Environment Systems and Decisions (2023) 43:161–177
https://doi.org/10.1007/s10669-022-09893-9

Resilience management processes in the offshore wind industry: schematization and application to an export-cable attack

Corinna Köpke[1] · Jennifer Mielniczek[2] · Christoph Roller[1] · Kerstin Lange[3] · Frank Sill Torres[4] · Alexander Stolz[5]

Accepted: 26 December 2022 / Published online: 16 January 2023

Abstract
Offshore wind energy (OWE) production is a crucial element for increasing the amount of renewable energy. Consequently, one can observe a strong and constant rise of the OWE industry, turning it to an important contributor of national energy provision. This trend, however, is accompanied by increasing pressure on the reliability, safety, and security of the OWE infrastructure. Related security threats are characterized by high uncertainty regarding impact and probability leading to considerable complication of the risk assessment. On the other hand, the resilience concept emphasizes the consideration of the system's response to such threats, and thus, offers a solution for dealing with the high uncertainty. In this work, we present an approach for combining the strengths of risk and resilience management to provide a solution for handling security threats in OWE infrastructures. Within this context, we introduce a quality assessment enabling the quantification of the trustworthiness of obtained results.

Keywords Offshore wind · Security · Resilience · Risk assessment · Key performance indicator

1 Introduction

With annual growth rates of nearly 30%, the offshore wind industry continuously increases its importance for the energy provision (O'Sullivan 2020). In 2019, the World Forum Offshore Wind (WFO) listed a cumulative global offshore wind power capacity of 27.2 GW, with a growth of 24% as compared to 2018 (WFO 2020). In 2019, the total offshore wind energy production in Europe was 67 TWh, which corresponded to 2.3% of the total EU electricity consumption (Komusanac et al. 2020). Furthermore, it is predicted that by 2030 the offshore wind power will be responsible for 8% of the total ocean economy adding 230 billion USD of value (OECD 2016).

Offshore Wind Farms (OWF) are typically composed of several wind turbines, for Germany ranging from 12 (Alpha ventus 2022) to 80 (Global Tech1 2022), connected via one offshore substation that bundles all produced energy and via cabling to the shore. Being key elements of the offshore wind energy infrastructure, OWF are facing numerous safety and security threats. This is mainly resulting from their complexity as infrastructure, their harsh environment as well as being a potential target of an attack because of their role as important power generation system. Several

✉ Corinna Köpke
Corinna.Koepke@emi.fraunhofer.de

Jennifer Mielniczek
j.mielniczek@entrawind.com

Christoph Roller
Christoph.Roller@emi.fraunhofer.de

Kerstin Lange
kerstin.lange@jade-hs.de

Frank Sill Torres
Frank.SillTorres@dlr.de

Alexander Stolz
alexander.stolz@mail.inatech.uni-freiburg.de

[1] Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI, Am Klingelberg 1, 79588 Efringen-Kirchen, Germany

[2] Safety Engineer (Freelancer), Hedwig-Augustin-Str. 27, 25348 Glückstadt, Germany

[3] Jade University of Applied Sciences Wilhelmshaven Oldenburg Elsfleth, Weserstr. 52, 26931 Elsfleth, Germany

[4] German Aerospace Center, Institute for the Protection of Maritime Infrastructures, Fischkai 1, 27572 Bremerhaven, Germany

[5] Albert-Ludwigs-Universität Freiburg, Emmy-Noether-Straße 2, 79110 Freiburg im Breisgau, Germany

reported incidents support this observation. First of all, failing components are a recurring obstacle in OWF. For example, in Carroll et al. (2016) the maintenance data of about 350 offshore wind turbines located in several European OWF have been analyzed and an average failure rate of approximately ten failures per offshore wind turbine per year have been extracted. In Crabtree et al. (2015) similar values for OWF in Great Britain are reported. Still, OWF possess well-established maintenance processes such that common failures pose no real threat to the functionality of the OWF. Given the number of operators and especially human resources involved in maintenance processes, makes OWF a socio-technical infrastructure.

In contrast, unforeseen events can have more severe consequences. For example, in 2009 three out of eight circuit breakers failed at the same time on the land side substation of the OWF "West Wind" near Wellington, New Zealand. Consequently, for a short period of time the power of the voltage output dropped below a required threshold, leading to a brief interruption of service in Wellington (Brown 2012). In 2019, a lightning stroke the transmission network in Great Britain. The following simultaneous shutdown of a gas-fired power plant and the OWF "Hornsea" lead to a nearly one hour of power down affecting more than one million users (The Guardian 2020).

Despite the fact that there have been no reported physical and cyber-attacks against OWF, there is a large threat potential to this maritime infrastructure just as for any other major energy infrastructure. Single substations distribute similar amounts of energy as centralized plants such as lignite, coal, natural gas, or nuclear power plants (see Deutsche Wind Guard 2022; Bundesnetzagentur 2022 and Table 1). Consequently, the OWFs are similarly critical in case of breakdown and thus pose similar attractiveness for attacks. This includes terrorist attacks, pirate attacks, or hybrid attacks as discussed in Masala and Tsetsos (2013) and Savolainen et al. (2019). Similarly, there is a rising interest in the susceptibility against terrorist cyber-attacks and cyber-crime. Especially the Moller–Maersk case in 2017, that was likely a consequence of governmental organized cyber-crime against the Ukraine (Hopcraft and Martin 2018; Associated Press 2020), gained much attention not only in the maritime business. Cyber-threats for OWF gain increased attention by recent research studies but also by the certifiers for this branch of industry (Staggs et al. 2017; Freudenberg 2018).

Table 1 Comparison of energy producers in Germany, *till 2025 two additional with up to 0.9 GW, till 2030 additional 6 with up to 2.0 GW

Power plant	Lignite	Coal	Natural gas	Nuclear power	OWF
Total net [GW]	18.9	19.0	32.1	4.1	7.8
Number	53	90	710	3	27
Top 3 [GW]	0.9–1.1	0.8–1.1	0.6–0.8	1.3–1.4	0.4–0.5*

Data taken from (Deutsche Wind Guard 2022; Bundesnetzagentur 2022)

One way to handle such threats in complex socio-technical systems such as OWF is focusing on its resilience, which can be understood as the "ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management" (UNISDR 2009). Following this general definition, resilience can be understood not only as a conceptual approach but also as a quantifiable measure, e.g., as discussed in Deutsche Post DHL Group (2021) and Häring et al. (2016). The corresponding resilience cycle describes the system's ability to behave in a resilient way as function of time. It is divided into five phases, i.e., prepare, prevent, protect, respond, and recover (Edwards 2009; Thoma 2014).

On the other hand, risk management is a common practice in industry to address threats with respective measures, e.g., by employment of the ISO standard 31000:2018 (2018). It describes a process that comprises five steps, i.e., context analysis, risk identification, risk analysis, risk evaluation, and risk treatment. Based on this process, in Häring et al. (2017) a resilience management process, which consists of nine main steps, is presented. These are (1) context analysis, in which the system of interest including its stakeholders is described, (2) system analysis, during which the system is modeled. The resulting model, e.g., a mathematical model, flow model, network model (Hiermaier et al. 2017), agent-based model (van Dam et al. 2013), or probabilistic model (Stroeve et al. 2009) is a simplification of the natural environment and processes. The next steps identify as (3) system performance functions and (4) possible threats and disruptions. In step (5), the combination of threats and system functions is analyzed, followed by step (6) overall resilience quantification, which considers not only the disruption but also the recovery of the system. In step (7) resilience and cost evaluation, mitigation options are simulated and compared. Finally, in steps (8) and (9), mitigation options are selected and implemented in the system of interest. This nine-step approach has been applied in various fields summarized in Häring et al. (2021) and in Fig. 1 it is presented how the nine steps fall into the main pillars of classical risk assessment (RA).

In this paper, we propose an extended risk management process (see Fig. 1) which extends the classical RA by the assessment of the quality of the RA in terms of reliability of the data and studies. This extended methodology is motivated by the need to consider dynamics in socio-technical systems and the uncertainty of treats

