Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
©2022 ESREL2022 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_S16-05-494-cd

A scenario based threat assessment using Bayesian networks for a high voltage direct current converter platform

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

The climate change challenges a variety of aspects in our society. One aspect is the energy production and the composition of the energy mix. Through the last years the amount of offshore wind farms has increased as well as the structure of the electricity producing infrastructure has changed from a more centralized (power plant oriented) to a more regional mode (decentral (offshore) wind farms and solar panels) of production. The vulnerability of the power-generating infrastructure is also changing. Therefore a quantification of the threat level is necessary. This paper should evaluate if a Bayesian network as a quantitative risk assessment model can be used to assess the threat level of an offshore wind farm. Common approaches build a Bayesian network based on a qualitative risk assessment. The Bayesian network presented in the paper is build based on a Functional Resonance Analysis Method (FRAM) based process model because a threat is strongly influenced by the scenario under consideration. The developed approach will be applied to the case study "unauthorized access to an high voltage direct current converter platform (HVDCC)".

Keywords: Bayesian network, Functional Resonance Analysis Method, threat assessment, high voltage direct current converter platform, unauthorized access, offshore wind farm.

1. Introduction

The adaptation to the climate change poses new challenges to energy production. The overarching goal is to minimize the production of greenhouse gases. Therefore the electricity mix of the individual countries needs to be restructured from a fossil based to a mainly renewable based energy mix. To support this paradigm change, according to the German government, the expansion target of the offshore wind industry for 2030 should be 20 GW, which corresponds to an increase of 260% (as of May 2022). The European Union announced support measures with a volume of 800 billion € (Bundeswirtschaftsminister 2016; Internationales Wirtschaftsforum Regenerative Energien 2021; Stratmann 2020) . For this reason it can be expected that the amount of offshore wind energy will increase in medium term. In the past, already a few attacks against offshore platforms took place, like in Nigeria 1998 or Brent Spa 1995 (Kashubsky 2011). The current safety and security status of an offshore infrastructure can be determined using a quantitative risk assessment. This approach is limited when it comes to man-made mutual threats to offshore infrastructures. Therefore paper presents an approach to build a Bayesian network (BN) based on a FRAM. Bayesian networks (BNs) have the advantage that the network structure is represented graphically. Thus, the causal relationships between the nodes can be easily captured by the user. Furthermore, uncertain or incomplete knowledge can be included in a BN. If the value of individual probabilities changes during the development or application of a BN, they can be updated. In addition, after initialization it is possible to make abductive and deductive statements. In contrast to fault trees or event tree analyses, the number of hypotheses per subunit is not limited to a binary logic. The approach is applied to the use case of an unauthorized access to an HVDCC as the core part of all offshore wind farm (OWF).

Section 2 describes the infrastructure “OWF” including the HVDCC and the connection to the land side power grid. This is followed by Section 3 which defines a fictitious attack scenario that combines two past attacks in the offshore industry. In Section 4 the methods FRAM and BN are introduced. Afterwards in Section 5 the transformation from a FRAM to a BN is shown and in Section 6 the approach is tested for a case study. The closing is a conclusion in Section 7.

2. Offshore wind farm

An OWF consists of multiple wind turbines and an offshore substation. The offshore energy is produced by the wind turbines and then forwarded to the offshore substation through the inner grid. From the offshore substation the electricity is then transmitted to an HVDCC. An HVDCC transforms the electricity of multiple offshore wind farms (OWFs) from alternating current to direct current and transmits the electricity to the shore. Onshore, the power is fed into the shore based power grid through an onshore substation. The grid between the offshore and onshore substation is called external grid. (Hau 2014; Robak and Raczkowski 2018) The HVDCCs play a significant role because when the HVDCCs stop operating the energy production of multiple OWFs cannot be submitted to the shore. An HVDCC consists of a support structure which combines the foundation of the HVDCC and the substructure. The substructure carries the topside structure. It combines the technical equipment like the transformer or the cooling system but also supporting areas like accommodation for the staff members. The average distance to the shore amounts to 67,44 km. This distance can be overcome either by helicopter or by ship. For this cases the HVDCC provides a pier and a helicopter landing deck. (Tecklenburg 2021)

