Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26246-cd

A framework for designing security zones in Offshore Wind Farms

Sarra Majri

Department for Resilience of Maritime Systems, Institute for the Protection of Maritime Infrastructures, German Aerospace Center (DLR). E-mail: sarra.majri@dlr.de

Jan Stockbrügger

Department for Resilience of Maritime Systems, Institute for the Protection of Maritime Infrastructures, German Aerospace Center (DLR). E-mail: jan.stockbruegger@dlr.de

Frank Sill Torres

Department for Resilience of Maritime Systems, Institute for the Protection of Maritime Infrastructures, German Aerospace Center (DLR). E-mail: Frank.SillTorres@dlr.de

Offshore Wind Farms (OWFs) are critical maritime infrastructures and play a key role in the green energy transition generating sustainable clean energy. Unlike terrestrial infrastructures like power plants, OWFs lack physical barriers such as fences, making conventional security measures ineffective or impractical. Therefore, defining appropriate security zones is essential to mitigate security risks. This paper proposes a probabilistic time-based framework to model attack and intervention times for determining both the temporal and spatial dimensions of OWF security zones. The framework integrates a vulnerability analysis to identify critical and exposed components of the infrastructure, which forms the basis for determining the recommended locations and size of security zones. Within this framework, a way-time diagram represents the potential attack–intervention process and considers the attack vector. Based on these phases, attack and intervention times are estimated using kinematic equations. To capture the inherent variability and uncertainties in attack velocities, Monte Carlo simulation is employed. This approach generates numerous random samples of kinematic parameters within realistic bounds, producing a distribution of possible intervention times rather than a single deterministic value. By analyzing these distributions, the framework probabilistically estimates required intervention times under different attack scenarios and uses these results to dimension corresponding security zones. This methodology represents an initial step toward defining dynamic security zones for offshore environments. Future research will extend this model by integrating different types of physical barriers, their stopping capabilities and how this influence required reaction and attack times.

Keywords: Offshore Wind Farm, Attack and Intervention time, Monte Carlo, Security zones, Framework.

1. Introduction

Offshore wind farms (OWF) play a critical role in the global energy transition producing clean and sustainable electricity. In 2024 OWF generated over 83 gigawatts of power, that is enough to supply more than 73 million households (GWEC 2025). Their deployment is rapidly increasing worldwide and because of that, protecting them against attacks, especially physical attacks, becomes essential. This growing importance is underscored by recent incidents in the North Sea and the Baltic Sea, where several maritime infrastructures were most likely sabotaged, resulting in damages. Notable examples include the Nord Stream pipeline, the C-Lion1 cable and the EstLink 2. In addition, the incident involving the vessel PETRA L, which collided with an offshore wind turbine, highlights the vulnerability of these installations to both safety and security threats.

While no documented attacks on offshore wind parks have been confirmed (as of December 2025), the potential for terrorist, pirate or hybrid attacks remains a serious concern (Köpke, et al. 2023).

Media reports further indicate growing interest in targeting these facilities. For instance, one report describes a vessel that disabled its AIS and

approached an offshore wind park under the guise of conducting hydrographic surveys, potentially for espionage on submarine cables, military infrastructure or wind farm operations. This aligns with a statement by the former German General Hans-Werner Wiermann, who warned that such actors could cause significant damage and escape undetected (tagesschau 2024).

These developments underscore the need for a systematic approach to defining security zones based on the temporal dynamics of attacks and response times, as well as the vulnerability of critical infrastructure components. The framework proposed in this paper addresses this need by integrating time-based risk modelling with vulnerability assessment.

The paper is structured into six sections. Section 2 provides a short literature review on offshore wind park security and risk-based protection approaches. Section 3 introduces and explains the proposed framework. In Section 4, the framework is applied for an exemplary demonstration. Section 5 discusses the results and limitations. Finally, Section 6 concludes the paper and outlines directions for future research.

2. Literature Review

Regarding the security of OWFs publications on protection systems, vulnerability assessments and risk assessments exists. To lay the foundation for the proposed framework, this section outlines key concepts related to OWFs, physical protection systems, vulnerability assessment and time-based risk modelling.

2.1. *Offshore wind farm infrastructure*

An OWF is a complex infrastructure composed of multiple interconnected components that work together to generate and transmit electricity. At its core, an OWF consists of wind turbines, underwater cables, offshore substations and High Voltage Direct Current platforms. Beyond these components, the internal electrical grid, is a critical element of OWF design. This grid connects individual wind turbines to the offshore substation and is typically implemented as an alternating current collection system. Common topological configurations include radial, ring and star-shaped layouts. These configurations influence operational reliability and security (Fjellstedt 2023). This structural complexity directly influences the vulnerability of the OWF and, consequently, the design of security zones.

