Threat analysis of offshore wind farms by Bayesian networks – a new modeling approach

Alexander Gabriel
German Aerospace Center - Institute for the Protection of Maritime Infrastructures
Alexander.Gabriel@dlr.de

Babette Tecklenburg
German Aerospace Center - Institute for the Protection of Maritime Infrastructures
Babette.Tecklenburg@dlr.de

Yann Guillouet
German Aerospace Center - Institute for the Protection of Maritime Infrastructures
Yann.Guillouet@dlr.de

Frank Sill Torres
German Aerospace Center - Institute for the Protection of Maritime Infrastructures
Frank.SillTorres@dlr.de

ABSTRACT

As a result of the ongoing commitment to climate protection in more and more countries and the corresponding expansion of renewable energies, the importance of renewables for the security of electricity supply is increasing. Wind energy generated in offshore wind farms already accounts for a significant share of the energy mix and will continue to grow in the future. Therefore, approaches and models for security assessment and protection against threats are needed for these infrastructures.

Due to the special characteristics and geographical location of offshore wind farms, they are confronted with particular challenges. In this context, this paper outlines how an approach for threat analysis of offshore wind farms is to be developed within the framework of the new research project "ARROWS" of the German Aerospace Center. The authors first explain the structure of offshore wind farms and then present a possible modeling approach using Qualitative function models and Bayesian networks.

Keywords

Threat analysis, bayesian networks, process modeling, critical infrastructure.

INTRODUCTION

Climate change is forcing a shift away from conventional, fossil-based power generation to renewable and thus much cleaner methods of energy production. Since the early 2000s, wind power has been increasingly commercialized for energy generation (Arbeitsgemeinschaft Energiebilanzen e.V. 2020; BP p.l.c. 2020). Although the largest share of power generation is accounted for by onshore wind turbines, the offshore wind energy sector has been able to show higher growth rates in recent years in some cases (Deutsche WindGuard GmbH 2021a, 2021b; Fraunhofer Institute for Wind Energy Systems 2018). As a result, offshore wind farms (OWF) are becoming increasingly important for the power supply and are therefore more relevant in terms of security of supply.

While an individual wind turbine may not be a critical infrastructure in the true sense of the term, an OWF in its entirety qualifies as a critical infrastructure (German Federal Ministry of the Interior 2009). It is assumed that the failure of a large wind farm would have a similar impact as that of a conventional power plant (German Federal Office for Information Security 2015). Wind farms in the North Sea meanwhile achieve power outputs of several hundred megawatts, so that they are also formally considered critical infrastructures by the legislator (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, 2016). Accordingly, the individual infrastructure elements in offshore power generation and OWFs require an approach to evaluate and, if necessary, increase their safety and security.

The common approaches of risk analysis in the (wind) industry are sufficient for the consideration of technical risks and hazards, but show considerable deficiencies in the analysis of socio-technical and highly complex, interconnected systems. Since wind farms fulfill the criteria of complex infrastructures with regard to their corresponding structures and a view to the entire life cycle of the wind farm (Dunović et al. 2014), the implementation of more advanced methods for risk and threat analysis is required. To date, there is no holistic approach to threat analysis of offshore infrastructures using probabilistic methods. Due to the specificities of these offshore structures, this paper will present an approach by using Bayesian networks as they are able to deal with high degrees of uncertainty and allow a reasonable estimation of the likelihood for probable attack vectors. As such, the authors believe Bayesian networks can provide a building block for a holistic view of the threat assessment for OWF.

The paper focuses on developing a probabilistic threat assessment model for this infrastructure by qualitatively modeling the possible threat scenarios and a subsequent quantification of the individual nodes. In the paper, the authors first outline the general structures of an OWF to introduce the topic and its relevance. They then discuss some exemplary threat scenarios that have been qualitatively described. The subsequent development of a qualitative model based on the knowledge of attack processes and wind farm systems provides the basis for the development of a corresponding Bayesian network. Using two particular examples, the authors demonstrate how to parameterize the network and what results the network might be capable of producing in the future, followed by an outlook on potential future research and applications.

DESIGN, LAYOUT AND INFRASTRUCTURE ELEMENTS IN OWF

According to Sill Torres et al. (2020), OWF can be regarded as complex cyber-physical and socio-technical systems. The wind farms consist of several subsystems and components, some of which interact with the other. Besides the individual wind turbines used for power generation, the main components are the cable connections within the wind farm. These connect the wind turbines to the offshore transformer substations located on offshore platforms and, via a central undersea cable, to a transformer substation onshore that connects the wind farm to the landside power grid. The connection between the wind turbines and the offshore platform can take the form of a star-shaped cabling or branching of the individual wind turbines to the platform or it can be a ring-shaped connection.

Besides this mere perspective on the infrastructure side, the control and maintenance processes are of particular importance in the operation of a wind farm. Central control is provided by onshore control and operation centers. Predominantly, automated control via Supervisory Control and Data Acquisition (SCADA) is used for this purpose. The data automatically collected from each wind turbine is evaluated and used for planning maintenance and repair activities. For these maintenance measures, personnel are deployed by vessels or helicopters from onshore or the offshore transformer substations. A simplified depiction of the overall structure of an OWF is shown in Figure 1.

