Although other roles—such as *Technical Experts*—may play a greater part in resolving complex aspects of an incident, the Incident Handler is often the first point of contact and initiates the response process.

Emergency Coordinator: This role is functionally analogous to the *Incident Manager* in the context of safety-related emergencies. The primary responsibility of the Emergency Coordinator is to supervise and coordinate the overall emergency response, ensuring effective collaboration among all involved roles and entities. As the individual with the highest level of responsibility during an emergency, the Emergency Coordinator can take time-sensitive and potentially far-reaching decisions.

Emergency Handler: This role holds a distinct function within the context of safety regulations, primarily focused on administering immediate aid and responding to physical injuries during an incident. The Emergency Handler's objective is to ensure that emergency actions are carried out in accordance with the tactics and priorities established by the designated emergency coordinator.

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 operator). The role serves two primary objectives. 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.

Legal Advisors: This role supports the incident response team by providing legal guidance and ensuring regulatory compliance throughout the incident lifecycle. Depending on the nature of the incident, the Legal Advisor may assist in matters related to data privacy, breach notifications, evidence handling, or formal communication with external authorities.

The most recognized variation of this role is the *Data Protection Officer*, particularly in cases involving personal or sensitive data. In safety-related contexts, some regulatory frameworks recommend engaging legal advisors after the emergency response phase is complete, to ensure that all legal obligations are properly addressed [12].

Media Relations / Communication: Security or safety incidents can significantly impact an organization's reputation. Accordingly, the way the incident is communicated to authorities, business partners, and the public plays a critical role in maintaining stakeholder trust and ensuring business continuity. Due to its

relatively limited scope within the incident response team, this role is often delegated to the *Incident Manager* or top-level management, particularly in smaller organizations or teams without dedicated communication personnel.

Human Resources: This role supports the incident response process by addressing internal threats and managing human-related security or safety vulnerabilities. In larger or distributed incident response teams, the Human Resources role may be responsible for monitoring internal threats—such as potentially malicious behaviour by employees—and may also take on additional responsibilities delegated by the *Emergency Coordinator* or *Incident Manager*. These may include recruiting external consultants, manage administrative tasks, and organize personnel training related to incident preparedness and response.

Physical Security / Facility Management: Physical access to compromised endpoints can be as critical as digital access in incident response scenarios. This role is responsible for tasks that require direct physical interaction with devices or infrastructure that are otherwise inaccessible to regular personnel. Additionally, this role plays a preventative function by securing facilities and restricting unauthorized physical access, thereby reducing the risk of both intentional and accidental security or safety incidents.

Recovery / Rescue: This is a secondary role within the incident response team, focused on enabling the rapid recovery of digital systems once the incident has been resolved and no active threats remain. While the role remains inactive during the initial response phase, it becomes essential in the aftermath—ensuring that recovery efforts are coordinated with digital forensics and evidence collection.

Typical responsibilities include preparing for system restoration, supporting the switch to backup systems, and facilitating a smooth transition to normal operations. From a safety perspective, the *Emergency Coordinator* holds overall responsibility for physical rescue operations and facility re-entry. They may delegate related tasks to this role. In such contexts, priorities shift toward saving lives, protecting critical equipment, and preventing environmental or hazardous material leakage.

Call Center Response: Based on the ENISA guide [11], this role serves as an extension of the Incident Handler role. It functions primarily as a standby operator, responsible for receiving incoming incident reports and delegating them to the appropriate available handlers. It is considered optional and typically does not need to be explicitly represented within the access control system.

Logistics Responsible: In the context of a safety incident, this role ensures the timely procurement and coordination of necessary physical resources, transportation, or supplies. Depending on the severity and nature of the incident, the Logistics Responsible is tasked with contacting relevant internal stakeholders to fulfil logistical needs.

While not always activated during minor incidents, this role becomes crucial when operational continuity depends on the availability of equipment, personnel movement, or material support.

Installation / Maintenance (service provider): This role applies to third-party personnel commissioned to install or maintain security products within the asset owner's infrastructure. Members assigned to this role function similarly to those in the *Service Provider* role on the upper ecosystem level (described above). Depending on the scope of involvement, this role may be responsible for multiple products across different systems, thereby requiring broader technical coordination and a more diverse access profile.

2.1.2 Specific roles handling cybersecurity incidents in the Norwegian petroleum industry

The CBM project, published in Gnanasekaran et al. [13], identified and analysed specific roles for incident response in the petroleum industry. These specific roles described are largely based on one organization. Thus, the naming of roles may vary across other organizations; some roles may be combined, while others may not exist or may be supplemented by additional roles. Differences across organizations stem primarily from variations in size and structural complexity. In smaller organizations, individuals often assume multiple roles due to limited personnel and resources, leading to significant role overlap. In contrast, larger companies typically have dedicated personnel across specialized departments or divisions, allowing for a clearer separation of responsibilities. Nonetheless, the roles presented should offer valuable insights for cross-organizational comparison.

Figure 2.3 summarizes the central actors, their roles and the relationships between the roles in form of a UML (Unified Modelling Language) class diagram. Aggregation in the diagram (bottom-up relations with assigned numbers of relations) means that the role is a part of the originating role, either as a subordinate or as the role itself. The arrows indicate direct interaction associations, in this case the notification of an incident. Green refers to roles normally located onshore and blue to roles normally located offshore. Specific tasks related to incident response are indicated for some of the roles and actors, these are described in more detail in Section 3.1.