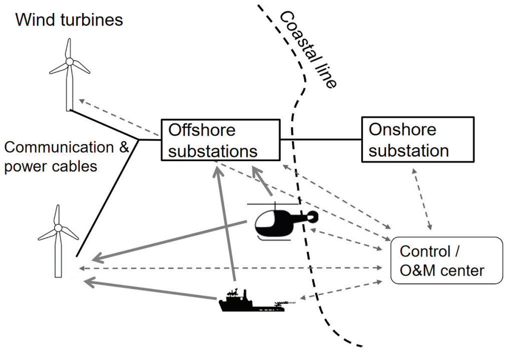


Fig. 1. Exemplary draft of an OWF (source: Sill Torres et al. 2020)

3. Selected scenarios

In the last years a few attacks against energy production as well as storages took place. In one reported incident, a burglary at an onshore substation led to a blackout (unserort.de 2015; waz 2015). Also in the maritime domain attacks by climate activists against oil and gas infrastructures are known. In 1995, Greenpeace activists occupied Brent Spa, an offshore oil storage facility, to prevent the decommissioning operation of the facility. In Nigeria in 1998 over 100 unarmed and peaceful protesters occupied an oil production platform to highlight environmental and distribution topics. (Kashubsky 2011) To be capable of acting in such a situation the operating companies need to know against what kind of scenarios they need to prepare and if the scenario poses a threat to the own process or infrastructure. For this paper an unauthorized access to an HVDCC should be assumed.

4. Method

The aim of this paper is to present an approach that quantifies the probability of occurrence for a selected threat scenario. The method uses FRAM and Bayesian networks. In the beginning a threat scenario is defined and verbally described. This description is the foundation for a FRAM model. From the scenario description the functions and aspects for the FRAM are derived and included in the FRAM model. The FRAM model allows the user to develop a deeper understanding of the scenario. This is possible because a FRAM uses six aspects (input, time, control, output, precondition and resource) that describe under which circumstances and restrictions any respective function (a task or activity) can be executed and therefore guide the user. (Hollnagel 2012) The next step of the approach is to transfer the FRAM into a Bayesian network. First the network structure is defined. Therefore the nodes and edges are derived from the functions and aspects as well as their relation to each other. Second the probabilities are included in the Bayesian network. The data sources can be for example databases, literature information or expert knowledge. (Tecklenburg 2021)

4.1. *Functional Resonance Analysis Method*

The FRAM is used to develop socio-technical systems. The challenge of socio-technical systems is that they are difficult to predict and change before they are completely described. Therefore FRAM does not represent physical components instead the mode of action is shown. There are two main applications for a FRAM either to analyze an incident or a task. Depending on the type of analysis it is often based either on a verbal description or on a Hierarchical task analysis (HTA). During the first development stage of a FRAM the functions and aspects are determined. Thereby the functions describe one or more activities that needs to be achieved to reach a specific goal. A function is depicted as a hexagon. In each corner an aspect is located. The aspects define under which circumstances the function can take place. They are divided into input, output, time, control, resource or precondition. A short description of the aspects can be seen in Table 1. The predecessor and successor nodes are connected by arrows at input and output (see Figure 2). (Hollnagel 2012)

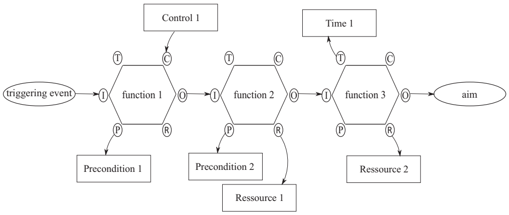


Fig. 2. An exemplary FRAM

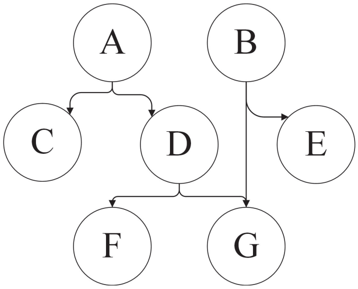


Fig. 3. An exemplary DAG

4.2. *Bayesian network*

BNs belong to the quantitative risk assessment methods. They combine individual risks to an entire risk of the system. The causal relationship is represented in an directed acyclic graph (DAG). It consists of nodes and edges. Thereby the nodes represent the random variables and the edges illustrate the causal correlation (c. f. Figure 3). For example in Figure 3 the node D depends on the node A but is independent of node B. Lets consider the random variables $K_1, \cdots, K_n$. The probability distribution can be determined as in Eq. (1). This mathematical correlation applies for child nodes (nodes with predecessor nodes). In this case the probability depends on the direct parent nodes. This causal correlation can be quantified by the use of the Bayes theorem (see "Eq. (2)"). E describes an event and K_j is a hypotheses of the node K. The probability of the events can be stated like $P(K)$ and $P(E)$. More precise that are marginal probabilities. $P(K|E)$ is the conditional probability that the event K occurs under the condition of event E. Root nodes (nodes with no predecessor nodes) requires marginal probabilities.