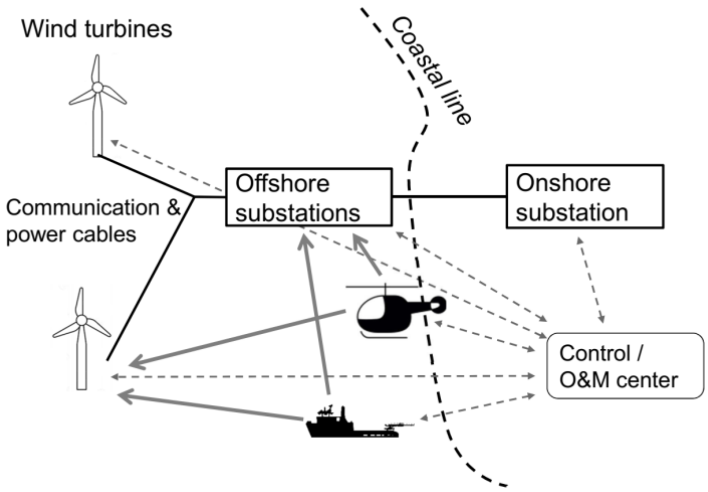

Figure 1. Simplified representation of an OWF (Source: Sill Torres et al. 2020)

Of particular interest are the submarine cables connecting the OWF to the onshore substation and the offshore platforms themselves. As central elements of the wind farm, these platforms carry the direct current or alternating current substation. In Germany, mostly direct current substations are used, as they have a lower loss due to the

long transmission distances.

The platforms themselves are divided into a substructure with a mooring for boats and ships and the so-called topside with the living and recreation area for crew and maintenance personnel as well as the actual transformer stations (Robak and Raczkowski 2018). The number of transformers depends on the size of the wind farm and can vary accordingly. The upper deck of the platform usually has a helicopter platform in addition to workshops and social rooms for the crew's stay and supplies. Depending on their location, the wind turbines or offshore platforms are marked with lights to indicate that they are an obstruction to shipping and are also named and listed accordingly on the freely available nautical charts.

THREAT SCENARIOS IN OWFs

OWFs face a variety of different threats. These can be of natural or anthropogenic origin, whereby the latter may include technical failures as well (Carroll et al. 2016; Crabtree et al. 2015; Staggs et al. 2017). A comparatively facile determination of probabilities can be made for natural threats in particular, since for extreme weather events, for example, sufficient multi-year data such as wave height and wind speed are often at hand. Anthropogenic threats, on the other hand, can be divided into accidents and deliberately caused incidents. In addition to accidents involving ships and aircraft as well as accidents during normal operations of the offshore platforms, the installation and disassembly phases in particular are likely to be associated with such safety-related incidents. In addition, aging and failure-related events also play a role here. These unintentional events are also relatively easy to grasp statistically and thus to evaluate, so that the established methods of risk analysis are usually sufficient here.

Intentionally caused, security-related events, however, cannot be statistically analyzed, because there is a lack of sufficient data and because there are too complex relationships, especially for intended events, which are not easy to resolve probabilistically (Brown and Cox 2011). In this paper, we will mainly focus on these events. These may include minor incidents such as theft, but also intentional damaging, arson or unauthorized access to the facilities and platforms by third parties. In addition to purely physical attacks using various means of attack, cyber-physical threats in particular may pose a considerable danger in the future (Gabriel et al. 2018).

A common tool in the safety and security research is to design scenarios which are used to evaluate threats and especially the efficacy of countermeasures (Dutch Ministry of Justice and Security, National Coordinator for Security and Counterterrorism 2009; Kim and Cha 2012; Liu et al. 2012). Four exemplary security incidents or rather scenarios have been identified for this paper. These are to be understood as a first approach to test the usability of qualitative models and derived Bayesian networks for threat analysis. The scenarios presented therefore serve as examples demonstration purposes and will have to be supplemented by further scenarios at a later stage of the project.

For the example of an OWF four possible scenarios have been identified (Progoulakis and Nikitakos 2019). Each of these scenarios was assigned a short qualitative description of the process and a short description of the attacker and accordingly its characterization (c.f. attacker types in Gabriel et al. 2018). The exemplary scenarios including the descriptions can be found in Table 1. The considerations are based on the working hypotheses from Gabriel et al. (2017) with regard to the motivation and approach of possible attackers.

