Modeling Offshore Wind Farm Disturbances and Maintenance Service Responses within the Scope of Resilience

Arto Niemi*, Bartosz Skobiej, Nikolai Kulev, Frank Sill Torres

German Aerospace Center,
Institute for the Protection of Maritime Infrastructures,
Fischkai 1, 27572 Bremerhaven, Germany.

Abstract

Offshore wind farms are becoming ever more important means of energy production. Accordingly, they are started to be considered critical infrastructures with heightened attention on their protection and resilience. This paper studies how the maintenance service can sustain or recover offshore wind farm operations under different stressors. We conduct this study by modeling the failures in an offshore wind farm and how maintenance service is able to correct them. Our model enhances the traditional cause-consequence trees by including dynamical aspects, and the modeling of the maintenance process. Special attention in the maintenance model is given to limited personnel and material resources, as well as limited access to wind turbines. This limit is a result of occasional harsh weather conditions that make conducting repairs unsafe. The model is applied for two representative disturbance scenarios: a cyber-attack leading to high failure rates and a high-impact incident causing numerous simultaneous failures. The second scenario integrates results from a physical power system simulation that are used for depicting the incident. The results show that our model can present scenarios where different stressors challenge the operations. These can be used for testing and defining requirements for future countermeasures to improve the resilience.

Keywords: Offshore wind farm, Maintenance, Fault modeling, Risk scenarios, Recoverability

1. Introduction

Offshore Wind Farms (OWF) are of rising importance for energy provision. In Germany, the current plan is to increase the production capability to 30 GW

*Corresponding author, arto.niemi@dlr.de
URL: `http://www.dlr.de/mi` (Arto Niemi)

by the year 2030 and at least 70 GW by 2045 [1]. Similar policies have been introduced globally to scale up the energy production by OWFs [2]. This shift away from fossil energy sources has been motivated by environmental factors. The present crisis in Ukraine has brought into focus the geopolitical risks related to fossil fuels, which has further motivated the green energy transition [3].

The increased societal dependency on OWFs as means of energy production will result in a situation where they become critical for societal well-being. Already in Germany, OWFs with installed net nominal power higher than 104 MW are considered critical infrastructures (CI) [4]. So far, efforts have been taken to protect CI from disruptions. But as discussed in section 2.1, there is a recent transition from CI protection to CI resilience [5]. One of the leading ideas to achieve this transition is to adapt the United Nations' (UN) disaster resilience concept to be used in CI [6]. This view of resilience covers all the phases of traditional crisis management. It includes preventive measures before the crisis, response during the crisis, and recovery after it. In the case of CI, a crisis is an incident that disrupts or has the potential to disrupt operations [5].

The ability to operate OWF depends on many factors including the ability to maintain these infrastructures. Published literature on OWF maintenance focuses mainly on economical aspects. A summary of this literature is given in Section 2.2. This focus is understandable, as energy production is foremost an economic activity that has to be financially viable. Thankfully, economic and resilience topics overlap each other. From the commercial and resilience points of view, system reliability, the ability to quickly restore operational capabilities, and the optimization of the required resources are of interests. Regardless of this overlap, the focus of resilience is more on High-Impact Low-Probability (HILP) scenarios than on frequent minor issues. Also, CIs are often more complex than many other applications where safety and reliability studies are being conducted. Due to these reasons, improving the fault modeling compared to existing OWF operation models is required. Section 2.3 presents the state-of-the-art in resilience modeling and motivates our approach.

Our aim is to use best practices in existing OWF and resilience modeling approaches and adapt them to model the recoverability and operational sustainability of OWFs. A challenge in modeling OWF operations and maintenance (O&M) is that it forms a human-technical system where the maintenance of OWF depends on access to offshore assets. The ability to access these installations requires vessels, maintenance technicians, and sufficient weather conditions. Our approach that considers these factors is presented in section 3. It uses a combination of an O&M model, cause-consequence trees, and a synthetic weather generator to model OWF reliability and maintenance.

The approach enhances traditional fault tree assessments (FTA) and event tree assessments (ETA) with the integration of the human-technical O&M model. Having these traditional failure modeling techniques further allows us to include results from a multi-domain engineering-physical simulation of the OWF power system to the O&M model. This approach presents a solution for testing the resilience of complex technological systems, i.e. offshore wind farms. While our solution is closely related to the reliability assessments of these infrastructures,

the novelty is that we address infrastructure resilience instead of reliability and availability. In practice, this novelty is demonstrated with a HILP scenario, where an accident is first simulated with the OWF power system model. These results are then represented with FTA and ETA approaches in the O&M model. This setup captures detailed aspects of the system response to an accident in two different time scales. We can model the immediate electrical perturbation, which causes the automated protection systems to interrupt the OWF power generation, as well as the restoration of the power generation within the context of O&M.

