Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P427-cd

Perception of threats in Offshore Windfarms and possible countermeasures

Babette Tecklenburg

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

Alexander Gabriel

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

Frank Sill Torres

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

In 2021 a change in legislations lead to new definition of Critical Infrastructure (CI). The threshold value has been lowered. This means that almost all German offshore wind farms (OWFs) belong to the CI, which leads to increased requirements for operators with regard to the security of the facilities and the provision of their core services. This paper aims to determine how the perception of the implemented measures compared to the perceived threats are. Therefore an interview guideline has been developed and conducted with 23 participants, who work in different positions in the German offshore wind industry. With the interviews a list of received threats and risks could be developed. The most mentioned threat is severe weather/ natural hazards. Furthermore, implemented countermeasures in the OWFs could be determined. The countermeasures were examined with regard to two aspects. Firstly, it was determined whether the measure was safety or security focused. Secondly, the type of action (preventive or reactive) was determined. Interesting to see is that more safety risks than security threats are mentioned by the interview participants. But equally safety and security countermeasures are stated. It seems like that passive countermeasures play a major role for the protection of offshore CI than active countermeasures.

Keywords: Offshore Windfarms, Guideline-based interviews, Maritime, Critical infrastructure, threats, countermeasures.

1. Introduction

With the legislative amendment of German Critical Infrastructure (CI) regulations in 2021, the threshold value for energy production infrastructures falling under the CI regulation has been lowered from 420 MW to 104 MW (§ 2 Abs. 6 Nr. 2 BSI-KritisV). Consequently, nearly all offshore wind farms (OWFs) are considered CI, which leads to increased requirements for operators with regard to the security of the facilities and the provision of their core services. The legislator for example requires measures against the failure of the process or to prevent damages. The offshore wind industry is a comparable young industry. Therefore not so many accidents or incidents toke place. One example is the collision of an offshore supply vessel with an offshore wind turbine in the offshore wind farm (OWF) "Arkona Becken Südost". Due to a human error the vessel collided with offshore wind turbine which has been under development. Federal Bureau of Maritime Casualty Investigation (2019) The aim of this paper to outline the current perception of threats and risks as well as countermeasures in the German offshore wind industry. The authors thereby us the term "threats" for possible security related incidents and the term "risks" for possible safety related accidents. The differentiation is necessary because the nature of the events differ. A threat is always oriented from a person or a group of persons and is an intended act. While a risk can be oriented by either a natural, technical or human origin (human error). But the appearance of the risks can not be determined for a specific date. For the determination of the threats and risks, 18

guideline interviews have been performed with participants from the offshore wind industry.
This paper is structured as follows: In the beginning OWFs as well as the design and the sub infrastructures are described (see section 2). The next section points out both used methods. In section 3.1 guideline-based interviews are described. The second subsection describe the qualitative content analysis. The fourth section explain the used interview guide as well as the sample and the execution of the interviews. The following section (section 5) describe the results of the guideline-based interviews. Also part of the section is a discussion of the results and a comparison to previous research. A conclusion is drawn in section 6.

2. Offshore wind farm

The electricity power is produced by multiple wind turbines in the OWF. The inner grid forwards the power to the Offshore Substation (OSS). From there on two ways exist to transmit the power to the landside power grid. That depends on the distance to the shore. The first option is that the OSS forwards the power to the high voltage direct current converter platform (HVDCC). They combine the electricity of multiple OWFs and transmit the power from alternating current to direct current. From the HVDCC the power is forwarded to the shore (see fig. 1, lower connection). In second option is to connect the OSS directly to the onshore substation (see fig. 1, upper connection). This link is an alternating current connection. For higher distances the loss is greater. Therefore the offshore wind farm clusters in the German North Sea are designed like first described. For the transportation of material and staff, OWFs are accessible by boat or helicopter.Hau (2014); Robak and Raczkowski (2018); Tecklenburg et al. (2022) For the scope of this paper two legislations need to be considered. According to the Regulation on the International Regulations for Preventing Collisions at Sea 1972 a 500 m radius around the OWF are forbidden to enter (VSeeStrO). Except are only boats to are necessary for the operation of the OWF or boats below the length of 24 m. Furthermore, The United Nations Convention On The Law Of The Sea should be considered. It states that it needs to be possible that shipwrecked persons need to be able to rescue themselves (SOLAS).