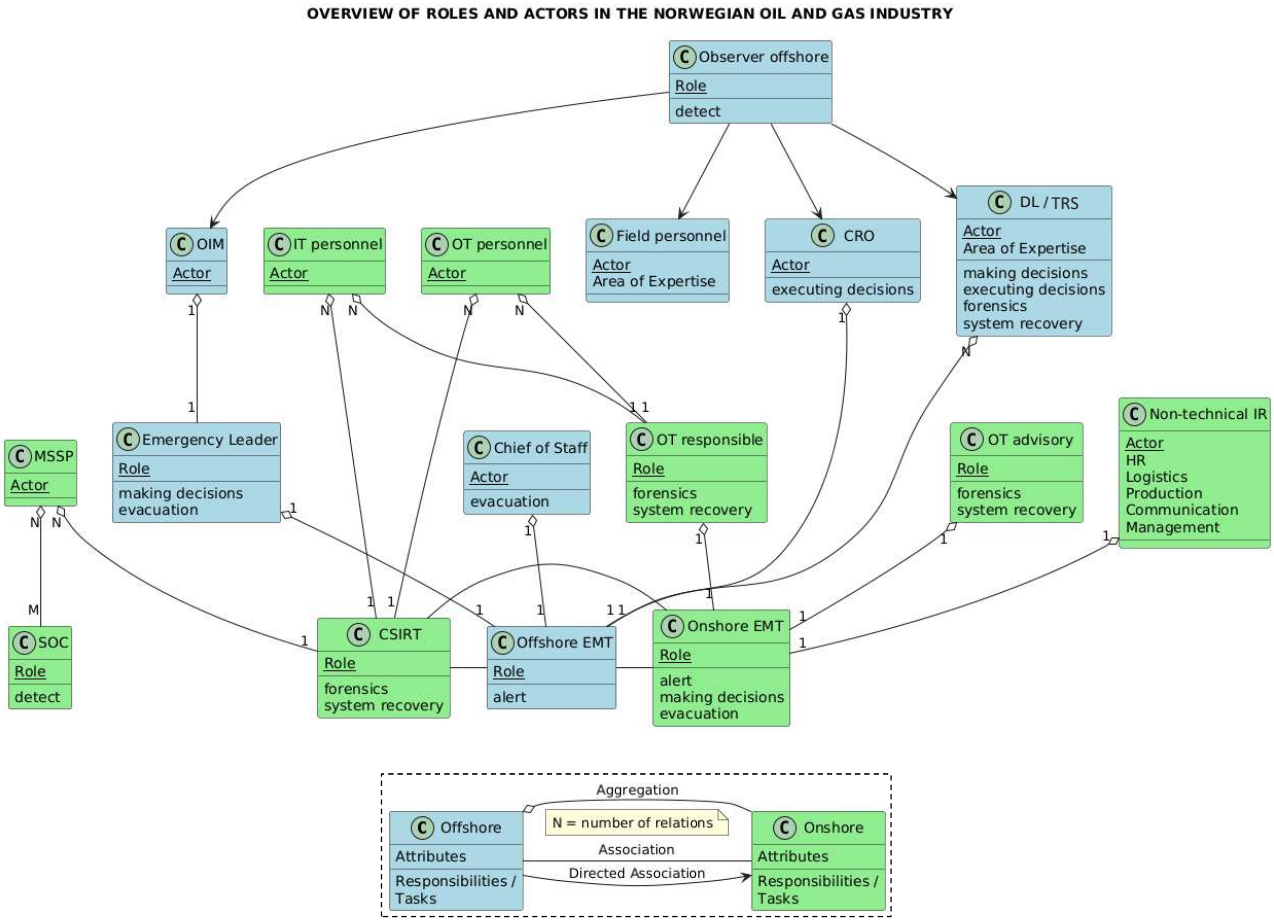

Figure 2.3 The UML class diagram depicts the most central actors, their roles and their relationships during the incident response in OT (in this case starting from an incident observed offshore). The numbers attached to the roles relate to the number of people that have this role, where N and M indicate multiple not defined people.

The following roles were identified:

Offshore Installation Manager (OIM) / Emergency Leader Offshore (EL): The OIM serves as the highest-ranking authority on an offshore oil installation and is responsible for leading incident response efforts. During emergencies, the OIM is the central decision-maker and receives all critical information, including reports related to cybersecurity attacks and operational disruptions.

Given that the OIM often lacks specialized cybersecurity expertise, support is provided by the *OT Responsible* and *OT Technical Support* personnel. These include *Discipline Leads (DL),* in Norwegian: Fagansvarlig (FA)*,* e.g., FA Electro and FA Instrument, who act as intermediaries—translating technical and cybersecurity-related information into actionable insights for the OIM. This enables informed decision-making while maintaining safety and operational integrity on the platform. The role of EL relates to the role of *Emergency coordinator* and *Incident manager* mentioned in the previous section.

Second Line of the Emergency Response Group, Onshore (Onshore EMT): This group forms the onshore support structure for managing emergencies and consists of a designated leader and personnel responsible for engaging with relevant third-party actors. These may include national and sectoral entities such as InfraCERT, the Norwegian National Security Authority (NSM), Havtil, the police (in case of sabotage), emergency services, and the media or press contacts.

The group typically includes representatives from *OT Responsible*, *Production Watch*, and other relevant emergency response functions. During a cyber incident, both OT Responsible and Production Watch assume critical roles in situational awareness and system continuity. However, due to the particularly central and specialized nature of OT Responsible in cyber incident handling, this role is often considered independently from the broader Onshore EMT structure.

The onshore EMT includes roles described in the previous section, such as, *Technical Experts*, *Legal advisors, Media relations/communication, Human Resources, Recovery/Rescue, Call Center Response, Logistics Responsible.*

OT responsible: The *OT responsible role*, also referred to as the OT Responsible, is fulfilled by personnel from IT or OT operations teams, often rotating between personnel. These individuals are stationed onshore as part of the *Second Line of the Emergency Response Group* and are available 24/7 during their assigned shifts. They serve as a critical communication bridge between the onshore and offshore teams—maintaining direct contact with the *OIM* and consulting closely with the *DL for Instrumentation (FA Instrument)*.

The OT Responsible is immediately alerted by the *Security Operations Center (SOC)* when a high- or critical-severity cyber incident is detected. As the personnel most familiar with ongoing cyber threats, they provide vital situational awareness and technical insight to other response roles—both offshore and onshore. Following a cyberattack, the OT Responsible can also coordinate the verification of the integrity of backup systems to ensure that no data has been infected or tampered with prior to system restoration.

Discipline Lead (DL) / Technical System Responsible (TRS) for electrical, instrumentation, or tele-communication: These *OT technical support* personnel hold the most in-depth knowledge of their respective systems—electrical, instrumentation, or tele-communication—and work in close collaboration with the *Chief Control Room Operator*. While the operator manages real-time system operations, the DL/TRS oversee

all additional technical operations not covered by the control room. DL and TRS are *technical experts* as descried in the previous section.

Located offshore as part of the *first-line response team* (**Offshore EMT**), these individuals are also responsible for revoking work permits that have been issued for the day, since such permits are only verified offshore. Their role is critical during incident detection and diagnosis, especially in coordination with the *OT Responsible*. For example, during the early stages of an incident, the OT Responsible may consult the *Discipline Lead for Instrumentation (FA Instrument)* to determine whether system anomalies are due to planned maintenance or other authorized activities that could affect instrumentation integrity.

Control Room Operator (CRO): During an offshore incident, *Control Room Operators* are responsible for monitoring the *Safety and Automation Systems (SAS)* to verify that they are functioning as expected. One of the earliest physical indicators of a potential cyberattack offshore may include the loss of control over safety or automation systems, or unexpected deviations in system behaviour. However, such anomalies can also arise from non-cyber causes, requiring further investigation. CRO are *technical experts* as descried in the previous section.

The CRO also conducts systematic reviews of *Human-Machine Interfaces (HMI)* and *Engineering Workstations (EWS)* to ensure uninterrupted operation. In collaboration with other technical personnel, the CRO assists in diagnosing and debugging system anomalies, contributing to the identification of root causes and the preservation of safe operational conditions.

Security Operations Centre (SOC): The SOC is a key cybersecurity actor whose primary objective is to detect *Indicators of Compromise (IoCs)* and abnormal system behaviour within the customer's network environment. It continuously monitors network traffic, system logs, and security alerts to identify potential threats. The SOC consists of *technical experts* by a *Service Provider* as descried in the previous section.

SOC interactions are typically governed by a *Service Level Agreement (SLA)* and involve close communication with the customer's designated *Point of Contact (PoC)* to validate suspected incidents. If necessary, the SOC also provides advisory or hands-on support during incident handling. In many cases, the SOC is outsourced and operated as part of a *Managed Security Service Provider (MSSP)*, though internal SOCs may exist depending on the organization's size and capability.