2.2. Physical protection system

Physical Protection Systems (PPS) are widely used in land-based settings to protect against theft, sabotage or attacks. The design of PPS typically consists of three steps: threat detection, delay and response (Garcia 2008).

The implementation of a PPS requires the allocation of resources and is therefore very cost sensitive. The effectiveness of a PPS describes its ability to prevent or interrupt a potential attack before the protected asset is compromised. In addition to these core functions, deterrence plays a role in security design. According to Garcia (2008), deterrence is considered as a secondary function, as its effect is difficult to quantify. Nevertheless, it can be significant, since the visible presence of protective measures may discourage attacks while simultaneously providing protection in the event that an attack occurs.

An important principle by PPS design is the concept of defense in depth. Defense in depth refers to the use of multiple layers of protection, realized through physical barriers, detection systems and controlled zones. The aim is to increase the time required for an adversary to reach a protected asset, thereby improving the probability that detection and response occur before a successful attack is completed. (Gregoire 2023)

2.3 *Vulnerability assessment*

Vulnerability assessment constitutes a central element of security analysis and PPS design and evaluation (Garcia 2008). The aim is to identify critical components. It is a process to identify and quantify risk sources and how they affect a system's operation. In general, it is divided in three steps: planning the assessment, conducting it and reporting and using its results. It is a part of a risk assessment and can also be used predict PPS component performance and overall system effectiveness by identifying exploitable weaknesses for a defined threat. (M. L. Garcia 2025).

According to Diaz-Sarachaga and Jato-Espino (2020), vulnerability assessment takes into account physical, social, economic and environmental issues and vulnerabilities and how they

interact, increasing the susceptibility of communities and facilities to hazards (similar to ISO 23000). Other methodological approaches like FRAM, scenario-based analyses and multi-criteria decision methods exist as well. These methods differ in scope and level of detail but have the same objective of identifying where, why and how a system is vulnerable.

2.4. Probabilistic models in security evaluation

Several publications have used probabilistic modelling to assess the effectiveness of assessments to protect assets and to enhance decision making under uncertainty.

An early example is the work of Martz (1987), who developed probabilistic system analysis models to evaluate the protection of valuable assets against overt terrorist attacks. Their MS-codes model scenarios such as ambushes on road convoys and attacks on fixed-site facilities. The objective of this work was to support resource allocation by ranking sensitive areas according to their survivability under a hypothesized attack. In this context, time plays an essential role, as the models consider how long an adversary requires to overcome protective measures and barriers.

McGill et al (2007) proposed a framework and risk assessment for decision making for critical infrastructure protection based on five steps. One step is to evaluate the threat likelihood, including capturing adversary tendencies to shift their preferences response to security investments. In this work, threat intensity is also considered based on Martz (1987).

Building on this line of research, Jang et al. (2009) applied probabilistic methods to evaluate the effectiveness of Physical Protection Systems. Their approach estimates the probability of interruption along vulnerable paths and depends on variables related to detection, delay and response. The analysis is based on heuristic methods and predefined attack paths through the protection system.

Next, Ramírez-Agudelo et al. (2021) provide a probabilistic approach for assessing safety and security risks for OWP based on Bayesian network modelling. Their method focuses on structuring and formalizing expert knowledge by representing safety- and security-relevant functions and their interdependencies within a graphical probabilistic model. This allows the authors to capture causal relationships between different system functions and to analyses how failures or degradations in one function may propagate through the overall system. Tecklenburg et al., moreover, develop a framework to analyses physical protection measures for maritime infrastructures and to protect critical assets such as converter platforms that sustain the overall system.

Lichte et al. (2023) address the challenge of uncertainty in scenario likelihood for security risk analysis. They used a unified time-based and probabilistic metric for detection and intervention for attack path analysis. For the attack path, they used two spatial elements, zones and barriers, which represent the effective area of measures, differentiating between different zones, like protected, observed and intervention zones.

However, differences exist between these models and the framework proposed in this paper. Most existing models explicitly rely on physical barriers and predefined attack paths. In offshore environments, such assumptions are only partially possible, as attacks may occur from the open sea without clearly defined paths. Furthermore, while time is a central variable in the models discussed here, probabilistic sampling methods such as Monte Carlo simulation are not often used to generate distributions of attack and intervention times.