Table 1. Exemplary scenarios and qualitative description

	Qualitative description	Characterization of the attacker
Unauthorized access	Out of curiosity one or more pleasure boaters decide to enter an unmanned offshore platform. Not all areas of a platform are CCTV monitored. As they enter an area which is monitored, the staff in the onshore control room gets aware of the intruders. Via speakers installed on the platform, the intruders are requested to leave the platform and at the same time alarm is issued to the Coast Guard.	Hobbyists usually neither have the technical expertise nor the equipment for complex attacks. Nevertheless, vandalism can cause considerable damage if adequate security measures are not in place.
Helicopter crash	During the normal transfer of personnel, an improvised explosive device (IED) ignites shortly before the helicopter lands on the platform. Due to the lack of inspections, the IED had been placed on board of the helicopter unnoticed in a backpack by a disgruntled employee. The crash of the helicopter onto the platform causes a fire on the platform and damage to its structure.	Internal attackers may be either aware of the security measures and could thus bypass them, or these measures only take effect externally. The principle of perimeter protection may be applicable only to a limited extent.
IED attached to platform structure	A group of attackers attaches an IED to the support structure of the platform, which the attackers approached using a rigid inflatable boat. The explosive device is not detected in time. Therefore, no countermeasures take place and the explosive device detonates, leading to a failure of the supporting structure.	This complex form of attack requires an intelligent and coordinated approach and planning. The development/acquisition of expertise and the financing of such operations is only feasible with support of organized structures.
Vessel proximity hazard	The maritime traffic control center notices a change in the heading of a vessel and the deactivation of its automatic identification system (AIS) transponder. Attempts to contact the crew are unsuccessful, whereupon the platform situated ahead is notified and evacuated. The platform is cleared before the ship arrives at the platform.	Using a ship as a weapon requires a highly planned and orchestrated approach. The necessary resources and logistics can only be provided by organized groups or state-affiliated /-financed actors.

MODELLING ATTACK PROCESSES IN OWF

Qualitative process models were developed for each of these four scenarios. These process models describe the steps required to achieve the respective objectives of an attack (Gabriel et al. 2017). This approach of using the attacker's perspective has proven to be very feasible for qualitative modeling, but shows considerable shortcomings when it comes to quantification of probabilities in Bayesian networks. As described above, it is difficult or impossible to estimate valid probability values for intended attacks. Accordingly, it was necessary for the development of Bayesian networks to adopt a perspective from the "defender's" point of view, i.e., from the point of view of safeguarding the protection goals of the infrastructure. As could be determined from previous research by Köpke et al. (2019), the protection goals of wind farm operators include:

- accident prevention (avoidance of accidents between the plant and e.g. ships),
- security (defense against e.g. attacks, vandalism),
- compliance (respecting laws and regulations),
- occupational safety (safety of people in the OWF),
- environmental protection (protection of flora and fauna),
- reputation (image of stakeholders),
- plant safety (functioning of the OWF including operation and maintenance),
- supply reliability (guarantee of energy supply),

- finance (monetary interests).

Qualitative Function Modeling

A common approach for the representation of complex systems or processes is the use of function models (FMs). FMs are a structured representation of the functions, e.g. activities, actions, or operations, the elements of the system or process contribute to its operation. The interaction between individual functions, usually represented by connecting arrows, can be preconditions or flows of mass, energy or information.

Process models were developed for each of the four exemplary scenarios, which describe the process qualitatively and from the perspective of an attacker. In each scenario, the objective is the successful execution of the respective attack or action. The thick black arrows indicate the flow of main functions or process steps, while the dashed arrows connect sub-processes, conditions or framework parameters for carrying out the actual process step.

Figure 2 depicts the example of unauthorized platform access. This scenario has been chosen, as only limited technical equipment is necessary to execute this attack (Table 1). The only technical equipment required is a boat. The knowledge that is needed for this attack covers knowledge with regard to navigate and steer a boat as well as knowing the location of OWFs. The technical and knowledge requirements for a successful execution of the other attack types by far exceeds that level of knowledge and abilities. This in turn highlights the comparatively low threshold to successfully commit an unauthorized access and is the reason why it has been chosen to presented as the example in this paper.