Communication is bidirectional—SOC analysts may initiate alerts based on threat detection, but customer personnel may also contact the SOC to investigate suspected anomalies or performing a detailed search of network and log data. The nature and scope of SOC involvement can vary based on whether the service is outsourced or in-house, and on the breadth of cybersecurity services available (e.g., digital forensics, threat intelligence, or incident response support).

The SOC's primary PoC within the organization is the *OT Responsible*, due to their operational expertise and contextual understanding of system alerts. This ensures that detected incidents are interpreted and addressed accurately within the industrial environment.

Computer Security Incident Response Team (CSIRT): The CSIRT serves as the dedicated *emergency task force* activated in response to cybersecurity incidents. Its primary responsibilities include performing digital forensics, identifying the root cause, mitigating the threat, and coordinating technical recovery efforts.

The team's composition varies depending on the nature of the incident and the organization's structure. In cases involving cyber incidents with potential or actual physical consequences, the CSIRT typically emphasizes *Operational Technology (OT)* advisory roles and cybersecurity personnel, while still including *Information Technology (IT)* staff. The team may also involve external consultants, such as representatives from *Managed Security Service Providers (MSSPs)*, *Security Operations Centres (SOCs)*, and *system vendors*.

Key operational tasks include malware removal, restoration using clean backups, and ensuring system integrity. The CSIRT also plays a central role in post-incident activities—such as compiling lessons learned, conducting incident debriefs, and recommending improvements to strengthen future cyber resilience.

The CSIRT has the role of *Incident handler* as described in the previous sections and consists of *technical experts*.

The **OT advisory** provides in-depth, installation-specific knowledge about the affected installation(s) systems, existing issues, and planned maintenance, among others. However, asking for their assistance is optional. It is comprised of OT personnel and other discipline experts as needed.

Non-technical Internal Resources (IR) are filled by different supporting functions, such as HR, Logistics, communications, and media relation. They support the non-technical aspects of incident resolution.

Notification of external actors

In addition to notifying system vendors and *Managed Security Service Providers (MSSPs)*, other external actors must be alerted due to regulatory obligations and the importance of preventing similar incidents across the industry. Timely notification enables broader situational awareness and supports sector-wide risk mitigation.

For example, any Norwegian organization is required to report potential data breaches to the *Norwegian Data Protection Authority* in accordance with privacy regulations. Furthermore, under the forthcoming *NIS2 Directive*[3], companies operating in critical sectors will be required to report significant cybersecurity incidents within 72 hours of discovery to the *Norwegian Ocean Industry Authority (Havtil)*. This expanded reporting framework underscores the importance of cross-organizational coordination and timely disclosure in strengthening national and sectoral cyber resilience.

2.2 Performance requirements

Requirements regarding barriers are stipulated in Section 5 of the Management Regulations (MR § 5), titled *Barriers*. Subsection 4 states:

> "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."

Furthermore, Subsection 5 states:

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

[3] https://eur-lex.europa.eu/eli/dir/2022/2555

Subsection 4 establishes that performance requirements must be defined for each barrier element — including non-technical elements — which typically necessitates follow-up over a medium- to long-term timeframe.

Subsection 5, on the other hand, introduces a requirement independent of performance criteria: the operational status of each barrier and its elements must be known at all times. This necessitates short-term monitoring — in other words, real-time or near-real-time tracking of barrier functionality.

Together, these subsections provide the foundation for the monitoring and follow-up of barriers, which is described in Section 2.3, and also further elaborated in the technical barrier report.

However, before proceeding further, it is necessary to clarify the concept of performance requirements. A performance requirement is defined as *"a verifiable requirement for the properties of the barrier elements in order to ensure the barrier is effective"* [14].

It is important to note that requirements found in cybersecurity standards and guidelines commonly applied in the petroleum industry — such as IEC 62443 — do not necessarily qualify as performance requirements under the Management Regulations § 5. These standards often stipulate the presence or implementation of cybersecurity measures, but not the expected performance level of the measures themselves.

In contrast, performance requirements as outlined in MR § 5 pertain to how well the barriers — typically the individual barrier elements — must perform with respect to specific properties such as functionality, integrity, and robustness (PSA, 2017) [14]. These attributes are essential to ensure that each barrier element contributes effectively to the overall function of the barrier.

If performance requirements are included in the selected standards and guidelines (i.e. IEC 62443, NOROG 104), they can be incorporated into the set of requirements compiled in the Safety Standards. However, these requirements must be clearly specified and made operational to enable verification of performance. In cases where the standards or guidelines do not explicitly state performance requirements, these must be derived from the characteristics of the barrier elements, ensuring coverage of relevant properties.

Examples of such properties and corresponding performance requirements for non-technical barrier elements within the safety domain are discussed by Hauge and Øien [5]. These examples — illustrated in Figure 2.4 — can also serve as a basis for defining performance requirements for non-technical cybersecurity barrier elements. At the very least, they provide a starting point for considering equivalent performance attributes in the cybersecurity domain. As with safety barriers, the performance requirements for cybersecurity barriers must also be clearly defined and operationalized to allow for performance verification, i.e., they must be *specific* and *operational*.

Specific means that the performance requirements should be tailored to the particular facility in question, and, where appropriate, further refined to address specific zones, systems, or equipment. This tailoring should be informed by the results of the risk assessment.

Operational means that the performance requirements must be defined in such a way that the method for verification is clearly described. This includes specifying how performance will be measured and what criteria determine whether the outcome is acceptable.

Regarding Figure 2.4, it should be noted that the *human* barrier element within the cybersecurity context is categorized as *organizational (Org.)*. In this context, the *operational (Op.)* barrier element refers specifically to procedures that describe how a task is to be performed. This interpretation deviates from the definition used by Havtil, which classifies procedures not as barrier elements but as performance-influencing factors (PIFs).