In previous works, B. Skobiej et al. [7] introduced the O&M model and explored a scenario where a lack of personnel would hinder maintenance. B. Skobiej and A. Niemi [8] further showed how a synthetic weather generator can be connected to the O&M model. Compared to these works, this paper focuses on modeling technological issues that can hinder OWF operations.

We present three scenarios in section 4 that test the abilities of the maintenance service to sustain operations. This consideration is akin to the idea presented in [9] where resilience is defined as the ability of the studied system to maintain functionality and recover, given that one or more adversarial events occur, whether these events are known or not. The first scenario in section 4.1 describes normal operations, where the maintenance activities are driven by scheduled maintenance and failure repairs. This case provides a reference to which other cases will be compared. The second scenario in section 4.2 is motivated by the cyber-attack against Iranian uranium enrichment facilities where Stuxnet malware caused the equipment to operate with wrong settings to cause failures [10]. In our scenario, we assume that operating OWF with wrong settings results in higher failure rates.

The third scenario in section 4.3 presents a HILP incident. The chosen scenario is triggered by a ship collision with an offshore wind turbine (OWT) resulting in a significantly long short-circuit disturbance. Due to the disturbance, all other OWTs are shut down by their protection systems and have to be inspected. This scenario incorporates results from a physical energy provision system model to the O&M model using cause-consequence trees. This combination of models allows us to capture detailed aspects of the system behavior in two drastically different time scales. The duration of the electrical disturbance is less than a second, while the recovery can last weeks.

The obtained results from disturbance cases clearly show the capability of the proposed model to explore the consequences of high-impact scenarios. This capacity is of utmost importance for assessing CI resilience. Consequently, it paves the way for defining resilience enhancing measures.

2. Background

2.1. CI resilience

Public policies are a fundamental aspect of safeguarding CI. The same laws that define the required actions for safeguarding often also denote what is considered CI in a certain nation. Both in the USA [11] and Europe [5], the concept

of CI protection is evolving to become CI resilience. This change in the legislation will bring new requirements for CI operators.

This paragraph provides a brief description of the shift from protection to resilience and the new European Union (EU) directive on Critical Entities Resilience (CER) [5]. A more detailed discussion of this topic can be found in [12, 13]. The CER directive defines resilience as the ability to prevent, resist, mitigate, absorb, accommodate to and recover from an incident that disrupts or has the potential to disrupt the operations. This is somewhat similar to the UN's definition where resilience is the ability of a system, community, or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions. The CER directive defines a critical entity as a CI operator. The proposal argues that protecting the CI is an insufficient approach and the resilience of the CI operators needs to be improved. It further has an all-hazards approach. This is a shift from the previous directive on CI protection that was partly motivated by the terrorist attacks in the early 2000s.

The CER directive in the EU is part of a larger trend. In the USA, a presidential policy directive [11] mentioned CI resilience already in 2013, where again the definition resembles the one from the UN, and the focus is on all hazards. Several motivations exist for this shift from CI protection to resilience. The review document [14] broadens the lens of CI protection frameworks by integrating concepts such as adaptability, flexibility, and robustness. The resilience-based perspective is prompted by the considerable degree of uncertainty about the intensity and complexity of future disasters and their potential impacts on infrastructure. This creates a need for approaches that prepare assets and systems with capacities to be restored and rehabilitated swiftly. For example, effects of the climate change may call for infrastructure relocation. Also, B. Rød et al. [15] argue that the resilience concept was needed because complete protection can never be guaranteed. Moreover, achieving the desired level of protection is normally not cost-effective in relation to the actual threats.

2.2. Related work on OWF maintenance modeling

Several approaches have been developed to model OWF maintenance. Already in 2011, M. Hofmann [16] wrote a review article listing models for different purposes of operation and maintenance; production, failures, and reliability; micro-siting and layout; component costs; installation and access; and management tools. The paper presented 20 approaches for operation and maintenance, production, failures, and reliability. Due to this abundance of published works, this review focuses on recent examples of these approaches.

