Modeling unauthorized access to offshore platforms using a Bayesian network

1st Babette Tecklenburg
Institute for the Protection of Maritime Infrastructures
German Aerospace Center
Bremerhaven, Germany
Babette.Tecklenburg@dlr.de, ORCID 0000-0003-0606-0381

2nd Alexander Gabriel
Institute for the Protection of Maritime Infrastructures
German Aerospace Center
Bremerhaven, Germany
Alexander.Gabriel@dlr.de, ORCID 0000-0002-9660-1366

3rd Frank Sill Torres
Institute for the Protection of Maritime Infrastructures
German Aerospace Center
Bremerhaven, Germany
Frank.Silltorres@dlr.de, ORCID 0000-0002-4028-455X

Abstract—**Platforms in the offshore wind energy industry are of particular importance for the uninterrupted functioning of the power grid due to their increasing relevance for the security of supply. Therefore, they require an increased level of protection. The paper presents an attempt for a probabilistic threat modeling and assessment based on a Functional Resonance Analysis Method (FRAM). The approach is tested for the attack scenario "unauthorized access to a high voltage direct current converter platform (HVDCC)".**

Index Terms—**Bayesian network, offshore platforms, threat modeling, Functional Resonance Analysis Method**

I. Introduction

In the last ten years, the proportion of renewable energies in the German electricity mix has doubled [1]. One reason is that climate change necessitates a reduction in carbon dioxide emissions. In addition to the advantage that renewable energies do not produce carbon dioxide emissions, no fuel has to be imported. This is in contrast to fossil fuels, with 100 % of hard coal and 94.4 % of natural gas imported in 2020. [2] German society is dependent on energy imports to maintain reliability of supply. Due to geopolitical conflicts, however, there may be a decline in supply, resulting in a significant price increase [3]. To support the energy independence an option would be to increase the amount of renewable energies in the German electricity mix. A high increase can be expected in the offshore wind industry due to the new expansion goals for 2030 [4].

With a higher share of renewable energies in the electricity mix, the transmission grid an beyond structure is also changing. From a more centralized grid structure, dominated by power plants, to a more decentralized grid structure, where renewable energies account for a large share. This changing grid structure leads to new demands (see [5]). Part of the adapted grid structure are, among others, new infrastructures, such as high voltage direct current converter platforms (HVDCCs). They hold a key position because, inter alia, they bundle the produced energy from several offshore windfarms (OWFs) and convert the voltage type from alternating voltage to direct voltage [6]. For this reason, the HVDCC should be specially protected. To achieve this the current threat status needs to be known. This paper presents an approach to determine the current threat level of an offshore windfarm (OWF). Therefore first a model of an attack process using a FRAM is built and then the FRAM is turned into a Bayesian network (BN).

This paper is structured as follows. First, the results of the expert survey and a verbal description of the derived attack scenario is presented in section II. Section III describes the FRAM. The second method, BN, is described in section IV. In section V the combination of FRAM and BN is applied to the attack scenario "unauthorized access to a HVDCC". Followed by section VI, which presents the results and the outlook.

II. Expert interviews in the offshore industry and scenario under consideration

In a recent survey 31 employees and executives from the offshore wind energy industry were questioned about the most relevant attack scenarios in an OWF. The most frequently mentioned scenarios where man-made threats. In particular, terrorism was named first and cyber attacks and collisions with ships was mentioned second. Events such as extreme weather or sabotage, on the other hand, play a more subordinate role in the perception of risks and threats [7].

Terrorism includes a wide range of attacks. Starting with uncoordinated attacks such as a knife attack executed by supposed follower of Islamic state in November 2021 [8]. Or very complex attacks like the September 11 attacks or the Paris attacks in 2015 [9], [10]. The latter attacks need significantly more time for preparation. As well as the offenders needs to be highly organized and connected within the organized crime. Another characteristic how to divide attacks could be the motives of the terrorist that could either be political or ideological as well as religious [11]. In this publication an attack of low complexity is studied. Therefore the authors decided to focus on the scenario of an unauthorized access. A group of young attackers has a sailboat. They spontaneously decide to look at a HVDCC. For this purpose they sail to the HVDCC. There they can moor to the pier as well as enter the superstructure of the platform. Through the internal structure of the platform, they reach the helicopter landing deck. There they are discovered by means of CCTV system and asked to leave the platform. [22]