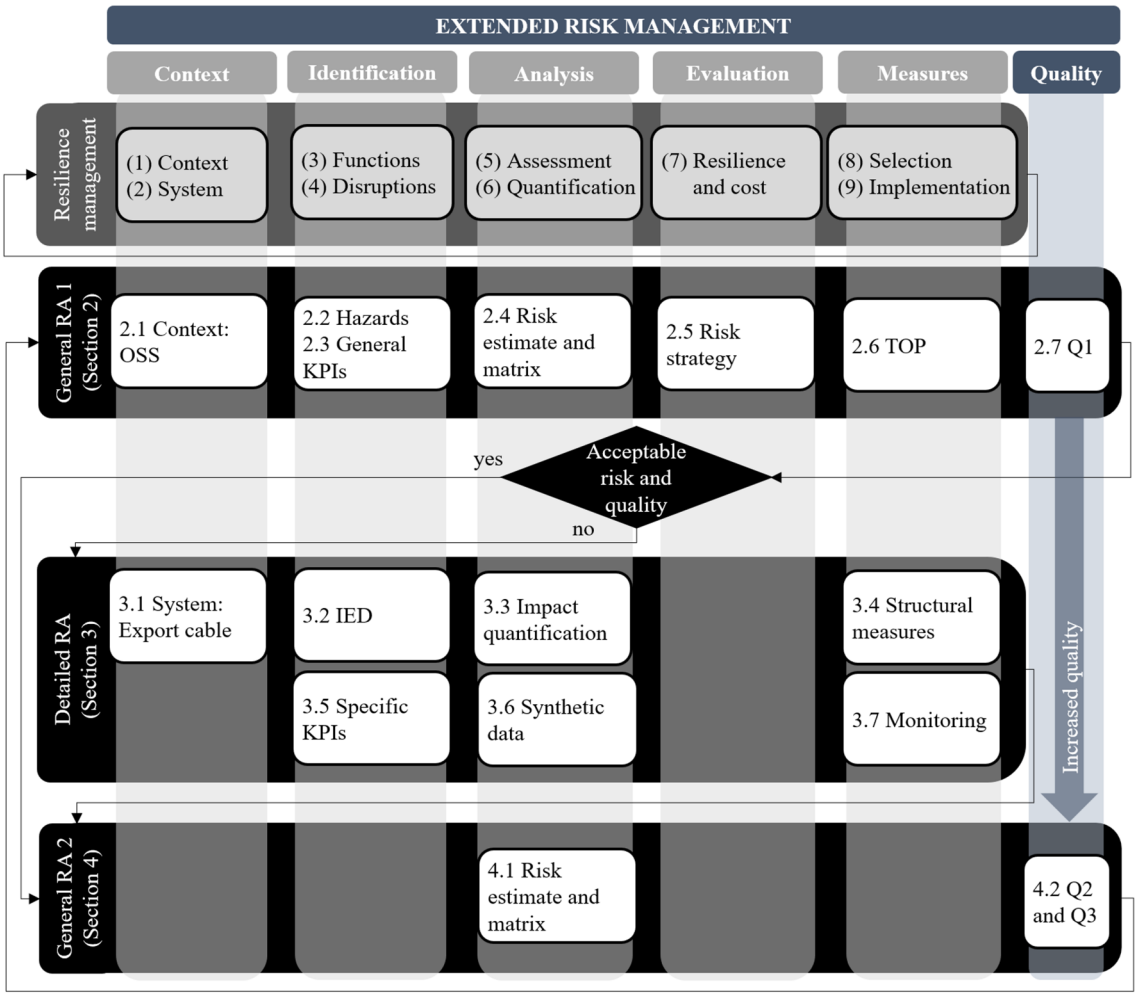

Fig. 1 The extended risk management process suggested in this paper is based on (ISO 31000:2018 2018; Häring et al. 2017) and extended by quality assessments. First, a general risk assessment (RA) covers the main pillars of risk management extended by Quality Q1. If risk and quality are not acceptable for specific hazards a detailed RA is performed adapting steps of the resilience management. Based on the developed measures in the general RA 1 and the detailed RA, a general RA 2 is performed to assess the residual risk and the Quality Q2 and Q3

(Linkov et al. 2015). The proposed approach starts with a first general RA which analyzes potential sources of danger and hazards on a high level, here exemplified for the Offshore Sub-Station (OSS) and mainly security risks to narrow down the focus. The approach can be applied to any asset and any kind of threat. But this general RA also adapts steps of the resilience management process like the development of Key-Performance Indicators (KPIs) which can be, e.g., employed for monitoring the effectiveness of measures. In this first general RA, the quality of the measures following the TOP (technical, operational, personal) principle is assessed. If the risk and the quality assessment for a certain hazard is not in an acceptable range, a hazard-specific detailed RA is performed. Here, the impact of improvised explosive devices (IED) on an export cable is quantified to derive more suitable safety measures. In a second step of the detailed RA, hazard-specific KPIs are developed and synthetic data are generated to observe the performance as a function of time. This analysis again is used to derive counter measures to reduce the risk. When the risk and quality for all hazards are in acceptable ranges or after finalization of the detailed RA, a second general RA is performed to assess the residual risk considering all suggested measures. The quality of the general RA 1 and 2 is assessed and the procedure starts again from the beginning. Note, some aspects of the resilience management steps have been adapted like the quantification of functions, the detailed system analysis, and the simulation of impacts and estimation of performance–time curves. Finally, the resilience quantification and evaluation are only performed for a certain specific aspect of the OSS, namely the J-tube. As there are many different flavors of

risk and resilience cycles where the nine-step approach is one of them (see e.g., Häring et al. 2020), every problem requires another weighting of the proposed steps.

The remainder of this work is structured as follows: Section 2 introduces the extended risk management approach and the first general RA is presented. Section 3 presents the quantitative studies that have been performed in the detailed RA. The second general RA that considers the suggested example measures is given in Sect. 4. Finally, Sect. 5 concludes this work by emphasizing the need to strengthen OWF towards security threats.

2 Extended risk management

This section introduces the extended risk management approach proposed in this work. Further, it contains the first part of the general RA. Classical RA is often based solely on expert knowledge and it is not visible in RA if any additional, e.g., quantitative assessment has been performed. Qualitative approaches like interviews and questionnaires are frequently used in the context of risk and resilience assessment for critical infrastructure (Cantelmi et al. 2021). To rate the trustworthiness of the RA itself, we propose to extend the classical RA by three quality measures. First, Q1 measures the quality of safety measures considered. Here, the quality of countermeasures depends on the TOP principle. The second quality measure Q2 rates the research and/or quantitative study and the quality of the available information. Finally, the aim is the calculation of an overall quality level Q3 which combines the two quality values and can be used as an indicator for the trustworthiness of RA. Q3 also considers the risk strategies such as risk avoidance, risk elimination, risk reduction, risk transfer, or risk sharing.

In the following, the steps of the first general RA being part of the extended risk management process presented in Fig. 1 are discussed in more detail starting from the context analysis.

2.1 Context analysis

First, RA needs to be placed in the context of the analyzed system and boundary conditions for the assessment are needed to be defined. The following boundary conditions apply: (1) The life cycle phase 'construction' and 'O &M' are considered. (2) The RA is general which requires additional specific assessments. (3) The assessed example OWF is located in the German Exclusive Economic Zone (EEZ). (4) German national and international law applies (such as SOLAS/MARPOL for vessels). (5) The maximum number of people assumed on a Wind Turbine Generator (WTG) is 3 and on the OSS is 12. (6) The RA has four categories: person, environment, asset, and organization (Arbschg 2015). In this work, the focus is set on 'asset' and security threats. Note that the general RA is performed without any additional assessments or studies as only the methodology shall be demonstrated.

Furthermore, the RA in this work focuses on a specific asset, which is the OSS platform including the interface of export cable. This choice is based on the results of the project Offshore Wind Energy—Protection/Safety and Security (OWISS) funded by the German Federal Ministry of Education and Research. It was found that the submarine cable and the OSS are very vulnerable components in the OWF. In Spalthoff (2018), it is described that the repair of submarine cables in case of destruction is costly and time-consuming as it commonly crosses shipping routes. Further, the replacing material is rarely available and the installation of cable parts needs additional UXO cleared areas. Especially, the destruction of the OSS is critical because (i) it may lead to immediate disruption in energy production, (ii) the replacing material is only available with delays of approximately one year, and (iii) secondary damage might occur on wind turbines due to idle state.

Here, we consider Riffgat OSS as an example. Figure 2 shows a schematic of Riffgat OSS. The components, which are given in Fig. 2 are the supporting structure, the heli-deck, the main-deck, the cable-deck, the boat-landing, the AIS antenna, and the J-tube. The latter contains the export cable.

Typically, the context analysis comprises also a stakeholder analysis. In the offshore wind industry, stakeholders are, e.g., owner, operator, maintenance provider, logistic companies, grid connection, public authorities, coast guard, trade control, rescue forces, vessel and air traffic services, insurance companies, investors, society, fishery, and shipping (see, e.g., Köpke et al. 2019; Ramírez-Agudelo et al. 2021). Here, we work together with the Offshore-Windpark RIFFGAT GmbH & CO. KG operated by Omexom Renewable Energies Offshore GmbH (former EWE OSS GmbH) to validate our findings. Stakeholder involvement is particularly important in risk and resilience management because the used approaches and models need to be approved by the stakeholders or end-users. This ensures that suggested mitigation options and safety and security measures are accepted and could be implemented.

2.2 Hazard identification

The threats affecting the most vulnerable and critical assets, i.e., the OSS and the export cable, are multifaceted. In order to demonstrate the synchronization of the procedure, we focus on security treats which intentionally aim at harming the OWF infrastructure. For example, in the project OWISS, several security threat scenarios have been identified, such as crash of flying object, damage of submarine cable or land cable, direct fire/shelling, occupation,

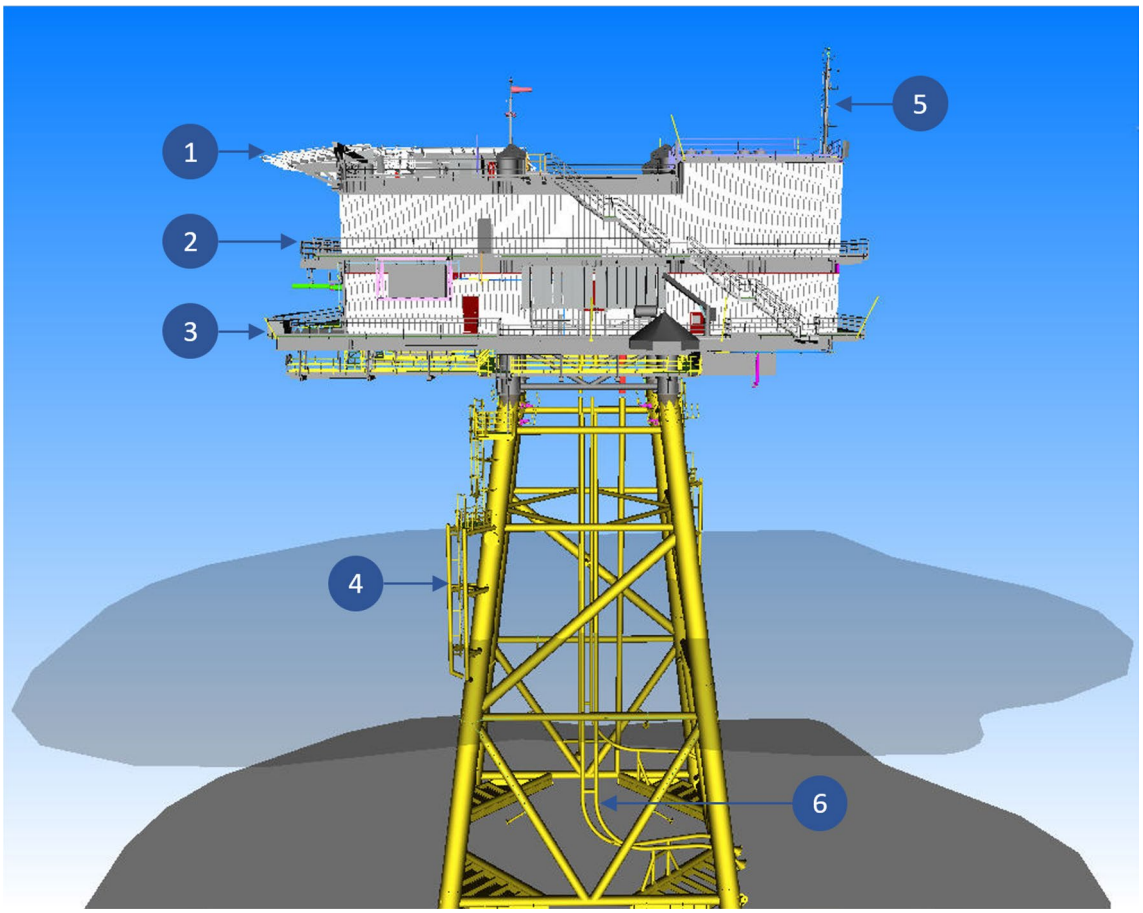

Fig. 2 Schematic representation of the Riffgat OSS based on a jacket-type support structure. Components of the OSS are, e.g., (1) heli-deck, (2) main-deck, (3) cable-deck, (4) boat-landing, (5) AIS antenna, and (6) J-tube

planned obsolescence, cyber-attack, intentional collision, intentional misconduct, bombing/detonation, vandalism, and intentional electro-magnetic pulse (EMP) (Jahn et al. 2018). Furthermore, additional threats such as theft and smuggling are considered. These initial incidents can lead to severe consequences such as fire/explosion, structural failure, intentional shutdown, and failure of components. Consequently, the converter platform, OSS, submarine, and land cable are affected and thus disturb the public power supply (Jahn et al. 2018).

