Environment Systems and Decisions (2025) 45:67
https://doi.org/10.1007/s10669-025-10055-w

Securing maritime infrastructures: a framework to evaluate physical protection measures for offshore wind farms

Babette Tecklenburg[1] · Jan Stockbruegger[1] · Arto Niemi[1] · Frank Sill Torres[1]

Received: 15 March 2025 / Accepted: 1 November 2025

Abstract

Offshore infrastructures such as subsea pipelines and data/ electricity cables are proliferating and expanding rapidly, playing a growing role in ensuring energy supplies and global data flows. Yet these infrastructures are increasingly threatened by hybrid threats and sabotage attacks disguised as accidents. Protecting offshore infrastructures against hybrid threats is difficult, however, due to the very distinct physical environment at sea with large distances, extreme weather conditions, and underwaters vulnerabilities. With this work, the authors propose a framework to determine systematically the resilience capacity of possible Physical Protection Measures (PPM) in the offshore industry based on specific performance indicators including costs, personnel and technical requirements, and attack vectors. We provide an overview of offshore wind farm (OWF) protection goals and functional needs and analyze two specific PPMs to protect OWF, namely protection nets and cardinal marks, to illustrate our framework. We conclude by discussing how physical protection measures can increase the resilience of maritime infrastructures and offshore industries.

1 Introduction

Offshore infrastructures are expanding rapidly and play an increasingly important role in sustaining global communication and energy supplies (Jouffray et al. 2020). The global subsea data cable network has grown to nearly 1.4 million kilometers and carries almost all internet data traffic (TeleoGraphy), and in Europe alone 21.18 GW of wind energy capacity is installed offshore (European Union). The European Union (EU) aims to increase its offshore wind capacity to 60 GW in 2030 and up to 300 GW in 2050 (European Commission 2020). There are currently 13 EU funding programs promoting research, technology transfer and business support in the offshore wind industry, and in 2024 close to 47,000 employees worked directly or indirectly in the European offshore wind industry (European Commission).

Germany is the EU's biggest producer of offshore wind energy with a capacity of 9,2 GW in 2025. The country plans to increase its offshore wind energy production capacity to 30 GW in 2030, 40 GW in 2035 und 70 GW in 2045 (Deutsche Windguard 2025). Nearly all offshore wind farms (OWF) in Germany are already listed as critical infrastructure (CI) because they produce more than 104 MW energy, the CI threshold in the country (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz 2016; Zweite Verordnung zur Änderung der BSI-Kritisverordnung 2021).

Yet offshore infrastructures including OWFs are increasingly threatened by sabotage attacks. For example, the Nord Stream pipeline was destroyed in an attack in September 2021 (McGuinness 2025), and in recent years several subsea data and electricity cables have been sabotaged, demonstrating the vulnerability of offshore energy and communication infrastructures (Hobhouse 2025). Protecting these infrastructures has thus become vital.

A large literature studies Physical Protection Systems (PPS) for critical infrastructure (CI) resilience. PPS refer to a set of measures and technologies designed to protect physical assets, facilities, or individuals from physical security threats such as unauthorized access, theft, damage, or other potential threats (Kampova et al. 2020). These systems typically involve a combination of hardware, software, and procedural elements to prevent, detect, and respond to physical security breaches. PPS include specific Physical Protection Measures (PPM), that is concrete tools, technologies, and practices that, taken together, form integrated security

✉ Babette Tecklenburg
Babette.tecklenburg@dlr.de

[1] The Institute for Protection of Maritime Infrastructures, German Aerospace Center, Bremerhaven, Germany

Published online: 01 December 2025

systems. For example, PPS can include "mechanical barriers (e.g., fences, grilles, roller shutters, and locks) and alarm systems (e.g., alarms, cameras, access control systems, electrical fire alarms)" (Rehak et al. 2022). PPS methodologies evaluate protection systems to identify vulnerable paths and access points, and to help infrastructures operators combine and integrate PPMs as part of comprehensive and effective PPS for their facilities (International Atomic Energy Agency 2021; Kampova et al. 2020; Mary Lynn Garcia 2008).

Yet the debate on offshore PPS for subsea cables, pipelines, and OWFs is only emerging. A Scopus search of "Physical Protection System" in "Article title, Abstract, or Keywords" produces 253 English language journal articles and conference papers between 2015 and 2025. But doing the same search adding "maritime" or "offshore" produces only six journal articles or conference papers. One analyses railway systems and cannot be considered "maritime" (Flammini et al. 2009). Three articles study floating nuclear installations (Hara and Sagara 2025a, b, c), one ports (Munyai and Govender 2024), and one offshore oil and gas platforms (Iaiani et al. 2022). None of these articles investigates PPS or PPM for OWFs. By comparison, a Scopus search of "Physical Protection System" and "nuclear" in "Article title, Abstract, or Keywords" produces 99 articles and conference papers, including the three articles on floating nuclear installations mentioned above. This strongly suggests that offshore PPS and PPM – especially for OWFs - have not yet received much attention in the PPS literature.[1]

A small number of studies has investigated physical security threats and measures concerning OWFs. This includes studies on risk and threat scenarios using Bayesian networks and other methods (Gabriel et al. 2022; Ramírez-Agudelo et al. 2021; Tecklenburg & Sill Torres 2025) as well as studies on threat perceptions (Tecklenburg et al. 2023), resilience measures (Köpke et al. 2023), and communication systems (Thompson 2010). Moreover, scholars have studied safety, resilience, and reputation goals for OWFs (Köpke et al. 2020). However, these studies have not investigated specific PPMs for OWFs.

There is of course a large literature that investigates specific physical security measures for maritime infrastructures. This includes, for example, studies of barrier systems in ship operations (Mišković and Wang 2025) and methods for early identification of vessels that could threaten maritime infrastructures (Wielgosz and Malyszko 2025). There are also studies of specific sensors for threat detection (Lampropoulos et al. 2023), including underwater operations and sensor vulnerabilities (Alamleh and Karabacak 2024). However, none of these studies develops a comprehensive analytical framework to investigate offshore PPMs systematically and comprehensively, especially for OWFs.

Our paper contributes to the debate on critical offshore infrastructure and OWF protection. It

- categorizes human-made physical threats to offshore infrastructures and presents key challenges in designing effective offshore physical protection measures.
- introduces a methodology and framework to evaluate physical protection goals and measures for OWFs.
- provides an overview of OWF protection goals and functional needs and analysis specific PPMs to protect OWFs (protection nets and cardinal marks).
- discusses how physical protection measures can increase the resilience of maritime infrastructures and offshore industries.

Our paper proceeds as follows. The second section focuses on the protection of critical maritime infrastructures, existing threats as well as physical protection measures. The third section introduces the applied methods followed by an introduction of OWFs in section four. The fifth section develops a framework that will be tested in a case study in Section 6. Section 7 describes how the framework can contribute to the resilience of a maritime critical infrastructure. The journal contribution ends with a conclusion and outlook in Section 8.

2 Protecting offshore infrastructures

This section briefly introduces key challenges when it comes to protecting maritime infrastructures. We categorize threats to maritime infrastructures and argue that the ocean's physical characteristics present key challenges for physical protection systems and measures.

2.1 Physical threats to offshore infrastructures

Here we categorize physical human-made physical threats to offshore infrastructures. Offshore infrastructures are infrastructures that are located on the sea. This includes subsea data/ energy cables and pipelines as well as OWFs and other offshore platforms (e.g., oil and gas platforms). We exclude coastal infrastructures such as ports and cable landing stations that are located on the shore.

Human-made physical threats are physical threats that can damage or destroy the physical components of an infrastructure. Furthermore, it is also possible that workers

[1] However, there is a larger literature on cybersecurity and the security of cyber-physical systems that primarily studies cyber threats to information technology and operational technology systems in the maritime industry. Cyber threats can lead to physical damages, but addressing them does not require PPS to protect infrastructures. For a recent review see Harish, Tam, and Jones (2024).

are injured or even killed. All these actions originate from human beings. The physical threat is directly caused by a human being or organization or by a system produced, built, or controlled by humans (Fennelly 2016). This definition excludes cyberattacks, which are not physical (Harish et al. 2024) and natural disasters, which are not directly caused by humans or human systems or organizations (Gireesh et al. 2021).

The literature often divides human-made physical threats into safety and security threats (Cui et al. 2019; Şengül et al. 2023). In the maritime domain, safety threats are unintentional accidents that mainly involve civilian vessels and other vehicles that damage offshore infrastructure. This include merchant vessels and fishing boats that accidentally collide with an OWF or that damage subsea data cables with their anchors (The Maritime Executive 2023). Safety threats have always been a concern of infrastructure operators (Tang et al. 2018; Wang et al. 2021).