M. Scheu et al. [17], M. Sahnoun et al. [18], and later C. Gutschi et al. [19] have presented detailed approaches to model OWF maintenance. Their models consider several factors. These include 1) the number of OWTs in an OWF and their distance to the port, 2) the structure of an OWT with its subsystems and their failure modes, 3) the power curve of an OWT, 4) the number of vessels and

staff, including their availability, and 5) the limits of safe working conditions. A similar kind of approach has been proposed also by E. Byon et al. [20].

Other authors have emphasized different aspects of maintenance. The work by Y. Dalgic et al. [21] considered the vessels used for maintaining the OWF. Their model includes failure rates and repair times for vessel components as well as costs for repairs, staff, and fuel. A. Zitrou et al. modeled availability growth of OWF [22]. A. Saleh et al. suggested optimizing the maintenance of offshore wind turbines with intelligent Petri net that are obtained by combining the Reinforcement Learning technique with the principles of Petri nets [23]. M. Liu et al. [24] defined an asset integrity focused framework for OWF resilience that considered management and economic aspects in addition to OWF infrastructure and environment. D. Wilkie and C. Galasso [25] touched the subject of resilience assessment in their paper that studied the risk of environmental hazards on OWF. Similarly, S. Rose et al. [26] simulated tracks of hurricanes and potential damage caused to the planned OWFs in the U.S. Atlantic and Gulf coasts. D. Wilkie and C. Galasso measured resilience with an approach that was however close to the risk paradigm. They considered "fragility" to be the failure likelihood, which they linked to the financial losses occurring in an event. This is not different from a traditional risk approach where Risk = Likelihood∗Severity.

In difference to the approaches presented in [25] and [26], we intend to assess the recoverability of an OWF after a high-impact incident. We further exclude detailed risk assessments for mechanical structures, as our approach is system-based. In our opinion, approaches [17]-[20] capture the essential aspects of normal OWF operations and our first case study in section 4.1 is similar to them. However, section 4.3 shows that fault modeling is required to model failure propagation and other non-trivial cases that may not occur during normal operations.

2.3. Modeling approaches for resilience assessments

Several approaches have been used for resilience assessments. A. John et al. employed Bayesian networks to assess the resilience of a seaport [27], while H. Estrada-Lugo et al. argued that Bayesian networks cannot handle imprecise probabilities and used credal networks to model the resilience of an advanced thermal nuclear reactor [28]. C. Heracleous et al. adopted an open hybrid automaton framework that integrates state machines and differential equations in a single formalism to model CI system interdependencies [29]. C. Foglietta and S. Panzieri introduced an agent-based simulation software CISIApro that can calculate complex cascading effects [30]. H. Sun et al. suggested a STAMP-based approach for quantitative resilience assessment of chemical process systems [31]. R. Yan et al. used Petri nets to model the resilience of a nuclear power plant [32, 33], while Z. Tan et al. based their approach on Markov processes to study nuclear power plant's resilience against earthquakes [34]. S. Geng et al. used graphical evaluation and review technique (GERT) to assess resilience of satellite networks [35].

The variety of the presented modeling approaches indicates open questions about the most appropriate method for resilience assessment, and how to incor-

porate the classical risk assessment methods. I. Häring assessed the suitability of classical risk assessment methods for resilience engineering [36]. He discussed that FTA and ETA are well suited for preparing, preventing, and protecting the system from failures. Yet, these methods are only adequately suited for modeling a response to a failure and recovery from a failure. In this assessment, system modeling based on System Modeling Language (SysML) was seen as the most suitable approach. However, K. Clegg et al. [37] found that fault models have a much wider scope than the models defined in SysML. Due to this, part of the fault model cannot be incorporated into the SysML approach in a useful way.

These kinds of considerations have also been conducted within the model-based safety assessment discipline where a distinction can be made if the model includes failure logic, nominal flows[1], or both [38]. For example, F. Mhenni et al. [39] assess workplace safety in a case where a human operator works with a collaborative mobile robot to assemble systems. They integrated model-based system engineering, and safety approaches together with multi-physics simulations to model this case. These kinds of exhaustive models can be done in narrowly defined cases. For example, the analysis in [39] studied only whether the robot can harm the human operator.

When availability assessments for industrial-scale facilities are considered, A. Niemi et al. used FTAs and a semi-Markov model to model the availability of large particle accelerator facilities [40]. E. Zio et al. used a stochastic state model to assess the availability of a multi-output offshore installation [41]. F. Chiacchio et al. showed how a combination of a FTA with a physical model can be used for reliability modeling of an electrical motor, photovoltaic power plant, and industrial distillation system [42].