3. Method

3.1. *guideline-based interviews*

Guideline interviews are used in a variety of ways, e.g. in communication science or in journalism research. A distinction is made between standardized and non-standardized interviews. In standardized interviews the question content, the question sequence and, if applicable, the answer options are predetermined. An example is, among others, the questionnaire. Whereas in the non-standardized interviews only the topics of the interview are given (e.g. group discussions). The guided interview takes a middle position in this classification. It belongs to the partially-standardized interviews. It should be structured along a guideline. The guideline contains the topics and the questions. These can already be arranged in a meaningful order. The interview does not necessarily have to follow the prescribed sequence. The topics and questions should be derived from the research question. The aim is to obtain information or self-disclosure from the interviewee in relation to the research question(s). The guideline should also allow for a degree of comparability. Averbeck-Lietz and Meyen (2015)
Guided interviews are mostly conducted orally. Advantages of the guided interview method are, for example, the possibility of demand, both by the interviewer and by the interviewee. As well as a high flexibility in conducting the interview and

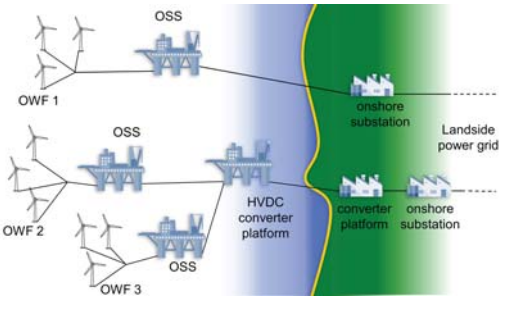

Fig. 1. network structure German OWF (source: authors)

a high degree of commitment. Guided interviews can be conducted in person but also by telephone or with the help of online telephony providers. They should come as close as possible to a ”natural” form of conversation. However, the interviewer should not lose control of the conversation, but the course of the conversation must not be restricted. Averbeck-Lietz and Meyen (2015)

3.2. *Qualitative content analysis*

Qualitative content analysis according to Mayring was used to evaluate the guided interviews. The goal of the qualitative content analysis is to determine the processed threats as well as the implemented countermeasures. Mayring divides between the inductive category formation and the deductive category application. During the inductive category formation the categories/ codes are formed while working with the text. In a next step the developed categories are organized into a coding guideline with main- and subcategories. For the deductive category application the codes are according to theories or literature developed. The coding guideline is developed before reading the transcribes of the interviews. It includes definitions, anchor examples and rules to divide the codes from each other. Mayring and Fenzl (2019) For this research work the authors decided to use the inductive category formation because so far not so much research work has been published in regard to threat scenarios in OWFs. An extract of the code guideline can be found in table 1. The transcribes have been automatically generated by f4x from audiotranskription and afterwards manually corrected. The coding of the transcribes have been done with MaxQDA.