III. Functional Resonance Analysis Method

The FRAM is a method to model socio-technical systems. Complex activity descriptions or accidents/ incidents are broken down into functions and aspects (see fig. 1). The functions describe intermediate steps, which are necessary to reach the target activity. Functions could be for example “reach platform” or “Successful mooring on platform”. The target activity describes the aim of the process or the caused damage in case of an accident investigation. Aspects define the boundary conditions so that the function can take place. The following six aspects are used: Input (I), Output (O), Time (T), Control (C), Precondition (P) and Resource (R). The input thereby describes what is necessary to start the function. It can be material, energetic or informational. The output determines the result of the function. In most cases the predecessor and successor nodes are connected through the input and output. The aspect “time” describes the duration of a function or the start/ end time. With the aspect “control” it is stated how the function is monitored e.g. through a control center or a task description. The precondition and the resource describes material, energetic and informational boundary conditions which are necessary so that the function can take place. The difference between the two aspects is that resources are needed through the entire function and preconditions only at the start of the function. The advantage of FRAM is that it gives the user a structure for the analysis through the fixed aspects. Furthermore, the effects of possible deviations of the functions can be examined. [12]

IV. Bayesian network for threat assessment

Bayesian networks (BNs) can be used for risk assessment. It can be divided between qualitative, semi-quantitative and quantitative risk assessment methods [14], [15]. The different sub types vary in the detail degree of the generated statements. BNs as a quantitative method make it possible to determine the probability of a certain event. The advantages of BNs are inter alia that also uncertain knowledge can be included and that they follow the logic of qualitative risk assessment [16].
BN can be built on either an qualitative risk assessment or on a FRAM. The authors chose to use a FRAM as a preparatory step because it enables the user to gain an understanding of the operation of a socio-technical process. For the development of a BN the construction and the initialization needs to be done. [22]

A. Construction of Bayesian network

A BN consists of nodes and edges. Thereby the nodes describes events, results or consequences. The edges show the (inter)dependencies between the nodes. During the construction nodes and edges are determined. Therefore the functions and aspects of the FRAM are transferred to the nodes. The edges in the FRAM represent the (inter)dependencies between the function and aspects. They are also transferred as edges to the BN. In the BN the nodes can be connected either serial, convergent or divergent. The network structure of the BN is defined as soon as all required edges are drawn between the nodes. The second part of the construction is the definition of the hypotheses. They define which condition an individual node can assume. The more hypotheses a BN has with the same number of nodes, the more detailed the BN is. [16], [17]

B. Initialization of Bayesian network

The initialization follows the construction. The initialization for root nodes (nodes with no parent node) varies from inner nodes (nodes with parent nodes). Root nodes require a-priori probabilities. An example for a root nodes is the node “type of boat” (see fig. 3).On the other hand, inner nodes require conditional probabilities. The condition emerges from the hypotheses of the parent node(s) (see “(1)” and “(2)”). Here E describes an event and K_j a hypothesis of the node K. A complete set of disjoint hypotheses is described with $j = 1, \ldots, m$. The parent nodes of an the node K_i are described as $parents(K_i)$. n describes the number of nodes. The probability for the event (evidence) E is represented as $P(E)$. If K takes place under the condition E, the notation is $P(K|E)$. The conditional probability table (CPT) include the probabilities for the node for all hypotheses of the parent node(s). For example a CPT for a child node with two hypotheses and two parent nodes (also two hypotheses) includes eight probabilities. The sum of all probabilities per node needs to be equal to one. [16], [17]