Within the resilience engineering field, these kinds of state models have been embraced and criticized. For example, S. Jackson et al. derived a state model of system resilience [43]. In turn, E. Engler et al. criticized this approach for 1) the inflexible specification of states [44] and 2) they also determined a gap in the representation and illustration of monitoring functions as supplementary services for situation assessment and situation-based adjustment. Yet, their paper considers state-based modeling to be a suitable approach for the design of resilient infrastructures if the ability of robust service provision and effective rebounding are addressed.

Our take from these findings is to combine a cause-consequence tree model with an O&M model to improve the modeling of response and recovery from a fault or other threat. As reference [37] discussed, having a fault model is advantageous, we do not currently seek to replace it with other methods. The abilities to model failure likelihoods, impacts of the failures, and restoration are essential aspects of asset reliability modeling. Therefore, we consider models developed for asset availability modeling as state-of-the-art approaches. In these fields, high amounts of work have been conducted to extend the classical static FTA

[1]These flows can represent, for example, energy, matter, or information.

formalism by introducing dynamic features [45]. As section 3.2 will describe, our FTA model includes some dynamic extensions, such as an ability to change failure rates based on external events. Yet, the main difference from a classical, static FTA is that we want to connect the fault model to an O&M model to correctly depict the restoration time.

This issue of modeling system restoration has been noticed in the resilience engineering community. For example, T. Aven [9], E. Engler et al. [44] and I. Häring [36] have stated that maintenance and recovery were not depicted correctly by classical risk modeling approaches or they were an example of supplementary services that simple state models do not include. As stated in [9], for many types of risk issues, simple models, and methods, as traditionally used in risk assessment, work fine and can be justified. But, these methods may have limitations when they are applied to resilience assessments. We consider that state-based models form a good foundation where selected aspects can be described with more detailed models when such a need arises. In the case of this paper, the O&M modeling and the modeling of the electrical disturbance for the HILP scenario (section 4.3) are aspects where a more detailed model is warranted.

3. OWF model

3.1. Introduction and concept

Similar to examples [40, 42], our model for OWF resilience combines a fault model with another model. Here the other model is the O&M model for maintenance. Figure 1 illustrates the model components. During simulations, the fault model generates failure events. They are sent to the O&M model which simulates the maintenance intervention. This model takes into account the personnel and vessel resources required to carry out the intervention as well as the availability of suitable weather. We use a copula-based model for generating synthetic weather data for individual simulation runs.

Section 3.2 describes the Simulink [46] library develop for fault modeling and section 3.3 describes the O&M model. However, we give only an overview of the copula-based weather generator in section 3.4, because this paper does not advance this work. A more thorough description of it is given in references [8] and [47].

3.2. Cause-consequence tree library for Simulink

Our aim is to extend cause-consequence trees that are also known as the bowtie method [48] for resilience assessments. This approach is credited to D. S. Nielsen [49] and combines FTA and ETA. FTA is an approach where an undesired state of the system is specified and the system is analyzed to find all credible ways in which this top event can occur [50]. The tree depicts the logical interrelationships of basic events that lead to the undesired top event. While several FTAs can be built to model different top events of a complex system, a FTA does not model all possible system failures or all possible causes for a

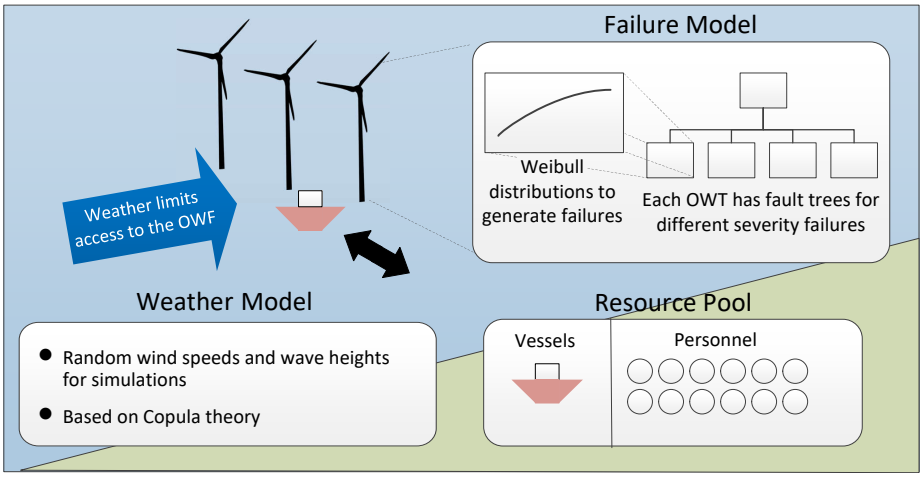

Figure 1: Illustration of the OWF model components.

failure. The trees should cover all the significant failure modes and include only those faults that contribute to top events.