3. Framework

This section presents the proposed framework for modeling attack and intervention times in order to calculate the dimension of security zones for OWFs. In this paper, the term framework is used in line with Binder et al. (2013) and McGinnis and Ostrom (2014) referring to a structured set of concepts, assumptions and analytical approaches. The framework integrates vulnerability assessment, scenario-based threat modeling and probabilistic time-based analysis to support security design decisions for offshore wind infrastructure.

3.1. *Describing the framework*

An overview of the framework is provided in Figure 1. The modelling of security zones begins with a vulnerability assessment to identify critical components within the OWF.

OWFs consist of numerous interconnected elements and not all components are equally important for OWF functionality. Identifying where and why the system is vulnerable is therefore important.

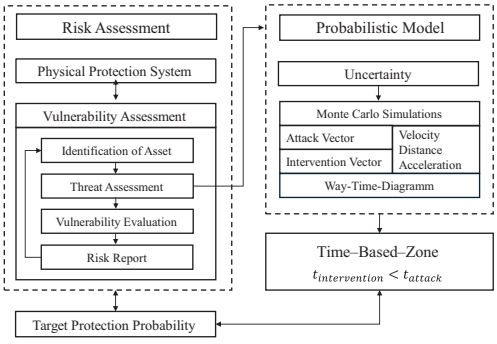

Figure 1: Framework to design security zones

This is consistent with approaches in risk analysis and resilience management, where the identification of critical assets forms the basis for further threat and consequence analysis (Francis and Bekera 2013).

A key step in the vulnerability assessment is the identification of attack vectors, which can be linked to scenario-based analysis. By combining the attractiveness of an asset with the capability of an adversary, the framework can generate plausible attack scenarios (Moteff 2007). In this framework, detailed adversary tactics are not modelled, since the primary goal is to quantify time margins rather than identify exact attack behaviors. It is sufficient to assume that an attack occurs along a defined vector.

For each scenario, three main parameters are required for both the adversary and the intervention. These are distance, velocity and acceleration. Environmental influences, maneuvering behaviors and detailed motion dynamics are not explicitly modelled but are treated as sources of uncertainty addressed through probabilistic analysis. Using this information, the framework calculates the probability that an intervention reaches the infrastructure in time to stop the adversary, thereby informing the dimensioning of security zones.

Time is calculated using the standard kinematic equation for uniformly accelerated motion. This formula allows for the calculation of the required time for both stationary and moving vehicles. Uniform acceleration is assumed due to the high uncertainty in real-world offshore scenarios, while Monte Carlo simulation generates a wide range of possible outcomes by sampling input parameters from predefined distributions. This produces a distribution of attack and intervention times rather than a single deterministic value.
The output of the Monte Carlo simulation is used to define time- and distance-based security zones. A security zone is defined as the spatial area around a critical asset within which intervention forces must achieve a predefined protection probability by preventing an adversary from reaching and compromising the asset. By varying distances and comparing attack and intervention times, the framework derives the size and shape of these zones, taking into account variability in distance, velocity and response delays.

In contrast to detection-focused models, this approach assumes that detection, identification and localization of the attacking object have already been achieved. The key principle for defining security zones is that the intervention time must be less than the attack time.

By performing thousands of simulations, the framework allows for the estimation of the probability of successful intervention under different scenarios, producing robust time margins and facilitating the design of security zones that reflect realistic operational constraints.

In addition to the technical modelling components, the framework incorporates a decision-oriented parameter referred to as the target protection probability. This parameter defines the acceptable likelihood that an intervention successfully prevents an attack by disrupting the adversary pathway. The target protection probability links vulnerability assessment and risk evaluation with the time-based modelling results. While vulnerability assessment identifies critical assets and potential consequences, the probabilistic time model estimates achievable protection performance. By combining both perspectives, the framework enables the derivation of security zones that reflect not only technical feasibility but also risk acceptance and protection objectives.

4. Applications

To demonstrate the proposed framework, we assume the key parameters from Table 1. The parameter values used in this illustrative application are based on simplified assumptions and are intended solely to demonstrate the methodological workflow of the framework. They are not intended to represent realistic operational conditions.

Table 1: Used values for the example

Parameters:	Adversary:	Intervention:
Distance [km]:	3	8
Acceleration [km/h]:	0,1 – 5	0,1 – 3

Based on these input parameters, velocities and travel times were calculated using the kinematic equation for uniformly accelerated motion.
To account for uncertainty in operational conditions, Monte Carlo simulation was applied using 10 000 samples for both adversary and intervention scenarios.

After performing the sampling procedure, the resulting travel time distributions were analyzed. The statistical characteristics of both adversary and intervention times are summarized in Table 2.