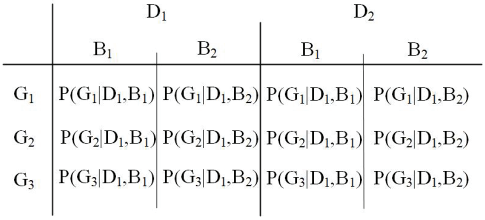
$$P(K_1, \ldots, K_n) = \prod_{i=1}^{n} P(K_i|parents(K_i)) \quad (1)$$

$$P(K|E) = \frac{P(E|K_j) \cdot P(K_j)}{\sum_{j=1}^{m} P(E|K_j) \cdot P(K_j)} \quad (2)$$

Table 1. Description of the aspects used in a FRAM

Abbreviation	Aspect	Short description
I	Input	The input activates or starts the function. It can be either a material, energetic or informative.
T	Time	This aspect covers time points (such as start and end) or time spans like durations for tasks.
C	Control	Objects and procedures that monitor or control the function are considered under this aspect.
O	Output	The output determines the result of the function. Often the output of the first function is the input of the second function.
R	Resource	Resources are subjects which are necessary or consumed during the execution of the function. That includes for example materials, energy or information.
P	Precondition	Requirements that needs to be fulfilled before the function can take place.

ource: (Hollnagel 2012)



	D_1		D_2	
	B_1	B_2	B_1	B_2
G_1	$P(G_1\|D_1,B_1)$	$P(G_1\|D_1,B_2)$	$P(G_1\|D_1,B_1)$	$P(G_1\|D_1,B_2)$
G_2	$P(G_2\|D_1,B_1)$	$P(G_2\|D_1,B_2)$	$P(G_2\|D_1,B_1)$	$P(G_2\|D_1,B_2)$
G_3	$P(G_3\|D_1,B_1)$	$P(G_3\|D_1,B_2)$	$P(G_3\|D_1,B_1)$	$P(G_3\|D_1,B_2)$

Fig. 4. CPT to the nodes B, D and G

Each node is characterized by a set of hypotheses. The number of hypotheses can be freely selected by the user. They describe the status that the node can assume. The probability for each hypothesis of the nodes is summarized in a Conditional Probability Table (CPT). In case of child nodes, all hypotheses of the parent nodes must be considered; if there are several parent nodes, all possible combinations must be listed. If we consider that the nodes B and D in Figure 3 include two hypotheses and the node G includes three hypotheses then the CPT would look like Figure 4.

5. Transformation of FRAM into a BN

This section presents an approach to transfer a FRAM into a BN. Therefore it is first described which preparatory method is often used (see Section 5.1). Then the development of a BN based on a fault tree analysis is described (see Section 5.2). Followed by an approach how to transfer the FRAM into a BN.

5.1. *Example for an often used preparatory method*

(Bobbio et al. 2001) introduce a method to build a BN based on a fault tree. The authors show how an AND, OR and implicit gate in a fault tree can be presented in a CPT. Several publications refer to this technique. For example (Khakzad et al. 2013) build a BN based on a fault tree to evaluate the risk of offshore drilling operations. Or (Yuan et al. 2015) use the method to determine the risk of a dust explosion. Fault trees are used to determine the cause of an event. The main application are large technical systems which are equipped with a high number of protection layers and where a high degree of reliability is required. The different events are connected by discrete logical operators. The two main connection possibilities are AND and OR gates. In case of an AND gate all input needs to be fulfilled. While for the OR gate only one of the inputs needs to be fulfilled. (Lees 2005) Often fault trees have a strong focus on the technical view of the system. For example the fault tree of the bow tie diagram (combination of fault tree and event tree) published by (Yuan et al. 2015) includes 24 root accidents and 20 intermediate events. Only one root accident and intermediate event is related to human behavior . According to (Smith et al. 2017) the accidents which (partly) caused by human errors vary depending on the industry between 75 % and over 90 %. Therefore the operators should not be excluded from the safety and security analysis.