3.2.1. Initial requirements

The O&M model is developed using the commercial Simulink software. Therefore, it was decided to develop the fault model with the same software. At first, a set of requirements were defined for the library. This list presents typical state-of-the-art requirements for a dynamic cause-consequence tree and is meant as a basis for future development. The library should support commonly used FTA and ETA techniques, with some specific requirements including:

- A failure may have multiple consequences. This allows modeling cross-system disturbances caused by system dependencies and common cause failures.
- A fault node may have different failure rates and distributions at different times.
- Faults shall be repairable.
- The model should allow changing the failure rate and/or distribution. For example, to take into account the maintenance or operation mode.
- Certain failures are defined by failure likelihood that is linked to events. Modeling this requires probability connections between events, there can even be a delay between the connected events.
- Develop an interface to use the model inside a simulation. This requires defining what commands and information other models need for communicating with the fault model.

- Graphical interface to design and display cause-consequence trees.
- Able to work in stand-alone mode, considering: 1) The repair times should then be stored in tree models, 2) obtaining results with Monte-Carlo simulation, and 3) The result should include availability, downtime, and numbers of failures as defined by IEC [51].

IEC defines availability as the ability to be in a state to perform as required. This is the opposite of the fault state which is the inability to perform as required, due to an internal state. In our model, however, we consider an item to be in a fault state when it is incapable of performing as required. Downtime is defined as the time an item is unable to perform as required, due to internal fault, or preventive maintenance. And, a failure is the loss of ability to perform as required, i.e. the number of failures measures how many times an item goes to the fault state.

3.2.2. Review on existing libraries

There have been several attempts to provide cause-consequence libraries in the Simulink environment. For example:

1. SHyFTOO library [52] is well presented in the literature. However, in this library, the FTAs were not modeled graphically, which contradicts one of the set requirements. Also, there were restrictions on connecting these trees to other models. The top event is given to Simulink through an input port. In our model, each OWT has a top event, which might make it hard to implement with the SHyFTOO library.
2. OpenCossan library [53] is mainly designed for structural safety assessments. It also contains a FTA implementation [54], but this implementation is rather simple.
3. K. Aslansefat et al. published a Simulink model on an underwater glider FTA along with their journal publication [55]. Yet, the published model has extremely limited functionality. For example, it does not include repairs, as the purpose of it was only to assess the reliability of the glider.
4. Additionally, a rather technical paper [56] by A. Chovanec and J. Bucha confirmed that creating logical connections for FTA in Simulink should be straightforward.

None of these libraries fully complies with our list of requirements. Having a green-field start was seen to be easier than trying to rework and include new functionalities into existing libraries. Hence, we decided to develop a new cause-consequence library.

3.2.3. Descriptions of selected features

Next, the information exchange between models, and the dynamic changing of failure rates are presented. Only the high-level functionalities of a fault node are shown to understand the implementation of these advanced features.

Fault node. A fault node or a basic event is defined as a Simulink subsystem block. A schematic of a node is shown in Fig. 2. The main task of a node is to determine if it is in a fault state. This is done within the fault state function. The function contains a failure time (t_f) generator with a failure distribution[2]. A three-parameter Weibull distribution [57] is implemented using equation

$$t_f = \gamma - \alpha \ln(u)^{1/\beta}, \tag{1}$$

where u is a random value between 0 and 1, α is the scale parameter, β is the shape parameter and γ is the so-called "safe life", when failures are not expected to occur. If $\beta = 1$, the failure rate is constant. When $\beta < 1$, the failure rate decreases, and when $\beta > 1$, the failure rate increases as the item ages. A failure cannot occur when the relative simulation time is smaller than γ. New failure times are generated stochastically from the distribution as described [58].