Considered sources of dangers are, e.g., misconduct, danger to submarine cable, danger to land cable, vandalism, technical defect, bombing, shutdown, international disease, sabotage, severe weather, collision, planned obsolescence, and theft. Sources of danger-related hazards are identified (see Table 2). Note, for the source of danger 'explosion' a hazard called 'bomb threat' has been identified. This hazard means either the announcement of a potential attack with explosives to blackmail or an unattended bag or parcel that is assumed to contain explosives. In both cases the situation is unclear because it is not known if the threat is real.

2.3 General KPIs

KPIs can be generally described as a—quantitative or qualitative—measure for the progress of an operational, tactical, or strategic activity of an individual or an organization (Kerzner et al. 2013). In the context of complex infrastructures, like OWF, KPI can relate solely to the system performance, but also to safety and security aspects (Gonzalez et al. 2017; Valdez Banda et al. 2016). Consequently, KPI is an important tool for decision-making processes by providing the stakeholders with valuable information regarding the status of the system or infrastructure. Furthermore, KPI can play an important role for resilience assessment, with its ability to represent the performance of a system service before, during, and after an incident.

In order to assure effective and applicable KPI, the following principal requirements should be satisfied: simplicity, measurability, relevancy, specificity, and traceability in

Table 2 Sources of danger and hazards along with identifiers

Source of danger	Hazard	ID
Misconduct	Misconduct during operation	A
Danger to submarine cable	Dropped anchor incident	B
Danger to land cable	Targeted and intentional damage	C
	Accidental damage	D
Vandalism	Unauthorized access	E
Technical defect	Improper installation	F
	Material exhaustion	G
	Exposure to offshore environment	H
Explosion	Bomb threat	I
	IED	J
	Detonation of UXO	K
Shutdown	Uncontrolled shutdown	L
International disease	Interrupted O &M	M
Sabotage	IT-attack	N
	EMP	O
	Occupation by third party	P
	Flying drone	Q
Severe weather	Exposure to offshore environment	R
	Exposure to extreme waves	S
Collision	Vessel collision	T
	Submarine collision	U
	Helicopter collision	V
Planned obsolescence	Material exhaustion	W
Theft	Theft of systemically relevant materials	X

IED improvised explosive device, *UXO* unexploded ordnance, *EMP* electro-magnetic pulse

time (Moran 2019; Gonzalez et al. 2017). Furthermore, KPI can be distinguished into lagging indicators, i.e., measures of past activities, and leading indicators, i.e., measures of activities with significant effect on future performance (Peng et al. 2007; Reiman et al. 2012).

Several works discuss KPI in the context of OWF. For example, Gonzalez et al. (2017) review existing KPIs that are applied in the operation and maintenance (O &M) of (offshore) wind farms. The authors identified the need for further detailed studies on such KPI and their implementation. The authors of Pfaffel et al. (2019) discuss KPI for the operational management of (offshore) wind turbines and provided several recommendations for the selection of related KPI. In Seyr and Muskulus (2016), safety-specific indicators for the offshore wind industry are analyzed and it is shown that most of the indicators used in the literature are relevant when compared to reported incident data.

The main service of the OSS is the export of the power it receives from the wind turbines to the shore grid (DNV GL 2016). Therefore, it steps up the inner grid voltage to the transmission voltage (Robak and Raczkowski 2018). The performance of this service can be measured in two manners: (i) The relation between the power received by the wind turbines and transmitted to the shore grid, (ii) via the fulfillment of the requirements of the transmission system operator, e.g., as defined in OFGEM (2019). The KPI for (i) can be defined as

$$\mathrm{KPI}_{\mathrm{OSS},1} = \frac{c_{\mathrm{loss}} \cdot c_{\mathrm{ctr\_strg}} \cdot P_{\mathrm{OSS,out}}}{\sum_{N_{\mathrm{WT}}} P_{\mathrm{WT},i}} \tag{1}$$

with $P_{\mathrm{OSS,out}}$ means the transmitted power of the OSS, N_{WT} is the number of all wind turbines connected to the OSS, and $P_{\mathrm{WT},i}$ refers to the power transmitted by the wind turbine WT, i to the OSS. Furthermore, c_{loss} and $c_{\mathrm{ctr\_strg}}$ are correction factors with values between 0 and 1 that refer to the known losses and the chosen control strategy (Schütt 2014). It should be noted that this KPI does not consider any other safety aspects, as the focus here is on security aspects.

There are several aspects that can be considered in terms of (ii), e.g., compliance with the demanded steady-state frequency, avoidance of unacceptable sub-synchronous oscillations or avoidance of unacceptably high voltage (OFGEM 2019). For the sake of simplicity, but without loss of generality, we consider one of these parameters, i.e., the second KPI, which is derived based on the methods proposed in Sill Torres et al. (2020). It follows from

$$\begin{aligned} \mathrm{KPI}_{\mathrm{OSS},2} &= \begin{cases} 0 & \text{if } K^*_{\mathrm{OSS},2} < 0 \\ K^*_{\mathrm{OSS},2} & \text{otherwise} \end{cases} \\ K^*_{\mathrm{OSS},2} &= 1 - \frac{|f_{\mathrm{OSS}} - f_{\mathrm{base}}|}{\Delta f_{\mathrm{lim}}} \end{aligned} \tag{2}$$

with f_{OSS} the steady-state output frequency of the OSS, f_{base} the statutory base frequency, and Δf_{lim} the absolute statutory limit for deviation of the steady-state frequency.

2.4 Risk analysis

Each hazard is associated with a risk factor. Based on the risk factors for the category P (personnel) which are, e.g., mechanical, electrical, or biological (Nohl 1989), similar risk factors have been developed for the category A (asset), like e.g., Design, logistics, O&M, stakeholders, and interfaces. The risk factors are decisive criteria for the consequence of the risk and assist further in the mitigation of the risk. The identified hazard is followed by a consequence of risk, which does not consider any safety or security measures. This well-established approach is employed in various domains such as urban security (Finger et al. 2021), risk for interconnected critical infrastructure (Kotzanikolaou et al. 2013), and cyber-security (Lee 2020).

Considering the example 'explosion,' the consequence of risk is damage to asset, unclear situation, or potential interrupted operation. Hazard-specific risks are evaluated according to a predefined risk matrix. The risk r is calculated as a function of probability p and severity s

$$r = p \cdot s \tag{3}$$

with p varying from very unlikely ($p = 1$) to very likely ($p = 5$) and s varying from slight damage ($s = 1$) to catastrophic damage ($s = 5$).

In order to visualize the outcome of the risk analysis of the first general RA, the different sources of danger given in Table 2 are visualized in a matrix. Figure 3 presents the outcome of the risk analysis. In the matrix, different sources of danger are plotted as the result of potential possibility and severity. The possibility of risk occurrence is classified in five categories: (1) never occurs/unlikely to occur, (2) rarely occurs, (3) could happen, (4) happens several times per year, (5) almost inevitable, while the possible severity of damage/loss is classified in the following five categories: (1) slight injury or damage, (2) minor injury/first aid or damage, (3) major injury or damage, (4) permanent total disability or major damage, (5) fatality, extensive, or catastrophic damage. This predefined matrix is highlighted in green (low risk), yellow (medium risk), and red (high risk). Each color is a visual indicator which describes the risk and its potential. Here, the categories are rather qualitative but for a specific infrastructure under consideration, these categories can be also expressed quantitatively such as in MIL-STD-882D (2020).

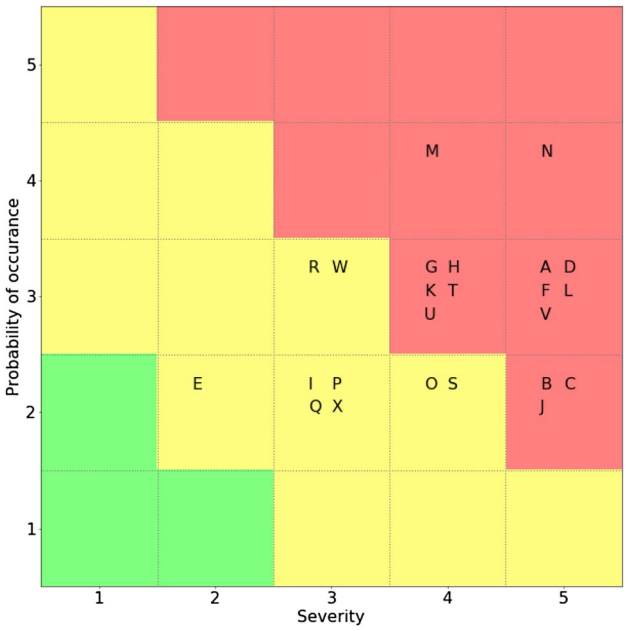

Fig. 3 Hazards given in Table 2 plotted as a function of probability of occurrence and possible severity. Color code: green (low risk), yellow (medium risk), and red (high risk)

The outcome of the risk analysis shows that all risks have been identified to be medium or high risk, which comes along with a need for action to reduce the risk according to the as low as reasonably practicable (ALARP) principle. For example, the specific hazard 'IED' has been evaluated to be of high risk $r = 10$ if no measures are taken. A high possible severity of damage/loss has been sensibly assessed in combination with a rare occurrence.