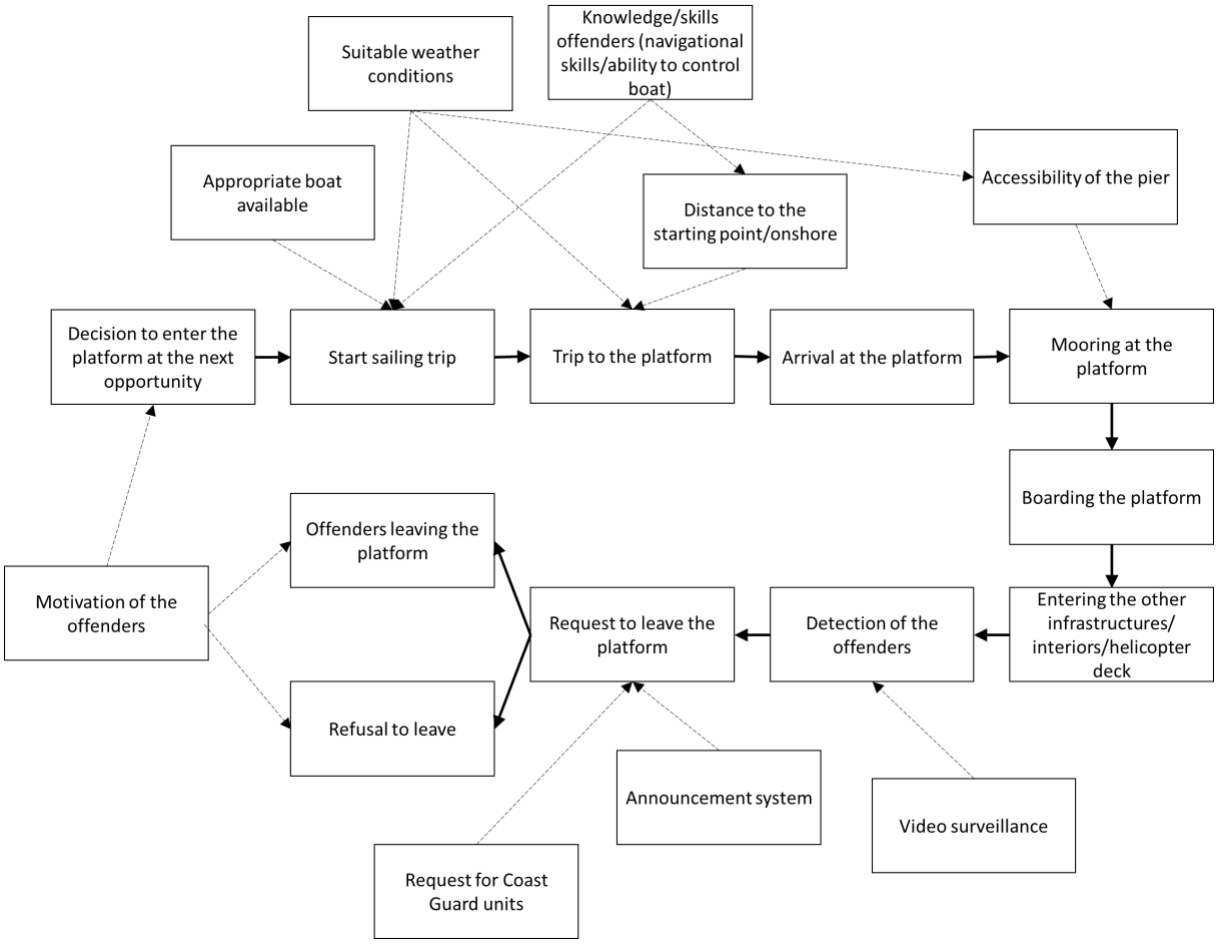

Figure 2. Qualitative function model of unauthorized access to platforms. Thick arrows indicate the flow of the main functions, dashed arrows connecting supporting functions/pre-requisites

Bayesian Networks for Threat Assessment

Risk management generally consists of the following steps: risk identification, risk analysis, risk assessment and subsequently risk treatment by the definition of countermeasures (DIN ISO 31000:2018-10). Hereby, the risk can be assessed using a qualitative, semi-quantitative or quantitative method. A qualitative method for example is a hazard and operability study (HAZOP). This method identifies risks by searching for deviations from the normal

process using keywords like “less” or “more” (Mannan and Lees 2005). Semi-quantitative methods are methods which still use verbal expressions but try to implement categories which can be compared (Brauner et al. 2014; Gabriel et al. 2018). Quantitative methods may be able to deliver the most precise results. They aim at issuing risk with a value which can be determined and ordered by size. Common quantitative methods are for example event tree analysis or Bayesian networks (Zinke et al. 2020).

Bayesian Networks

Several different research disciplines use Bayesian networks (Ramirez Agudelo et al. 2020). Their strength is that they can consider uncertain knowledge (Witte et al. 2020). Bayesian networks are used, for example, in plant safety, especially for determining the spread of pollutants, but also in the maritime sector (Wan et al. 2019; Zinke et al. 2020). Bayesian networks are probabilistic graphical models consisting of directed acyclic graphs. The nodes of such graphs represent the systems variables as probability distributions (PDs), while the edges represent their probabilistic dependencies. Thus, dependent nodes are represented by conditional probability distributions (CPDs) of the form $P\big(v\big|Pa(v)\big)$, where $Pa(v)$ represents the parent nodes of a node v. The notation $P(B|A)$ hereby describes the (conditional) probability that the event B occurs under the condition that A occurred.

The probability of a system of variables $v_i \dots v_N$ to be in a given state X then is the combined probability of the single variables to be in that respective state.

$$P(X) = \prod_{i=1}^{N} P\left(v_i = x_i|Pa(v_i)\right) \tag{1}$$

Since Bayesian networks allow to perform inference, i.e. to consider incomplete and uncertain evidence on observed variables and thus dynamically update the marginal distributions of the missing ones, this makes them especially useful for reasoning about the specific cause of the observations, as well as to estimate their consequences. In the context of risk analysis, it makes them a useful tool to keep track of the current threat level.

The qualitative function models predetermine the structure of the resulting Bayesian network (c.f. section Qualitative Function Modeling).

Modeling and Parametrization

Based on the above qualitative process model, a Bayesian network has been derived in multiple steps: First, the functions of the qualitative process model have been used to describe the series of actions leading to a certain threat to the OWF. Next, supporting functions and pre-requisites (like additional nodes describing the weather) have been added to the network. Finally, the states and their respective conditional probabilities have to be determined for each node.

Since no meaningful probabilities can be determined for some nodes (e.g., motivation of the offenders), these should consequently be excluded from the analysis and the focus shifted to the preservation of the protection goals by adopting the "defender" perspective. For some other nodes (e.g. skills of the offenders), in contrast, only the distinction between qualitative categories like “high” and “low” is possible.