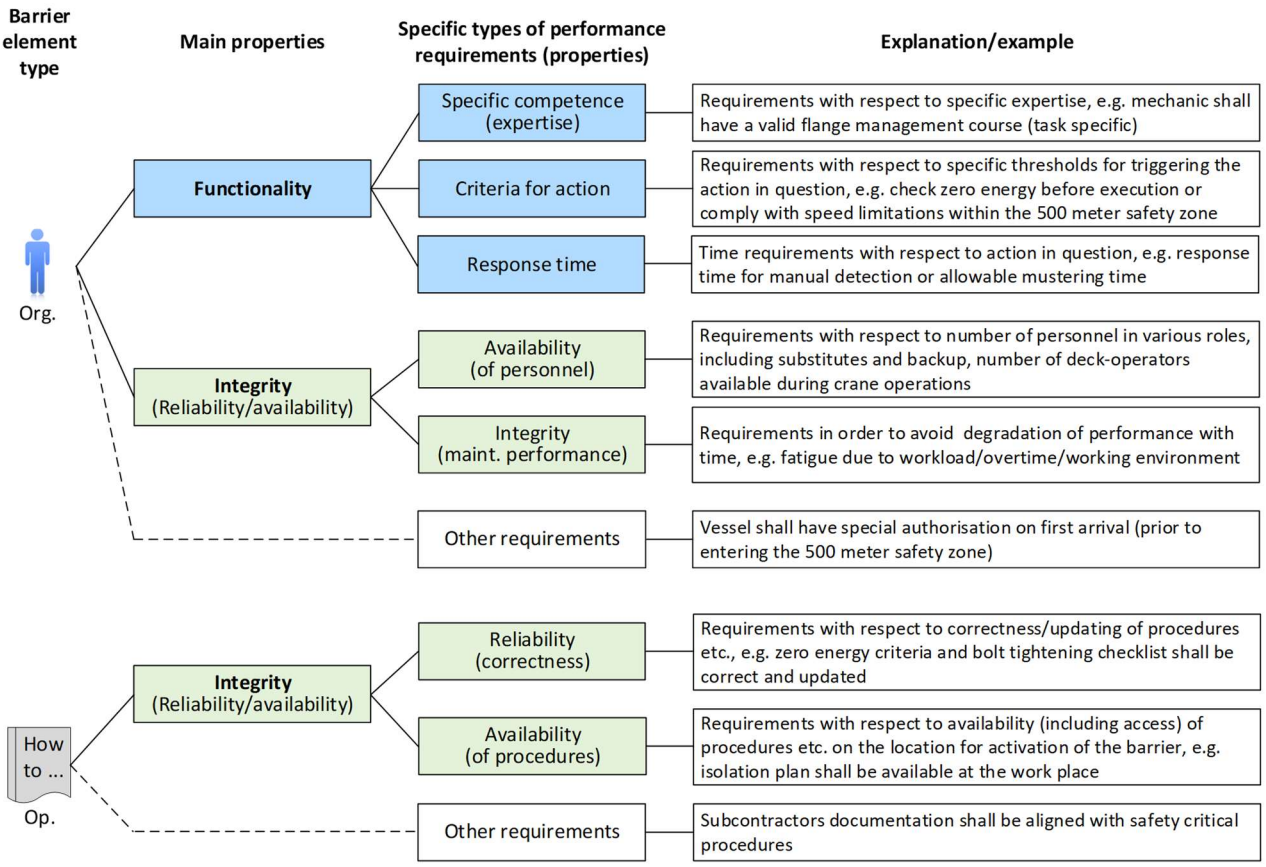

Figure 2.4 Types of performance requirements for non-technical barrier elements [5]

2.3 Follow-up of non-technical barrier elements

The barriers and barrier elements presented in the short-term status overview—typically provided by barrier status panels—are based on the *Barrier Strategy*. In contrast, the performance requirements subject to verification are documented in the *Performance Standard* (cf. Chapter 5, Fig. 5.1 in [1]).

Barrier status displays should reflect real-time conditions, indicating any non-functioning or impaired barriers—both at the functional and element level—in real time, reflecting the situation in the *short-term*. Conversely, verification of performance requirements is conducted periodically, using indicators, audits, or reviews. These activities are classified as *medium- to long-term* follow-ups, occurring over weeks to months or even years.

Each of these categories is described in the following subsections.

2.3.1 Barrier status overview – short-term follow-up

The day-to-day, or short-term, status of barrier functions and elements is based on information that verifies or indicates the current functioning of those functions and elements—that is, the degree to which the barriers are impaired. A common tool used for this purpose in safety barrier management is the *barrier panel,* as illustrated and discussed in the technical barrier report (Section 5.1.1 [1]).

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.

Rule sets define which status indicators correspond to red, yellow, and green signals. Examples of such rule sets for technical barrier tags are presented in the *Technical Barrier Report* [1]. However, as outlined in the *Barrier Handling Report* [3], the primary challenge lies in the short-term monitoring and visualization of non-technical barrier elements.

Tools such as the barrier panel are well-suited for displaying the real-time status of technical barriers but are less effective for representing non-technical elements. Relevant data—such as personnel competence, training status, and procedural readiness—is often distributed across separate source systems. Integrating this information into real-time visualization tools remains complex and constitutes a major obstacle to achieving full situational awareness regarding the health of non-technical barriers. This challenge is similar in the safety and cybersecurity domains.

Nevertheless, Table 2.1 provides examples of status indicators 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 non-technical barrier elements.

Table 2.1 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 elements show 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.

2.3.2 Barrier performance verification – medium- and long-term follow-up

The *Technical Barrier Report* references MR § 5, subsection 3, which states: *"The operator … shall stipulate the strategies … that form the basis for … maintenance of barriers …"* 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 to external systems, such as maintenance management systems or other relevant systems.

Alternatively—or in addition—these links to verification activities may be provided through the *performance standards*, ensuring traceability and integration across documentation.

For non-technical barrier elements, 'maintenance' typically consists of activities such as training, retraining, drills, and exercises. The verification of these activities is documented and monitored through systems such as the HRM-system.

Table 2.2 provides examples of verification activities applicable over medium- to long-term intervals for non-technical barrier elements. These are developed based on the classification of performance requirements shown in Figure 2.4 and have been adapted specifically to the cybersecurity context to ensure relevance and applicability within that domain.

Table 2.2 Examples of medium-term and long-term cybersecurity measure verification activities

Type of performance requirement	Verification mechanism	Follow-up period	Description
Specific competence (expertise)	Review of certifications	Medium-term Long term	Implement process and measures to regularly review if required personnel has valid certificate that are required for their role. Implement process to alert personnel before certificates become invalid. The follow up can be implemented through the HRM system.
	Review of completed trainings	Medium-term Long term	Implement process and measures to regularly review if required personnel has valid undergone required training for their role. Implement process to alert personnel before retraining is necessary. The follow up can be implemented through the HRM system.
Criteria for action	Review of decision-criteria	Long-term	Implement a process to review decision criteria, i.e., alarm triggers for their adequacy. New threats may challenge the adequacy of decision criteria (both in the technical system and for the personnel). The review should take into account incidents (CISA, internal, etc.) and technological trends being observed.
Response time	Review of decision process	Long-term	Have a process in place to assess the adequacy of the process related to the timing requirements. The timing requirements need to be assessed in the context of the whole operation, including the roles and tasks of critical personnel and available tools and information sources. Safety-critical task analysis and workload assessments can be tools in the evaluation process.
Availability (of personnel)	Verify presence/ availability of personnel	Medium-term	Ensure that staffing requirements can be met with personnel available, through the HRM system.
Integrity (maintenance of performance)	Review of workload	Long-term	Have a process in place to assess the adequacy of the process related to the workload of personnel. This needs to be assessed in the context of the whole operation, including the roles and tasks of critical personnel and available tools and information sources. Safety-critical task analysis and workload assessments can be tools in the evaluation process.
Reliability (correctness)	Review correctness and suitability of checklists and procedures	Long-term	Assess the applicability of procedures, checklists and processes with respect to their correctness. Work as done and work as imagined may differ and the procedures, processes and checklists need to be viewed in the total context to verify that the steps therein are correct and adequate to fulfil the required tasks. Findings of inadequate/ incorrect procedures should trigger a revision.
Availability (of procedures)	Verify availability of procedures and checklists at required locations	Medium-term Long-term	Check if required procedures and checklists have been defined and if they are available to the required personnel, through for example the inventory management system.

These verification activities are generic in nature and must be linked to specific cybersecurity barrier elements—or to broader cybersecurity measures, depending on the defined scope. Examples of specific cybersecurity barrier elements are provided in the following section.