Table 2: Statistical characteristics of simulated travel times

Statistic:	Adversary [min]:	Intervention [min]:
Mean:	47,88	72,85
Median:	38,16	70,46
Minimum:	27,24	57,40
Maximum:	192,06	99,41

The fastest time to reach the asset for the adversary is 27 min and the slowest is 192 min, indicating a large variety of possible attack scenario time frames. For the intervention, on the other hand, the fastest time to reach a target is 57 min and the slowest time is 99 min. This shows that there is possible time space of 134,66 min in which the intervention unit reaches the target before the adversary.

To evaluate system effectiveness, adversary and intervention travel times were directly compared for each Monte Carlo iteration. The probabilistic comparison revealed that in 86.76 % of simulated scenarios, the adversary reaches the asset before intervention forces can respond. This result indicates that the initially assumed deployment configuration does not provide sufficient protection reliability.

To analyses how spatial configurations influence intervention success probability, the adversary starting distance was incrementally increased while maintaining identical simulation assumptions. The resulting intervention success probabilities are shown in Table 3.

Table 3: Intervention Success Probability for different adversary distances

Distance [km]:	4	6	8	10
Probability [%]:	18,2	29,2	37,43	49,1

The results demonstrate that increasing the distance between the adversary starting point and the protected asset improves the probability of successful intervention. However, even at a distance of 10 km, the intervention success probability remains only approximately 50 %, indicating that the system still operates at a relatively high vulnerability level.

The primary objective of the proposed framework is to derive the design of security zones based on probabilistic time margins between adversary and intervention forces. To achieve this, a target protection probability must be defined. For this illustrative application, a protection reliability of 95 % successful intervention is assumed as a design criterion. The results therefore indicate that either larger spatial separation, faster intervention deployment or additional protective measures would be required to achieve the desired level of asset protection. To further analyses the relationship between spatial separation and protection performance, additional adversary distances were simulated and visualized in figure 2.

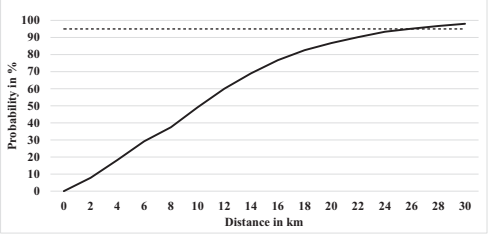

Figure 2: Intervention Success Probability vs. Distance

Figure 2 illustrates the relationship between adversary starting distance and intervention success probability. The results show a clear increase in protection performance with increasing distance between adversary and asset.

The intersection between the success probability curve and the predefined target protection probability represents the minimum required security zone radius. Based on the simulated

parameter set, the target protection probability of 95 % is reached at approximately 26 km. Consequently, the critical asset in this case would need a security zone of at least 26 km under the given modelling assumptions.

5. Discussion

The application demonstrates that probabilistic time-based modelling is a valuable tool for designing security zones in OWPs. Intervention success is highly sensitive to the spatial relationship between the adversary and the protected asset. Even small increases in adversary distance can improve the probability of a successful intervention.

A central contribution of the framework is the integration of vulnerability assessment with time-based simulations. By identifying critical assets first, the framework ensures that resources are prioritized effectively according to risk exposure. The definition of a target protection probability also plays a key role. This approach also allows for flexible adaptation to different offshore layouts, adversary characteristics and operational conditions. Nevertheless, several limitations exist:

- Simplified motion assumptions: Uniform acceleration is assumed, neglecting hydrodynamics, currents and complex vessel maneuvering.
- Detection is instantaneous: The model does not incorporate potential delays in detection, identification or localization, which could affect intervention timing.
- Demonstration parameter values: Input parameters were illustrative and not operationally validated, so results represent methodological illustration rather than real-world security performance.

Despite these limitations, the framework provides insight into offshore security zone design planning, showing how probabilistic modelling supports structured decision-making.

6. Conclusion and Outlook

This paper presented a probabilistic time-based framework for designing security zones in offshore wind farms. By combining vulnerability assessments, scenario-based threat modelling, kinematic motion modelling and Monte Carlo simulation, the framework provides a structured method to support evidence-based security planning for critical maritime infrastructure.

The application demonstrates that the distance between adversary and asset is a critical factor for intervention success. Probabilistic simulation allows the identification of minimum distances required to meet target protection levels, translating abstract timing metrics into actionable spatial security planning.