Security threats (Baker and Benny 2013), including offshore physical security threats, on the other hand, are intentional attacks. This includs acts of sabotage against offshore infrastructures committed by hostile state and non-state actors, like criminals and terrorists, and may involve weapons and other military grade instruments (Bueger and Edmunds 2024). Examples are Russian attacks against Ukrainian ports or the 2021 attack on the Nord Stream pipeline with explosives. The identity of the attackers remains unknown, but the incident involved explosives suggesting a high level of military training and capacities (Bueger 2022). Other security threats at sea include threats such as piracy, private armed guards (Bueger and Stockbruegger 2024; Stockbruegger 2021) or attacks involving warships on ports and merchant ships (Speller 2023).

Table 1 Human-made physical threats to offshore infrastructures

Threat	Motivation	Actors and platforms	Example
Safety	Unintentional accidents	Mainly civilian actors, platforms, practices, instruments	Accidents such as oil spills or collisions between vessels and OWFs
Security	Intentional attacks and sabotage acts	State or non-state security actors, using military platforms, practices, instruments	Russian attacks on Ukrainian ports and Nord Stream pipeline attacks in the Baltic Sea
Hybrid	Intentional acts of sabotage camouflaged as an unintentional accident	State and non-state security actors, using civilian platforms, practices, instruments	Merchant ships affiliated with Russia damage subsea electricity and data cables in the Baltic Sea

Intentional attacks and acts of sabotage are also often camouflaged as unintentional accidents. These attacks appear to be unintended safety incidents involving civilian actors and vessels – rather than military forces and practices. Yet they are perpetrated by hostile state or even non-state actors, and they may involve hidden security personal and equipment. Hybrid threats therefore blur the distinction between infrastructure accidents and sabotage attacks, posing a key challenge for security agencies and infrastructure operators. We define such attacks as hybrid threats that are located between safety and security threats.[2]

A key example of a hybrid threats are incidents whereby vessels associated with Russia damaged European subsea cables with their anchors in November and December 2024. Both vessels were civilian ships that had sailed from Russian ports, but they did not fly the Russian flag, and they were not operated by Russian sailors or security forces. The crew and operators of one of the vessels thus continue to claim that the cables were destroyed accidentally (Blöcher et al. 2024; Staib 2024; Suchkov 2021). Indeed, as the European Subsea Cables Association points out, "Although intentional sabotage may be viewed as a "possible" threat, cables are at a far greater risk of being damaged by the very real threat of fishing and anchors, or other natural events and human activities" (European Subsea Cable Association). An accident scenario thus remains plausible, if unlikely, in contrast to the attacks on the Nord Stream pipelines. As these recent cable incidents have shown, lengthy forensic investigations and court proceedings are required to establish that the incidents were in fact an intentional attack and not an accident caused by technical failures (Kauranen 2025).

In short, the offshore safety and security landscape is becoming more complex. Safety risks remain a major concern, but security and hybrid threats are increasingly considered the most important and pressing challenge for governments and infrastructure operators. There is thus a growing need to develop effective physical protection measures for maritime infrastructures (Table 1).

2.2 Offshore infrastructures and physical protection

A PPS integrates personnel, procedures, and systems to protect infrastructures and facilities against theft, sabotage, and other malicious human actions. The effectiveness of a PPS is measured by its ability to withstand a potential attack and prevent adversaries from achieving their objectives. PPS effectiveness depends on the most vulnerable path through which an adversary may penetrate an infrastructure or facility, which is the optimal intrusion path from the adversary's

[2] Political Scientists define hybrid threats as threats that combine different attack strategies and that are often located below the threshold of war Caliskan (2019).

point of view (International Atomic Energy Agency 2021; Mary Lynn Garcia 2008).

PPS are based on a combination of measures for threat detection, delay, and response. Detection requires systems to detect an attacker or malicious actor such as alarm systems, cameras, or other sensors; delay is the slowing down of an adversary and can be accomplished by people, barriers, locks, and other measures; response refers to the ability of a PPS to respond to an incident with additional hardening or security measures such as deploying security personnel or ensuring police intervention.

Detection should be early and as far from the target as possible. Delay measures should be located nearer to the target and make it more difficult for the attacker to reach the target, requiring more time and the use of tools and technologies to overcome them. The incidence responses should be as fast and as strong and comprehensive as possible to stop the attack and detain the attacker. Deterrence can be accomplished if adversaries view a facility as an unattractive target and opt not to attack it, judging their likelihood of success as too small or the dangers to themselves as too great (International Atomic Energy Agency 2021; Mary Lynn Garcia 2008).

Yet the maritime physical environment affects the accessibility of offshore infrastructures and has major implications for the design and evaluation of offshore PPS and the deployment of specific PPMs. Offshore infrastructures such as OWFs are often located in remote areas far off the coast, and some infrastructure components such as cables are built on the ocean floor dozens of meters underwater. Germany, for example, is already building OWFs over 100 km off its coast and in water depths of over 40 m (Deutsche Windguard 2025).

Access to offshore infrastructures is also affected by harsh weather conditions including strong winds and high waves. One study, for example, finds that in the North Sea OWF "accessibility drops to values lower than 15% during winter and autumn" (Martini et al. 2017, p. 651). Attacking and defending OWFs and underwater infrastructures thus requires specialized and often expensive marine systems such as vessels, helicopters, or underwater vehicles – as well as the necessary skills, resources, and training to maintain and operate them under extreme weather conditions.

Beyond this, however, the marine environment also poses more specific challenges for threat detection, delay, and response. Sensors to monitor maritime spaces including radar, optical cameras, Automatic Identification System (AIS) and sonar and other underwater sensors have proliferated in recent years (Briguglio and Crupi 2024; Eleftherakis and Vicen 2020; Felemban et al. 2015; Şengül et al. 2023). Yet integrating these sensors into an effective PPS for infrastructure protection remains challenging, requiring advanced data integration and object detection algorithms, especially to detect vessels that don't have AIS, as well as effective alarm systems (Wielgosz & Malyszko, 2025). Marine conditions such as humidity, salt spray, waves and strong winds can lead to the degradation of sensors while weather condition can lead to poor visibility and cause false alarms (of birds, marine life, debris), making accurate threat detection harder. The monitoring of subsea infrastructures remains difficult due to poor underwater visibility and communication (Eleftherakis & Vicen, 2020).

The marine environment also makes it difficult to delay and slow down an attack. On land, many important infrastructures or infrastructure components such as converter stations are usually separated from their environment with walls or fences – an effective barrier to delay attacks and to slow down an adversary or safety threats (Kampova et al. 2020; Mary Lynn Garcia 2008). Yet one cannot build a wall at sea around an offshore converter platform in deep waters, requiring instead the use of specialized – and arguably less effective – marine surface barriers (Mišković & Wang, 2025) or suspension nets (see below). Subsea cables and pipelines can be buried under the seabed to better protect them against anchors and other threats. Yet doing so is costly, could damage the environment, and make it more difficult to access the subsea infrastructure for maintenance and repairs (Hobhouse 2025).

Finally, ensuring timely and adequate offshore responses to infrastructure threats remains a major challenge. Incidence response times are often very high due to the remote location of offshore infrastructures, as we have already pointed out. It can take hours for a coastguard or naval vessel to reach an OWF and to respond to an attack or a safety incident far off the coast. The vessel "Eagle S.", for example, damaged five submarine cables in the Gulf of Finland by dragging its anchor on the seabed for about 90 km before it was stopped by Finish security forces (Blackburn 2025).

Part of the problem is that the United Nations Convention of the Law of the Sea (UNCLOS) only allows for the creation of a 500-meter safety zone around OWFs where vessels and other vehicles are not allowed to enter. Subsea cables and pipelines crossing international shipping lanes with high traffic however usually do not even have such a small safety zone around them (tho Pesch 2015). UNCLOS also makes it difficult for security forces to stop, search and detain vessels in their 200-miles Exclusive Economic Zone (EEZ) where most OWFs and other offshore infrastructures are located (Beckman et al. 2025). For example, Finish security forces only boarded the Eagle S. – which had already damaged five submarine cables – after the vessel had entered Finish territorial waters (Blackburn 2025).

In short, the marine environment poses specific challenges for PPS and threat detection, delay, and response to secure offshore infrastructures. The following sections develop and illustrates a framework to evaluates specific PPMs for OWFs, focusing especially on the maritime dimension of PPMs. Next, we introduce our method for developing and illustrating the framework.

3 Methods

This paper develops and illustrates a (visual) evaluation scheme for PPMs for an OWF. We used three methods to develop and explore this framework. As we have shown in the introduction, to our knowledge very few scientific studies evaluate the physical protection of offshore infrastructure and OWFs. Therefore, we cannot conduct a literature review to develop such a framework. Instead, we relied primarily on maritime security experts with experience in offshore infrastructure and OWF protection and tried to identify methods to collect such expert knowledge and experience. We thus selected methods that ensure flexibility in data collection and organization and that do not provide a strict framework – such as questionnaires. We first conducted brainstorming sessions with security experts from the offshore wind industry to collect information about protection measures. Second, we used this information to develop Key Performance Indicators (KPIs) for PPMs. And third, we used these KPIs to evaluate two OWF PPMs theoretically to demonstrate the practical utility of the framework. We describe these three methods below.