2.4 Examples of non-technical cybersecurity barrier elements

The *Technical Barrier Report* [1] provides examples of barrier functions and elements, including non-technical barrier elements. These examples pertain to activities such as the detection of security breaches and the backup of control systems. Table 2.3 offers further elaboration on these non-technical barrier elements.

The table also includes, in its first three columns, the identification of relevant barrier requirements, which serve as the basis for deriving corresponding barrier functions. For example, the detection of security breaches through an Intrusion Detection System (IDS) is linked to System Requirement (SR) 6.2 from IEC 62443-3-3 [15]. Similarly, the requirement for control system backup corresponds to SR 7.3 from the same standard.

This section expands on the two mentioned examples related to non-technical BEs. Table 2.3 provides a broader overview of such elements, consolidating additional findings relevant to their identification and classification. In particular:

- The BE–Human column suggests specific roles associated with each barrier element, as outlined in Section 2.1.
- The BE–Operational column has been extended to include explicit tasks linked to each barrier sub-function, thereby clarifying their operational significance.

Table 2.3 Examples of human and operational BEs for "Continuous monitoring" and "Control system back-up" extended from the technical barrier report [1]

Req. ID	Req. title	Requirement	Barrier function	Barrier subfunction	BE-Technical	BE-Human	BE-Operational
SR6.2	Continuous monitoring	The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner. (NOTE Response time is a local matter outside the scope of this standard.)	Detect characterize and report security breaches in a timely manner	Intrusion detection	Intrusion detection system	IDS operator (i.e., IT/OT responsible, OT security technician, SOC)	Detect
				Characterize intrusion	Intrusion detection system	IDS operator (i.e., IT/OT responsible, OT security technician, SOC)	Analyse and characterize
				Report security breach	Reporting system, ticketing system	IDS operator (i.e., IT/OT responsible, OT security technician, SOC)	Report based on criticality
SR7.3	Control system backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.	Conducting backups (manual)	Backing up required files	Back-up mechanism (tools and servers)	Back-up responsible (i.e., OT technician, TRS instrumentation)	Taking back-up (manually)

Table 2.4 presents examples of generic performance requirements applicable to the cases of continuous monitoring and control system backup.

Table 2.4 Examples of generic performance requirements for "Continuous monitoring" and "Control system back-up" extended from the technical barrier report [1]

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 (i.e., 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 (i.e., IT/OT responsible, OT security technician, SOC)	Analyse and characterize	Availability of personnel	Response time
			Report security breach	IDS operator (i.e., 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 (i.e., OT technician, TRS 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 Technical Barrier Report [1] provides an example of a control system backup verification strategy, which consists of a set of verification activities. One of these activities, titled *Check Backup Logs*, is described as follows: *"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."*

The performance requirement defined for the technical barrier element 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 Table 2.4.

Verification that backups are performed as scheduled can be operationalized as shown in Table 2.5, where daily manual backups are assumed. The corresponding performance requirement specifies that 90% of the backups must occur on schedule. Verification methods may vary and can include traffic light systems—as in this example—character scales, pass/fail criteria, and other approaches.

Table 2.5 Example of operationalizing manual backup performance verification

Context – 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 Interaction between IT and OT domains

The following sections summarize the findings of the CBM project. Additional details can be found in references [16], [17], [18].

3.1 IT/OT interaction in a cybersecurity barrier context

A joint IT/OT cyber incident response playbook was developed in the project to address cyber incidents originating in IT systems that may have physical consequences in the production environment. The playbook is based on the incident management of one petroleum company and on studies conducted with two actors in the oil and gas industry. The playbook is described in more detail in [18]. The relevant roles and actors involved in incident response are described in Section 2.1.2. Figure 2.3 illustrates how these actors associate with their roles during the response to an OT-related cyber incident. Key actions are indicated for some key roles and actors in the diagram.

The incident response playbook addresses the following key questions, each corresponding to a specific actor's role in the process:

- Who is responsible for detecting the security incident and alerting the relevant roles?
- Who makes decisions based on the potential consequences of the incident for the offshore installation?
- Who executes the response actions based on those decisions?
- Who leads the evacuation efforts from the platform, if necessary?
- Who performs digital forensics and system recovery?

The incident response playbook emphasizes the interaction between two key roles: the Security Operations Center (SOC) and the customer's IT/OT security team. In this context, the "customer" refers to industrial companies that procure SOC services from a Managed Security Service Provider (MSSP). A central focus of this collaboration is addressing the unique challenges associated with monitoring operational technology (OT) environments. Effective detection, response, and coordination in these environments require close cooperation between the SOC and the customer's IT/OT security team. As part of the response workflow, the SOC is responsible for alerting offshore management and the first-line response team, including the Offshore Installation Manager (OIM).

Cyber incidents may be detected through two primary channels:

- Onshore: By a Security Operations Center (SOC)
- Offshore: By an observer located on the platform

For onshore detection, the SOC may be alerted through its monitoring tools and network sensors, which detect Indicators of Compromise (IOCs). Additionally, the SOC can receive threat information from external sources such as Computer Emergency Response Teams (CERTs) and Cyber Threat Intelligence (CTI) providers. The SOC is primarily staffed by IT personnel, who work in close collaboration with the customer's OT personnel to accurately interpret and respond to the collected information. This cooperation is essential to ensure that incident response efforts are context-aware and aligned with the operational environment.

For offshore detection, an observer—such as a process engineer or Control Room Operator (CRO)—may notice faulty or unresponsive signals. For instance, an operator might detect the smell of gas despite gas detectors showing no signs of leakage. If a suspicion is confirmed or an anomaly is identified, the observer is responsible for alerting offshore management and the first-line response team, including the OIM.

After assessing the physical impact and potential consequences of the incident, offshore management notifies the second-line emergency response team. Activation of the second-line team also triggers the involvement of the organization's cybersecurity resources, which may include both the in-house cybersecurity team and the SOC.

Although the incident response playbook accounts for two distinct detection origins—offshore and onshore—it follows a unified process after detection, progressing through a common sequence of actions. The primary objective of the joint incident response Playbook is to protect personnel and the physical environment while minimizing damage to operational systems. Consequently, digital forensics is addressed only briefly, as the focus remains on immediate safety and operational continuity. The main steps in the incident response playbook are as follows:

1. **Detection and alerting** include the observation of an ongoing security incident and alerting of all relevant internal roles.
2. **Hazard limitation** includes limiting physical damage by assessing the hazard potential of the incident and determining whether to bring the oil and gas platform to a fail-safe mode. If there is reason to suspect that the perpetrator is physically present—either offshore or onshore at the company's premises—a physical search is conducted. In such cases, other incident response playbooks may also be triggered.
3. **System saving** includes limiting actions towards system isolation and production shutdown are evaluated and executed, if necessary. These actions are carried out primarily by field personnel and OT personnel, with support from the Onshore EMT.
4. **Evacuation** depending on the severity of the incident, non-essential and, if required, essential offshore personnel are evacuated from the platform. Non-essential personnel refer to service employees (e.g., chefs, cleaning staff, etc.). In parallel, the physical impact of the security incident is further assessed—this includes identifying injuries, casualties, and equipment damage. The cybersecurity aspect of the incident is addressed by onshore personnel, including IT and OT staff, who assist essential offshore personnel in troubleshooting systems and identifying and removing malware.
5. **Recovery** includes identifying and restoring the latest clean backup to return systems to operational status. This phase also involves maintaining continuous communication between internal roles and external actors (e.g., CERTs, regulators, law enforcement). An independent team contributes to the recovery process by providing an audit report, delivering evidence to the forensics team, and compiling and sharing lessons learned from the response phase.
6. **Malware removal** includes security providers initiating digital forensics playbooks—such as log collection, analysis, and evaluation of malware spread to other installations—if sufficient information is available. This phase may run concurrently with other response and recovery activities, as security teams typically continue working from the point of incident detection onward.