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

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

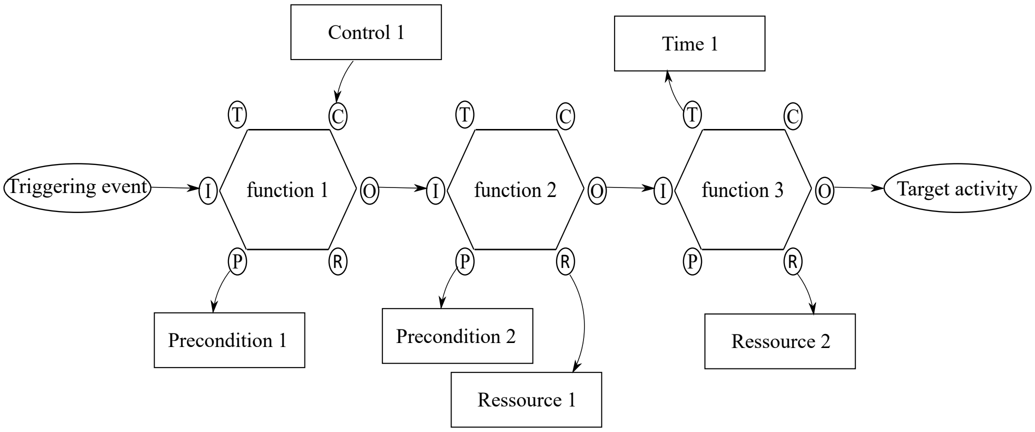

Fig. 1. Exemplary FRAM [13]

V. Case study "unauthorized access to the HVDCC"

Based on the scenario description, a FRAM was developed. First the main steps of the attack were determined. These were then put into a time sequence and connected by arrows at the input and output. It is also possible that functions take place in parallel. When all functions are determined, the aspects of each function are included. An overview of the first function and the related aspects can be seen in table I. During the development of the FRAM, experts as well as scientific publications were consulted for selected issues. [18]–[21] An extract of the FRAM can be seen in fig. 2.
Based on the FRAM the BN was developed. For this the described method from section IV was used. For this purpose, the functions and aspects were transferred into nodes as well as the dependencies. Afterwards the definition of the hypotheses followed. For the node "suitable weather condition for reach platform" for example two hypotheses were defined "yes" or "no" (see fig. 4). By defining the hypotheses, the network construction is completed. Next comes the initialization. Different data sources were used depending on the topic of the node. The source of the data was marked at each node using a colored rectangle. Here, a green rectangle represents a database or maps as the source. Literature sources were marked in yellow. If reasonable assumptions were made, this node was marked red. [22]

As already described, the CPT differ depending on whether it is a root node or an inner node. As an example of the CPT for a root node, consider the node "fine dust". The hypotheses are "increased" and "decreased". [22] The measured values were obtained from the "Norderney" monitoring station of the German Federal Environmental Agency [23]. The following calculation was used to determine the probability. Here D describes the sample of datapoints and # the number of data points in a given set. [22]

TABLE I
First function and the related aspects [22]

function	type of aspect	title of aspect
Reach platform	I	Pleasure boaters sails to the platform
	T	Depending on distance and weather conditions
	O	function: Successful mooring on platform
	O	target activity: Cancellation of sail
	R	Knowledge/ competence offender
	R	Pleasure boat
	P	Suitable weather conditions

TABLE II
CPT for the node "fine dust" according to [22]

hypotheses of the node "fine dust"	probability distribution of the node "fine dust"
increased	0.3416
decreased	0.6584

$$\begin{aligned} p(c_{fine\ dust} \leq 15) &= \frac{\#\{d \in D | c_{fine\ dust} \leq 15\}}{\#\{D\}} = 0.658 \\ p(c_{fine\ dust} > 15) &= \frac{\#\{d \in D | c_{fine\ dust} > 15\}}{\#\{D\}} = 0.342 \end{aligned} \tag{3}$$

The CPT for the node "fine dust" can be seen in table II.

For the inner nodes the calculation of the probabilities looks similar. However, since a conditional probability is used for inner nodes (see section IV-B), the hypotheses of the parent nodes must be taken into account. As an example, the formula for determining the probability for a significant wave height of less than 1.2 m under the condition that the wind and swell induced wave height is also less than 1.2 m, is shown here:

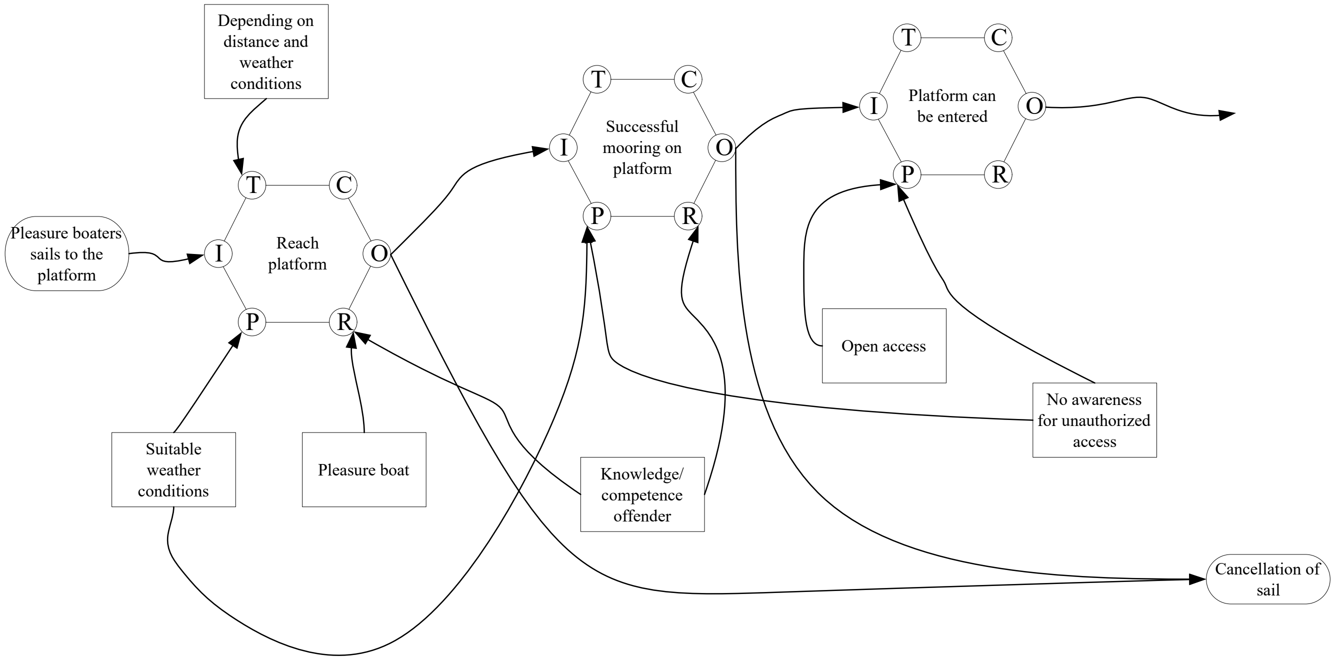
Depending on distance and weather conditions
T
C
I
O
P
R
Pleasure boaters sails to the platform
Reach platform
Successful mooring on platform
Platform can be entered
Suitable weather conditions
Pleasure boat
Knowledge/ competence offender
Open access
No awareness for unauthorized access
Cancellation of sail

Fig. 2. Extraction of the developed FRAM for the attack scenario "unauthorized access" [22]

TABLE III
Extract of the CPT for the node "wave height" according to [22]

swell induced wave height	**< 1.2 m**			
wind induced wave height	**< 1.2 m**	**1.2 m-1.5 m**	**1.5 m-2 m**	**> 2 m**
< 1.2 m	0.8497	0	0	0
1.2 m-1.5 m	0.1362	0.4703	0	0
1.5 m-2 m	0.0141	0.5297	0.7155	0
> 2 m	0	0	0.2845	1

$$\begin{aligned} & p(\textit{wave height} < 1.2 | \textit{wind wave} < 1.2, \textit{swell wave} < 1.2) \\ & = \frac{\#\{d \in D | \textit{wind wave}(d) < 1.2, \textit{swell wave}(d) < 1.2\}}{\#\{d \in D | \textit{swell wave}(d) < 1.2, \textit{wind speed}\}} \\ & = 0.8497 \end{aligned} \tag{4}$$

After the remaining probabilities are determined, they are transferred to the CPT. The CPT for the "wave height" node is shown in table III. All other nodes are quantified in the same way. Once all nodes are initialized, the development of the BN is complete. The BN for the scenario "unauthorized access to a HVDCC" is shown in fig. 3 and fig. 4.

