Bayesian Network Model for Accessing Safety and Security of Offshore Wind Farms

Oscar Hernán Ramírez-Agudelo

Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center, Germany.
E-mail: oscar.ramirezagudelo@dlr.de

Corinna Köpke

Fraunhofer Institute for High-Speed-Dynamics, Ernst-Mach-Institut, EMI, Germany. Formerly at: Institute
for the Protection of Maritime Infrastructures, German Aerospace Center, Germany.
E-mail: Corinna.Koepke@emi.fraunhofer.de

Frank Sill Torres

Institute for the Protection of Maritime Infrastructures, German Aerospace Center, Germany.
E-mail: Frank.SillTorres@dlr.de

The offshore wind industry experience a rising importance for the worldwide energy production, which is accompanied by increasing amount of wind turbines and Offshore Wind Farms (OWFs). However, due to its harsh environment and its role for energy provision, OWFs are confronted with several threats that are impacting its safety and security. Consequently, decision making at design as well as run time plays an important role for providing safe and secure operation in OWFs. We propose in this work the application of a Bayesian Network (BN) for a high-level representation of the safety and security state of an OWF. The developed BN-model is based on the safety and security goals and related functions defined in Köpke et al. (2019). The derived model enables a user to analyze the overall importance of high impact functions, like compliance, environmental protection, supply reliability or accident prevention. Obtained results indicate that the proposed BN-model enables decision makers to explore cross-system interrelations, and thus, to define requirements for implementations on lower design levels.

Keywords: Offshore Wind Farms, Safety, Security, Bayesian Network.

1. Introduction

The offshore wind industry provides a reduced emission form of energy production that is continuously gaining importance in the world-wide energy provision with annual growth rates of nearly 30% (see O'Sullivan, 2020). In 2019, Europe had a total offshore wind energy production of 67 TWh, which corresponds to 2.3% of the total EU electricity consumption (Komusanac et al., 2020). This trend also has economic implications, reflected by the prediction that by 2030 the offshore wind power shall be responsible for 8% of the total ocean economy adding USD 230 billion of value (OECD, 2016).

However, Offshore Wind Farms (OWFs) are confronted with plenty safety and security threats. This results mainly from its harsh environment, the considerable complexity as well as its role as a relevant power generation system. For example, failing components are recurring obstacles in OWFs requiring well-established maintenance processes (Carroll et al., 2016). These processes, though, are prone to further challenges in terms of safety and security.

Several works have focused on the employment of indicators for supporting the assessment of the safety level of OWFs. For example, Pfaffel et al. (2019) discuss the application of Key Performance Indicators (KPIs) for the operational management of offshore and onshore wind turbines. Seyr and Muskulus (2016) analyze safety specific indicators for OWF and conclude that most of the indicators applied today are relevant when compared to reported incident data. Furthermore, Gonzalez et al. (2017) review KPIs for the operation and maintenance of offshore and onshore wind farms.

However, indicator-based solutions are restricted by the vast complexity and multitude of stakeholders of OWFs. Consequently, only few works discuss the interrelation between requirements in terms of safety and security as well as economy, environment and compliance with regulations (see for example Aghahowa and Allen, 2007). Based on this observation, Köpke et al. chose a different approach by using a functional model (see Section 3 of Köpke et al., 2019). The authors identified and classified the main stakeholder goals in OWFs and employed the Functional Resonance Analysis Method (FRAM; Hollnagel and Goteman, 2004; Hollnagel, 2012) in order to represent the correspondent relations. Furthermore, the authors integrated a straightforward probabilistic model and Monte-Carlo simulations for the determination of the functions of OWFs that are most susceptible to failures.

In this work, we propose an extension of this model by adopting a Bayesian Network Analysis (BNA), which leads to a more formal approach for exploring relations within OWFs in terms of safety and security. Using the resulting model and with help of expert knowledge one can determine how a failing function impact other functions in this complex system as well as to help to how design changes, e.g. the hardening of selected functions, influence the system stability.

The rest of this work is structured as follows. Section 2 reviews the identified safety and security goals. Section 3 describes the methodology adopted in this work. The model is presented on Section 4. The results and implications are discussed in Section 5. Conclusions are summarized in Section 6.