Through systematic observational studies and interviews with key informants, the relationship between an industrial customer and an outsourced OT SOC was analysed, the results are also summarized in Gnanasekaran et al. [18]. The goal was to understand the onboarding processes required for this type of SOC and how these differ from those used in a traditional IT SOC. This highlights the importance of IT/OT interaction during the initial establishment of such an SOC. Similar challenges and interaction patterns may also be observed in the day-to-day collaboration between IT and OT personnel within one company.

Identifying Operational Issues

The emerging use of OT SOCs helps to uncover operational issues in OT systems, such as default vendor passwords, outdated software, and system misconfigurations. These issues are not directly related to

resolving cybersecurity incidents, but they are essential during the onboarding process to ensure proper system hardening. Onboarding refers to the initial phase when the OT-SOC is taken in operation and the OT-SOC is becoming familiar with the facilities to be monitored, by understanding and learning about the different information sources, flows and relationships, including system assets and configurations.

Each system is configured differently, and after the Site Acceptance Test (SAT), systems are typically not verified as thoroughly as during the SAT itself. Therefore, the onboarding process is vital to identify and correct any initial misconfigurations before the monitoring service is fully deployed. IT and OT personnel must collaborate closely during this phase to effectively identify and resolve these operational issues.

IT/OT Collaboration regarding Network Sensor Finetuning and Whitelisting

Understanding the criticality of generated alerts requires an understanding of the OT systems and facility-specific knowledge to accurately identify false positives. Facility-specific knowledge includes, for example, installed equipment, known or historical faults, and personnel changes. IT and OT personnel must collaborate closely to create the necessary level of understanding of the OT system to support the whitelisting and finetuning. Although identifying operational issues can help resolve many configuration-related challenges, some alerts may still be irrelevant. These alerts can be whitelisted either at the network sensor level or within the SOC, for example, by applying a custom rule set for alert filtering, requiring insights from the OT-side.

However, an outsourced SOC may limit the use of custom rules to maintain standardization across multiple customers, creating alarms that the OT-side need to explain repeatedly. Similarly, the customer often prefers to retain full access to network sensor data, even if this means keeping potentially important log information rather than filtering it out entirely, creating a higher analysis load for the SOC.

Challenges with System Vendors

Organizing meetings with the system vendors to aggregate system logs to the OT SOC was emphasized as an important activity. The OT SOC personnel represent the non-technical (human) barrier element in abnormal situations, and their function is affected by information provided by the system vendors. However, not all system vendors are willing to send data to an external service, due to warranty and intellectual property concerns. Instead, vendors often prefer to offer their own proprietary monitoring services to the customer. This approach can create operational challenges, as customers would then be required to manage multiple vendor-specific OT SOC services. This can be both time-consuming, costly and redundant. This situation has led to an increase in the use of vendor lock-in mechanisms. Despite these challenges, companies often choose to bypass vendor guidelines by leveraging alternative log-collection tools and services to ensure centralized data aggregation toward the OT SOC.

3.2 Work process for improved IT/OT interaction

This section presents empirical findings on expectations and demarcations in IT/OT interactions. These findings are based on studies conducted within the CBM project, the NORCICS Centre[4], and the Tecnocrazi project[5], which collectively informed the publication referenced in [17]. The Riskwork framework [19] distinguishes between two types of interaction: frontstage interactions—those governed by formal policies, procedures, and protocols—and backstage interactions, which refer to informal dynamics such as social relationships, organizational culture, and communication practices.

[4] https://www.ntnu.edu/norcics

[5] https://www.sintef.no/projectweb/tecnocraci/abouttecnocraci/

The distinction between frontstage and backstage interactions is another dimension to the well-established differentiation between sharp-end personnel and blunt-end management personnel, as described in Section 2.1. In this context, sharp-end personnel are those who directly realize a barrier function—they serve as the human barrier element. In contrast, blunt-end management personnel provide supporting functions, some of which can be classified as performance influencing factors (PIFs). Consequently, IT/OT backstage interactions extend beyond the direct management of cybersecurity barriers, encompassing broader organizational and cultural dynamics that influence overall system resilience.

Expectations and demarcations have proven to be valuable for expressing the cultural dimensions of IT/OT relationships. They are particularly effective in highlighting the border zones where safety and security concerns intersect, as well as in identifying potential blind spots in IT/OT interactions that could hinder the effective management of both normal and emergency operations.

Both IT and OT cultures—despite operating in different contexts—have evolved and solidified through a technology-specific, rather than company-specific, process. This process can be understood as being "invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration" [20].

OT culture is comparatively "older" than IT culture, and this distinction has several implications. One key difference is that IT personnel tend to place greater emphasis on procedural compliance and are generally more receptive to managerial guidance. Despite the relative stability of these cultural positions, the findings indicate a shared recognition—on both sides—of the need for increased flexibility in collaboration and decision-making.

The prospect of an IT-driven Security Operations Center (SOC) expanding into OT systems tends to generate expectations and demarcations among OT personnel. An OT SOC is often perceived, by OT staff, as an extension—or proxy—of IT, potentially reinforcing existing cultural divides. However, its introduction can also create a constructive space for enhancing IT/OT collaboration. The findings indicate a shared recognition of the need for mutual understanding and adaptation between the two domains. Notably, the explicit call for a dedicated "translator" role highlights awareness of the cultural distance and the importance of bridging communication and operational gaps.

Since virtually all infiltrations of OT systems use IT technologies as entry points, and because IT technologies are generally relied upon to detect and prevent incidents, emphasizing this can help OT personnel better understand the importance of collaboration with IT teams. Based on this, IT-driven SOCs are well-suited for detection and monitoring. However, any actions taken as part of an incident response must be coordinated through OT personnel to avoid disrupting or compromising critical systems.

Cybersecurity barriers can be understood through the lens of resilience, where cybersecurity barrier elements (BEs) contribute to both the robustness of a system and its capacity to recover from expected and unexpected disturbances. Effective IT/OT interaction is a critical prerequisite for strengthening the adaptive capacity of both the organization and its technical systems. This interaction supports the expansion of their adaptive repertoire in response to environmental changes, including irregular or previously unexperienced events [16], [21].

Non-technical BEs should ideally support not only reliable performance during routine operations within their design parameters, but also the capacity to manage irregular or previously unexperienced situations. Prior research [22] has shown that cultivating a *mindful culture* is essential for addressing such ambiguities productively, rather than avoiding them due to discomfort or fear. In this context, mindfulness refers to the

ability to remain focused on present challenges, actively identifying and scrutinizing potential problems, while enabling employees to explore and engage with these issues. A mindful culture embraces multiple ways of handling ambiguity: “integration denies it, differentiation selectively clarifies it, and fragmentation accepts it” [22, p. 112]. This cultural orientation is supported by key organizational conditions: a reporting culture, a just culture, a flexible culture, and a learning culture.