Depending on the node, different techniques were used to obtain the conditional probabilities: While there exists a wide variety of high-quality quantitative data for e.g. any weather-related variables, some nodes need to be defined further, based on scientific publications, technical literature or even expert judgement (Directive 2013/53/EU of 20 November 2013 on recreational craft and personal watercraft, 2013; Hu et al. 2019; Mell 2008; Witte et al. 2020). The following examples shall illustrate these different approaches:

The node “Beaufort wind force ocean” describes the strength of the wind and depends only on the season. For the present analysis, it is only of interest if it is too strong for an intruder to reach the platform, i.e. above six Beaufort. The respective probabilities can be derived from weather data from the Copernicus Climate Change Service and the second data set from the German Weather Service (German Meteorological Service 2021; Hersbach et al. 2018), by counting the points in time, in which the conditions of interest are actually reached in the respective season. The datasets used in this case contains data for the period from January 2019 to February 2021 for a previously determined reference point in the German North Sea north-west of the offshore island of Heligoland. The time resolution of the datasets is one hour.

$$p(windforce > 6|season = s) = \frac{\#\{d \in D|windforce(d) > 6, season(d) = s\}}{\#\{d \in D|season(d) = s\}}$$

$$where\ d\text{: sample of datapoints}, \#\text{: number of datapoints in a given set}$$

The resulting conditional probabilities for the node “Beaufort wind force ocean” are depicted in Table 2. It can be clearly stated that especially in winter the probability of wind forces above six Beaufort is significantly higher than for summer or the other two seasons.

Table 2. Conditional probabilities for the node "Beaufort wind force ocean"

season / wind force	spring	summer	autumn	winter
below 6 Beaufort	0,9771	0,9968	0,9732	0,9119
above 6 Beaufort	0,0229	0,0032	0,0268	0,0881

For other nodes like “successful mooring on platform”, no representative data is openly available. It therefore requires reasonable assumptions to describe its dependencies on its four parent nodes “offender’s knowledge”, “type of boat”, “reach platform” and “suitable weather conditions for successful mooring”. Some of them can be logically deducted from the processes (if the platform has not been reached, it is not possible to moor at the platform, i.e. $p(moor \vee notreached) = 0$) or from limit cases (if the weather conditions are not suitable it is not possible to moor at the platform, i.e. $p(moor \vee unsuitableweatherconditions) = 0$).

If the weather conditions for the type of boat are moderate, the probability depends on the knowledge of the offender. With a higher degree of assumed knowledge, the probability for successful mooring rises. An extract of conditional probabilities is presented in Table 3.

Table 3. Extract of conditional probabilities for the node "successful mooring at the platform"

(M= Monohull, C=Catamaran)

reach platform	yes											
type of boat	Monohull (M)											
offender’s knowledge	High				Medium				low			
Suitable weather conditions / Successful mooring	Yes	Moderate for…		no	Yes	Moderate for…		no	Yes	Moderate for…		no
		M	C			M	C			M	C	
yes	1	0,75	0	0	1	0,6	0	0	1	0,5	0	0
no	0	0,25	1	1	0	0,4	1	1	0	0,5	1	1

As can be seen from the table excerpt, suitable weather is assumed to have a significant influence on the probability of a successful landing and this influence exceeds the influence of an attacker's individual skills or knowledge.

RESULTS

Following the approaches describes in the above sections, the software GeNIe was used to generate the Bayesian network shown in Figure 3. This depiction of a Bayesian network for the scenario of unauthorized access considers the qualitative dependencies from Figure 2 and quantifies them in a reasonable manner. In its current state of development, the network consists of 14 nodes and 21 edges. Once the offenders have boarded the platform, the countermeasures have to be actively taken to preserve the security goals. This in turn means that the threat has occurred, which ends the determination of probability values by the Bayesian network.