2. OWF safety and security goals

This section reviews the safety and security goals in OWFs and discusses a functional model of OWF presented in previous works.

2.1. *Stakeholder perspective*

In order to derive safety and security goals, Köpke et al. (2019) identified stakeholders and their objectives in the field of *OWFs*. Stakeholders are e.g. owners, operators, work-managers, coastguards, vessel and air traffic services. The authors continued to analyze their tasks and objectives in the OWF and proceeded to classify their goals in nine different categories (see Table 1).

Table 1. OWF safety and security goals taken from Köpke et al. (2019).

#	Safety and security goals
1	Accident prevention
2	Security
3	Compliance
4	Occupational safety
5	Environmental protection
6	Reputation
7	Plant safety
8	Supply reliability
9	Finance

It is important to note that the goals are interrelated. It means any change in the status of any category may have an impact on the others. For example, if the surveillance of an *OWF* is not sufficient in a way that it leads to an accident. Then the safety of the plant may most likely be compromised; namely a change in accident prevention decreases the plant safety and may even affect security.

Subsequently, Köpke et al. focused on five safety and security goals, i.e. #1, #2, #4, #5, and #7 (see Table 1). They detailed these five objectives in 64 different functions. The functions are presented in Table 2 where they are organized in sub-categories, namely: *i)* detailed safety and security goals (function #1 to 21), *ii)* safety and security measures (function #22 to 53), and *iii)* analysis of sensor data (function #54 to 64) (see Table 1 of Köpke et al., 2019).

2.2. *Probabilistic FRAM model*

In Köpke et al. (2019), interrelations between safety and security goals as well as all the functions in Table 2 are defined. These relations were implemented using a *FRAM-model*. Based on the interrelated functions, the authors proceed to carry out a *Monte Carlo* simulation where each function had three features, i.e. *i)* a scalar which represented the probability to fail, *ii)* a scalar providing the time (in days) it takes to restore the function when it got broken, and *iii)* a factor with which that particular function may influence the ones it is related to.

In this work, we are using the *FRAM-model* in order to implement the *BN-model* in Sect. 4. The failure probabilities given in Table 2 represent the probability of being false F. Conditional proba-

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference

1758

Table 2. List of all functions with probability to fail p and influencing factor f. *ROV* (Remotely Operated Vehicle), *OSS* (Offshore Sub-Station), *Unexploded Ordnance*, *PPE* (Personal Protection Equipment), *AIS* (Automated Identification System), *CMS* (Condition Monitoring System), *EPIRP* (Emergency Position-Indicating Radio Beacon), *CCTV* (Close-Circuit TeleVision), *PLB* (Personal Life Beacon).

#	Function name	p	f	#	Function name	p	f
1	Protect plants	L	L	33	Firefighting	L	H
2	Protect water quality	M	M	34	Fire detection	L	H
3	Protect whales	L	L	35	Safe transfer	L	H
4	Protect fish	L	L	36	Measures Helicopter	L	H
5	Protect birds	L	L	37	Measures climbing	M	M
6	Protect bats	L	L	38	Measures diving	M	M
7	Safety plane	L	H	39	Rescue chain	L	H
8	Safety helicopter	M	H	40	Telemedicine	M	M
9	Safety ship	M	H	41	Shelter	L	M
10	Safety ROV	H	L	42	Regular maintenance	L	H
11	Safety submarine	L	H	43	Traffic control	L	M
12	Protect foundation	L	H	44	Guard vessel	M	L
13	Protect tower	L	H	45	PPE	M	L
14	Protect rotor/nacelle	M	H	46	Landing area	M	L
15	Protect cable	L	H	47	Trainings	L	L
16	Protect OSS	L	H	48	Decompression chamber	L	L
17	Protect converter station	L	H	49	IT-security	M	H
18	Safety of worker	M	M	50	Prevent espionage	L	H
19	Shipwrecked men rescued	L	L	51	Repel attacks	L	H
20	Safe communication	M	M	52	Avoid manipulation	L	H
21	Safe data	L	M	53	Access Control	L	H
22	Avoid pollutants	L	H	54	Observe leakage	L	M
23	Bubble curtain	L	L	55	Observe water quality	L	M
24	Observe population	L	L	56	AIS	L	H
25	Avoid collision plant/animal	M	M	57	Weather data	M	M
26	Collision avoidance	L	M	58	Heat detection	L	H
27	Sonar transponder	L	M	59	Smoke detection	L	H
28	Warning lights	M	M	60	CMS	L	M
29	Weather measures	M	M	61	EPIRB	L	H
30	UXO clearance	L	H	62	People tracking	L	M
31	Avoid technical failure	M	M	63	CCTV	M	M
32	Lightning protection	L	H	64	PLB	M	L