3.1 Brainstorming

Brainstorming was introduced into the business world by marketing expert Alex F. Osborn in 1953. Brainstorming is an intuitive-creative technique that is based on the principle of free association (Antosch-Bardohn 2021). It can either be performed as an individual or as a group (Antosch-Bardohn 2021). Groups should have between five and seven participants to ensure effective communication and debate (Hölzl 2012). Conducting individual brainstorming activities with each group member can generate more ideas because it provides individuals more time and space to express their thoughts. (Antosch-Bardohn 2021; Hölzl 2012).

The following four rules should be followed when conducting brainstormings: let thoughts run freely (every idea is welcome), do not criticize (an evaluation takes place later), quantity is more important than quality (the focus should be on collecting as many ideas as possible) and take up the ideas of other individuals and group members (all ideas can be used by other team members which leading to new combinations). Brainstorming is a fast technique that should take between 20 and 40 min (Hölzl 2012).

As pointed out before, we specifically used brainstorming with experts for this paper because it allowed us to flexibly collect qualitative data including a broad range of insights and expertise about a relatively new and unexplored area of research – PPMs in the offshore wind industry. Brainstorming was thus a more suitable data collection method for this study than structured interviews or questionnaires that do not provide this flexibility.

3.2 Key performance indicators

KPIs were originally introduced in business administration to evaluate the performance of companies and to help the management to determine whether or not a company is successful. Before 1992, KPIs only considered financial issues, but were then extended to other critical areas of business performance, including “customer”, “internal process”, and “learning and growth”. Since then, the literature on business administration has developed qualitative or quantitative KPIs (Woolliscroft et al. 2013), including measurements based on ratios and percentage instead of raw numbers (Peterson 2006). Around ten KPIs is usually considered a suitable number to ensure a comprehensive evaluation of business performance (Woolliscroft et al. 2013).

In recent years KPI’s have also been increasingly used in other areas, including safety, security and maintenance. Gabriel and Sill Torres, for example, define KPI’s to determine the safety and security of an OWF. Their KPIs capture a broad set of factors that determine the safety level of OWF, such as wind farm composition and layout, operation and maintenance, and location and environment, among others (Gabriel and Sill Torres 2023).

Saihi et al., on the other hand, developed an overarching system of KPIs to capture the “Environmental”, “Social” and “Economic” sustainability of infrastructures. Working closely with experts, they created different categories and sub-categories within each area, such as the category “resource use” and the sub-category is “land use” in the area of “environmental” sustainability, with a specific ranking scale for each indicator (Saihi et al. 2022). Using these indicators, they were able to assess the different dimensions of sustainability of a specific infrastructure comprehensively.

We used KPIs in this paper as a framework to organize the insights of experts on OWF protection and to identify the most important indicators to evaluate PPM for OWFs.

3.3 Evaluating protection measures

Different approaches exist to assess and evaluate PPMs using KPIs. This includes the exercise or experimentation method, the simulation method, and the theoretical or analytical approach.

In the experimental approach, a specific PPM is studied in the real world. The PPM is installed in either a real application or in a laboratory environment. The experimenter than tests if the PPM detects attacks and how the countermeasure can be overcome. The experimental approach is very common in the IT security domain. Moro et al. for example studied the robustness of selected software schemes against fault injection on embedded programs focusing on microcontroller (Moro et al. 2014). The advantage of the experimental approach is that the PPM is tested under real application conditions allowing for the elimination of cross sensitivities regarding for example lights or humidity.

Another way to test or evaluate a PPM is the simulation approach. In this approach the infrastructure and the PPM are simulated. A common approach is to conduct an attack on an infrastructure to see if and how it can succeed (Brauner et al. 2015). This approach is especially useful for large facilities where the installation on a trial basis is time consuming. The other advantage is that multiple configurations can be tested to identify the best one. One example for this approach is Marroni et al., who investigated different scenarios to determine fragility models for a chemical plant and to establish the likelihood that the PPSs resists an explosive attack (Marroni et al. 2022).

The last approach is the analytical or theoretical approach. In this approach, an advanced set of criteria, categories, and goals for protection is defined. Then each protection measure is evaluated based on these criteria and compared with one another. Based on this comparison, the most suitable measures are selected. The advantage of this approach is that it is less costly and does not require extensive preparation and complicated set-ups. No detailed information about the infrastructure layout is necessary. One example is the work presented by Brauner et al. (Brauner et al. 2015).

We used the theoretical approach as it allowed us to examine PPMs drawing KPIs based on expert knowledge without conducting complex simulation and field tests. Yet such field exercises and simulation would be required in a next step to develop and test PPS for the offshore industry.

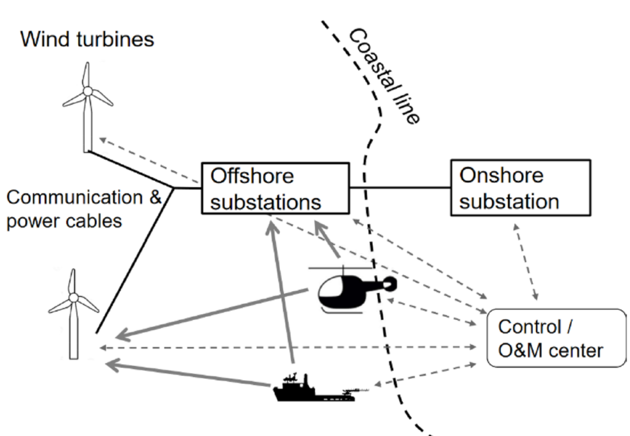


Fig. 1 Schematic structure of an OWFSource: (Sill Torres et al. 2020)

4 Offshore wind farms

Next, we use these methods to develop and illustrate a framework for evaluating physical protection measures for an OWF. Here we provide an overview of the technical components and subsystems of OWFs that require protection against safety, security, and hybrid threats.

4.1 Layout of an offshore wind farm

An OWF consists of multiple Wind turbines (WT), an offshore substation and an underwater cable that connects the wind farm to shore-based electricity grid (see Fig. 1). The WTs produce electricity which is then transported to the offshore substation through the inner grid. The offshore substation (OSS) transforms the energy from medium voltage level to high voltage level. The electricity is then forwarded to the high voltage direct current converter station (HVDCC), which collects the electricity from multiple OWFs and changes the type of current. In the last step, the energy is transported to the shore. An onshore substation feds the electricity into the land based power grid (Hau 2014; Robak and Raczkowski 2018).

A loss of a HVDCC would have significant consequences, as the energy produced in multiple OWFs could not be fed into the grid. An HVDCC consists of a top structure which include workshops, operation rooms and accommodation facilities. The top structure is built onto a support structure. Maintenance workers and spare parts are transported to the HVDCC either by vessel or by helicopter. For this purpose, HVDCCs have a pier and a helicopter landing deck (Robak & Raczkowski, 2018). OWFs are monitored at an onshore control room. With a Supervisory Control and Data Acquisition (SCADA) system, the operators in the control room receive information about the current and past operating states of all infrastructure elements. Furthermore, they also supervise the offshore crews and vessels in the OWF (MacAskill and Mitchell 2013).

4.2 Protection goals for offshore wind farms

The installation of PPM is not an end in itself for the owners and operators of OWF. They need to fulfil goal or purpose such as preventing fire emergence or protecting facilities against unauthorized access. This aim is called protection goal. Protection goals are socially excepted and defined in public law as well as in internal guidelines of companies and institutions (Zehfuß 2020). Protection goals can

Table 2 Common protection goals for CI in Germany

Domain	Protection goals	Legal level	Addressee	Source
Fire protection	Prevention of fire development Prevention of fire & smoke spreading Enable the rescue of people & animals Enable effective extinguishing measures	Regional State level	Operators	Musterbauordnung (2023)
Security	Averting dangers to public security Prevention of criminal acts	Regional State level	Authorities	(Bremisches Polizeigesetz (2024)
Civil protection	Highest level of protection for personal Maintaining functionality Fulfilment of legal requirements Prevention of economic loss Prevention of potential image loss	Federal level	Operators	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2011)
Hazardous Incident Ordinance	Prevention of tampering by unauthorized persons by operators	Federal level	Operators	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge, (2024)
Critical Infrastructure resilience	Prevention of accidents/ incidents Appropriate physical protection of property and critical plants Reacting to accidents/ incidents, repelling an attack and limit its impact Quick restoration of critical service	European level	Operators	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge, (2024)Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (2024)

Table 3 Summary of protection goals and related functional needs

Protection goals	Functional needs
Occupational safety	Prevent accidents & enable rescue in a timely manner
Environmental protection	Limit impact on flora/ fauna
Plant safety	Safe operation of plant
Reputation/ Compliance	Ensure positive public opinion (general public, stakeholders, staff) can be influenced
Finance	Ensure that financial liabilities can be met
Security	Prevent unwanted influence from the outside including criminals, terrorists and other threat actors
Supply reliability	Ensure the availability of maintenance staff and spare parts

be applied in the safety and security domain but also in the business domain. As mentioned in Section 2.1, hybrid threats are often camouflaged as unintentional accidents. Therefore, they could be seen as part of the safety or the security domain. Depending on the domain, protection goas are either defined in public law (European or state law) or governance guidelines of industries or even companies. It needs to be stated that not all laws and guidelines consider hybrid threats already.