4. Conducting the interviews

4.1. *Interview guide*

The interview guide exists of 7 topic blocks with a total of 32 questions. The first topic block relates to the introduction and welcome. The interviewees were asked to introduce themselves. The focus should thereby be on the current position, duration of execution and necessary qualifications or trainings. The second block is called safety, threats and risks. The block started with an assessment of the general safety and security situation of an OWF. After that the interviewee should mention possible risks and threats as well as for the physical vulnerability and the cyber vulnerability. Also the interviewees should estimate the frequency of occurrence of the threats and risks. The last question in the block is regarding a potential safety or security threat based on the potential dual use of areas in the OWF. The third topic block relates to maintenance. The questions focus on missing maintenance inter alia the threshold when no maintenance can be executed or after that duration of no maintenance relevant problems arise. The fourth block focus on protection goals. The interviewee should name the company own protection goals and their achievement as well as critical areas of an OWF or platform. The fifth block center on situational picture and crisis management. The questions with regard to the situational picture focus on the existence of a company own situational picture. What information are already included and what could be beneficial. Also the collaboration with other stakeholders was addressed. The second part of the block focuses on the crisis management. The interviewees where asked, if they have a threshold to change from the day-to-day operation into crisis mode. Furthermore the crisis management structures as well as trainings and the collaboration with authorities and other companies was addressed. The sixth and last content related block deals with countermeasures. For example the interviewees where asked if the OWFs are protected enough or if a security check of new employees take place. In addition a possible training to prepare employees for the work in sensitive areas as well as safety and security techniques for cyber-physical attacks where addressed. The last question focuses on company own standards. The last block is the closing block. The interviewees where ask if they would like to add anything and if they can recommend possible interviewees.

4.2. *Sample and execution*

In total 18 interviews with 23 participants were executed. 15 interviews have been analyzed. All

Table 1. Extract of the codeguideline

Codeno.	Content of question	Answer possibilities
C 6.1	Statement sufficient protection of OWF now and in future	yes; no; partly
C 6.2	Security check or Access control before entering	yes; no; partly; in extent to...
C 6.3	Preparation of employee to work in sensitive areas	yes; no; in extent to...
C 6.4	security and surveillance technologies for cyber-physical attacks	mentioning of specific technologies
C 6.5	company own standards	name specific tasks or processes

interviewees work with regard to OWFs in the German Exclusive Economic Zone (EEZ). That involve authorities, fire departments, owners, operators, insurances and consultants. The distribution of the participants within the management hierarchy can be seen in fig. 2. The experience of the interviewees within the offshore industry varies from 5 to 25 years (see fig. 3). The average experience amounts to 13.9 years.

Potential interviewees have been contacted via E-mail. In total 102 persons or organizations have been requested. The response quote amounts to 17.6 %. The interview toke place as onside interviews or as online interviews via a video conference provider. The audio of each interview has been recorded with the permission of the interview partners. The interviews have been performed between March and June 2022. In total the duration of the interviews varies from 35 to 97 minutes with an average length of 58 minutes.

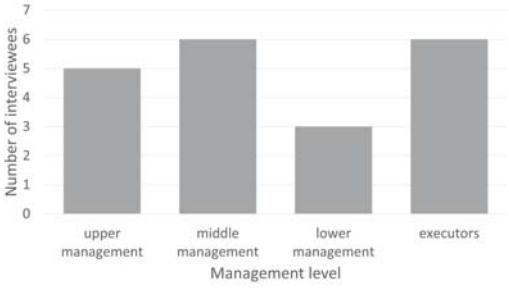

Fig. 2. Current position of interview participants (source: authors)

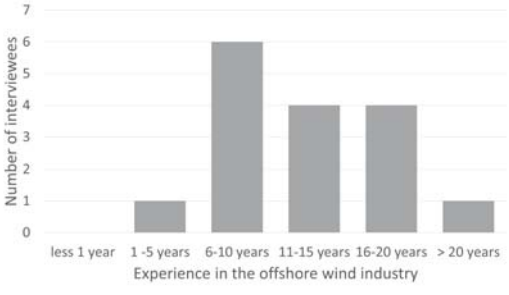

Fig. 3. Participants experience in the offshore wind industry (source: authors)

5. Results and discussion

In the following section the results of the interviews of are presented and discussed. The most often mentioned threat is natural hazard or severe weather. 10 interview participants mentioned this threat. Explicitly mentioned are inter alia high waves, strong winds and lightnings. With nine mentions shipping related threats and human errors are equally often stated. Shipping related threats include collisions of vessels with offshore structures but also damages originating from the anchor. In the context of human error missing experience and occupational work is mentioned. Figure 4 shows a summary of all the determined threats for OWFs.