VI. Results and outlook

Through this work, it was shown that a BN can be developed based on a FRAM. This allows a statement to be given about the threat state at the time of analysis. Together with the information whether the threat state is elevated, it can be determined whether a countermeasure is necessary or not. Thus, decision makers can derive their actions based on the probability of the target node. However, a limitation is that the probability distribution of this network has not yet been validated. This will be the subject to future research. One approach is to divide the BN into sub networks and validate these individually. Furthermore, a BN can be used to determine favoring or inhibiting factors for an attack. The advantage in combining FRAM and BN is that it combines a method that focuses more on technical aspects with one that also considers socio-technical aspects. In table IV the methods are compared based on selected criteria. It is interesting to note that in both methods the amount of information needed is high. However, the type of information differs. For a FRAM, information regarding the functions, functional interaction and the variability is needed. Whereas for a BN information regarding the components, probabilities and (in)dependencies is needed. Furthermore, the amount of knowledge about the system at the beginning of the analysis also varies. To develop a BN, prior knowledge about the process or system is necessary. Whereas in the development of the FRAM, the user must have less detailed knowledge at the beginning of the analysis, but must involve experts during the development. A major difference between the two methods is that the development of the FRAM is a guided process in which the six different aspects are specified. While the development of the BN is a free process. A big difference is that a FRAM is a qualitative

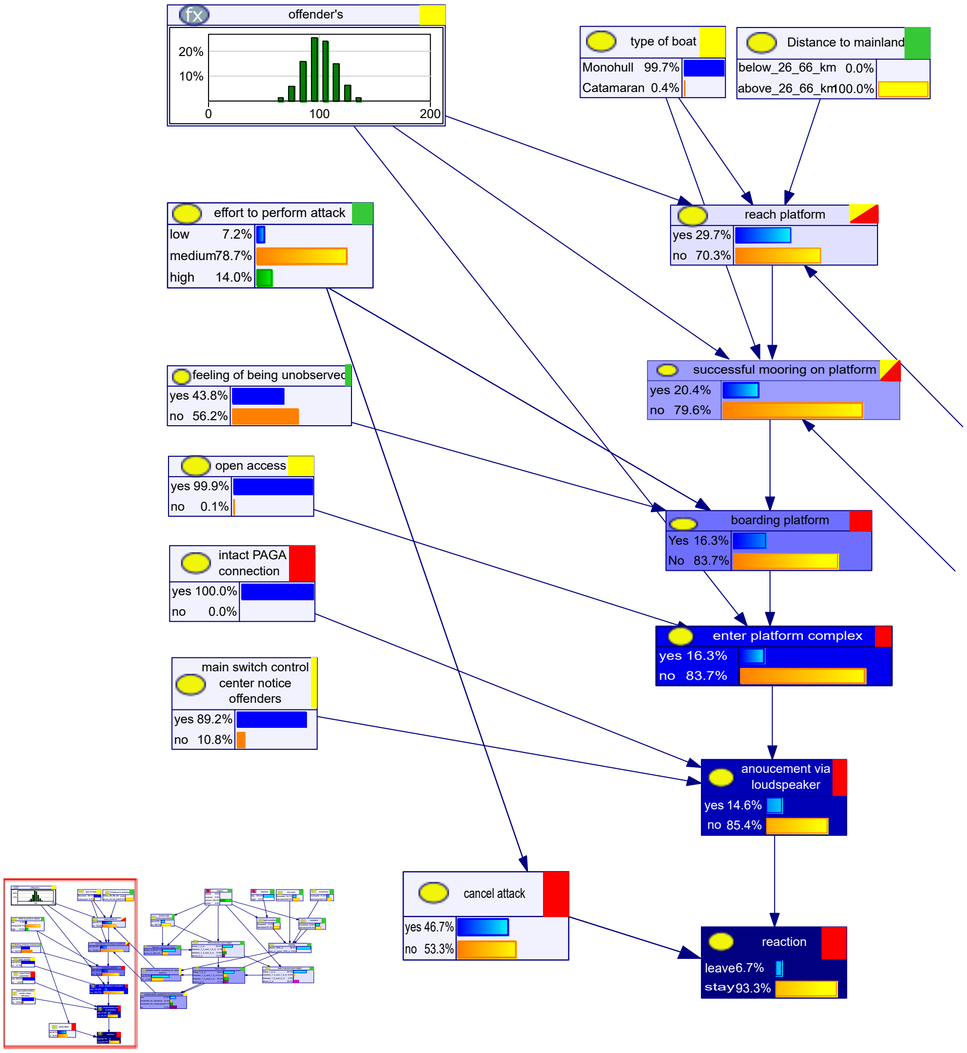

Fig. 3. Bayesian network of the scenario unauthorized access part 1

TABLE IV
COMPARISON OF THE METHODS PROCESS MODEL AND BAYESIAN NETWORK FOLLOWING [22]

topic of comparison	**FRAM**	**Bayesian network**
amount of information required	high	high
type of information required	functions, functional interaction and variability	components, probabilities and (in)dependencies
degree of knowledge about system	for user lower, but expert needs to be at hand	prior knowledge needed
system description	guided	unguided
quantifiable	no	yes

model, while a BN is a quantitative model. Thus, the two methods can complement each other well.