A summary of standard protection goals for specific domains is presented in Table 2. Protection goals are usually very general because they focus on CI broadly and not on specific infrastructure types. CIs vary in the size, extension and purpose. Airports for example are very different infrastructures than hospitals. Protection goals need to fit all of kinds of CIs. Scientific publications sometimes define protection goals for specific infrastructures. Köpke et al. name the following protection goals for OWFs: Accident prevention, Security, Compliance, Occupational safety, Environmental protection, Reputation, Plant safety, Supply reliability, Finance (Köpke et al. 2020).

For an optimal protection of infrastructure, protection goals must be considered holistically. There are protection goals for different types of incidents, e.g., for fire protection for the prevention of fire development or effective extinguishing measures but also security-oriented protection goals such as preventing criminal acts and tampering by unauthorized persons. Besides that, protection goals can also refer to business-oriented issues such as minimizing financial and reputational costs. In the vast majority of cases, the definition of protection goals focusses on private actors such as infrastructure operators, and in rare cases also on public authorities. Protection goals from different domains also sometimes overlap (see Table 2).

While protection goals define the reason for adopting specific protection situation, functional needs describe how protection goal should be (technically) reached. For the protection goal “occupational safety”, the functional need could be “prevention of accidents at work”. The performance criteria, on the other hand, is more concrete. They describe under which conditions the functional need can be considered as being achieved. For the functional need “prevention of accidents at work”, the performance criteria would be a certain number of accepted accidents at work. Such performance criteria are usually defined by each company individually - often in collaboration with trade associations. For example, a common performance criterion includes “zero accidents”.

To define protection goals for OWFs, we use the results of a series of qualitative interviews that we conducted in 2021 with stakeholders from the German Offshore wind industry. In total 28 participants with different professional backgrounds like authorities, operators or maintenance companies were interviewed. The interviews did not aim at statistical significance but to gather insights and expertise on OWF protection. For more information regarding the interviews see (Tecklenburg et al. 2023).

One question asked the interview participants to state specific protection goals. The interview participants listed the following protection goals: occupational safety, environmental protection, plant safety and business goals. Thereby the interview participants elaborated occupational safety with functional needs: no accidents, immediate rescue, technical requirements for helicopters. For the business goals the participants stated a high quality and plant availability (the term “high quality” is not any further defined).

We compared the results of the interviews with the protection goals shown earlier in this section to produce a combined list of protection goals. The results can be seen in Table 3. For each protection goal a functional need has been defined. The authors decided not to add the performance criteria because that needs to be done in accordance to OWF layout and company values and therefore cannot be part of a more general scientific research paper. The determination of the functional needs which a PPM would benefit has been included as a criterion to the framework as well.

Table 3 Overview of the experts involved in the brainstorming

No.	Gender	Age	Experience	Domain
1	Female	Below 30 years	4 years	Researcher, Domain: safety and security aspects in Offshore Wind industry
2	Male	Below 30 years	2 years	Researcher, Domain: economics in Offshore Wind industry
3	Male	Above 30 years	7 years	Senior Researcher, Domain: Safety and Security aspects in transportation and Offshore Wind industry
4	Male	Above 30 years	10 years	Senior Researcher, domain: maritime security
5	Male	Below 30 years	2 years	Researcher, domain: Operation of offshore wind industry

5 A framework for evaluating offshore wind farm PPMs

In the following section, we describe the development and visualisation of a framework to evaluate physical protection measures for an OWF. We first conducted individual brainstormings with offshore security experts to identify the most important indicators for evaluating PPM and then discussed the results together with all exports in a group brainstorming. In doing so, as described by Antosch-Bardohn, we avoided mental barriers and were able to collect a wide range of PPM most commonly used in the industry. A short description of the experts can be found in Table 3. The research question for the brainstorming was: What are possible dimensions to determine the suitability of a PPM for OWF? The following list shows the results of the brainstorming:

Training effort for staff	Safety and security
Time factor	Above water, below water, air
Costs including effort	Infrastructure level
Human/ no human	Stationary or portable
Selectivity	Effect level
Scope of device	Specialty
Kind of information	Effectivity
Downtimes after trigger	Preventive and reactive
Requirements (autonomous, not autonomous)	

Some of the ideas and measures provided by the experts overlapped and were mentioned several times, even though they often used different words. The authors organized these indicators into groups and, based on expert assessments collected through brainstorming, defined their possible values, including either quantitative or qualitative values. The indicators are designed to analyze specific characteristics of PPM. An overview of the categories and indicators, including their scale and description is provided in Table 4.

Table 4 provides an overview of performance indicators to evaluate offshore PPMs comprehensively and from different functional, financial, and technical perspectives. We first include indicators that allow us to evaluate the costs of a PPM, including acquisition costs, maintenance costs and human resource costs. The second set of indicators helps us to evaluate a PPM's technical detection and protection performance, including its specificity (risk of false alarm), sensitivity (positive alarm rate), weather compatibility (e.g. rough winds), effects (e.g., detection, alarm, or countermeasure), selectivity (attack vectors), and underwater capability. We then include performance indicators that refer specifically to the location of a PPM at an infrastructure and which infrastructure component it covers or protects (e.g., the wind turbine, the converter platform, or a specific access point). Finally, we include indicators that capture issues of time and timing, such as whether or not a PPM is reactive or preventive, and what downtime it can cause, and other important device properties including if the PPM is portable, if it can be controlled remotely, and its size.

Table 4 includes descriptions of each indicator. We also provide specific measurement scales for each performance indicator. The scales allow users to practically measure and evaluate the indicators within these categories. Moreover, Table 4 contains information on how the maritime environment affects the evaluation of the PPM's performance indicator. This not only helps users to better evaluate PPMs, but it also documents the importance of considering the marine environment when designing and evaluating PPMs and PPS.

Furthermore, the authors developed a documentation that describes the KPI's in Table 4 in more detail including the evaluation categories. Below we provide an exemplary documentation of "maintenance costs".

> This category describes the maintenance costs (MC) for a PPM. This includes wear parts, such as filters, but also spare parts or, if necessary, personnel costs to carry out the PPM. Again, the values are divided into "Low", "Medium" and "High" (see Table 6). Low maintenance costs would be, for example, if it is only necessary to check once a year whether the functionality is still given. Medium maintenance costs are when wear parts have to be replaced more frequently, while high maintenance costs exist if specialized personnel must be permanently employed or if high-quality wear parts must be replaced regularly.
>
> Example: A smoke detector without connection to the professional fire department has low maintenance costs since its functionality only has to be tested every year or even less frequently.

In addition, a graphical representation of the KPIs has been developed. Depending on the KPI, that is either a 2-D or 3-D scatter diagram. These visualizations help to compare PPMs across selected indicators and to evaluate them comprehensively. Depending on the focus of the comparison, two types of diagrams are possible. For each category an overview of the related indicators has been designed. Thereby each indicator is allocated to one axis. For selected combinations two or three categories are compared. Figure 2 for example shows the comparison of the categories "device properties", "location" and "time".

To determine a value for an entire category, the dot in the scatter diagram is defined as a vector starting from the origin of the coordinate system. Equation (1) exemplarily shows the length for the category "time" with the indicators "Downtime" and "preventive or reactive".

$$Value_{Time} = \sqrt{Value^2_{downtime} + Value^2_{preventiv\ or\ preactive}} \tag{1}$$

We exemplify this framework in Fig. 2. The center of the figure is the comparison of the categories "device properties", "location" and "time" for the PPM "smoke detector". The value for each category has been determined with Eq. (1). In smaller diagrams each category of the related indicators are illustrated. For example, a smoke detector can be considered a preventive measure with a downtime in the range of minutes.