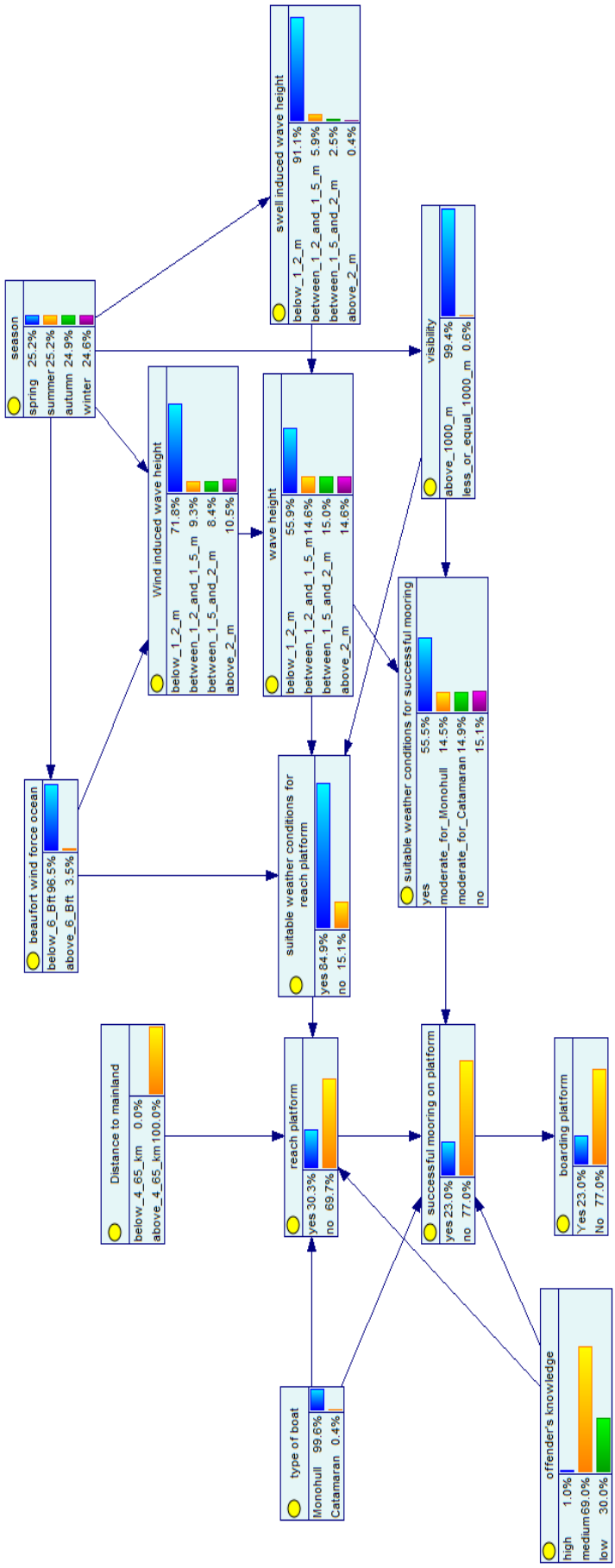

Figure 3. Bayesian network for the threat of unauthorized access to the platform

Using this network, a case study has been carried out as a first test of the Bayesian network. To do so, the states of two nodes are considered to be known, namely the nodes “offenders” and “season”. The first one has been chosen because from previous research it was assumed that the knowledge of the attacker or offender is important for the success of an attack (Gabriel et al. 2017). The second parameter has been chosen because suitable weather conditions are a key factor for a successful arrival at the offshore platforms.

The resulting probability values for the different cases considered in the case study are outlined in Table 4. The overall probability for a successful boarding of the platforms are higher during summer than in winter. However, the knowledge of the offender is crucial to exploit this advantage, as low knowledge will most likely lead to the failure of his attack in any case. In this context, it should be noted that because the qualitative model and the resulting Bayesian network have not yet been validated, the statements can only provide indications. As the subject of further research, these must be substantiated and tested.

Table 4. Probability for successful boarding depending on the season and the knowledge of the offenders

Probability for successful boarding / Knowledge	summer		winter	
	Yes	No	Yes	No
High	82,5%	17,5%	54,8%	45,2%
Medium	40,3%	59,7%	26,5%	73,5%
Low	0,3%	99,7%	0,3%	99,7%

OUTLOOK AND CONCLUSION

The previous research results show that it seems to be possible in principle to determine a threat level for offshore infrastructures and wind farms based on the environmental parameters and capabilities of the attackers or offenders. For the scenario introduced previously, first indications of a possible influence of the various parameters are already provided by the Bayesian network. For example, it can be seen that, depending on the season, the probability of reaching the offshore platforms in the cold seasons is lower than in the warm season. At the same time, the influence of capabilities and wind in particular seem to be of considerable importance for the threat level.

The currently limiting factor is the availability of sufficiently valid probability values for some nodes and edges. In addition to the availability of information, the increasing complexity of the network with the incorporation of additional parameters has to be examined further. For example, the node “offender’s knowledge” could be further separated. Surely the knowledge of the offender influences the outcome of the attack. But only because a possible offender knows how to moor at a platform that doesn’t necessary mean that the person is able to moor at the platform. Accordingly, a distinction between theoretical and practical or procedural knowledge seems advisable.

Using this node as an example, it is apparent that a major problem in Bayesian networks is their validation. The as yet open question of the approach presented here remains the validation of both the qualitative process model on which the Bayesian network is based and the Bayesian network itself. If sufficient information about the network is known, this could be used or a comparison with real events could be performed. However, if, as in the example presented in this paper, the lack of real events and thus of data does not allow validation in the common way, a new solution has to be developed.

For the planned future expansion, it is therefore necessary to involve experts in order to make more meaningful estimates for the probability values of nodes that cannot yet be determined from the literature or from data. At the same time, limitations are also apparent in the application of Bayesian networks in general. For example, the Bayesian network can only ever determine the probability value for the current situation. An estimation of future developments is therefore only possible to a limited extent, whereby the use of dynamic Bayesian networks could offer a worthwhile possibility to at least partially overcome this limitation.

Within the research project ARROWS, it is planned to extend the approach presented here to further scenarios and to link the Bayesian network with other already existing models. This means that e.g. for current wave heights no more probability values have to be determined, but these data can be fed in real time from existing weather models. On this basis, the current threat situation can be predicted even more accurately and future developments can be predicted more precisely. Thus, a set of Bayesian networks should ultimately contribute to support wind farm operators in assessing their current state of security and to assist in the implementation of situation-adapted security measures. A possible further development to evaluate the effectiveness of safety measures also seems worth considering. In conclusion, Bayesian networks can make a valuable contribution to the security of critical

and complex infrastructures, but a meaningful assessment of intentional threats and attacks is only possible in conjunction with other methods (Ezell et al. 2010).