The empirical study reveals a more interactive and dynamic relationship between IT and OT practices than previously portrayed in the literature. For instance, it was observed that work descriptions for operational barriers can —and should—be revised more frequently. This flexibility reflects evolving adaptive capacities influenced by “near saturation” experiences during combined IT/OT exercises or real cyber incidents, and backstage negotiations—informal adjustments to work processes negotiated between IT and OT personnel. Importantly, this finding suggests that formal alignment of IT and OT operational cybersecurity barrier work descriptions is not strictly necessary. What matters more is that these descriptions capture each domain’s adaptive capabilities and are grounded in ongoing communication and shared exploration of ambiguity, supported by a mindful culture. Dragos [23] further emphasizes that IT cybersecurity professionals should engage directly with OT personnel—beginning by listening, learning, and cultivating mutual trust.

This also implies that joint practices for managing routine variability can be collaboratively developed and intrinsically coordinated between IT and OT personnel. Such outcomes may stem from formalized *frontstage* activities. However, in the absence of explicit managerial involvement in, these collaboratively developed practices are unlikely to be incorporated into formal work descriptions. Consequently, they are categorized as *work-as-done*—the actual practices carried out in the field—rather than *work-as-imagined* or *work-as-prescribed*, which represent formalized expectations or procedural documentation.

A key practical implication of the presented findings is that complete alignment between IT and OT operational barrier terminology, practices, and processes is not strictly necessary. As long as *backstage* interactions take place and boundary conditions are jointly explored in a mindful and reflective manner, IT and OT personnel can establish common ground and build mutual understanding without the need for enforced alignment. Through this process, tentative adaptations to irregular and novel situations help form a shared understanding of each domain’s concerns and priorities. This shared foundation also facilitates joint adaptations to more routine disturbances—*work-as-done*—as they naturally emerge. When conducted thoroughly and systematically, for instance through resilience training, this approach enhances the system’s preparedness to manage both unexpected disturbances and complex cyber events.

4 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 establish and integrate non-technical barrier elements in cybersecurity barrier management?
2) How can interaction between IT and OT domains be improved through new innovative work processes?
3) How to align practice, culture and language between users of office IT systems and ICS?

1. How to establish and integrate non-technical barrier elements in cybersecurity barrier management?
The establishment or identification of both technical and non-technical barrier elements typically begins with a *top-down approach*, where barrier functions are first defined and then associated with specific elements. Alternatively, a *bottom-up approach* may be employed, in which individual barrier elements are identified directly based on observed practices or system configurations. These methodological approaches are described in detail in the technical barrier report [1].

Non-technical barrier elements comprise both human and operational components. *Operational barrier elements* refer to the actions an operator is required to perform in order to support or fulfil a cybersecurity barrier function. These actions often involve the activation or use of a *technical barrier element* by a human operator—also referred to as the *human barrier element*. The lower the level of automation within the system, the more critical the operator's role becomes in ensuring the effectiveness of the barrier function.

Top-down identification of non-technical cybersecurity barrier elements
A top-down approach for identifying non-technical cybersecurity barrier elements can be based on cybersecurity standards, similar as described for technical barrier elements in the Technical Barrier Report [1]. The requirements outlined in relevant standards often address organizational and procedural dimensions of cybersecurity in addition to technical cybersecurity measures. Through a functional breakdown cybersecurity barrier functions are decomposed into their constituent elements, including both *human barrier elements* and *operational barrier elements*. The breakdown enables a clear mapping of responsibilities and actions required to support the intended barrier function.

Bottom-up identification of non-technical cybersecurity barrier elements
A review of an organization's incident response plans for cybersecurity incidents offers valuable input for identifying relevant roles and personnel that may function as *human barrier elements*. These documents often detail the practical distribution of responsibilities and actions during an incident, providing insight into how human and operational components contribute to barrier effectiveness.

This report outlines typical roles and personnel groups involved in incident response, which serve as a foundation for identifying human barrier elements, as elaborated in Section 2.1.

It is essential to distinguish between roles and actions that directly contribute to the reliable execution of a cybersecurity barrier function and those that act as *Performance Influencing Factors* (PIFs). PIFs are elements that affect the performance of a barrier function—either positively or negatively—but are not integral to its core functionality. Accurate classification and documentation of *operational* and *human barrier elements* is crucial to ensure clarity in barrier management and to avoid conflating supporting influences with core operational components.

The ***integration*** of non-technical cybersecurity barrier elements can follow the same principles used for incorporating non-technical safety-related barrier elements, as outlined in Chapter 6 of the technical barrier report [1].

Performance requirements must be defined for all non-technical barrier elements and operationalized to support systematic ***follow-up and verification***. These requirements ensure that both human and operational barrier elements can 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
- Availability

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.

To operationalize and monitor non-technical barrier elements effectively, data must be collected from multiple sources and integrated into the organization's overall barrier follow-up system. For non-technical cybersecurity barrier elements, this may require the use of different systems than those typically employed for technical barriers.

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

A key challenge in non-technical cybersecurity barrier management 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 significantly less capable of capturing and representing the dynamic and context-dependent nature of *non-technical* elements. Integrating relevant data into real-time visualization tools remains a complex task and continues to hinder the attainment of full situational awareness regarding the health and effectiveness of non-technical cybersecurity barriers.

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—that is, 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.

2. How can interaction between IT and OT domains be improved through new innovative work processes?
An innovative work process that can enhance interaction between IT and OT domains is the establishment and integration of Operational Technology Security Operations Centers (OT SOCs). These centres can be implemented in-house or delivered through a Managed Security Service Provider (MSSP). The OT SOC concept adapts the well-established IT SOC model to the OT environment, with the primary goal of improving real-time monitoring and threat detection across OT systems.

Because SOC practices originate from 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 characteristics of OT systems, while OT personnel become more familiar with IT security tools, monitoring methodologies, and how these can be effectively applied in OT contexts.

Such joint work processes not only enable the successful deployment and operation of OT SOCs, but also serve as broader enablers for sustained IT/OT integration and the advancement of cross-domain cybersecurity maturity.

Similarly, IT/OT interaction can be strengthened by establishing structured meeting arenas where IT and OT personnel regularly collaborate and exchange knowledge. These dedicated forums provide opportunities for IT personnel to gain a deeper understanding of OT equipment, its operational characteristics, and its contextual constraints. At the same time, they allow both IT and OT staff to develop a shared understanding of IT security tools—their capabilities, limitations, and appropriate applications within OT environments.

Such structured interactions foster trust, bridge cultural and technical gaps, and support the co-evolution of cybersecurity practices that are both context-aware and operationally viable.

Establishing and maintaining structured meeting arenas requires active managerial support, including the allocation of time, resources, and organizational commitment. Deliberate efforts to explore common ground and foster mutual understanding and trust are essential to enabling effective IT/OT interaction. Participation in these collaborative activities should be recognized as an integral part of routine responsibilities—not deprioritized in favour of immediate operational demands.