2.5 Risk evaluation

Based on the previous evaluated risk, a strategy needs to be decided. Distinction is made between RS1 risk avoidance (best option), RS2 risk elimination (good option), RS3 risk reduction (medium option), RS4 risk transfer (sufficient option), and RS5 risk sharing (unfavorable option). The chosen strategy is considered as a quality level and therefore as an influencing factor on the final quality level.

2.6 Development of measures

All safety measures minimizing the risk to an acceptable level are to be mentioned. For all these measures, the trade-off between risk reduction and additional cost/effort needs to be considered as well as potential interference with the already-implemented measures. See Table 3 for some example measures.

2.7 Quality assessment

The first quality assessment Q1 rates between 0 and 20. Q1 specifies the meaningfulness of safety measures. Here, the rating of Q1 is in proportion to the TOP measures in combination with the number of experts considering this conclusion. Here, Q1 is rated with 7 for all hazards (see Table 3) as a single expert was developing the suggestions. Additionally, no industry standards are employed.

A summary of the main steps is given in Table 3 with a detailed view on 'explosion' and 'sabotage.'

3 Detailed risk assessment

As mentioned in Sect. 1, for any kind of hazard associated with a high risk value and/or a low quality of the risk strategy and the measures, a detailed RA is recommended. High reliability and quality is needed that can be accomplished by incorporating quantitative studies. Performance functions can be defined for quantification and monitoring which can be combined into KPIs.

Table 3 General RA 1: The probability of occurrence *p*, the severity *s*, and the risk *r* represent the risk analysis

Source of danger	Hazard	Risk factor	Consequence	*p*	*s*	*r*	RS	Example measures	Q1
Explosion	Bomb threat	Design, Logistics, O &M, Stakeholders, Interfaces	Unclear situation, potential interruption	2	3	6	RS3	Emergency response, protection by material design	7
	IED	Design, Equipment, Worker Human, Stakeholders, Interfaces	Damage to asset, functionality of the infrastructure	2	5	10	RS3	Enclosed substation, CCTV	7
	Detonation of UXO	Planning, Design, Equipment, Stakeholders, Interface	Damage to asset	3	4	12	RS3	UXO clearance	7
Sabotage	IT-attack	Planning, Design, Equipment, Stakeholders, Interfaces	Damage to asset, functionality of the infrastructure	4	5	20	RS3	Redundancies, training	7
	EMP	Design, Equipment, Standards Legislation, Stakeholders	Interrupted Operation	2	4	8	RS3	CCTV, emergency response	7
	Occupation by third party	Stakeholders, Equipment, O &M, Interfaces	Interrupted O&M	2	3	6	RS3	CCTV, maritime surveillance	7
	Flying drone	Design, Equipment, Worker Human, Stakeholders, Interfaces	Spying	2	3	6	RS3	CCTV	7

Q1 quality of the measures. The considered category for all hazards is 'asset.' *IED* improvised explosive device, *UXO* unexploded ordnance, *EMP* electro-magnetic pulse

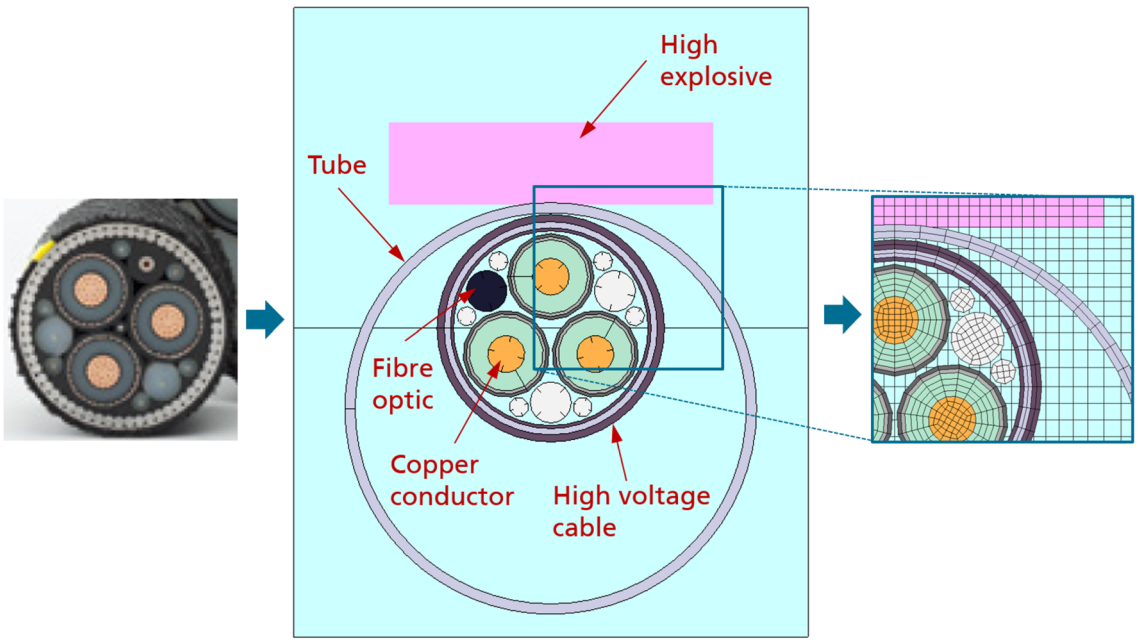

Fig. 4 Example export cable cross-section taken from NSW (2020) and the derived spatially discretized model placed in the tube. White circles represent plastic filling material and light green areas are insulators

3.1 System analysis

In the first step, a detailed model of the system under consideration is developed—here the export cable in the J-tube.

Figure 4 displays the cross-section of the reference 155kV emission cable (NSW 2020), the developed numerical model of the cable, its surrounding tube and the high explosive as well as the mesh resolution. The model of the cable includes all decisive components such as conductors, lead casing, spacers, and PP surface with simplified material models.

3.2 Identification of the threat

In order to demonstrate the detailed RA, the example of an explosion in close proximity of a tube including an export cable was chosen. This refers to the hazard 'IED' of the first general RA. An IED is defined by the United Nations Mine Action Service to be 'A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores, but is normally devised from non-military components' (UNMAS 2017). In this work, the IED could be, e.g., person-born, which means that the device is worn or carried by a person. Further, it can be classified as 'anti-infrastructure,' which is defined as 'primarily intended to damage or destroy physical infrastructure such as pipelines, communications towers, bridges, buildings, utility lines and/or facilities such as electrical transformers or water pump houses (UNMAS 2017). In the scenario considered in this paper, the IED acts on the export cable housed in the J-tube.

3.3 Impact quantification

To quantify the degree of damage advanced numerical simulation can be applied. Specialized modern finite-element methods are counted among the most powerful and versatile prediction techniques to assist damage analysis and design of building components against explosion effects (Riedel 2008). All results described in the following are calculated using the commercial hydrocode (Zukas 2004) AUTODYN (Cowler and Birnbaum 1997), a code using finite methods and explicit time integration to link shock wave propagation and structural response of the exposed components.

For analysis, two spatial arrangements have been simulated with two different ambient conditions each. In case 1, the charge was placed next to the conductor cross-section outside the tube to initiate most direct damage, as displayed in Fig. 4. In case 2, the cable was rotated by 60° so that detonation hits the area of the spacers to create most deformation of the optical fiber (highlighted in black) and the two adjacent conductor sections. These cases have been analyzed assuming ambiance of air on the one hand and of water on the other hand.

A first impression of the criticality of the threat is given in Fig. 5 by the example of simulation case 1 in air. All parts of the emission cable and its outside layers are apparently destroyed. Since the same magnitude of damage is observed for all of the 4 initial configurations, a second scenario with 10 cm stand-off of the charge was assumed and simulated for all 4 configurations.

Figures 6 and 7 give an overview of the resulting plastic strains and damage propagation, over the decisive cross-sections of the copper conductors and the optical fiber for stand-off detonations in air and underwater, respectively. The comparison shows significant differences between the assumed ambient conditions as expected since the destructive nature of underwater detonations are common knowledge in this field (Cole and Weller 1948; Swisdak 1978). Regarding the location of the high explosive, the effect in degree of damage is rather small compared to whether the detonation took place in air or in water.

Based on the numerical results which suggest that in any case the isolation of the cable will be damaged, especially in the case of water ambiance, a short circuit can be expected. For the OWF, this means that the circuit breaker at the end of the cable will cut the connection through the

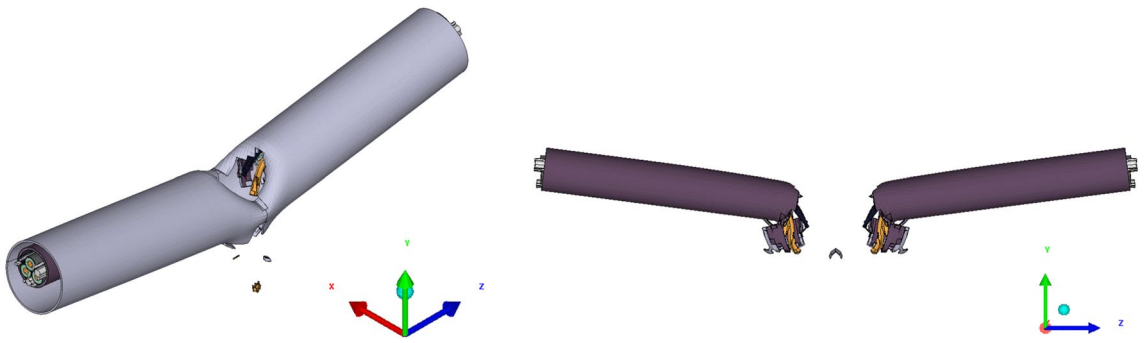

Fig. 5 Simulation case 1 in air for the no-stand-off scenario. Left: the damaged tube is presented. Right: The broken cable is shown