ACKNOWLEDGMENTS

The research project ARROWS (Applied Research on Resilience-driven Offshore Wind Farm Safety and Security) is funded by the German Aerospace Center.

The results for the weather conditions were generated using the Copernicus Climate Change Service information [2018]. Neither the European Commission nor ECMWF is responsible for any use that may be made of the Copernicus information or data it contains.

REFERENCES

Arbeitsgemeinschaft Energiebilanzen e.V. (2020) Stromerzeugung nach Energieträgern 1990 - 2020. o.O. Retrieved from https://ag-energiebilanzen.de/index.php?article_id=29&fileName=ausdruck_strerz_abgabe_dez2020_anteile_.pdf

BP p.l.c. (2020) Statistical Review of World Energy 2020: 69th edition. London, UK. Retrieved from https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2020-full-report.pdf

Brauner, F., Baumgarten, C., Bentler, C., Kornmayer, T., Lotter, A., Lechleuthner, A. M. and Mudimu, O. A. (2014) Methode zur Bestimmung der Vulnerabilität eines schienengebundenen ÖPV-Systems: Interner Projektbeitrag zum AP 4.1. Köln.

Brown, G. G. and Cox, L. A. T. (2011) How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Analysis : an Official Publication of the Society for Risk Analysis*, *31*(2), 196–204. https://doi.org/10.1111/j.1539-6924.2010.01492.x

Carroll, J., McDonald, A. and 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

Crabtree, C. J., Zappalá, D. and Hogg, S. I. (2015) Wind energy: UK experiences and offshore operational challenges. *Proceedings of the Institution of Mechanical Engineers, Part A: Journal of Power and Energy*, *229*(7), 727–746. https://doi.org/10.1177/0957650915597560

Deutsche WindGuard GmbH (2021a) Status des Offshore-Windenergieausbaus in Deutschland: Jahr 2020. Retrieved from https://www.wind-energie.de/fileadmin/redaktion/dokumente/publikationen-oeffentlich/themen/06-zahlen-und-fakten/Status_des_Offshore-Windenergieausbaus_-_Jahr_2020.pdf

Deutsche WindGuard GmbH (2021b) Status des Windenergieausbaus an Land in Deutschland: Jahr 2020. Retrieved from https://www.wind-energie.de/fileadmin/redaktion/dokumente/publikationen-oeffentlich/themen/06-zahlen-und-fakten/Status_des_Windenergieausbaus_an_Land_-_Jahr_2020.pdf

DIN Deutsches Institut für Normung e. V. (2018). *Risk management – Guidelines*. (Norm, DIN ISO 31000:2018-10): Beuth Verlag.

Dunović, I. B., Radujković, M. and Škreb, K. A. (2014) Towards a New Model of Complexity – The Case of Large Infrastructure Projects. *Procedia - Social and Behavioral Sciences*, *119*, 730–738. https://doi.org/10.1016/j.sbspro.2014.03.082

Dutch Ministry of Justice and Security, National Coordinator for Security and Counterterrorism (2009) Working with scenarios, risk assessment and capabilitiesin the National Safety and Security Strategy ofthe Netherlands. Retrieved from https://www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf

Ezell, B. C., Bennett, S. P., Winterfeldt, D. von, Sokolowski, J. and Collins, A. J. (2010) Probabilistic risk analysis and terrorism risk. *Risk Analysis : an Official Publication of the Society for Risk Analysis*, *30*(4), 575–589. https://doi.org/10.1111/j.1539-6924.2010.01401.x

Fraunhofer Institute for Wind Energy Systems (2018). Ausbau der Windenergie in Deutschland: Bisherige Entwicklung und Ausbauszenarien für die Windenergie on- und offshore. Retrieved from http://windmonitor.iee.fraunhofer.de/windmonitor_de/1_wind-im-strommix/1_energiewende-in-deutschland/5_Ausbau_der_Windenergie/

Gabriel, A., Brauner, F., Lotter, A., Fiedrich, F. and Mudimu, O. A. (2018) The determination of critical components of European Rail Traffic Management systems towards cyber-attacks. In K. Boersma & B. Tomaszewski (Eds.), *15th International Conference on Information Systems for Crisis Response and*

Management ISCRAM 2018, Rochester Institute of Technology, Rochester, NY, USA: Conference proceedings (pp. 291–303). Rochester, NY: Rochester Institute of Technology. Retrieved from http://idl.iscram.org/files/alexandergabriel/2018/2108_AlexanderGabriel_etal2018.pdf

Gabriel, A., Schleiner, S., Brauner, F., Steyer, F., Gellenbeck, V. and Mudimu, O. A. (2017) Process modelling of physical and cyber terrorist attacks on networks of public transportation infrastructure. In T. Comes, F. Bénaben, C. Hanachil, M. Laurasa, & A. Montarnal (Chairs), *14th International Conference on Information Systems for Crisis Response And Management,* Albi, France. Retrieved from http://idl.iscram.org/files/alexandergabriel/2017/2028_AlexanderGabriel_etal2017.pdf

German Federal Ministry of the Interior (2009) Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Berlin. Retrieved from https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf;jsessionid=83A0DAC0E11B828CE2061E9CB9DEEB95.2_cid364?__blob=publicationFile&v=3