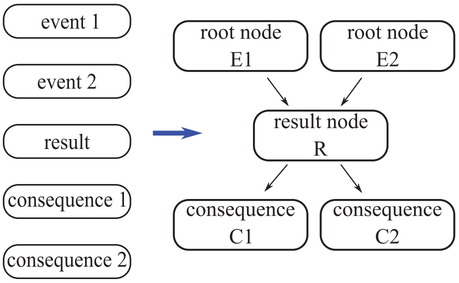


Fig. 5. Construction of the network design (source: Tecklenburg 2021)

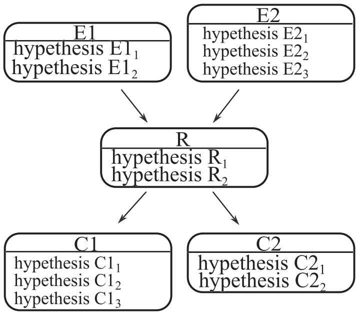


Fig. 6. Determination of hypotheses (source: Tecklenburg 2021)

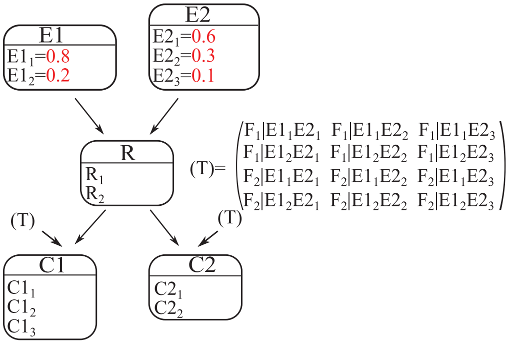

E1
$E1_1$=0.8
$E1_2$=0.2
E2
$E2_1$=0.6
$E2_2$=0.3
$E2_3$=0.1
R
R_1
R_2
(T)=
$F_1|E1_1E2_1$ $F_1|E1_1E2_2$ $F_1|E1_1E2_3$
$F_1|E1_2E2_1$ $F_1|E1_2E2_2$ $F_1|E1_2E2_3$
$F_2|E1_1E2_1$ $F_2|E1_1E2_2$ $F_2|E1_1E2_3$
$F_2|E1_2E2_1$ $F_2|E1_2E2_2$ $F_2|E1_2E2_3$
(T)
(T)
C1
$C1_1$
$C1_2$
$C1_3$
C2
$C2_1$
$C2_2$

Fig. 7. Integration of probabilities (source: Tecklenburg 2021)

5.2. *Development of a BN based on fault tree analysis*

The development of a BN can be subdivided into four main development steps: construction of the network design, determination of hypotheses, integration of probabilities and determination of related vectors. Before the construction of the network design takes place a qualitative risk assessment needs to be done. During the qualitative risk assessment the effects and the causes of the considered events are determined. During the construction of the network design the events, results and consequences are used to generate the network structure. Therefore the nodes represent the events, results and consequences while the edges illustrate the dependencies. The construction of the network design is illustrated in Figure 5.

In the second step the definition of the hypotheses for each node takes place. For a short description of the hypotheses see Section 4.2. The detail degree of the BN is reflected by the number of hypotheses. Figure 6 shows the determination of hypotheses.

After the determination of hypotheses the integration of probabilities follows. Therefore it needs to be divided between root nodes and child nodes (see Section 4.2). The data source for the probabilities can be for example literature data, expert judgement, statistical information/ database extractions or even reasonable assumptions. Important is that the probability distribution is needed for all previous defined hypotheses (see Figure 7).

During the determination of the related vectors. The $\vec{\lambda}$, $\vec{\pi}$ and $\overrightarrow{BEL}$- vectors are associated with the root and child nodes. The π- value describes the current measure for the causal support of a hypotheses. The λ- value illustrates the current measure of diagnostic support of a hypothesis by the child nodes. The BEL-value shows the measure of total confidence in a hypothesis in case that an specific event has been observed. Figure 8 illustrates the determination of the vectors. When all vectors are assigned the construction of the BN is completed. (Tecklenburg 2021)

5.3. *Construction of a BN based on a FRAM*

In case that the BN should be built based on a FRAM instead of an qualitative risk assessment. The procedure is similar to the process which is described in Section 5.2. The main difference is that the construction of the network design varies. First the functions of the FRAM are transferred into nodes of the BN. Thereby the causal connec-