Source: Table adopted from Köpke et al. (2019).

bilities are derived from these basic failure probabilities influenced by adjacent functions and the respective factors f (see Sections 3.1 and 4). The restoration times are not employed as in Köpke et al. (2019), they were only used in their work to carry out the Monte-Carlo simulation. The probability of failure p has the values of low (L, 0.005), medium (M, 0.015) and high (H, 0.02). The factor to influence functions f has the values of low (L, 1.05), medium (M, 1.2) and high (H, 1.35), as adopted in Köpke et al. (2019, see also Table 2).

3. Methodology

This section presents preliminary information regarding the theory behind Bayesian Networks as well as the supporting programming library.

3.1. *Bayesian Networks — BNs*

BNs are one of the most popular probabilistic graphical models. Its application are wide and vary from Computer Vision to support of Medical Diagnosis (for some examples see Zhou and Huang, 2006; Luciani et al., 2003). BNs are *Di-*

rected Acylic Graphs − *DAGs* − which represent random variables and their conditional dependencies. BNs combine the *DAGs* with probability theory to provide practical means for representing and updating probabilities about events of interest. In order to do so, BNs make use of the *Bayes rule* for calculation of the posterior estimate.

Lets consider two different variables A and B, where their probabilities are expressed as $P(A)$ and $P(B)$, respectively. The conditional probability $P(A|B)$, following *Bayes rule*, is given by:

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)} \qquad (1)$$

where in Eq. 1, $P(A)$ is the prior estimate, $P(B)$ is the marginal probability of B, $P(B|A)$ is the likelihood, which is the probability of B given A. Finally, $P(A|B)$ is known as the posterior distribution, which is the probability of A given B.

The *DAG* consists of nodes and a set of edges. As its name suggests, the nodes are directly connected. Figure 1 shows an exemplary schematic representation of such a *DAG*. In this example, one of the edges goes from A to C, meaning that C is the child of A and at the same time A is the parent of C and D. In the same way, one can continue and mention the rest of the sets of parents and child of the representation shown in this figure.

In this formulation the nodes can either be independent or dependent. In Fig. 1 the node A and B are the *independent nodes* and C, D, and E are the *dependent nodes*. For each *dependent node*, its probability value is provided by a *Conditional Probability Table* (CPT) on the parent node(s), respectively. Such CPT contains one probability value for every possible combination of child and parent states (Murphy, 2012).

Lets assume a BN with the following structure (X, E), where X represents the random variables $X = \{x_1, x_2, ..., x_N\}$ of the nodes and E represents the edges with conditional independent probabilities between the nodes. The *join probability distribution* of this BN with N nodes has the following form:

$$P(X) = \bigcap_{i=1}^{N} P(x_i|Par(x_i)) \qquad (2)$$
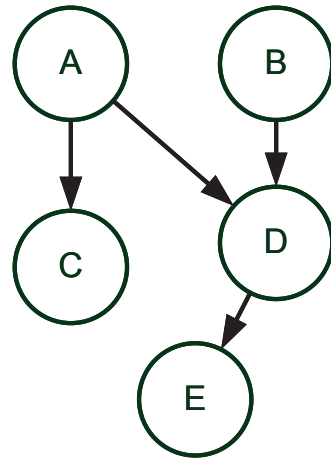
where in Eq. 2 has been used the chain rule,

Fig. 1. Schematic representation of the *DAG*.

besides $Par(x_i)$ denotes the set of parent nodes of the random variable x_i. The nodes outside $Par(x_i)$ are conditionally independent of x_i.