Promoting a mindful and collaborative work environment further strengthens cross-domain understanding and supports the development of sustained cooperation between IT and OT personnel. Over time, this contributes to a more resilient organizational culture and a more integrated cybersecurity posture.

3. How to align practice, culture and language between users of office IT systems and ICS?
The empirical study suggests that full alignment between IT and OT domains—across practices, culture, and language—may not be necessary. Each domain operates within distinct operational contexts and is guided by inherently different priorities, which naturally shape their respective approaches to cybersecurity. For instance, IT security practices are typically guided by the principles of confidentiality, integrity, and availability (CIA), whereas OT systems tend to prioritize safety, availability, and integrity, with a strong emphasis on maintaining operational continuity.

Recognizing and respecting these fundamental differences can support more effective collaboration between IT and OT personnel, without imposing artificial or counterproductive alignment. Instead of forcing convergence, fostering mutual understanding and complementary interaction enables each domain to contribute its strengths toward shared cybersecurity goals.

With respect to language and culture, the empirical study found that full cultural alignment between IT and OT domains is not a prerequisite for effective collaboration. Instead, fostering mutual awareness and understanding of each other's cultural norms and domain-specific language provides a sufficient foundation for successful interaction—both during routine operations and in response to irregular or unexpected situations.

IT/OT interaction can evolve and mature when actively supported by management through the allocation of necessary resources and organizational commitment. A key enabler of this development is the establishment of appropriate meeting arenas—structured, recurring forums where personnel can:

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

Such collaborative environments foster mutual understanding, trust, and shared problem-solving. They enable effective IT/OT interaction without requiring full cultural alignment, instead supporting integration through dialogue, adaptability, and ongoing learning.

References

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

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

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

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

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

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

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

[8] PSA, 'Principles for barrier management in the petroleum industry - Barrier Memorandum 2017', Petroleum safety authority Norway, 2017.

[9] V. Gnanasekaran, R. Neudert, P. E. Heegaard, and G. Pernul, 'A Role Taxonomy in Security-Safety Incident Response', presented at the TrustBus 2025, In press.

[10] M. Aarland, 'Digital Supply Chain Roles in the Power Industry', in *Information Technology in Disaster Risk Reduction*, vol. 706, J. Dugdale, T. Gjøsæter, and O. Uchida, Eds, in IFIP Advances in Information and Communication Technology, vol. 706. , Cham: Springer Nature Switzerland, 2024, pp. 185–199. doi: 10.1007/978-3-031-64037-7_12.

[11] M. Maj, R. Reijers, and D. Stikvoort, 'Good practice guide for incident management', European network and information security agency (ENISA), 2010. [Online]. Available: https://enisa.europa.eu/sites/default/files/publications/Incident_Management_guide.pdf

[12] ISO 22320:2018, *Security and resilience — Emergency management — Guidelines for incident management*, Standard, Nov. 2018.

[13] V. Gnanasekaran, F. Urooj, and P. E. Heegaard, 'Increasing Role Collaboration in Security-Safety Incident Response', *International Journal of Information Security*, Submitted to IJIS.

[14] 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

[15] 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

[16] S. Pettersen and T. O. Grøtan, 'Exploring the grounds for cyber resilience in the hyper-connected oil and gas industry', *Safety Science*, vol. 171, p. 106384, Mar. 2024, doi: 10.1016/j.ssci.2023.106384.

[17] S. Pettersen, V. Gnanasekaran, and T. O. Grøtan, 'Understanding techno-cultural shaping of cyber resilience in the nexus of safety, security, IT and OT', *submitted to Safety Science, Special Issue on Risk and Resilience in Crisis and Emergency Management*, 2025.

[18] V. Gnanasekaran, M. Bartnes, T. O. Grotan, and P. E. Heegaard, 'Cyber-incident Response in Industrial Control Systems: Practices and Challenges in the Petroleum Industry', in *Proceedings of the 2024 ACM/IEEE 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS) and 2024 IEEE/ACM Second International Workshop on Software Vulnerability*, Lisbon Portugal: ACM, Apr. 2024, pp. 53–60. doi: 10.1145/3643662.3643958.

[19] M. Power, Ed., *Riskwork: Essays on the Organizational Life of Risk Management*. Oxford, New York: Oxford University Press, 2016.

[20] E. H. Schein, *Organizational culture and leadership*, 5th Edition. Hoboken, New Jersey: Wiley, 2017.

[21] T. O. Grøtan, S. Antonsen, and T. K. Haavik, 'Cyber Resilience: A Pre-Understanding for an Abductive Research Agenda', in *Resilience in a Digital Age*, F. Matos, P. M. Selig, and E. Henriqson, Eds, in Contributions to Management Science. , Cham: Springer International Publishing, 2022, pp. 205–229. doi: 10.1007/978-3-030-85954-1_12.

[22] K. E. Weick and K. M. Sutcliffe, 'Managing the unexpected: resilient performance in an age of uncertainty', *Choice Reviews Online*, vol. 45, no. 06, pp. 45-3293-45–3293, 2007, doi: 10.5860/CHOICE.45-3293.
[23] R. M. Lee and D. Alperovitch, 'Bridging the IT and OT Cybersecurity Divide | Dragos'. Accessed: Nov. 05, 2023. [Online]. Available: https://www.dragos.com/resource/bridging-the-it-and-ot-cybersecurity-divide/

Appendix A Abbreviations and definitions

Abbreviations

Abbreviation	Description
BE	Barrier Element
BE-H	Human Barrier Element
BE-O	Operational Barrier Element
BE-T	Technical Barrier Element
CBM	Cybersecurity Barrier Management
CE	Missing Certificate
CCR	Central Control Room
CERT	Cybersecurity Emergency Response Team
CRO	Control Room Operator
CSIRT	Computer Security Incident Response Team
CTI	Cybersecurity Threat Intelligence
DL	Discipline Lead
DQ	Degraded Qualifications
EIT	Electro/Instruments/Telecom
EMT	Emergency Response Group
EL	Emergency Leader
EPT-C	Incomplete Emergence Preparedness Training
ETC	Emergency Training Compliance
EWS	Engineering workstation
FA	Fagansvarlig (Norwegian for DL)
Havtil	Norwegian Ocean Industry Authority
HMI	Human Machine Interface
HRM	Human Resource Management
ICS	Industrial Control System
IDS	Intrusion Detection System
IoC	Indicator of Compromise
IP	Incorrect or Unsuitable Procedures
IR	Internal Resources
IT	Information Technology
MR	Management Regulation
MSSP	Managed Security Service Provider
MTO	Man-Technology-Organization
NSM	Norwegian National Security Authority
OIM	Offshore Installation Manager
OT	Operational Technology
PIF	Performance Influencing Factor
PoC	Point of Contact
PSA/PTIL	Petroleum Safety Authority (now Havtil)
SAS	Safety and Automation System
SLA	Service Level Agreement
SOC	Security Operations Center
TRS	Technical System Responsible
UBP	Unavailability of Backup Personnel
UML	Unified Modelling Language

UP	Unavailable Personnel
UPR	Unavailable Procedures
UQ	Unqualified personnel
WL	High Workload

For definitions, see the technical barrier report [1].