The study suggests further research in the following areas to extent the model:

- Incorporating detection and monitoring system performance into the model.
- Integrating environmental influences and realistic vessel maneuvers.
- Integrating deterrence mechanisms to increase adversary delay and improve intervention effectiveness.
- Optimizing the allocation of intervention units using algorithmic decision support.
- Validating the framework with operational data from offshore wind farms or maritime authorities.
- Developing adaptive security zones that adjust dynamically to threat levels, operational conditions or available intervention resources.

Overall, the framework bridges vulnerability assessments and operational security design, offering a transparent and reproducible methodology for offshore wind farm protection under uncertainty. This approach is relevant in a time of hybrid threats.

References

Binder, Claudia R., Hinkel Jochen, Bots Pieter W. G., and Pahl-Wostl Claudia. 2013. “Comparison of Frameworks for Analyzing Social-Ecological Systems.” *Ecology and Society* 18 (4). https://www.ecologyandsociety.org/vol18/iss4/art26/

Diaz-Sarachaga, Manuel Jose, and Jato-Espino Daniel. 2020. “Analysis of Vulnerability Assessment Frameworks and Methodologies in Urban Areas.” *Natural Hazards* 103: 437–457. https://doi.org/10.1007/s11069-019-03805-y.

Fjellstedt, Christoffer. 2023. *Grid Connection of Offshore Renewable Energy Sources*. Uppsala: Uppsala University. https://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-496087.

Francis, Royce, and Bekera Behailu. 2013. "A Metric and Frameworks for Resilience Analysis of Engineered and Infrastructure Systems." *Reliability Engineering & System Safety* 121: 90–103. https://doi.org/10.1016/j.ress.2013.07.004.

Garcia, Mary Lynn. 2008. Design and Evaluation of Physical Protection Systems. Elsevier. doi: https://doi.org/10.1016/C2009-0-25612-1.

Garcia, Mary Lynn. 2025. Vulnerability Assessment of Physical Protection Systems. Elsevier.

Gregoire, Olivier. 2023. "The Application of Defence in Depth in Nuclear Security." Paper presented at the 42nd Annual Conference of the Canadian Nuclear Society, Canada.

Jang, Sung Soon, Sung-Woo Kwak, Hosik Yoo, Jung-Soo Kim, and Wan-Ki Yoon. 2009. "Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection Effectiveness (SAPE)." *Nuclear Engineering and Technology* 41 (6): 747–752.

Köpke, Corinna, Mielniczek Jennifer, Roller Christoph, Lange Kerstin, Sill Torres Frank and Stolz Alexander. 2023. "Resilience management processes in the offshore wind industry: schematization and application to an ex-port cable attack." *Environment Systems and Decisions* 161-177. doi: https://doi.org/10.1007/s10669-022-09893-9.

Martz, Harry F., and Johnson Mark E. 1987. "Risk Analysis of Terrorist Attacks." *Risk Analysis* 7 (1): 35-47.

McGill, William L., Bilal M. Ayyub, and Mark Kaminskiy. 2007. "Risk Analysis for Critical Asset Protection." *Risk Analysis* 27 (5): 1265–1281. https://doi.org/10.1111/j.1539-6924.2007.00955.x

McGinnis, Michael D., and Elinor Ostrom. 2014. "Social-Ecological System Framework: Initial Changes and Continuing Challenges." *Ecology and Society* 19 (2). http://dx.doi.org/10.5751/ES-06387-190230

Moteff, John. 2007. Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences. Washington, DC. https://digital.library.unt.edu/ark:/67531/metadc812925/.

Ramírez-Agudelo, Oscar Hernán, Corinna Köpke, Yann Guillouet, Jan Schäfer-Frey, Evelin Engler, Jennifer Mielniczek, and Frank Sill Torres. 2021. "An Expert-Driven Probabilistic Assessment of the Safety and Security of Offshore Wind Farms." *Energies* 14 (17). https://doi.org/10.3390/en14175465

tagesschau. 2024. Systematische Spionage in der Ostsee. September 25. Accessed January 05, 2026. https://www.tagesschau.de/investigativ/ndr-wdr/russland-ostsee-spionage-100.html.

Tecklenburg, B., J. Stockbruegger, A. Niemi, and F. Sill Torres (2025). Securing maritime infrastructures: a framework to evaluate physical protection measures for offshore wind farms. Environmental Systems and Decisions 45, 1– 17.

Global Wind Energy Council (GWEC). 2025. "Offshore Wind Installed Capacity Reaches 83 GW as New Report Finds 2024 a Record Year for Construction and Auctions." Accessed March 15, 2026. https://www.gwec.net/news/offshore-wind-installed-capacity-reaches-83-gw-as-new-report-finds-2024-a-record-year-for-construction-and-auctions.