3.2. *Pomegranate*

In order to implement our *BN-model*, we made use of *pomegranate* (Schreiber, 2017), which is a machine learning package. It has implemented several probabilistic models; such as: General Mixture, Markov Chains, Bayesian Networks, Naive Bayes, etc. Its great advantage is that: *(i)* it is an open source package, *(b)* it works with *Python* and its implementation is being done in *Cython* in order to speed up the calculations, and *iii)* it allows multi-threaded parallel execution so that can handle big amount of data. Therefore, Schreiber made *pomegranate* a versatile tool ready to be applied to a wide variety of cases.

4. Bayesian Model for safety and security

This section presents a model that relies on Bayesian Networks (BNs) and permits the investigation of safety and security goals in OWFs. First, we introduce the parametrization of the probabilities adopted for the *independent nodes*, i.e. discrete distributions, and *dependent nodes*, i.e. CPTs. This is followed by the presentation of the implemented OWF *BN-model*.

4.1. *Parametrization*

A common challenge of BNs is the definition of the probabilities. If sufficient data are available

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference

1760

one can employ e.g. the maximum likelihood approach Le Cam (1990) or other learning techniques. However, for high-level abstractions as considered inhere, one has to rely mostly on expert knowledge (Lichte and Wolf, 2019). Here, we make use of expert knowledge provided in Section 2. Table 2 summarizes this knowledge by introducing the failure probability and the influence factor for each node as described in Köpke et al. (2019).

In our BN approach, the probability P of a node N being true T or false F depends on whether the node is dependent or independent of other nodes. For independent nodes, the probability of failure, i.e. $P(N = F)$, and the probability of functional as desired, i.e. $P(N = T)$, are given by the following discrete distribution:

$$P(N_i = F) = p_i \qquad (3)$$
$$P(N_i = T) = 1 - p_i \qquad (4)$$

where p_i refers to the probability of failure of node N_i given in Table 2.

For the dependent nodes, probabilities of being true T or false F are given by conditional probabilities, i.e. CPTs, dependent on their parent nodes (see Section 3.1). Assuming that the node N_i is now a dependent node, it has a set of M parent nodes, i.e. $Par(N_i) = \{X_1, X_2, ..., X_M\}$. The conditional probability of failure for the dependent node is given by:

$$P(N_i = F|Par(N_i)) = p_i \bigcap_{j=1}^{M} F_j \qquad (5)$$

where

$$F_j = \begin{cases} 1 & \text{if } P(X_j = T) \\ f_j & \text{otherwise} \end{cases}$$

The factor f_j is given along with p_i in Table 2. The probability of a dependent node working as desired is given as:

$$P(N_i = T|Par(N_i)) = 1 - P(N_i = F|Par(N_i)).$$

Finally, equations 3-5 are employed to determine the probabilities used as input values for the safety and security *BN-model* of the OWF.

4.2. *Generic OWF model*

Having the probabilities, we can then proceed to work out our model based on the interrelations defined in the *FRAM-model* (see Section 2 and Köpke et al., 2019).

Figure 2 shows the overall safety and security model of a generic OWF as *directed acylic graph*. In this representation, the sixty-four (*64*) functions of Table 2 become the *nodes* and their relations the *edges*. The *nodes* are formed by: (*i*) goals, (*ii*) measures, and (*iii*) analysis of sensor data. There are in total twenty seven (27) *independent* and thirty-seven (37) *dependent* nodes, respectively. The *independent nodes* are boldfaced in the first column of Table 1. This model has been implemented as a *BN-model* by using *python-pomegranate* (see Section 3.2; Schreiber, 2017).

After all values of the *BN-model* have been computed, each node inherits the probability of $P(T)$ and $P(F)$, which corresponds to the probability of whether that node is functional or not[a]. That probability, i.e. whether a node is functional or not, depends on the joint probability. For the *dependent nodes*, the joint probability is a function that considers the probabilities of the nodes on its incoming edges and the probability of the node itself, which is represented via its CPT (see equation 2 in Section 3.1). For example, in Figure 2, the value of node *Avoid Pollutants* depends on the nodes *Observe Leakage* as well as *Observe Water Quality*.