6 Case study

As a prove of concept the authors conduct a case study. Therefore, a number of PPMs in a generic OWF should be investigated. The selected PPMs are inspired by results from the interviews with OWF security officials that we

Table 4 Key performance indicators for offshore wind farm physical protection measure

Category	Indicator	Description	Maritime factor	Scale
Finance, Costs	Acquisition cost	Purchasing costs including material and personal costs. Less expensive measures are often preferred.	Equipment which is exposed to the maritime environment faces harsher impacts like salty air and strong winds,. Therefore equipment requirements are higher, increasing acquisition costs.	Low, medium, high
	Maintenance costs	Maintenance costs including material- and personal costs. Less expensive measures are often preferred.	Maintenance cannot be performed throughout the entire year. Every spare part needs to be transported to the OWF by ship. Maintenance workers require specific training.	Low, medium, high
	Human resource costs	If and to what degree the involvement of human agents is needed. The involvement of humans increases personnel costs and the risk of human error.	Offshore personal requires training. Not all offshore infrastructures are permanently crewed.	Yes and no
Performance criteria	Effect	The effect that the PPM produces. This includes the provision of information about intruders (e.g. an alarm), warning signals as well as the initiation of PPM.	Reducing intervention times is key to protecting infrastructures. This requires early detection and information sharing so that intervention forces can react quickly and adequately.	No information, only information, loud alarm and countermeasure initiated
	Selectivity	Attack vectors covered by the PPM. For maritime infrastructures the underwater vector is especially important.	Maritime infrastructures are exposed to two more attack vectors than land-based infrastructures (above and below water).	Between 1 and 5 (below water, above water, air, land, internal)
	Sensitivity	Describes how often an alarm is not triggered even though it should have been triggered	Due to large distances and the limited number of workers on site, sensors and alarm technologies need to be very reliable.	No failures; low medium- and high number of failures
	Specificity	Risk of false alarms. The higher the risk, the less efficient a measure is.	Due to great distances, alarms cannot be verified by staff member. The harsh environments (salty air, humidity, strong winds) may have a negative impact on sensor performance and alarm rates.	No false alarms, the exact number of false alarms; low-, medium-, and high- number of false alarms
	Weather compatibility	Describes if the PPM can properly function in all relevant weather conditions (high waves, strong winds, salty air).	Weather conditions at sea vary significantly from conditions on land, influencing PPM performance.	Yes, partially, no
	Underwater capability	Can the PPM operate below the water line?	The foundation as well as significant parts of the structure of maritime infrastructures are located below the water line.	Yes, no
Location	Infrastructure component	In or on which infrastructure component the PPM is implemented. Installing PPMs is more difficult on some infrastructure components than on others	OWFs consist of different infrastructure on which PPMs be installed.	HVDCC, OSS, WT, cable, land
	Effect level	The infrastructure component which is protected by the PPM.	For PPMs different types of sensors exist, and not all sensors have the same coverage. Therefore, the infrastructure component where the PPM is located and the infrastructure that it protects are not always identical.	HVDCC, OSS, WT and cable
Time	Preventive or reactive	If the PPM triggers a reaction automatically or not	One challenge in the maritime domain is that reaction times are longer than on land. Therefore, a PPM that triggers an automatic reaction is might be preferred.	Preventive or reactive
	Downtimes	Duration of downtimes after a PPM is triggered. The longer the downtime, the more hesitant operators are to use it	Offshore maintenance work can only be performed during certain weather conditions and seasons. Therefore, long downtimes can have a huge impact to infrastructure performance	Seconds, minutes, hours, days, weeks

Table 5 (continued)

Category	Indicator	Description	Maritime factor	Scale
Device properties	Stationary or portable	If the PPM is moveable or not.	Moveable PPMs can be transported to a different infrastructure of the same OWF or even to a different OWF. This increases the flexibility of the PPM. It is even possible to bring the PPM to the coast for maintenance works.	Stationary or portable
	Remote controllable	Is the PPM remotely controllable?	Offshore infrastructures are not permanently manned. Therefore, a PPM that requires staff members onside to be operable cannot be active the entire time.	Yes, no
	Size of measures	How much space a PPM needs	The costs of building an offshore infrastructure are significantly higher than for a similar infrastructure on land. Therefore, the necessary space for the PPM should be as small as possible.	No additional space, mm^3, cm^3, dm^3, room filling or multiple rooms affected

Table 6 Thresholds for the different values within the "maintenance costs" category

Value	Threshold
Low	$\leq$ 100 €/ year
Medium	200 < MC/ year $\leq$ 1000€
High	> 1000€/ year

mentioned in Sect. 4.2. Below we list key PPMs and other health and safety measures mentioned most frequently in the interviews and brainstorming activities:

Start-work-briefing	Cardinal marks
Simulated attacks	VPN tunnel
IT security concept	Drug control
Access to word wide web limited	Audit of plants
Firewalls	Telemedicine
Instructions	Certification
2-factor-registation	Emergency exits
Redundancy	Intruder barrier (sensor)
Alcohol control	Access management after retiring
Dual control principle	Secure data line
Medical examinations	Smoke alarms
Closed entrance	Hydrogen alarm

As a first comparison the authors picked cardinal marks. Cardinal marks are the green and red buoys that mark the waterway or point out hazardous areas. The authors compared them to suspension nets, that is metal nets which are stretched between infrastructures. They function as a physical barrier that inhibits vessels or underwater vehicles to enter the protected area.

Figure 3 shows the time related indicators for the PPM "suspension nets" and "cardinal marks". It can be seen that both PPMs cause no downtimes. This is can be explained by the fact that they do not trigger any further actions. Assuming that one of them performs their intended use, the WTs can still produce energy. A key difference between cardinal marks and suspension nets is that cardinal marks fall into the category of preventive countermeasure. They inform the captains of passing vessels about the presence of hazards. In case that the captain intentionally or unintentionally avoids this information, no further action is triggered. On the other hand, suspension nets fall into the category of reactive PPMs. They do not only inform passing vessels and their crews that they should not cross into a certain area, but they actively prevent vessels from entering that area.

Figure 4 illustrate the performance criteria of both PPMs. It can be seen that they are quite similar in terms of effectiveness but vary in terms of selectivity and underwater capability. Cardinal marks only protect against one attack vector, while suspension nets block two attack vectors. For cardinal marks, the attack vector is "above water" because they can only be seen by passing vessels and their crews (technically it can also be seen from above, for example from an aircraft but this is not a relevant attack vector). Below the water surface, the chain is visible but the information where the hazard occurs is missing. Therefore the "underwater" attack vector is not addressed. Suspension nets, in contrast, are stretched above the waterline but also fall below it, thus addressing attack vectors. Neither PPM prevents attacks from within an OWF (e.g. by a maintenance worker on the platform) because people familiar with the OWF and its PPMs will likely find ways to circumvent protection measures.

Figure 5 shows a comparison of different security-oriented PPMs. For comparison the two main categories "performance criteria" and "financial expenditure" have been chosen. It can be seen that in terms of financial expenditures, the PPMs cover mostly the middle to high part of the scale. In terms of the performance criteria, on the other hand, the PPMs cover almost everything from the bottom to the top of the scale, though most PPMs fall into the middle part of the scale. The left part and parts of the upper middle part are empty. So no PPMs with that criteria are considered. In a real application, that could mean that no PPMs with