In 2021 a survey with 31 participants have been conducted within our research group. The participants work as well in the German offshore wind industry. But the participants from this interviews have significantly more experience than the participants from the survey. Only 6 % of the survey participants have more than 10 years of experience in the offshore industry. Gabriel et al. (2022) While the average experience of the participants in the interviews amount 13.9 years (see section 4.2) A description and assessment of the

Table 2. Qualitative analysis on the perception of currently most relevant threats and risks for offshore wind farms Gabriel et al. (2022)

Risk or Threat scenario	*Number of mentions*
Cyberattacks	9
Technical failure/Poor maintenance	6
Natural hazards/Extreme weather	7
Terrorism	10
Sabotage	6
Human error/Organizational shortcomings	6
Collision with ships	9
Helicopter incidents/Fire on platform	4

survey can be found in Gabriel et al. (2022). The threats that have been determined by the survey can be seen in table 2. Even through that the order of mentions is not the same. A lot of the threats (for example natural hazards or collisions) are mentioned in both analyses. Interesting to see is that the threat "Terrorism" is the most mentioned threat in the survey. A few of the interview participants mentioned threats regarding physical security, which also included terrorism, but also piracy, unauthorized access or killing spree are stated. In general it needs to be said that the interview guideline has been prepared to cover safety and security concerns. But unfortunately a lot of the participants had more a safety-orientated view to the topic. "So actually, that's something [Security] I haven't dealt with [...] or that's why I haven't dealt with it, because I don't think I've ever come across it in practice." Interview partner 8 (2022)

The interview participants named a number of different countermeasures. A summary of them can be seen in fig. 5. All of the stated countermeasures have been sorted into the following categories: safety related, physical security related and/or cyber security related. Table 3 show the allocation of the countermeasures into the categories. Noticeable is that almost the same number of safety orientated countermeasures (14) as security orientated countermeasures (15) have been mentioned by the interview participants. While for the security oriented countermeasures more of them are cyber related (11 versus 8). What is especially interesting because most of the risks and threats in fig. 4 are safety related risk. The questions regarding the countermeasures and threats address security topic in the same matter. Therefore it could be assumed that the share of security and safety related answers are for both questions equal. Maybe the focus of the two topics is different. One reason for that could be that in the day-to-day life the stakeholder are obligated by the

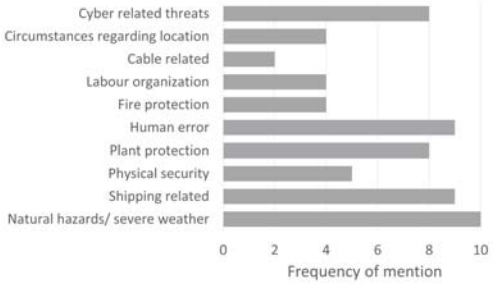

Fig. 4. Mentioned threats and risks by the interviewees (source: authors)

Fig. 5. Overview of the mentioned countermeasures by the interview participants (source: authors)

Table 3. Allocation of countermeasure if they are safety or security oriented

Countermeasure	Safety	Security	
		Physical security	Cyber security
start-work-briefing	X		
access management		X	X
medical examination	X		
closed entrance		X	
alcohol and drug control	X		
CCTV		X	X
telemedicine	X		
intruder barriers and sensors		X	
emergency exits	X		
simulated attacks		X	X
cardinal marks	X		
fire walls			X
hydrogen alarm	X		
limited access to word wide web			X
smoke alarm	X		
vpn tunnel			X
audits	X		
secure data line			X
instructions	X		
IT security concept			X
2 factor registration			X
AIS and radar	X	X	
certificates	X	X	X
dual control principle	X	X	X
redundancy	X	X	X

Table 4. Active and passive countermeasures mentioned by the interview participants

Active countermeasure	Passive countermeasure
closed entrance	medical examination
2 factor registration	Radar and automatic identification system (AIS)
digital access management	cardinal marks
secure data line	smoke alarm
	Closed Circuit Television (CCTV)
	simulated attacks
	dual control principle/ start-work-briefing/ instructions
	audits and certificates
	alcohol and drug control
	emergency exit
	redundancy

legislator to focus on topics like fire protection and occupational health. While less regulations exists for the security topics.