REFERENCES

[1] German Environment Agency, Renewable energies in figures , https://www.umweltbundesamt.de/themen/klima-energie/erneuerbare-energien/erneuerbare-energien-in-zahlen#ueberblick, accessed: 09.03.2022.

[2] German Environment Agency, Primärenergiegewinnung und -importe , https://www.umweltbundesamt.de/daten/energie/primaerenergiegewinnung-importe, accessed: 09.03.2022.

[3] tagesschau, Ölpreis steigt weit über 100 Dollar, https://www.tagesschau.de/wirtschaft/konjunktur/oelpreis-brent-100-dollar-101.html, accessed: 09.03.2022.

[4] Bundeswirtschaftsminister (2016). Gesetz zur Entwicklung und Förderung der Windenergie auf See.

[5] A. Gabriel et al. (2021), Threat analysis of offshore wind farms by Bayesian networks – a new modeling approach. In: A. Adrot, R. Grace, K. Moore and C. Zobel (eds.): Proceedings of the 18th ISCRAM Conference. Blacksburg.

[6] E. Hau, Windkraftanlagen, Vol. 5, SpringerLink, Heidelberg, 2014.

[7] A. Gabriel et al. (2022, in publication), Threat and risk scenarios for Offshore wind farms and an approach to their assessment. In: H. Karray, A. de Nicola, N. Matta and H. Purohit (eds.): Proceedings of the 19th ISCRAM conference. Tarbes.