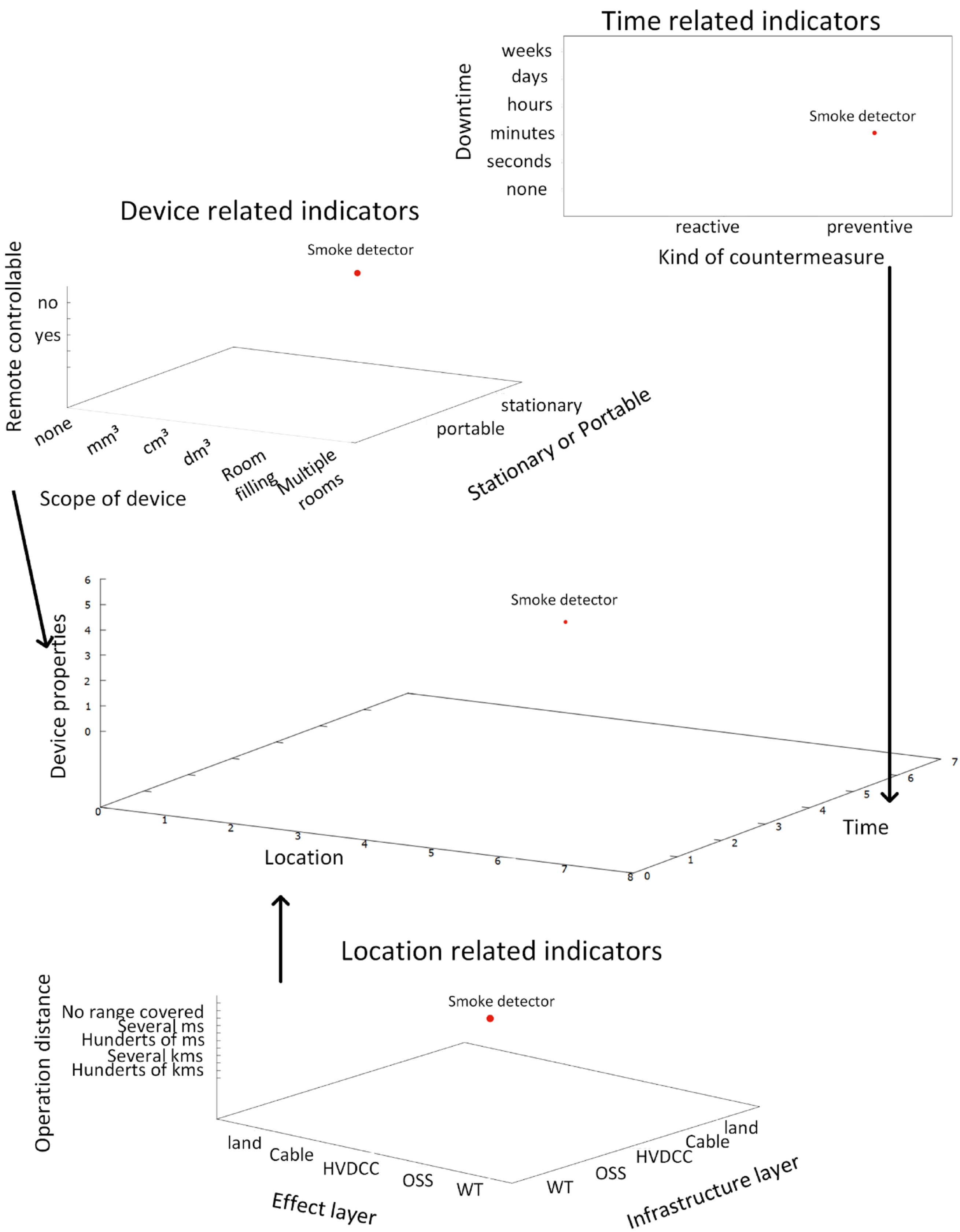


Fig. 2 Different options to visualize the indicatorsSource: Authors

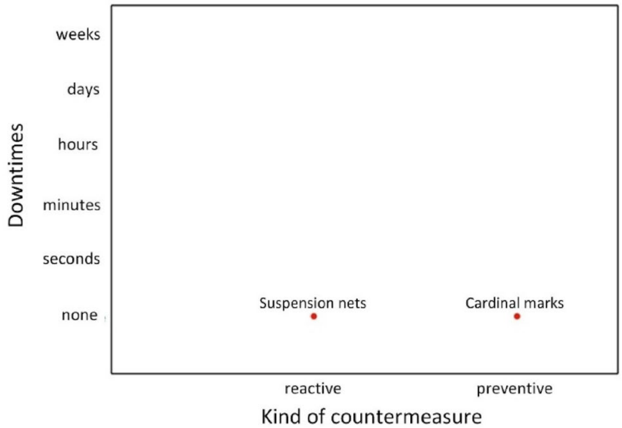


Fig. 3 Comparison of cardinal marks and suspension nets in regard to timeSource: Authors

this portfolio have been installed. For the comparison of the "performance criteria" and "financial expenditure" it needs to be said that a high-performance PPM with low financial expenditure is unlikely. Most effective PPMs are costly.

7 How the framework can contribute to critical infrastructure resilience

PPS and PPM receive growing attention in policy debate to enhance CI resilience. The European Union's 2022 directive on the resilience of critical entities for example mandates that critical infrastructure owners and operators take measures to ensure the resilience of their facilities, which includes measures to protect their facilities against physical threats (Rehak et al. 2024). The directive defines resilience as a critical entity's ability to "take technical, security and organisational measures (….) so as to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident (…) whether natural or man-made, accidental or intentional" (Resilience of critical entities 2022). In Germany, the draft critical infrastructure umbrella acts – which aims at implementing the EU's Critical Entities Resilience directive at the national level – includes provisions for infrastructure operators to enhance physical protection systems among other resilience measures (Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen 2024). Physical protection measures have also been introduced in the United States as part of efforts to enhance CI resilience, including through security management, security force, and information sharing (Petit et al.

Fig. 4 Comparison of cardinal marks and suspension nets in regard to the performance criteria-Source: Authors

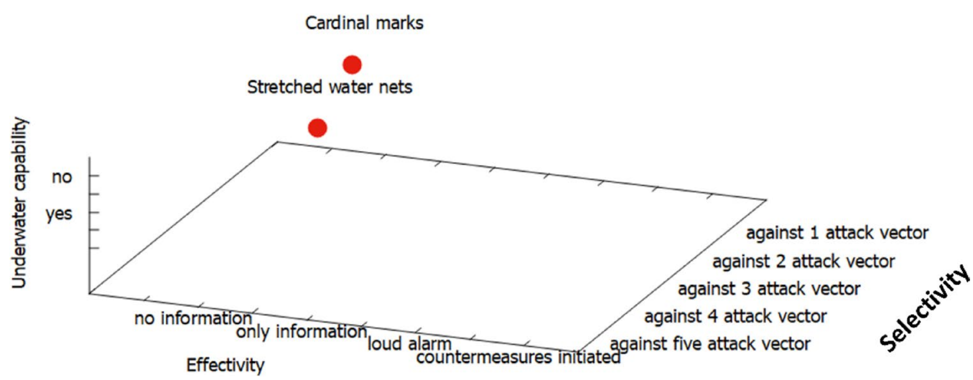
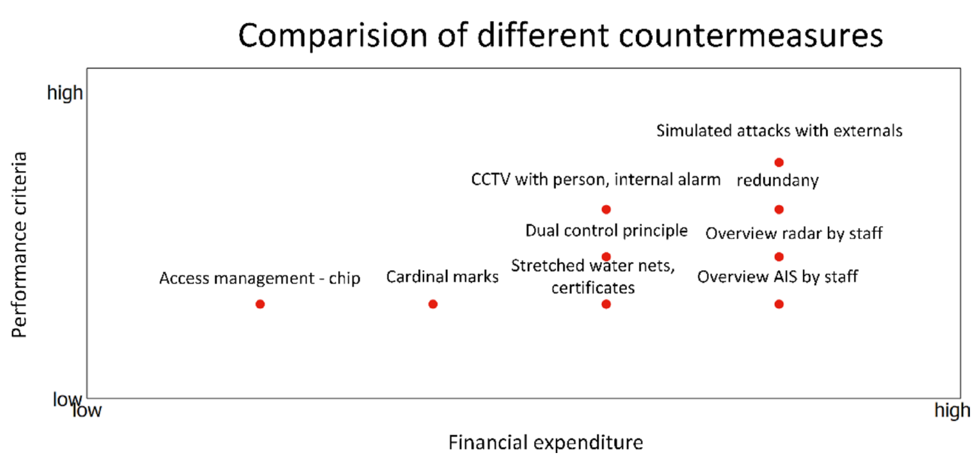


Fig. 5 Comparison of different countermeasuresSource: Authors



2013; Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience 2013).

Moste works on PPS consider terrestrial infrastructures, due to the abundance of terrestrial CI. Consequently, practical guidelines exist to design and analyze PPS and PPM for terrestrial CI, including for nuclear facilities (Baker & Benny, 2013; International Atomic Energy Agency 2021). Our paper, instead, considers the protective physical security measures for offshore infrastructures and especially OWFs. It can be used as a practical guideline for infrastructure operators and security managers.

The framework that we have developed can help the operator to determine the resistance of the OWF and to design comprehensive and more effective PPS to protect converter platforms or electricity cable networks against physical attacks and safety incidents. The indicator "Specialty", for example, provides information on how many attack vectors are covered by a PPM, thus allowing operators to uncover blind spots in their protection system, while the indicator "Sensitivity" describes how often an alarm is not triggered even though it should have been triggered, and the indicator "Specificity" captures the risk of false alarms. Moreover, the indicators developed in this paper allow operators to consider the financial and human resource aspects of PPS including the costs of specific PPMs.

Thus, the framework outlined in this paper provides a practical guide to plan and evaluate PPS and specific PPMs for OWF and other offshore CI that operators can use. The framework can also help the authorities to evaluate the PPMs and PPS of infrastructure operators, especially considering that such measures might soon become mandatory due to the EU's Critical Entities Resilience directive and relevant national legislation.

8 Conclusions and outlook

Maritime infrastructures are proliferating and expanding rapidly, and they are increasingly threatened by hybrid threats and attacks that are disguised as accidents and that blur the distinction between intentional attacks and unintentional accidents. With this work, the authors propose a framework to determine systematically the resilience capacity of possible PPMs. Based on multiple criteria such as costs or performance criteria the PPM can be semi- quantitatively evaluated. The framework has been applied to the offshore wind industry. Furthermore, it also aligns the PPM to existing protection goals of the offshore wind industry. It has a strong focus on maritime infrastructures but it might be possible to apply it partially to land based infrastructures, especially if they are built at and can be accessed from the sea. It is a holistic framework that can evaluate PPM from the safety andsecurity domains. Furthermore, also uncovered spots in the protection landscape can be determined and suitable PPM can be purposefully designed and developed using the framework developed in this paper.

The plan for future research is to validate the criteria and their characteristics with stakeholders in the offshore wind industry and to test them in through real-world experiments. The framework can also be adapted to other offshore industries and platforms.

Acknowledgements This conference contribution is part of the research project Applied Research on Resilience-driven Offshore Wind Farm Safety and Security (ARROWS) which is financed by the German Aerospace Centre.

Author contributions B.T. wrote the main manuscript text and prepared the figures and tables. J.S. supported during the development of the framework as well as wrote the abstract, introduction, Physical threats to maritime infrastructures and Physical protection measures for critical maritime infrastructures. A.N. wrote the section "How the framework can contribute to resilience". All authors reviewed the manuscript.