German Federal Office for Information Security (2015) KRITIS-Sektorstudie: Energie. Öffentliche Version - Revisionsstand 5. Februar 2015. Bonn. Retrieved from https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Sektorstudie_Energie.pdf?__blob=publicationFile

German Meteorological Service (2021). Aktuelle stündliche Stationsmessungen der Windgeschwindigkeit und Windrichtung für Deutschland. Retrieved from https://opendata.dwd.de/climate_environment/CDC/observations_germany/climate/hourly/wind/recent/

Hersbach, H., Bell, B., Berrisford, P., Biavati, G., Horányi, A., Muñoz Sabater, J., Nicolas, J., Peubey, C., Radu, R., Rozum, I., Schepers, D., Simmons, A., Soci, C., Dee, D. and Thépaut, J.-N. (2018). ERA5 hourly data on single levels from 1979 to present: Copernicus Climate Change Service (C3S) Climate Data Store (CDS). Retrieved from 10.24381/cds.adbb2d47

Hu, B., Stumpf, P. and van der Deijl, W. (2019) Offshore Wind Access 2019. Petten. Retrieved from TNO website: https://repository.tno.nl/islandora/object/uuid:e8f05155-aa5a-4aad-a7ba-8bed2e9b08fe

Kim, Y.-G. and Cha, S. (2012) Threat scenario-based security risk analysis using use case modeling in information systems. *Security and Communication Networks*, *5*(3), 293–300. https://doi.org/10.1002/sec.321

Köpke, C., Schäfer-Frey, J., Engler, E. and Wrede, C. P. (2019) A joint approach to safety, security and resilience using the functional resonance analysis method. In *Proceedings of the 8th REA Symposium on Resilience Engineering: Scaling up and Speeding up.* Lnu Press. https://doi.org/10.15626/rea8.10

Liu, C. [Chunlin], Tan, C.-K., Fang, Y.-S. and Lok, T.-S. (2012) The Security Risk Assessment Methodology. *Procedia Engineering*, *43*, 600–609. https://doi.org/10.1016/j.proeng.2012.08.106

Mannan, S. and Lees, F. P. (2005) Lee's loss prevention in the process industries: Hazard identification, assessment, and control (3rd ed.). Amsterdam, Boston: Elsevier Butterworth-Heinemann. Retrieved from http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10186251

Mell, W.-D. (2008) Strukturen im Bootsmarkt: FVSF-Forschungsbericht Nr. 1. Köln. Retrieved from Forschungsvereinigung für die Sport- und Freizeitschifffahrt e.V. website: https://www.bvww.org/forschung/forschungsprojekte/strukturen-im-bootsmarkt?tx_ccdocumentlist_fe%5Baction%5D=download&tx_ccdocumentlist_fe%5Bcontroller%5D=View&tx_ccdocumentlist_fe%5Bfile%5D=898&cHash=eecf652abbe383da1894fcaaf7264a8f

Progoulakis, I. and Nikitakos, N. (2019) Risk Assessment Framework for the Security of Offshore Oil and Gas Assets (IAME 2019 Conference). Athens, Greece. Retrieved from https://www.researchgate.net/publication/334226724_Risk_Assessment_Framework_for_the_Security_of_Offshore_Oil_and_Gas_Assets

Ramirez Agudelo, O. H., Köpke, C. and Torres, F. S. (2020) Bayesian Network Model for Accessing Safety and Security of Offshore Wind Farms. In P. Baraldi, F. Di Maio, & E. Zio (Chairs), *30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference,* Venice, Italy. Retrieved from https://elib.dlr.de/140545/

Robak, S. and Raczkowski, R. M. (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). https://doi.org/10.24425/124268

Sill Torres, F., Kulev, N., Skobiej, B., Meyer, M., Eichhorn, O. and Schafer-Frey, J. (2020) Indicator-based Safety and Security Assessment of Offshore Wind Farms. In *Proceedings of Resilience Week 2020* (pp. 26–33). IEEE. https://doi.org/10.1109/RWS50334.2020.9241287

Staggs, J., Ferlemann, D. and Shenoi, S. (2017) Wind farm security: attack surface, targets, scenarios and

mitigation. *International Journal of Critical Infrastructure Protection*, *17*, 3–14. https://doi.org/10.1016/j.ijcip.2017.03.001

Wan, Y., Liu, C. [Chengyong] and Qiao, W. (2019) An Safety Assessment Model of Ship Collision Based on Bayesian Network. In *Proceedings of the European Navigation Conference 2019* (pp. 1–4). IEEE. https://doi.org/10.1109/EURONAV.2019.8714177

Witte, D., Lichte, D. and Wolf, K.-D. (2020) Threat Analysis: Scenarios and Their Likelihoods. In P. Baraldi, F. Di Maio, & E. Zio (Chairs), *30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference,* Venice, Italy. Retrieved from https://www.researchgate.net/publication/343335721_Threat_Analysis_Scenarios_and_Their_Likelihoods

Zinke, R., Melnychuk, J., Köhler, F. and Krause, U. (2020) Quantitative risk assessment of emissions from external floating roof tanks during normal operation and in case of damages using Bayesian Networks. *Reliability Engineering & System Safety*, *197*, 106826. https://doi.org/10.1016/j.ress.2020.106826