5. Results and Discussions

This Section explores the implemented and parameterized *BN-model* and discusses the results.

5.1. *Initial State*

Figure 3 shows the resulting distribution of $P(F)$ for each node in the network. Besides, the average failure probability of the network is $\overline{P(F)} = 0.008 \pm 0.005$. As expected, the results are similar to the ones reported in Köpke et al. (2019). However, in contrast to what was determined by Köpke et al., the most susceptible node is *Safety ROV*, and not *Safety of worker*. While the latter has a probability of failure of $P(F) = 0.0153$ (node number # 18 in Table 2), the former has probability of failure with $P(F) = 0.0201$ (node number # 10).

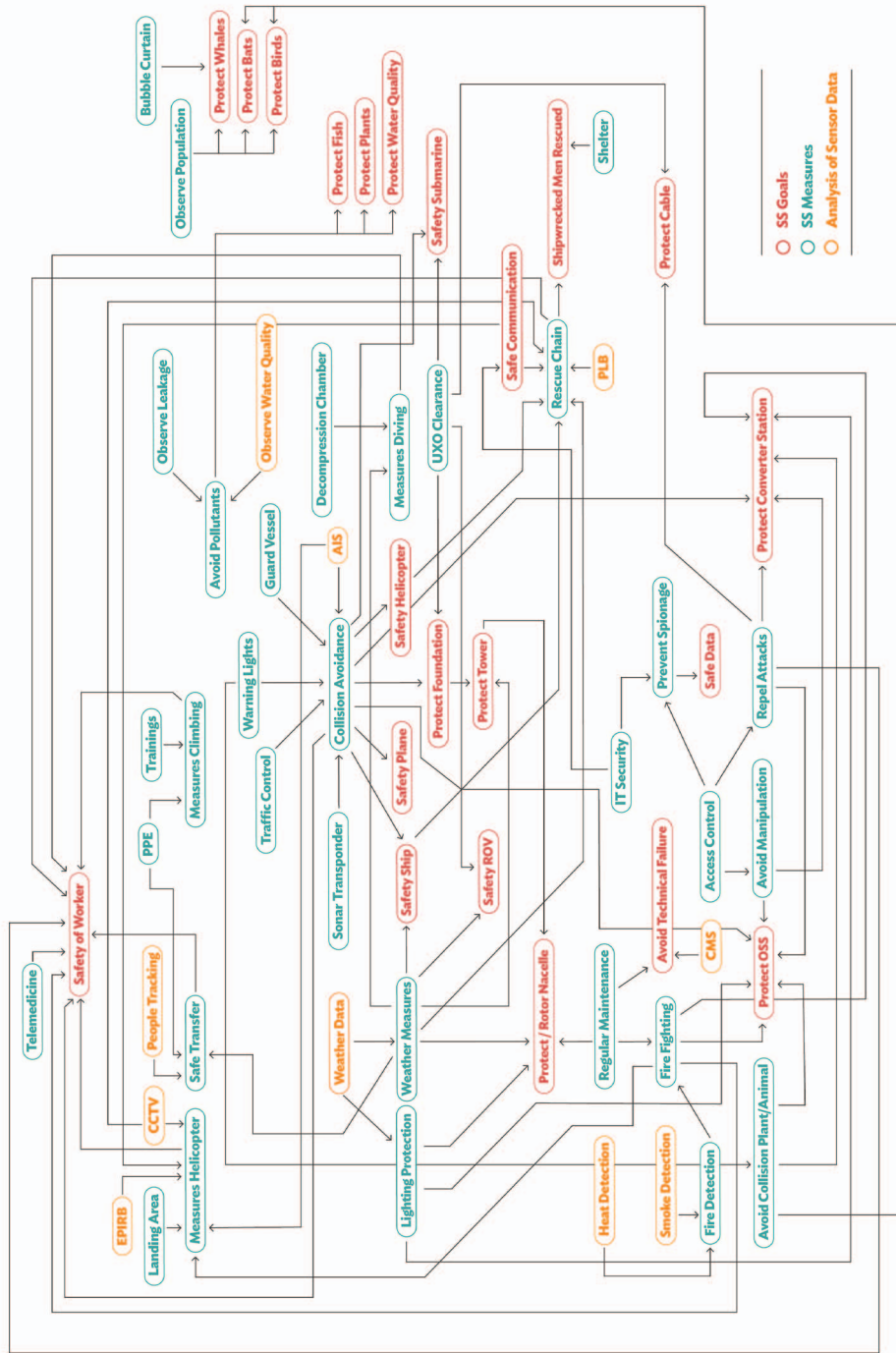[a]The sum of both needs to add up to one, i.e. $P(T) + P(F) = 1$.