Funding Open Access funding enabled and organized by Projekt DEAL.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

References

Alamleh H, Karabacak B (2024) Exploring the Security Landscape of Underwater Positioning and Navigation Systems: An Attack Surface Analysis. In *2024 IEEE 49th Conference on Local Computer Networks (LCN)* (pp. 1–7). IEEE. https://doi.org/10.1109/LCN60385.2024.10639769

Antosch-Bardohn J (2021) *Kreativität für die Wissenschaft: Wie Sie kreative Methoden in Forschung und Lehre einsetzen. UTB: Vol. 5712*. Paderborn: Brill/Schöningh. Retrieved from https://elibrary.utb.de/doi/book/10.36198/9783838557120 https://doi.org/10.36198/9783838557120

Baker PR, Benny DJ (2013) The complete guide to physical security. CRC

Beckman R, Nguyen T, Ong J (2025) Possible actions by coastal States to protect their marine environment from oil tankers in the dark fleet. The International Journal of Marine and Coastal Law 40(1):3–30. https://doi.org/10.1163/15718085-bja10219

Blackburn G (2025), August 11 Finland charges officers of Russia-linked Eagle S ship that damaged undersea cables. *Euro.News*. Retrieved from https://www.euronews.com/2025/08/11/finland-charges-officers-of-russia-linked-eagle-s-ship-that-damaged-undersea-cables

Blöcher M, Kempmann A, Strunz B, Schmidt A, Flade F (2024), November 20 Chinesisches Schiff unter Verdacht: Zerstörte Ostsee-Kabel. *Tagesschau*. Retrieved from https://www.tagesschau.de/investigativ/ndr-wdr/ostsee-datenkabel-100.html

Brauner F, Maertens J, Bracker H, Mudimu OA, Lechleuthner A (2015) Determination of the effectiveness of security measures for low probability but high consequence events: A comparison of multi-agent-simulation & process modelling by experts. In L. Palen, M. Büscher, T. Comes, & A. Hughes (Chairs), *Iscram 2015: The 12th International Conference on Information Systems for Crisis Response and Management 24–27 May in Kristiansand, Norway*. Retrieved from https://idl.iscram.org/files/florianbrauner/2015/1322_FlorianBrauner_etal2015.pdf

Bremisches Polizeigesetz (2024)

Briguglio G, Crupi V (2024) Review on sensors for sustainable and safe maritime mobility. Journal of Marine Science and Engineering 12(2):353. https://doi.org/10.3390/jmse12020353

Bueger C (2022) Nord Stream pipeline sabotage: how an attack could have been carried out and why Europe was defenceless. Retrieved from https://theconversation.com/nord-stream-pipeline-sabotage-how-an-attack-could-have-been-carried-out-and-why-europe-was-defenceless-191895

Bueger C, Edmunds T (2024) Understanding maritime security. Oxford University Press, Oxford

Bueger C, Stockbruegger J (2024) Oceans, Objects, and infrastructures: making modern piracy. Global Stud Q 4(3). https://doi.org/10.1093/isagsq/ksae063

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2011) *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden*. Berlin. Retrieved from https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis-leitfaden.pdf?__blob=publicationFile&v=8

Caliskan M (2019) Hybrid warfare through the lens of strategic theory. Defence and Security Analysis 35(1):40–58. https://doi.org/10.1080/14751798.2019.1565364

Cui J, Liew LS, Sabaliauskaite G, Zhou F (2019) A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. Ad Hoc Networks 90:101823. https://doi.org/10.1016/j.adhoc.2018.12.006

Deutsche Windguard (2025) Status des Offshore-Windenergiezubaus in Deutschland: Erstes Halbjahr 2025. Retrieved from https://www.offshore-stiftung.de/dokumente/publikationen/Status-of-Offshore-Wind-Energy-Development_First-Half-2024_final.pdf

Eleftherakis D, Vicen R (2020) Sensors to increase the security of underwater communication cables: A review of underwater monitoring sensors. Sensors 20(3). https://doi.org/10.3390/s20030737

Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (2024)

European Commission EU funding for offshore renewables. Retrieved from https://energy.ec.europa.eu/topics/renewable-energy/financing/eu-funding-offshore-renewables_en

European Subsea Cable Association Subsea Cable Security Frequently Asked Questions (FAQs). Retrieved from https://www.escaeu.org/faqs/subsea-cable-security/

European Union The EU Blue economy report 2025: Marine renewable energy. Retrieved from https://op.europa.eu/webpub/mare/eu-blue-economy-report-2025/blue-economic-sectors/marine-renewable-energy.html

European Commission (2020) *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: An EU Strategy to harness the potential of offshore renewable energy for a climate neutral future*. Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0741

Felemban E, Shaikh FK, Qureshi UM, Sheikh AA, Qaisar SB (2015) Underwater sensor network applications: A comprehensive survey. International Journal of Distributed Sensor Netwerks 11(11):896832. https://doi.org/10.1155/2015/896832

Fennelly LJ (ed) (2016) Effective physical security. Butterworth-Heinemann

Flammini F, Gaglione A, Mazzocca N, Pragliola C (2009) Quantitative security risk assessment and management for railway transportation infrastructures. In: Setola R, Geretshuber S (eds) Lecture notes in computer Science. Critical information infrastructure security, vol 5508. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 180–189. https://doi.org/10.1007/978-3-642-03552-4_16

Gabriel A, Sill Torres F (2023) Navigating Towards Safe and Secure Offshore Wind Farms: An Indicator Based Approach in the German North and Baltic Sea. In J. Radianti, I. Dokas, N. LaLone, & D. Khazanchi (Chairs), *Information Systems for Crisis Response and Management*, Omaha. Retrieved from https://idl.iscram.org/files/gabriel/2023/2551_Gabriel+Torres2023.pdf

Gabriel A, Tecklenburg B, Sill Torres F (2022) Threat and Risk Scenarios for Offshore Wind Farms and an Approach to their Assessment. In R. Grace & H. Baharmand (Chairs), *19th International Conference on Information Systems for Crisis Response and Management*, Tarbes, France. Retrieved from https://idl.iscram.org/files/alexandergabriel/2022/2407_AlexanderGabriel_etal2022.pdf

Gireesh Kumar P, Tejaswini V, Kesava Rao P, Jaya Shankar G, (2021) Disaster mitigation and its strategies in a global context - a state of the Art. Mater Today: Proc 45:6488–6492. https://doi.org/10.1016/j.matpr.2020.11.369

Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen (2024), Geräusche, Erschütterungen und ähnliche Vorgänge

Hara D, Sagara H (2025a) Design of a robust physical protection system for offshore floating nuclear power plants against shipboarding threats: (1) vital area identifications. Joural of Nuclear Science and Technology 1–10. https://doi.org/10.1080/00223131.2025.2520424

Hara D, Sagara H (2025b) Design of a robust physical protection system for offshore floating nuclear power plants against shipboarding threats: (2) timeline analysis. Journal of Nuclear Science and Technology 1–13. https://doi.org/10.1080/00223131.2025.2532865

Hara D, Sagara H (2025c) A simulation study of hypervelocity jet underwater: physical protection design of offshore floating nuclear power plant against light torpedo threats. Journal of Nuclear Science and Technology 62(3):278–287. https://doi.org/10.1080/00223131.2024.2424522

Harish AV, Tam K, Jones K (2024) Literature review of maritime cyber security: the first decade. Maritime Technololgy and Research 7(2):273805. https://doi.org/10.33175/mtr.2025.273805

Hau E (2014) Windkraftanlagen. SpringerLink, Heidelberg. https://doi.org/10.1007/978-3-642-28877-7

Hobhouse C (2025) *On a war footing: Securing critical energy infrastructure*. Retrieved from https://www.iss.europa.eu/publications/briefs/war-footing-securing-critical-energy-infrastructure

Hölzl C (2012) *Mind Mapping: Vernetztes Denken als gehirngerechte Methode im Fremdsprachenunterricht* (Diplomarbeit). Karl-Franzens-Universität Graz, Graz. Retrieved from https://unipub.uni-graz.at/obvugrhs/download/pdf/224313?originalFilename=true

Iaiani M, Tugnoli A, Macini P, Mesini E, Cozzani V (2022) Assessing the security of offshore Oil&Gas installations using adversary sequence diagrams. Chemical Engineering Transactions 91385–390. https://doi.org/10.3303/CET2291065

International Atomic Energy Agency (2021) *Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities*. IAEA Nuclear Security Series No. 40-T. Vienna: IAEA. Retrieved from https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1875_web.pdf

Jouffray J–B, Blasiak R, Norström AV, Österblom H, Nyström M (2020) The blue acceleration: the trajectory of human expansion into the ocean. One Earth 2(1):43–54. https://doi.org/10.1016/j.oneear.2019.12.016

Kampova K, Lovecek T, Rehak D (2020) Quantitative approach to physical protection systems assessment of critical infrastructure elements: use case in the Slovak Republic. International Journal of Critical Infrastructure Protection 30:100376. https://doi.org/10.1016/j.ijcip.2020.100376

Kauranen A (2025), August 25 Suspects blame technical faults for Baltic Sea cable breaches. *Reuters*. Retrieved from https://www.reuters.com/business/media-telecom/suspects-blame-technical-faults-baltic-sea-cable-breaches-2025-08-25/