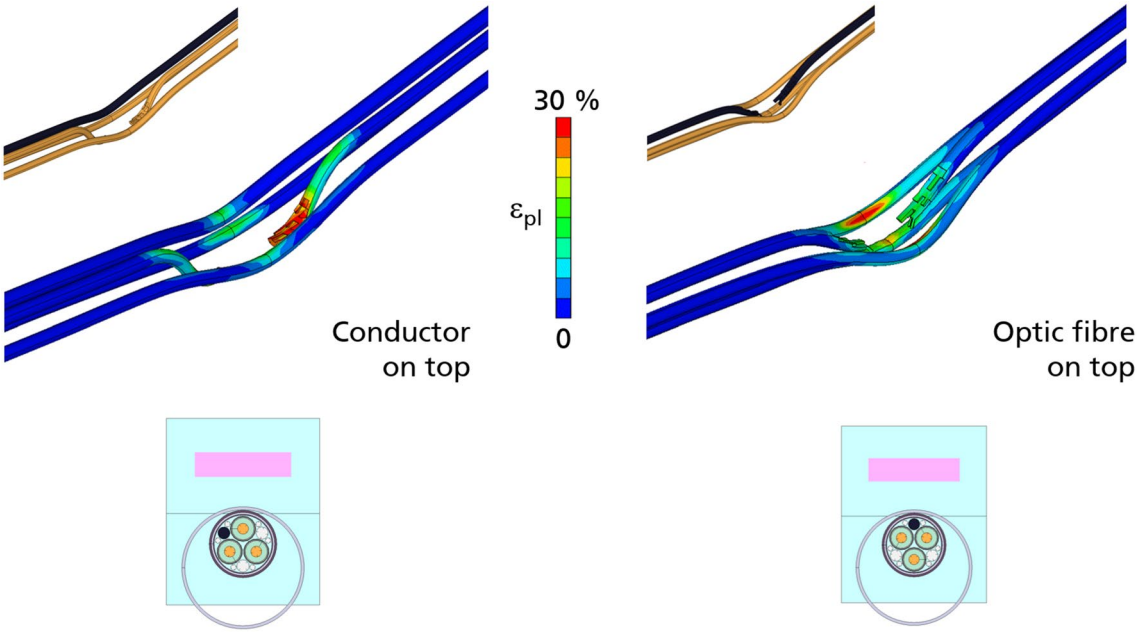

Fig. 6 Upper row: Orange represents the conductors and black the optical fiber. Middle row: Strain-related damage ϵ_{pl}. Blue equals to intact regions, whereas red represents regions at failure strain, meaning completely damaged regions. Lower row: Schematic of the 10 cm-stand-off scenario in air (light blue) with the explosive shown in pink

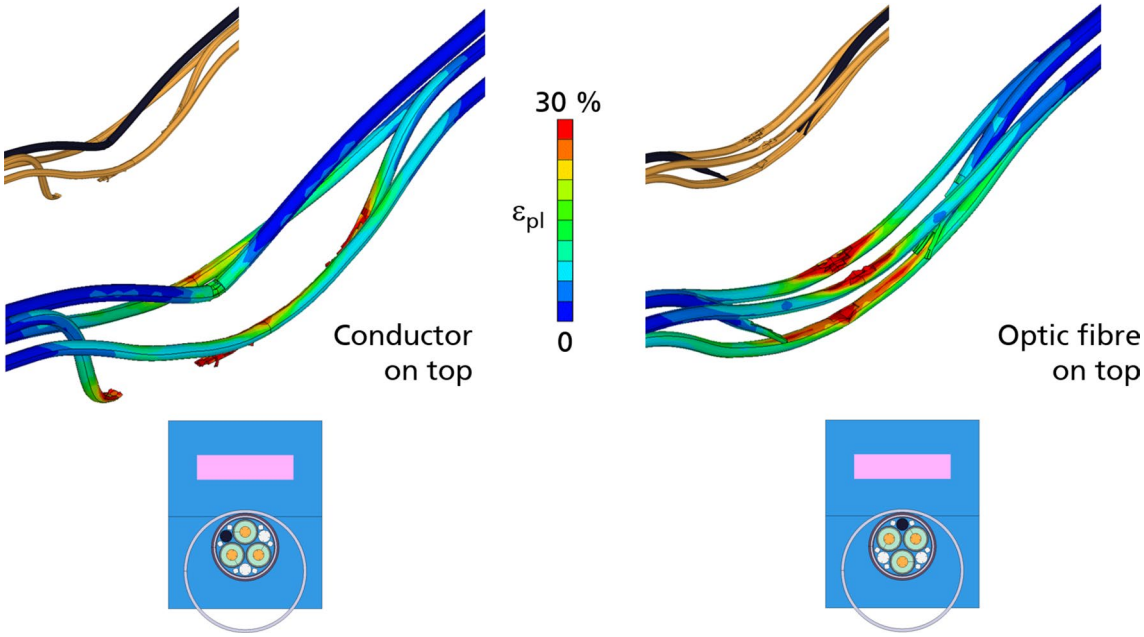

Fig. 7 Upper row: Orange represents the conductors and black the optical fiber. Middle row: Strain-related damage ϵ_{pl}. Blue equals to intact regions, whereas red represents regions at failure strain, meaning completely damaged regions. Lower row: Schematic of the 10 cm-stand-off scenario in water (blue) with the explosive shown in pink

protecting relay to avoid further damage. To fully recover the system, damaged cable parts need to be replaced. Under the assumption that the optical fiber fails with 10% of plastic deformation, the numerical results suggest that also the communication will fail in all cases (see Fig. 8). The delivery times for replacing parts highly depend on the availability. Besides replacing parts, personnel and ships are needed that

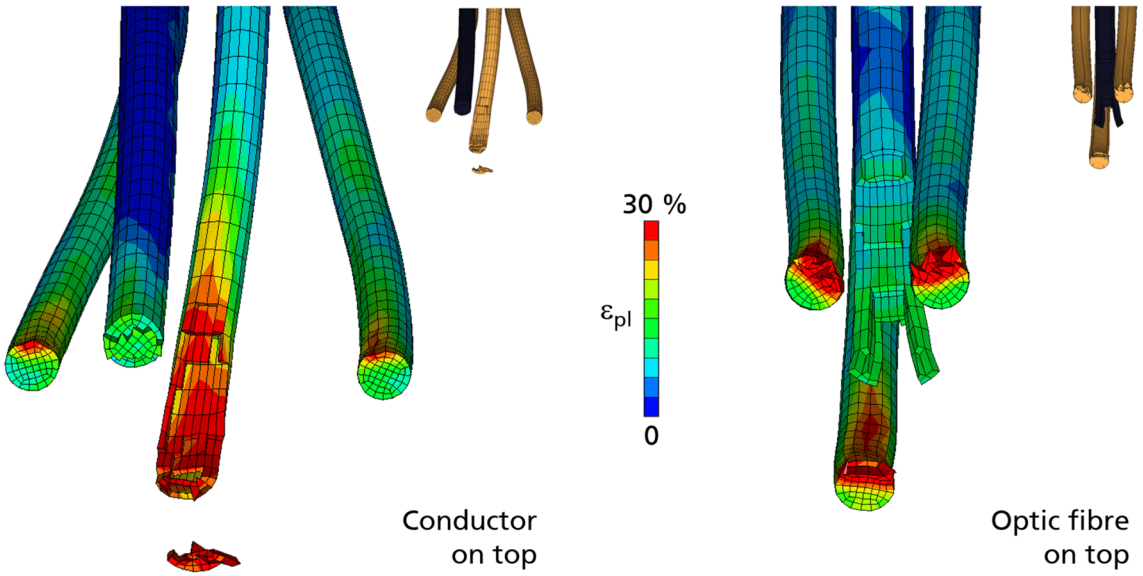

Fig. 8 Cross-section: Strain-related damage ϵ_{pl} for the 10 cm-stand-off scenario in water. Blue equals to intact regions, whereas red represents regions at failure strain, meaning completely damaged regions. In the upper right corner, respectively, orange represents the conductors and black the optical fiber

potentially increase the down time. Due to the damage of the IED happening in less than a second and very long restoration times because of uncertain delivery of replacing parts, no resilience assessment over the full resilience cycle is possible in this case.

3.4 Recommendations and measures

The simulation results quantify the impact of the IED on the export cable in the J-tube of the OSS. It could be shown that a stand-off between IED and cable or tube should be larger then 10 cm to avoid significant damage. The exact numbers depend on the surrounding medium and would have to be analyzed in subsequent studies. This kind of stand-off or frame can be achieved by an extra enclosure of critical components such as the export cable. Another possible approach to mitigate the impact would be to have a decentralized cabling system to distribute critical components. Further, a redundant cabling could reduce the impact when being targeted by an IED.

However, all these suggestions come with significant cost as they involve intensive structural measures. Further, the measures address the resilience phase 'prepare' with a focus on minimizing the impact. Another approach could be to focus on the resilience phase 'prevent' which tries to avoid the attack and would reduce the probability of occurrence. To this end, a monitoring system could be established which is presented in the following second part of the detailed RA.

3.5 Threat-specific OWF KPI

The general key performance indicators $\mathrm{KPI}_{\mathrm{OSS1}}$ and $\mathrm{KPI}_{\mathrm{OSS2}}$ are defined in Eqs. 1 and 2. In the following, more specific KPIs are derived for the two categories, (i) explosion and (ii) sabotage.

3.5.1 Explosion

The hazard 'IED' can be provoked by unauthorized access to the platform. Having in mind the exposed location of an OSS, the most probable form of access to such a platform is via a vessel. Hence, one has to install an appropriate monitoring system, usually radar, in order to expose all approaching vessels. Furthermore, trained personnel has to operate this system in order to separate known from unknown vessels. The consequent KPI follows from

$$\mathrm{KPI}_{\mathrm{radar}} = \frac{A_{\mathrm{radar}}}{A_{\mathrm{safe}}} \cdot K_{\mathrm{op}} \text{ with } K_{\mathrm{op}} = \begin{cases} 1 & \text{if } N_{\mathrm{op}} > N_{\mathrm{op,min}} \\ \frac{N_{\mathrm{op}}}{N_{\mathrm{op,min}}} & \text{otherwise} \end{cases} \quad (4)$$

with A_{radar} the area covered by the installed radar on the OSS, A_{safe} the area of the safety zone around the asset which is given as $A_{\mathrm{safe}} = \pi \cdot r_{\mathrm{sec}}^2$ with r_{sec} being the radius of the security zone around the OSS, N_{op} the amount of operators of the OSS radar, and $N_{\mathrm{op,min}}$ the minimum required amount of operators.