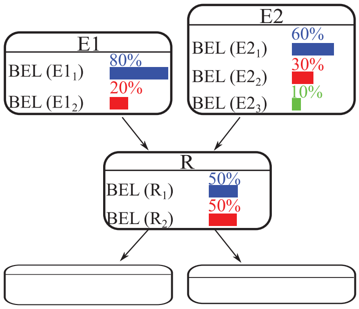


Fig. 8. Determination of related vectors (source: Tecklenburg 2021)

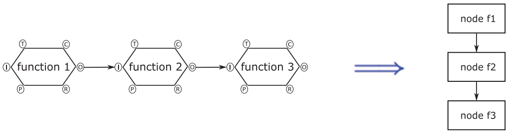


Fig. 9. Transformation of the functions

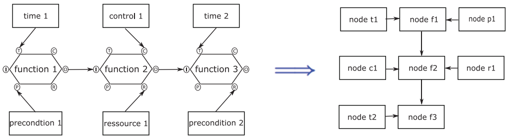


Fig. 10. Transformation of the aspects

tions of the functions are identically included in the BN (see Figure 9). The next step would be to include the aspects of the FRAM. They are also turned into nodes and than connected to the related node of the function. The maxim should be to include all aspects in the BN. But it could also be a decision of the user to leave aspects out in case that they can not be quantified (see Figure 10). When the construction of the network is completed the definition of the hypotheses follows the number of hypotheses should be as low as possible to reduce the complexity of the BN. For the integration of probabilities should be considered that in case it is not otherwise stated multiple aspects to one functions require an AND connection. The connection between the functions needs to be determined based on a content connections. It can be either an AND or OR connection. In the last step the determination of related vectors follows as described in Section 5.2 (Tecklenburg 2021)

6. Case study

The presented approach from Section 5 should be tested for its applicability. Therefore the scenario in Section 3 has been chosen. A scenario description has been developed by a previous thesis (Mieger 2021). This description is the foundation for the development of the FRAM. In this way, functions such as “reach platform” or “loudspeaker announcement: request to leave platform” could be determined. Also the aspects have been defined based on the scenario description. For related aspects to the function “loudspeaker announcement: request to leave platform” are “intact PAGA connection” and “detection pleasure boaters in control room”. This functions and aspects have been turned into the nodes of the BN and the causal connection is reflected by the edges. The BN has been built with the software GeNIe by BayesFusion see (BayesFusion 2020). During the “determination of hypotheses” the number of hypotheses per node depends on the content of the node. The amount of hypotheses should be as low as reasonable possible. For the most nodes two hypotheses have been defined. The maximum number of hypotheses per nodes amounts to four. The data foundation for the “integration of probabilities” varies depending on the nodes. For example probabilities published in the literature (marked in yellow) and data extractions from a database or maritime/ geographical maps (marked in green) have been included. In case that no suitable data could be found, reasonable assumptions (marked in red) have been made. The developed network can be seen in Figure 11. The proposed approach was tested through the case study. Based on the target node, a statement can be made about the current security threat to the process or infrastructure. In order to be able to make a reliable statement, a validated Bayesian network should be used for this purpose.

7. Conclusion

This paper presents an approach to use a BN for a threat assessment. In contrast to existing approaches the BN is built based on a FRAM instead of a qualitative risk assessment method. By using a FRAM as a preparatory method, it is possible not