Furthermore the countermeasures mentioned by the interview participants have been analyzed in regard to whether they are active or passive coun-

termeasures. Thereby active countermeasures are understood as countermeasures which can intervene in an attack or inhibit a risk. A passive countermeasure can only detect a risk or threat. The allocation of the countermeasures can be found in table 4. The interview results indicate that the security measures used to date primarily comprise passive measures such as automated alarms (e.g. smoke or hydrogen alarms) or meetings (e.g. start-work-briefings). These passive measures focus primarily on detecting threats rather than mitigating them or initiating countermeasures. Active security measures such as the (automated) initiation of countermeasures, e.g., digital access management, on the other hand, seem to play a minor role in CI protection to date.

6. Conclusion

This paper presents an approach to increase the safety and security of German OWFs. It uses guideline-based interviews to determine inter alia the perception of risks and threats in the German OWFs. As well as to analyze the already implemented countermeasures. It seems like that the focus is rather on safety related risks instead of security focused threads. Interestingly equally many safety than security related countermeasures are mentioned. The next steps in our research is to develop a more advanced evaluation method for the countermeasures. The aim is to better describe against what kind of risk and threats the countermeasure protect. Furthermore, it should be studied during which phases of the accident or incident they can be applied.

References

Averbeck-Lietz, S. and M. Meyen (Eds.) (2015). *Handbuch nicht standardisierte Methoden in der Kommunikationswissenschaft* (1. Aufl. 2016 ed.). Wiesbaden: Springer Fachmedien Wiesbaden.

Federal Bureau of Maritime Casualty Investigation (2019). Kontakt der vos stone mit windkraftanlage am 10.04.18 in der ostsee: Untersuchungsbericht 118/18: Weniger schwerer seeunfall. Weniger schwerer Seeunfall.

Gabriel, A., B. Tecklenburg, and F. Sill Torres (2022). Threat and risk scenarios for offshore wind farms and an approach to their assessment. In R. Grace and H. Baharmand (Eds.), *ISCRAM 2022 Conference Proceedings – 19th International Conference on Information Systems for Crisis Response and Management*, pp. 162–173.

Hau, E. (2014). *Windkraftanlagen*. Heidelberg: SpringerLink.

Interview partner 8 (2022). Interview guide arrows – applied research on resilience driven offshore wind farm safety and security. oral.

Mayring, P. and T. Fenzl (2019). Qualitative inhaltsanalyse. In N. Baur and J. Blasius (Eds.), *Handbuch Methoden der empirischen Sozialforschung*, pp. 633–648. Wiesbaden: Springer Fachmedien Wiesbaden.

Robak, S. and R. M. Raczkowski (2018). Substations for offshore wind farms: a review from the perspective of the needs of the polish wind energy sector. *Bulletin of The Polish Academy of Sciences: Technical Sciences 66*(4).

Tecklenburg, B., A. Gabriel, and F. Sill Torres (2022). A scenario based threat assessment using bayesian networks for a high voltage direct current converter platform. In M. C. Leva, E. Patelli, L. Podofillini, and S. Wilson (Eds.), *Proceedings of the 32nd European Safety and Reliability Conference*, Singapore, pp. 2637–2644. Research Publishing.

Acknowledgement

This conference contribution is part of the research project Applied Research on Resilience-driven Offshore Wind Farm Safety and Security (ARROWS) which is financed by the German Aerospace Center. The authors would like to thank all the interview participants for their participation. Without your contribution this work wouldn't be possible.