In the case of 'detonation of UXO,' a similar approach can be applied. To reduce the risk of UXO detonation in the vicinity of the OWF, prior to construction a certain area

A_{safe} needs to be cleared of UXO. The latter is named A_{clear}. However, the reliability of A_{clear} degrades over time t as currents v, sediment transport st can alter the sea floor, and thus move potential UXO. Consequently, the following KPI can be derived:

$$\begin{aligned} \mathrm{KPI}_{\mathrm{UXO}} &= \frac{A_{\mathrm{clear}}}{A_{\mathrm{safe}}} \cdot \frac{A_{\mathrm{safe}}}{\pi \cdot r^2_{\mathrm{UXOexplosion}}} \cdot \frac{N_{\mathrm{UXOsecured}}}{N_{\mathrm{UXOexpect}}} \cdot f(t, v, st) \\ &= \frac{A_{\mathrm{clear}}}{\pi \cdot r^2_{\mathrm{UXOexplosion}}} \cdot \frac{N_{\mathrm{UXOsecured}}}{N_{\mathrm{UXOexpect}}} \cdot f(t, v, st) \end{aligned} \tag{5}$$

with $r_{\mathrm{UXOexplosion}}$ being the radius of the area, that might be endangered when the largest expected UXO detonates. This parameter should be smaller than the safety area A_{safe}. Furthermore, $N_{\mathrm{UXOsecured}}$ means the number of secured UXO and needs to be related to the number of expected UXO $N_{\mathrm{UXOexpect}}$ in a certain area. The latter needs to be derived from statistical data or expect knowledge.

Note, this is a safety KPI and the function $f()$ is not further defined here. The exact calculation involves specific sea bed properties and target values need to be defined to finally receive a dimensionless number to be monitored as a function of time.

3.5.2 Sabotage

The KPI related to the threat *IT-attack* is $\mathrm{KPI}_{\mathrm{OSS1}}$ (Eq. 1), while the threat 'Electromagnetic Pulse (EMP)' is related to $\mathrm{KPI}_{\mathrm{OSS1}}$ (Eq. 1) and $\mathrm{KPI}_{\mathrm{OSS2}}$ (Eq. 2).

For the threat 'Flying drone' one can define an indicator that is similar to KPI_{radar} but focuses on the monitoring system based on CCTV (Eq. 4), which follows from

$$\mathrm{KPI}_{\mathrm{CCTV}} = \frac{S_{\mathrm{CCTV}}}{S_{\mathrm{safe}}} \cdot K_{\mathrm{op}} \text{with } K_{\mathrm{op}} = \begin{cases} 1 & \text{if } N_{\mathrm{op}} > N_{\mathrm{op,min}} \\ \frac{N_{\mathrm{op}}}{N_{\mathrm{op,min}}} & \text{otherwise} \end{cases} \tag{6}$$

with S_{CCTV} the space covered by the installed CCTV system on the OSS and the security space S_{safe} given as $S_{\mathrm{safe}} = 0.5 \cdot \pi \cdot r^3_{\mathrm{sec,vis}}$ with $r_{\mathrm{sec,vis}}$ being the radius of the security space around the OSS. The threat 'Occupation by third party' can be monitored by $\mathrm{KPI}_{\mathrm{radar}}$ (Eq. 4) and $\mathrm{KPI}_{\mathrm{CCTV}}$ (Eq. 6).

3.6 Thought experiment using synthetic data

Combining the findings of the numerical simulations presented in Sect. 3.3 with the KPI developed in Sect. 3.5 enables to simulate the relevant $\mathrm{KPI}_{\mathrm{radar}}$ in relation to the hazard 'IED' considered in this work. An operator could calculate this with real data, but here we generate synthetic data to present the concept. Assuming a random distribution of operators dependent on day and night shifts and random radar ranges which depend on weather conditions, the KPI can be estimated. Here, the number of operators varies between 1 and 4 and the radar range between 4 and 14 km. The area of the OWF is assumed to be 34 square kilometer and the security zone around that to be 500 m.

For the numerical simulations in Sect. 3.3 it is assumed that the attack is unnoticed till the energy transmission drops which is reflected in Fig. 9. Synthetic data are generated for operator availability and radar range which enables to calculate the $\mathrm{KPI}_{\mathrm{radar}}$. In this case, the attackers select a day with bad weather conditions, and thus, low radar range in combination with a late hour where the night shift consists of less operators to approach the OWF unnoticed. The attack leads to a drop in energy transmission as suggested by the numerical results. The sudden drop of large energy producers, as an offshore converter platform, impacts on the overall grid frequency ϵ based on Eq. 7 with the producers P and consumers C as a function of time t (Engel 2012).

$$P(t) = C(t) + f(\epsilon, t) \tag{7}$$

Under normal conditions both terms are in balance and for the European transmission grid the frequency is 50 Hz. If producers drop suddenly the grid frequency also decreases following the function $f(\epsilon, t)$ which is not further specified here. Dependent on the frequency deviation, certain regulatory mechanisms apply to stabilize the grid. It has been shown that in the event of a drop of producer blocks in the order of 2 GW a disturbance in the grid frequency is visible but no significant impact on the transmission grid is expected (Engel 2012). Thus, the disruption in production of a single OSS of typically 900 MW impacts the grid frequency only in the order of normal daily fluctuations.

The exact impact on the grid frequency depends on several factors such as the amount of power loss, the rapidity of the drop, the topology of the grid, and the time of the day. In Engel (2012), it is shown that the grid frequency is destabilized every hour and especially during night times because of trades on the European Energy Exchange. If such an event coincides with the disabling of several OSS at the same time, a severe impact on the grid frequency could be expected. In extreme cases and frequencies below 49 Hz, a controlled black-out of certain regions might be the only option to decrease the consumer term $C(t)$ in Eq. 7 and thus to stabilize the frequency (Engel 2012).

3.7 KPI-based early warning

Thus, to avoid the IED attack and the described potential impacts, the $\mathrm{KPI}_{\mathrm{radar}}$ could be established to notify operators of high-risk situations that could be exploited by potential

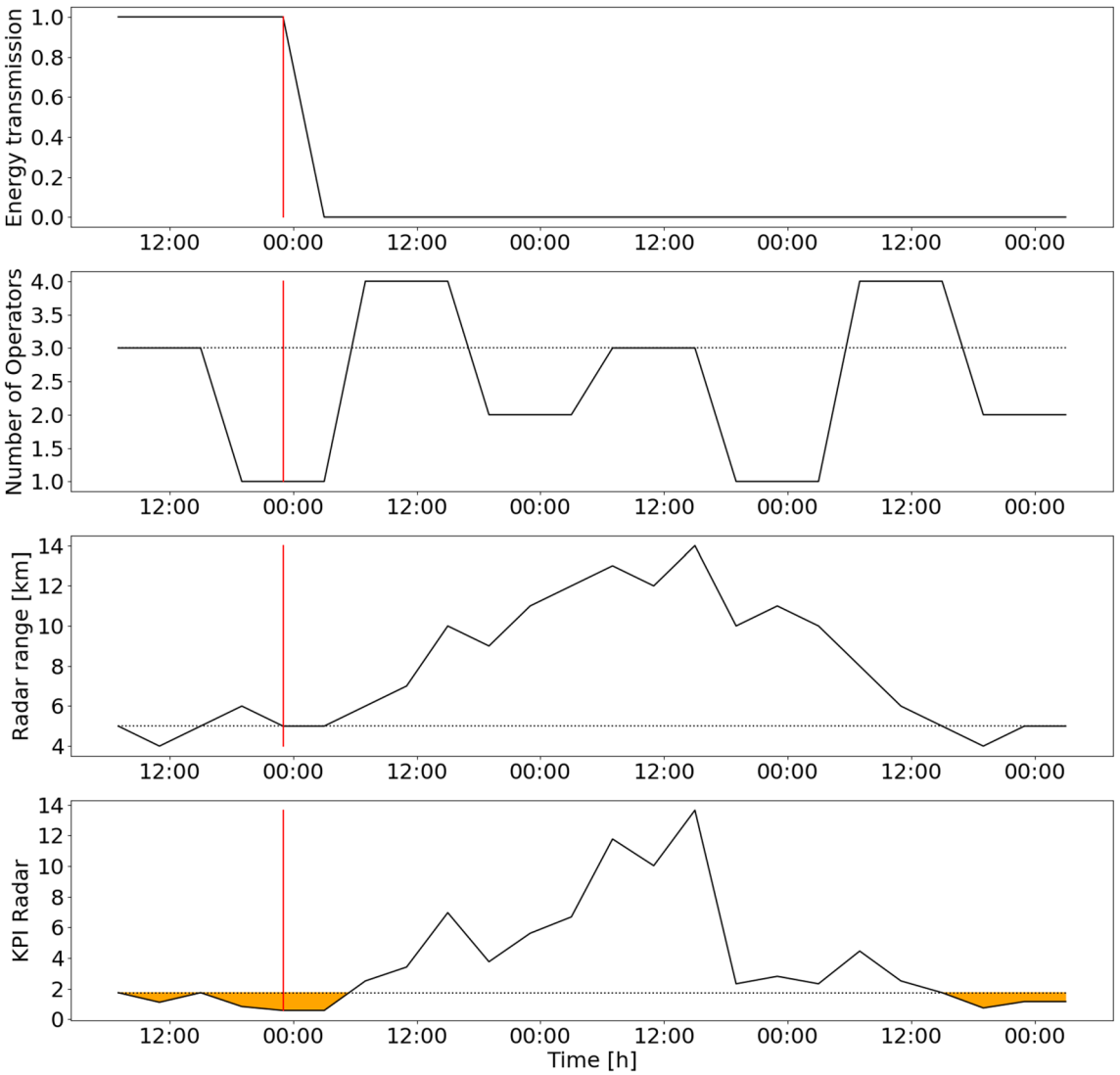

Fig. 9 First row: The drop of energy transmission due to the IED attack at 11:00 PM (red vertical line) is presented. As the re-connection to the transmission grid might take some days, no recovery is shown. Second row: Synthetically generated operator numbers. Third row: Synthetic radar ranges as a function of time. Last row: Estimated KPI_{radar}. Orange areas present the times in which an alarm should be raised because of limited radar coverage