Fig. 2. Bayesian Network model for accessing the Safety and Security (SS) in an OWF. The colors refer to *i*) detailed SS goals (red), *ii*) SS Measures (green), and *iii*) Analysis of Sensor Data (orange).

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference

1762

This results mainly from the different way of carrying out the analysis. While the authors in Köpke et al. (2019) analyzed the varying failure rate over time, the inference executed in here determines the overall probability.

5.2. *Variations of the initial model*

In order to explore the applicability of the developed model, we modified the failure probability of the *independent nodes* and determined the impact on the model (see Figure 4 for the ratios of the new failure probabilities). In detail, we decreased the failure probability of these nodes by 20 % (red stars in Figure 4), while in the second experiment we increased the failure probability by 20 % (green triangles). Figure 4a depicts the overall view of the resulting failure probability. The decreased and increased failure probabilities of the independent nodes is clearly noticeable, i.e. the indicators with values of 0.8 and 1.2, respectively, while the failure probability of the dependent nodes varied only slightly. The resulting change of these failure probabilities is more apparent in the zoomed in view shown in Figure 4b.

For example, in the first experiment, the probability of failure of the function *Collision avoidance* (node number #26 in Table 2) decreased by a factor 0.998 as a consequence of the decrease in the failure probability of its incoming functions (node numbers # 27, 28, 43, 44, 56; see also Figure 2). In the second experiment, the probability of failure of the same function (node number #26) increased by a factor of 1.002, given the increase of the failure probability of its incoming parameters. Similarly, it can be explained the remaining nodes in the *BN-model*.

Finally, one can argue that this relatively low change follows from the low failure probability and factor values initially determined by the experts. Nevertheless, these results clearly indicate the strength of the implemented *BN-model*. It enables decision makers to explore the impact of failure probabilities on the whole system and, based on that, extract requirements for the implementation of each node.

6. Conclusions

We introduced a Bayesian Network (BN) model for the high-level representation of the safety and security state of a generic Offshore Wind Farm
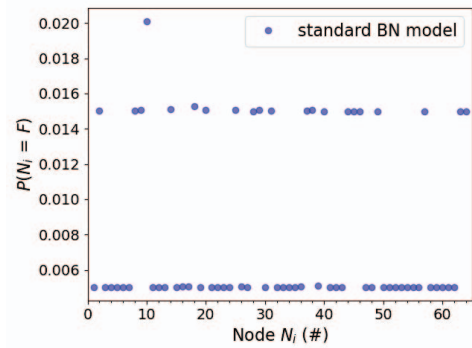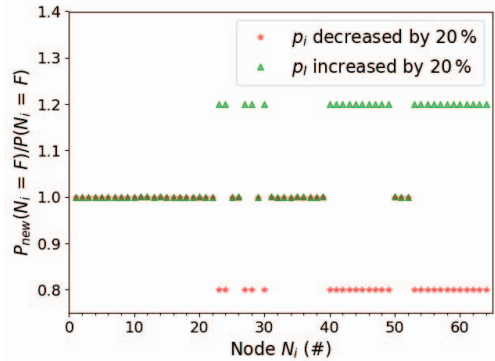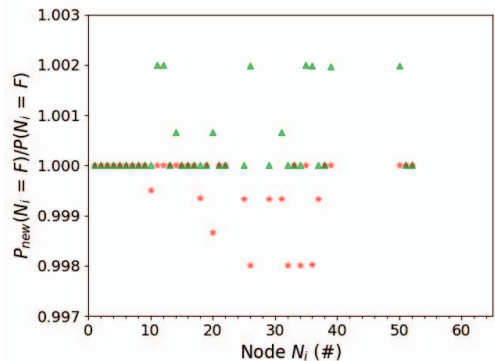

Fig. 3. Probability failure $P(F)$ value obtained in the model as a function of each of the siyty-four nodes. In the x-axis it is used a number for the node N_i provided in Table 2.