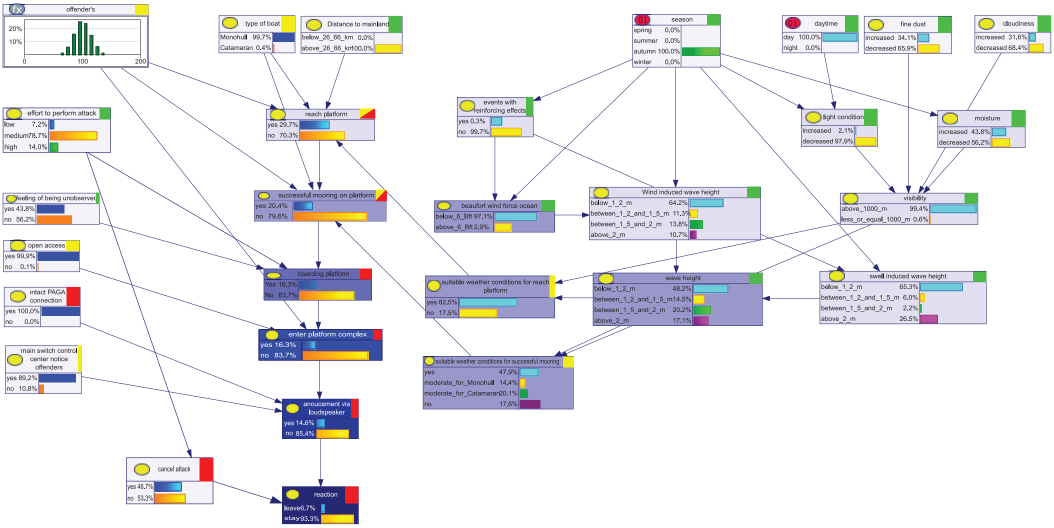


Fig. 11. BN for the scenario “unauthorized access to an HVDCC (source: Tecklenburg 2021)

only to model the technical system but also to consider the human interaction. Another advantage is that through the FRAM method, an understanding of the process can be developed by involving experts. However, one difficulty is that a FRAM does not explicitly represent the logical link between functions. Usually it is apparent from the context, but the method are no representation before. When transferred to the BN, the logical linkage is then represented. A challenge as with any BN is that a lot of data, especially probabilistic values, are needed. So far it is only possible to determine the current state of the threat. The objective of future research activities should be an assessment of the baseline for the related infrastructure as well as a determination of a threshold value which describe if the infrastructure faces a critical threat or not. From a method point of view the BN could be extended to a fuzzy Bayesian network or a dynamic Bayesian network.

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.

References

BayesFusion (2020). Genie modeler: User manual.

Bobbio, A., L. Portinale, M. Minichino, and E. Ciancamerla (2001). Improving the analysis of dependable systems by mapping fault trees into bayesian networks. *Reliability Engineering & System Safety 71*(3), 249–260.

Bundeswirtschaftsminister (2016). Gesetz zur entwicklung und förderung der windenergie auf see.

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

Hollnagel, E. (2012). *FRAM, the functional resonance analysis method : modelling complex socio-technical systems*. Farnham and Surrey and UK England: Ashgate.

Internationales Wirtschaftsforum Regenerative Energien (2021). Windparks in deutschland.

Kashubsky, M. (2011). *Offshore petroleum security: Analysis of offshore security threats, target attractiveness, and the international legal framework for the protection and security of offshore petroleum installations*. disseration, University of Wollongong, Wollongong.

Khakzad, N., F. Khan, and P. Amyotte (2013). Quantitative risk analysis of offshore drilling operations: A bayesian approach. *Safety Science 57*, 108–117.

Lees, F. (2005). *Lee’s loss prevention in the process industries : hazard identification, assessment and control* (3 ed.). Elsevier.

Mieger, J. (2021). *Konzipierung eines Leitfadens zur Erstellung von Schutz- und Sicherheitskonzepten*. Masterarbeit, Hochschule für Wirtschaft und Recht Berlin, Berlin.

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).

Sill Torres, F., N. Kulev, B. Skobiej, M. Meyer, O. Eichhorn, and J. Schäfer-Frey (2020). Indicator-based safety and security assessment of offshore wind farms. In *2020 Resilience Week (RWS)*, pp. 26–33.

Smith, D., B. Veitch, F. Khan, and R. Taylor (2017). Understanding industrial safety: Comparing fault tree, bayesian network, and fram approaches. *Journal of Loss Prevention in the Process Industries 45*, 88–101.

Stratmann, K. (5.11.2020). Eu-kommission macht offshore-windkraft zum 800-milliarden-euro-projekt.

Tecklenburg, B. (2021). *Modeling the safety and security status of a converter platform using Bayesian networks*. Master thesis, Otto von Guericke University Magdeburg and Magdeburg-Stendal University of Applied Sciences, Magdeburg.

unserort.de (2015). Essen: Einbrecher sorgten für stromausfall in altendorf 45143 e.-altendorf.

waz (2015). Einbrecher verursacht stromausfall in essen-altendorf.

Yuan, Z., N. Khakzad, F. Khan, and P. Amyotte (2015). Risk analysis of dust explosion scenarios using bayesian networks. *Risk analysis : an official publication of the Society for Risk Analysis 35*(2), 278–291.