Table 4 Example measures to be implemented theoretically and which are effective in different phases of the resilience cycle

Phase	Measure
Prepare	UXO clearance during the live cycle of the OWF
Prevent	CCTV, monitoring on the asset and improved maritime surveillance. Notification system for radar operators based on KPI
Crisis	
Protect	Improved material design to protect against specific hazards. Redundancies to mitigate the impact. A frame around the tubes to create a distance between cable and potential explosive material of more than 10 cm
Respond	Improved emergency response through training of the employees
Recover	The recovery after, e.g., the IED attack depends on the location of the OWF and the availability of replacing parts

Table 5 General RA 2

Source of danger	Hazard	Study	Q2	Additional measures	*r*2	*s*2	*r*2	Q3	KPI
Explosion	Bomb threat	HAZID	2	–	1	2	2	RS3, 30%	Eq. 4
	IED	HAZID, detailed RA	8	Stand-off, Early warning	1	4	4	RS3, 50%	Eq. 4
	Detonation of UXO	HAZID	2	–	2	3	6	RS3, 30%	Eq. 5
Sabotage	IT-attack	HAZID	2	–	2	5	10	RS3, 30%	Eq. 1
	EMP	HAZID	2	–	1	4	4	RS3, 30%	Eqs. 1, and 2
	Occupation by third party	HAZID	2	–	1	2	2	RS3, 30%	Eqs. 4, and 6
	Flying drone	HAZID	2	–	1	2	2	RS3, 30%	Eq. 6

The probability of occurrence *p*2, the severity *s*2 and the risk *r*2. It considers measures of the general RA 1 and the detailed RA. Q2: Quality of the studies included, Q3: Summary of RS, Q1, and Q2. *EMP* electro-magnetic pulse, *UXO* unexploded ordnance, *IED* improvised explosive device

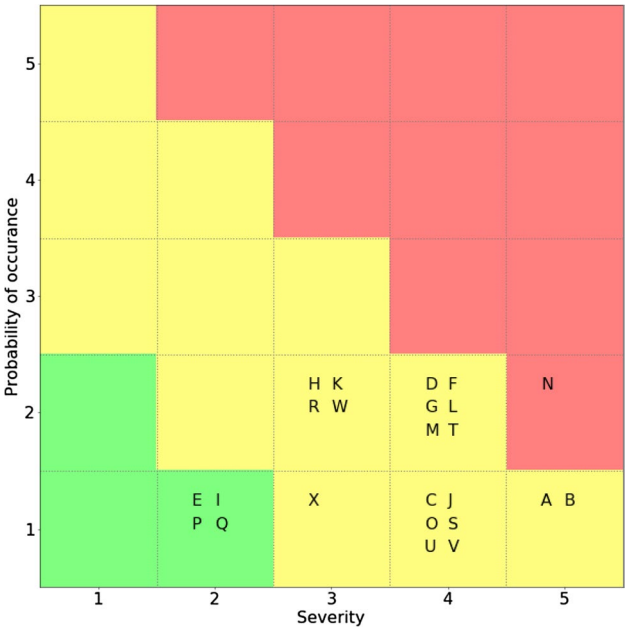

Fig. 10 Hazards given in Table 2 plotted as a function of probability of occurrence and possible severity after the implementation of security measures. Color code: green (low risk), yellow (medium risk), and red (high risk)

attackers. A threshold of acceptable risk can be defined in the KPI_{radar} and if the current values fall below the threshold, the notification is triggered (see the orange areas in Fig. 9). Here, we assume less than three operators at the same time and a radar range below 5 km as critical. This early-warning system could reduce the probability of such kind of attacks.

4 Implementation of mitigation measures

Measures are typically employed to avoid damage, prepare for a future threat, mitigate impact, recover the system, or to learn from past critical situations. Thus, the measures are effective in different resilience phases (see Table 4).

In the following, the safety and security measures suggested in this paper are theoretically implemented and incorporated in the RA. This refers to the second general RA of the extended risk management process presented in Fig. 1. This second general RA is given in Table 5.

4.1 Risk analysis with measures

Here, the residual risk which is the result of the risk mitigation and the implemented safety and security measures is considered. Figure 10 presents the outcome of the second risk analysis of the general RA and is based on the same predefined risk matrix as Fig. 3. The visualization shows that with the consideration of the exemplary applied safety and security measures, the residual risk is reduced. In most cases a medium residual risk is achieved. Specifically for the hazard 'IED,' the severity is reduced by the suggested stand-off and the probability by the potential early warning.

4.2 Quality assessment incorporating the detailed RA

For high-risk hazards, additional quantitative studies, besides the HAZID, might be performed such as detailed RA (see Sect. 3). Based on the included research and/or quantitative study the quality Q2 of the information input is assessed. The values for Q2 range between 0 and 10. With the input from the detailed RA and the numerical

simulations as described in Sect. 3, Q2 is rated here with 8 (see Table 5).

The final quality assessment Q3 consists of (i) the quality level of the risk strategy and (ii) the normalized sum of Q1 and Q2 in percent. From this it can be deduced how reliable the content of the RA is for a specific hazard.

4.3 Success monitoring

To continuously monitor the performance of the OWF and to achieve a good quality for the RA, hazard-specific quantification has been suggested in terms of KPIs (see Table 5). Note, the list of example KPIs presented in this work is not exhaustive.

5 Conclusion

In this work, an extended risk management approach is proposed that unifies aspects of classical RA and resilience management. The extension enables a safety and security engineer or any other stakeholder to question the results of the RA based on quantifiable and transparent criteria. The extended risk management bridges the gap between scientific studies and expert knowledge-based RA. It enables and explicitly asks for collaboration of disciplines which enriches and improves the RA.

Exemplary, security threats for an OWF have been presented and analyzed in the extended risk management framework. The specific threat of an IED that targets the export cable in the vicinity of the OSS is studied and the physical processes are simulated numerically. Thus, the severity and impact of this threat could be quantified. It was found that the explosion given the assumptions in this work will damage the export cable significantly. To reduce the damage a stand-off is suggested which could be achieved by, e.g., a frame. These results are especially to be highlighted with respect to most recent attacks on gas pipelines (The Guardian 2022). Thus, the security of critical infrastructure needs increased attention in the future.

Based on simulation and KPI development, example measures such as an early-warning system are discussed. They are effective in different phases of the resilience cycle and thus also impact the risk—probability of occurrence and severity—in different ways.

A fundamental challenge of each resilience management concept is its operationalization, i.e., its transfer from a concept to real application. This work deals with this challenge in the context of security of OWF, by adaptation of a given resilience management concept, the derivation of (semi-)quantitative performance indicators, and discussion of the application for an actual infrastructure. It is important to note that one must distinguish the consideration of safety and security aspects, even though there is some overlap (see e.g., Köpke et al. 2019). A consequent requirement is a critical discussion of the applicability of resilience indicators reported in related works (see e.g., Mentes and Turan 2019; Mentes and Mollaahmetoglu 2022; Ranasinghe et al. 2020). This work focuses on (semi-)quantitative performance indicators, which enable a more detailed consideration of infrastructure behavior and resilience enhancing measures. Such indicators, though, fall short in case of infrastructure aspects that are more difficult to measure, e.g., competency or management of change. In contrast, such capacities can be assessed via the more qualitative resilience indicators (see e.g., Mentes and Turan 2019; Mentes and Mollaahmetoglu 2022; Ranasinghe et al. 2020), which permit a more holistic view on the system capacities. Future works should address these aspects in more detail.

Finally, as most OWF stay below the limit of energy transmission that make an infrastructure critical, at the moment no legislation forces the operator/owner to account for security risks during the construction phase. OWF, however, are typically summarized in clusters which connect through one transformer station to the shore. The legislation with respect to protection against security threats should be rethought for OWF infrastructure especially for cyber-attacks which remain with a high residual risk in the RA presented in this work and gain more and more importance in general.

Acknowledgements The authors did not receive financial support from any organization for the submitted work. Still, the authors wish to thank Irina Lucke and Detlef Herzog from Omexom Renewable Energies Offshore GmbH for data and figures supporting this work. Further, we like to thank Marc Heumann of the Munitionsbergungsdienst (MBD) for valuable insights with respect to explosion related risks for offshore wind farms. Finally, we thank the reviewers for their comments that helped to substantially improve the manuscript.

Funding Open Access funding enabled and organized by Projekt DEAL.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

Arbschg (2015) Act on the implementation of measures of occupational safety and health to encourage improvements in the safety and health protection of workers at work (Arbeitsschutzgesetz, Arbschg). https://www.gesetze-im-internet.de/arbschg/

Alpha ventus (2022) Pacesetter der offshore industrie - und sinnbild des wandels. https://www.alpha-ventus.de/ueberblick. Accessed 16 Dec 2022

Associated Press (2020) Companies still hobbled from fearsome cyberattack. https://www.apnews.com/ce7a8aca506742ab8e8873e7f9f229c2/Companies-still-hobbled-from-fearsome-cyberattack. Accessed 20 Mar 2020

Brown R (2012) Wind power in the New Zealand power system, chap. 29. Wiley, Hoboken, pp 667–688

Bundesnetzagentur (2022) Kraftwerksliste. https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Erzeugungskapazitaeten/Kraftwerksliste/start.html. Accessed 28 Sept 2022

Cantelmi R, Di Gravio G, Patriarca R (2021) Reviewing qualitative research approaches in the context of critical infrastructure resilience. Environ Syst Decis 41(3):341–376

Carroll J, McDonald A, McMillan D (2016) Failure rate, repair time and unscheduled o &m cost analysis of offshore wind turbines. Wind Energy 19(6):1107–1119. https://doi.org/10.1002/we.1887

Cole RH, Weller R (1948) Underwater explosions. Phys Today 1(6):35

Cowler M, Birnbaum N (1997) Autodyn-interactive non-linear dynamic analysis software