Köpke C, Schäfer-Frey J, Engler E, Wrede C P. (2020) A joint approach to safety, security and resilience using the functional resonance analysis method. 8th REA Symp Resil Engineering: Scaling Up Speeding Up. https://doi.org/10.15626/rea8.10

Köpke C, Mielniczek J, Roller C, Lange K, Torres FS, Stolz A (2023) Resilience management processes in the offshore wind industry: schematization and application to an export-cable attack. Environment Systems and Decisions 43(2):161–177. https://doi.org/10.1007/s10669-022-09893-9

Lampropoulos F, Daramouskas I, Perikos I, Paraskevas M (2023) Analysis of data from UAVs for surveillance and threat identification in maritime areas. In *2023 IEEE/ACIS 8th International Conference on Big Data, Cloud Computing, and Data Science (BCD)* (pp. 32–37). IEEE. https://doi.org/10.1109/BCD57833.2023.10466306

MacAskill A, Mitchell P (2013) Offshore wind-an overview. Wiley Interdisciplinary Reviews: Energy Environ 2(4):374–383. https://doi.org/10.1002/wene.30

Marroni G, Landucci G, Tamburini F, Bartolucci A, Kuipers S, Broekema W, Moreno C (2022) V. Development of equipment fragility models to support the security management of process installations. In M. C. Leva, E. Patelli, L. Podofillini, & S. Wilson (Eds.), *Proceedings of the 32nd European Safety and Reliability Conference*. Singapore: Research Publishing

Martini M, Guanche R, Losada IJ, Vidal C (2017) Accessibility assessment for operation and maintenance of offshore wind farms in the North sea. Wind Energy 20(4):637–656. https://doi.org/10.1002/we.2028

Mary Lynn Garcia (2008) *Design and Evaluation of Physical Protection Systems*. Elsevier. Retrieved from https://www.sciencedirect.com/book/9780750683524/design-and-evaluation-of-physical-protection-systems https://doi.org/10.1016/C2009-0-25612-1

McGuinness D (2025) German arrest warrant over Nord Stream blast mystery. Retrieved from https://www.bbc.com/news/articles/cnvyz1472rpo

Mišković D, Wang H (2025) Exploring the impact of the maritime regulatory framework on the barrier system in ship operations. Journal of Marine Science and Engineering 13(7):1361. https://doi.org/10.3390/jmse13071361

Moro N, Heydemann K, Dehbaoui A, Robisson B, Encrenaz E (2014) Experimental evaluation of two software countermeasures against fault attacks. In *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*

Munyai MP, Govender D (2024) Mitigation of security risks at maritime ports of entry. Journal of Transportation Security 17(1). https://doi.org/10.1007/s12198-024-00279-3

Musterbauordnung (2023)

Peterson ET (2006) *The Big Book of Key Performance Indicators: Book Two in the Web Analytics Demystified Series* (1st ed.). Retrieved from https://analyticsdemystified.com/wp-content/uploads/2019/01/The_Big_Book_of_Key_Performance_Indicators_by_Eric_Peterson.pdf

Petit FD, Bassett GW, Black R, Buehring WA, Collins MJ, Dickinson DC, Peerenboom JP (2013) *Resilience Measurement Index: An indicator of critical infrastructure resilience* (No. ANL/DIS-13-01). Retrieved from Argonne National Laboratory website: https://publications.anl.gov/anlpubs/2013/07/76797.pdf

Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience (2013)

Ramírez-Agudelo OH, Köpke C, Guillouet Y, Schäfer-Frey J, Engler E, Mielniczek J, Torres S, F (2021) An Expert-Driven probabilistic assessment of the safety and security of offshore wind farms. Energies 14(17):5465. https://doi.org/10.3390/en14175465

Rehak D, Slivkova S, Janeckova H, Stuberova D, Hromada M (2022) Strengthening resilience in the energy critical infrastructure: methodological overview. Energies 15(14):5276. https://doi.org/10.3390/en15145276

Rehak D, Splichalova A, Hromada M, Walker N, Janeckova H, Ristvej J (2024) Critical entities resilience failure indication. Safety Science 170:106371. https://doi.org/10.1016/j.ssci.2023.106371

Resilience of critical entities (2022)

Robak S, Raczkowski RM (2018) Substations for offshore wind farms: a review from the perspective of the needs of the Polish wind energy sector. Bulletin of the Polish Academy of Sciences: Tech Sci 66(4). https://doi.org/10.24425/124268

Saihi A, Ben-Daya M, As'Ad R (2022) An investigation of sustainable maintenance performance indicators: Identification, expert validation and portfolio of future research. IEEE Access 10:124259–124276. https://doi.org/10.1109/ACCESS.2022.3224450

Şengül B, Yılmaz F, Uğurlu Ö (2023) Safety–Security analysis of maritime surveillance systems in critical marine areas. Sustainability 15(23):16381. https://doi.org/10.3390/su152316381

Sill Torres F, Kulev N, Skobiej B, Meyer M, Eichhorn O, Schäfer-Frey J (2020) Indicator-based Safety and Security Assessment of Offshore Wind Farms. In *2020 Resilience Week (RWS)*

Speller I (2023) Understanding naval warfare. Routledge, London. https://doi.org/10.4324/9781003272151

Staib J (2024), November 22 Hinweis an Anker von chinesischem Frachter: Zerstörte Kabel in Ostsee. *Frankfurter Allgemeine*. Retrieved from https://www.faz.net/aktuell/politik/ausland/ostsee-kabel-zerstoert-drohne-zeigt-verdrehten-anker-von-chinesischem-frachter-110127385.html

Stockbruegger J (2021) US strategy and the rise of private maritime security. Security Studies 30(4):578–602. https://doi.org/10.1080/09636412.2021.1976821

Suchkov MA (2021) Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military, and political practice. Small Wars Insurgencies 32(3):415–440. https://doi.org/10.1080/09592318.2021.1887434

Tang KHD, Dawal M, S. Z., Olugu EU (2018) A review of the offshore oil and gas safety indices. Safety Science 109:344–352. https://doi.org/10.1016/j.ssci.2018.06.018

Tecklenburg B, Gabriel A, Sill Torres F (2023) Perception of threats in Offshore Windfarms and possible countermeasures. In M. P. Brito, T. Aven, P. Baraldi, M. Čepin, & E. Zio (Eds.), *Proceedings of the 33rd European Safety and Reliability Conference*. Singapore: Research Publishing

Tecklenburg B, Sill Torres F et al Validation of Human Centred Bayesian Networks - Case Study on a Cable Cut of an Export Cable of an Offshore Wind farm. In *Maria Chiara Leva, Edoardo, Patelli, Podofillini (Hg.)* (2025) *– Proceedings of the 32nd European.* https://doi.org/10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P9362-cd

TeleoGraphy Submarine Cable Frequently Asked Questions [Press release]. Retrieved from https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

The Maritime Executive (2023), April 26 Cargo Ship Arrives in Germany with Large Hole After Striking Wind Farm. *The Maritime Executive*. Retrieved from https://maritime-executive.com/article/cargo-ship-arrives-in-germany-with-large-hole-after-striking-wind-farm

Tho Pesch S (2015) Coastal state jurisdiction around installations: safety zones in the law of the sea. The International Journal of Marine and Coastal Law 30(3):512–532. https://doi.org/10.1163/15718085-12341361

Thompson C (2010) Integration of protection and control systems within an offshore windfarm environment. In *10th IET International Conference on Developments in Power System Protection (DPSP 2010). Managing the Change* (p. 145). IET. https://doi.org/10.1049/cp.2010.0267

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (2016)

Wang H, Liu Z, Wang X, Graham T, Wang J (2021) An analysis of factors affecting the severity of marine accidents. Reliablity Engineering & Systems Safety 210:107513. https://doi.org/10.1016/j.ress.2021.107513

Wielgosz M, Malyszko M (2025) A method for early identification of vessels potentially threatening critical maritime infrastructure. Applied Sciences 15(15):8716. https://doi.org/10.3390/app15158716

Woolliscroft P, Jakábová M, Krajcovicová K, Púciková L, Cagánová D, Čambál M (2013) Global key Performance Best Practice. In M. T. Semmelrock-Picej & A. Novak (Chairs), *European Conference on Management, Leadership & Governance*, Klagenfurt, Austria. Retrieved from https://www.proquest.com/openview/e6070a317cfda0a3be628c48bd2202c4/1?cbl=1796418&pq-origsite=gscholar&parentSessionId=U71KAtBAWl2nGXcpsADuOFqSvlqy5QOTi7rEhyYViFA%3D

Zehfuß J (2020) *Leitfaden Ingenieurmethoden des Brandschutzes*. Münster, Braunschweig. Retrieved from https://www.vfdb.de/media/doc/technischeberichte/TB_04_01_Leitfaden_IngMethoden_4Auflage_2020-03-26.pdf

Zweite Verordnung zur Änderung der BSI-Kritisverordnung (2021) Bundesgesetzblat Teil I 4163