(a) Overall view

(b) Zoomed in view

Fig. 4. Ratio of failure probability $P_{new}(F)$ with respect to $P(F)$ for two cases; namely: *i)* p_i of the *independent nodes* decreased by 20 % (red stars) and *ii)* p_i of the *independent nodes* increased by 20 % (green triangles).

(OWF). The nodes of the model represent the main functions within an OWF, which can be functional or not, while the edges mean the correspondent relations. Obtained results indicate that the developed *BN-model* enables the exploration of the interrelations between all functions in terms of failures on high abstraction level, and thus, permits the extractions of requirements for the implementations of the functionality of an OWF.

References

Aghahowa, E. and S. Allen (2007, 05). Developing key performance indicators for airport safety and security. *Facilities 25*, 296–315.

Carroll, J., A. McDonald, and D. McMillan (2016). Failure rate, repair time and unscheduled o&m cost analysis of offshore wind turbines. *Wind Energy 19*(6), 1107–1119.

Gonzalez, E., E. M. Nanos, H. Seyr, L. Valldecabres, N. Y. Yürüşen, U. Smolka, M. Muskulus, and J. J. Melero (2017). Key performance indicators for wind farm operation and maintenance. *Energy Procedia 137*, 559 – 570.

Hollnagel, E. (2012). *Resonance Analysis Method*. Union Road Farnham, Surrey, GU9 7PT, England: Ashgate Publishing Limited.

Hollnagel, E. and O. Goteman (2004). The functional resonance accident model. In *Cognitive System Engineering in Process Control*.

Komusanac, I., G. Brindley, and D. Fraile (2020, 02). Wind energy in Europe in 2019. Trends and statistics. Technical report, WindEurope Business Intelligence.

Köpke, C., J. Schäfer-Frey, E. Engler, and C. P. Wrede (2019). A joint approach to safety, security and resilience using the functional resonance analysis method. In *8th REA symposium Embracing resilience: Scaling up and speeding up, Linnaeus University, Kalmar, Sweden*.

Le Cam, L. (1990). Maximum likelihood: an introduction. *58*, 153–172.

Lichte, D. and K. Wolf (2019). Bayesian network based analysis of cyber security impact on safety. In *Proc. European Safety and Reliability Conference (ESREL)*, pp. 1502 —- 1509.

Luciani, D., M. Marchesi, and G. Bertolini (2003). The role of bayesian networks in the diagnosis of pulmonary embolism. In *jth hournal of thrombosis and haemostasis*.

Murphy, K. P. (2012). *Machine Learning: A Probabilistic Perspective*. MIT Press.

OECD (2016). *The Ocean Economy in 2030*. Paris, France: OECD Publishing.

O'Sullivan, M. (2020, May). Industrial life cycle: relevance of national markets in the development of new industries for energy technologies – the case of wind energy. *Journal of Evolutionary Economics*.

Pfaffel, S., S. Faulstich, and S. Sheng (2019, oct). Recommended key performance indicators for operational management of wind turbines. *Journal of Physics: Conference Series 1356*, 012040.

Schreiber, J. (2017). Pomegranate: fast and flexible probabilistic modeling in python. *CoRR abs/1711.00137*.

Seyr, H. and M. Muskulus (2016). Safety indicators for the marine operations in the installation and operating phase of an offshore wind farm. *Energy Procedia 94*, 72 – 81.

Zhou, Y. and T. S. Huang (2006). Weighted bayesian network for visual tracking. In *18th International Conference on Pattern Recognition (ICPR'06), Hong Kong*, pp. 523–526.