Crabtree CJ, Zappalá D, Hogg SI (2015) Wind energy: UK experiences and offshore operational challenges. Proc Inst Mech Eng 229(7):727–746. https://doi.org/10.1177/0957650915597560

van Dam KH, Nikolic I, Lukszo Z (eds) (2013) Agent-based modelling of socio-technical systems. Springer, Dodrecht

Deutsche Post DHL Group (2021) Resilience360: supply chain risk management platform. https://www.resilience360.dhl.com/. Accessed 02 Mar 2021

Deutsche Wind Guard (2022) Status des offshore-windenergieausbaus in deutschland. https://www.windguard.de/. Accessed 28 Sept 2022

Edwards C (2009) Resilient nation demos

Engel T (2012) The mains frequency; die netzfrequenz. Sonnenenergie 6

Finger J, Ross K, Häring I, Restayn EM, Siebold U (2021) Open chance and risk management process supported by a software tool for improving urban security. Eur J Secur Res 6(1):39–71

Freudenberg WK (2018) Why windfarms need to step up cyber security. Offshore Ind 11(5):67–69

NSW (2020) General cable: submarine power cables for the future, delivered today. https://m.europages.com/filestore/gallery/74/34/16465664_eec8866c.pdf. Accessed 11 Dec 2020

DNV GL (2016) Offshore substation. Standard, DNV GL

Global Tech 1 (2022) Auf position inmitten der rauen nordsee. https://globaltechone.de/power/. Accessed 16 Dec 2022

Gonzalez E, Nanos EM, Seyr H, Valldecabres L, Yürüşen NY, Smolka U, Muskulus M, Melero JJ (2017) Key performance indicators for wind farm operation and maintenance. Energy Procedia 137:559–570. https://doi.org/10.1016/j.egypro.2017.10.385

Hiermaier S, Hasenstein S, Faist K (2017) Resilience engineering-how to handle the unexpected. In: 7th REA symposium on resilience engineering, poised to adapt: enacting resilience potential through design, governance and organization, Liege, Belgium, p 92

Hopcraft R, Martin KM (2018) Effective maritime cybersecurity regulation: the case for a cyber code. J Indian Ocean Reg 14(3):354–366. https://doi.org/10.1080/19480881.2018.1519056

Häring I, Ebenhöch S, Stolz A (2016) Quantifying resilience for resilience engineering of socio technical systems. Eur J Secur Res 1(1):21–58

Häring I, Fehling-Kaschek M, Miller N, Faist K, Ganter S, Srivastava K, Jain AK, Fischer G, Fischer K, Finger J et al (2021) A performance-based tabular approach for joint systematic improvement of risk control and resilience applied to telecommunication grid, gas network, and ultrasound localization system. Environ Syst Decis 41(2):286–329

Häring I, Sansavini G, Bellini E, Martyn N, Kovalenko T, Kitsak M, Vogelbacher G, Ross K, Bergerhausen U, Barker K, Linkov I (2017) Towards a generic resilience management, quantification and development process: general definitions, requirements, methods, techniques and measures, and case studies. In: Linkov I, Palma-Oliveira JM (eds) Resilience and risk. NATO science for peace and security series C: environmental security. Springer, Dordrecht, pp 21–80

Häring I, Ganter S, Finger J, Srivastava K, Agrafioti E, Fuggini C, Bolleta F (2020) Panarchy process for risk control and resilience quantification and improvement. In: Baraldi P, Di Maio F, Zio E (eds) Proceedings of the 30th European safety and reliability conference and the 15th probabilistic safety assessment and management conference (ESREL 2020–PSAM 15). Venice, Italy

ISO 31000:2018 (2018) Risk management - guidelines standard. International Organization for Standardization, Geneva

Jahn K, Gloystein S, Serkowsky J, Gabriel J (2018) Schlussbericht, verbundprojekt: offshore windenergie - schutz und sicherheit (owiss), teilvorhaben: Volkswirtschaftliche und gesellschaftliche sicht auf die versorgungssicherheit und sicherheit der bevölkerung

Kerzner H (2013) Project management metrics, KPIs, and dashboards: a guide to measuring and monitoring project performance, 2nd edn. Wiley, Hoboken

Komusanac I, Brindley G, Fraile D (2020) Wind energy in Europe in 2019

Kotzanikolaou P, Theoharidou M, Gritzalis D (2013) Assessing n-order dependencies between critical infrastructures. Int J Crit Infrastruct 9(1–2):93–110

Köpke C, Schäfer-Frey J, Engler E, Wrede CP, Mielniczek J (2019) A joint approach to safety, security and resilience using the functional resonance analysis method. In: 8th REA symposium on resilience engineering, embracing resilience: scaling up and speeding up, Kalmar, Sweden. https://doi.org/10.15626/rea8.10

Lee I (2020) Internet of things (IoT) cybersecurity: literature review and IoT cyber risk management. Future Internet 12(9):157

Linkov I, Kurth MH, Hristozov D, Keisler JM (2015) Nanotechnology: promoting innovation through analysis and governance

MIL-STD-882D: Mil-std-882d (2000) Standard, Department of Defense (DoD), STANDARD PRACTICE FOR SYSTEM SAFETY

Masala C, Tsetsos K (2013) The maritime dimension of the European union's and Germany's security and defence policy in the 21st century. ISPSW Publ 229:1–44

Mentes A, Mollaahmetoglu E (2022) A resilient approach of safety assessment for confined space operations on fpso units. Ocean Eng 252:111141

Mentes A, Turan O (2019) A new resilient risk management model for offshore wind turbine maintenance. Saf Sci 119:360–374

Moran J (2019) Key performance indicators (KPIs) for security operations and incident response. ACADIA

Nohl J (1989) Verfahren zur Sicherheitsanalyse: eine prospektive Methode zur Analyse und Bewertung von Gefährdungen. Erläuterung und Beschreibung der Gefährdungsfaktoren. Springer, Teil II, Cham

OECD (2016) The ocean economy in 2030. OECD Publishing, Paris

OFGEM (2019) National electricity transmission system security and quality of supply standard. https://www.ofgem.gov.uk/

O'Sullivan M (2020) Industrial life cycle: relevance of national markets in the development of new industries for energy technologies - the case of wind energy. J Evol Econ 30:1063

Peng W, Sun T, Rose P, Li T (2007) A semi-automatic system with an iterative learning method for discovering the leading indicators in business processes. In: Proceedings of the 2007 international workshop on domain driven data mining, DDDM '07, p. 33-42. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/1288552.1288557

Pfaffel S, Faulstich S, Sheng S (2019) Recommended key performance indicators for operational management of wind turbines. J Phys: Conf Ser 1356:012040. https://doi.org/10.1088/1742-6596/1356/1/012040

Ramírez-Agudelo OH, Köpke C, Guillouet Y, Schäfer-Frey J, Engler E, Mielniczek J, Sill Torres F (2021) An expert-driven probabilistic assessment of the safety and security of offshore wind farms. Energies 14(17):90. https://doi.org/10.3390/en14175465

Ranasinghe U, Jefferies M, Davis P, Pillay M (2020) Resilience engineering indicators and safety management: a systematic review. Saf Health Work 11(2):127–135

UNISDR (2009) United Nations Office for Disaster Risk Reduction, Terminology on disaster risk reduction

Reiman T, Pietikäinen E (2012) Leading indicators of system safety: monitoring and driving the organizational safety potential. Saf Sci 50(10):1993–2000. https://doi.org/10.1016/j.ssci.2011.07.015

Riedel W (2008) Chr. mayrhofer, customized calculation methods for explosion effects on structural building components. In: Proceedings of the international symposium on structures under earthquake, impact and blast loading

Robak S, Raczkowski R (2018) Substations for offshore wind farms: a review from the perspective of the needs of the polish wind energy sector. Bull Pol Acad Sci 66(No 4):517–528. https://doi.org/10.24425/124268

Savolainen J, Gill T, Schatz V, Ojala L, Jakstas T, Kleemola-Juntunen P (2019) Working Paper: Handbook on Maritime Hybrid Threats - 10 Scenarios and Legal Scans. Hybrid CoE

Schütt RJ (2014) Control of wind energy systems. Wiley, Hoboken, pp 340–368

UNMAS (2017) United Nations Mine Action Service: Improvised explosive device lexicon. Global CWD Repository 1257

Seyr H, Muskulus M (2016) Safety indicators for the marine operations in the installation and operating phase of an offshore wind farm. Energy Procedia 94:72–81. https://doi.org/10.1016/j.egypro.2016.09.200

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), pp 26–33. https://doi.org/10.1109/RWS50334.2020.9241287

Spalthoff O (2018) Schlussbericht, Verbundprojekt: Offshore Windenergie - Schutz und Sicherheit (OWISS), Teilvorhaben: Schutz und Sicherheit in der Betriebsphase

Staggs J, Ferlemann D, Shenoi S (2017) Wind farm security: attack surface, targets, scenarios and mitigation. Int J Crit Infrastruct Prot 17:3–14

Stroeve SH, Blom HA, Bakker GB (2009) Systemic accident risk assessment in air traffic by Monte Carlo simulation. Saf Sci 47(2):238–249

Swisdak Jr MM (1978) Explosion effects and properties. Part II. Explosion effects in water. Tech. rep., Naval surface weapons center white oak lab silver spting MD

The Guardian (2020) National grid blackout report expected to blame avoidable faults. https://www.theguardian.com/business/2019/aug/16/national-grid-blackout-report-avoidable-faults-blamed. Accessed 20 Mar 2020

The Guardian (2022) European leaders blame sabotage as gas pours into baltic from nord stream pipelines. https://www.theguardian.com/business/2022/sep/27/nord-stream-1-2-pipelines-leak-baltic-sabotage-fears. Accessed 30 Sept 2022

Thoma K (2014) Resilien-Tech:Resilience by Design: a strategy for the technology issues of the future. Herbert Utz Verlag

Valdez Banda OA, Hänninen M, Lappalainen J, Kujala P, Goerlandt F (2016) A method for extracting key performance indicators from maritime safety management norms. WMU J Marit Aff 15:237–265. https://doi.org/10.1007/s13437-015-0095-z

WFO (2020) World Forum Offshore Wind: Commissioned offshore wind farms worldwide. https://wfo-global.org/. Accessed 24 May 2020

Zukas J (2004) Introduction to hydrocodes. Elsevier, Amsterdam