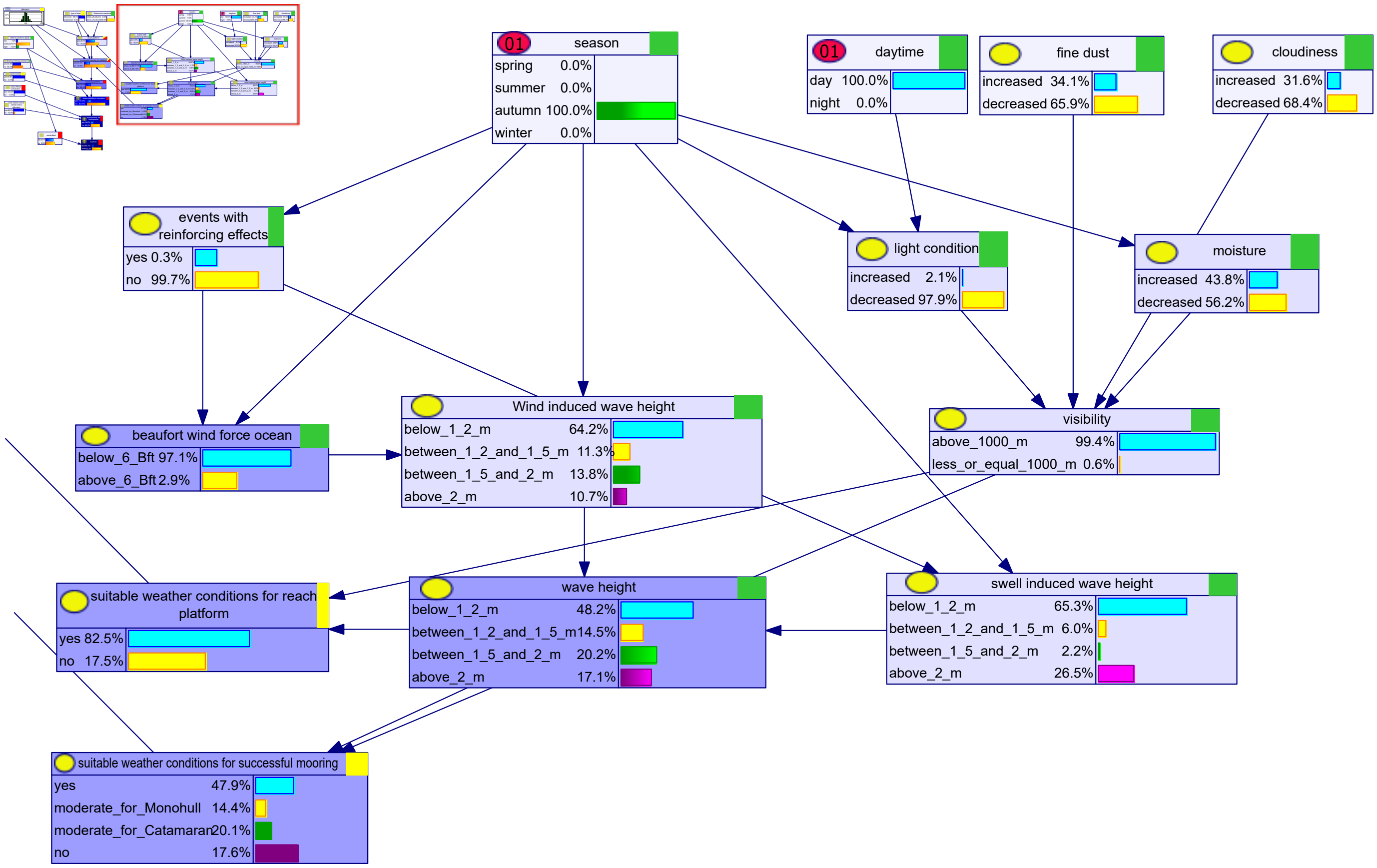

Fig. 4. Bayesian network of the scenario unauthorized access part 2

[8] Zeit online, ICE-Messerangriff womöglich islamistisch motiviert, https://www.zeit.de/gesellschaft/2021-11/messerattacke-ice-extremismus-ermittlungen, accessed: 09.03.2022.

[9] Y. Neria, D. Roe, B. Beit-Hallahmi, H. Mneimneh, A. Balaban, R. Marshall, The Al Qaeda 9/11 instructions: a study in the construction of religious martyrdom, Religion, Vol. 35, 2005.

[10] Europol, European union terrorism situation and trend report 2016 (TE-SAT), https://www.europol.europa.eu/cms/sites/default/files/documents/europol_tesat_2016.pdf, accessed: 09.03.2022.

[11] A. Gabriel et al. (2017), Process modelling of physical and cyber terrorist attacks on networks of public transportation infrastructure. In: T. Comes, F. Bénaben, C. Hanachi, M. Lauras, A. Montarnal, (eds.): Proceedings of the 14th ISCRAM Conference. Albi

[12] E. Hollnagel, FRAM: the functional resonance analysis method : modelling complex socio-technical systems. Farnham, Surrey, 2012.

[13] B. Tecklenburg, A. Gabriel, 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. Dublin.

[14] U. Hauptmanns, Prozess- und Anlagensicherheit, Vol. 2, Springer-Verlag, Berlin, 2020.

[15] J. Zehfuß, Leitfaden Ingenieurmethoden des Brandschutzes, Vol. 4, Vereinigung zur Förderung des Deutschen Brandschutzes (vfdb), Münster, Braunschweig, 2020.

[16] R. Zinke, J. Melnychuk, F. Köhler, U. Krause, 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, Vol. 197, 2020.

[17] B, Cai, Y. Liu, Z. Liu, Y. Chang, L. Jiang on Bayesian Networks for Reliability Engineering, Singapore: Springer Singapore Pte. Limited, 2020.

[18] B. Tecklenburg, Alarmierung Küstenwache, Telefon, 11.12.2020.

[19] B. Tecklenburg, Bedrohungsanalyse für offshore Windenergieparks, Telefon, 24.11.2020.

[20] United Nations, International Convention for the Safety of Life at Sea, 1974.

[21] G. Katsouris, L.B. Savenije, Offshore Wind Access, Petten: ECN, 2017.

[22] B. Tecklenburg, Modeling the safety and security status of a converter platform using Bayesian networks, Otto-von-Guericke University Magdeburg, 2021.

[23] Umweltbundesamt, Akltuelle luftdaten, https://www.umweltbundesamt.de/daten/luft/luftdaten/luftqualitaet/eJzrWJSSuMrIwMhQ19BA18hgUUnmQstFeakLFhWXLLY0MVqc4lYElzY0XpwSko-sOreKbVFuctPinMSS0w6eq-a20g8o5F4dPFrMBe8Ak1Q==, accessed: 05.07.2022.