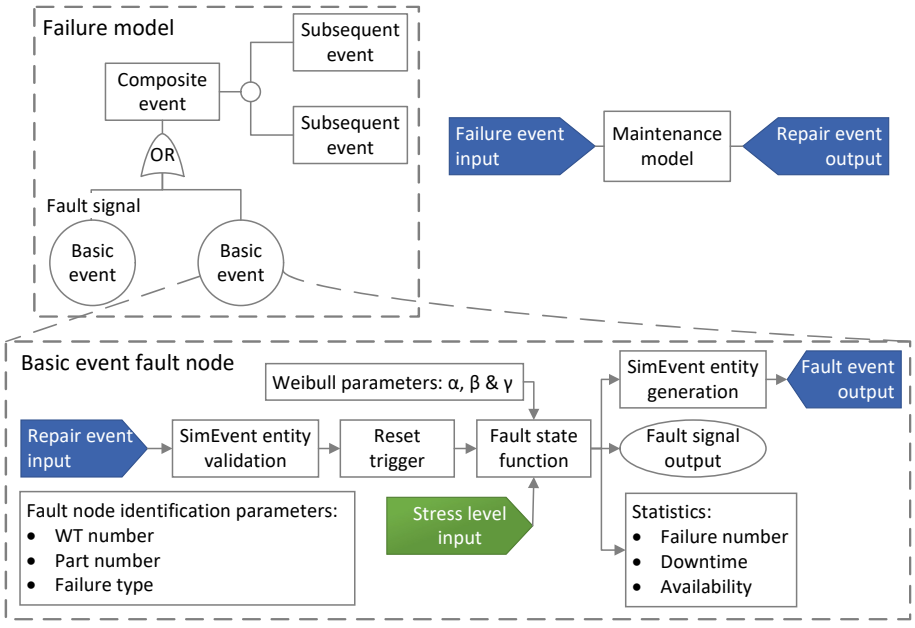

Figure 2: Fault node depicting a basic event in the Simulink library and an exemplary cause-consequence tree. Fault signal is used for representing the event state within the failure model, while the blue color indicates the fault and repair channels to communicate with the O&M model. The green color shows the channel to receive the stress level.

A failure causes the fault signal to become "true". This signal propagates through "Fault signal output" to operators. These can be gates in a FTA or events in an ETA, as shown in Fig. 2. This signal is also used for calculating event statistics. These are the number of failures, cumulative downtime, and

[2]The effect of the stress in Fig. 2 will be explained later in this section.

availability. The latter is calculated with equation

$$\text{availability} = \frac{\text{simulation time} - \text{downtime}}{\text{simulation time}}. \quad (2)$$

In a traditional FTA where maintenance is modeled, a failure would trigger a generation of a repair time after which the "Fault state function" would be reset and a new failure time generated. Instead of this approach, Fig. 2 shows an approach where the repairs are handled by an external model.

Model information exchange. Our approach uses SimEvents entities [59] to exchange information between models. In Fig. 2, the fault signal connects to the "SimEvents entity generator" that creates a failure entity when the fault signal becomes "true". This entity is sent to other models through "Fault event output".

The other models need to recognize the origin of the failure entity. For this reason, we store the "Fault node identification parameters" as attributes of the new entity. In the case of the OWF model, these attributes are the OWT number, part number, and failure type.

These parameters are further important when the O&M model sends an entity to inform the fault model about a completed repair. In this case, a repair arrives to a node through the "Repair event input" channel. The first step is to validate if the arriving entity is meant for a specific node. Function "SimEvents entity validation" compares the entity's attributes to the identification parameters stored in a node. If these values match, the entity activates the "Reset trigger" that resets the "Fault state function".

Altering failure behavior. The library provides two ways to alter a failure distribution. In the first approach, the failure distribution changes once an item reaches a set age. This approach can be used for example for modeling a classical "bathtub" curve with three Weibull distributions. In Fig. 3, the first distribution "A" has a decreasing failure rate, "B" has a constant rate, and "C" has an increasing rate. In the library, this behavior is modeled by changing the active failure distribution when the age of the modeled item reaches a specified point. In the library, these points and the parameters for different Weibull functions are stored as constants within a fault node.

The second implemented way to alter a failure distribution uses a so-called stress factor or acceleration factor. In literature, this approach has been used for example to define load-dependent failure rates for power converters [60]. In the library, a fault node has a failure time t_f that has been randomly generated from a failure distribution of the node. Normally, t_f is compared to the simulation time t_s to determine the failure time in a simulation. If the stress factor is used, t_f is compared to effective time t_{eff}, which is calculated using the stress factor f_s

$$t_{eff} = f_s t_s. \quad (3)$$

For example, if $f_s = 2$ the simulation will reach the t_f twice as fast, and if $f_s = 0.5$ it takes twice as long time for a failure to occur. The advantage of this

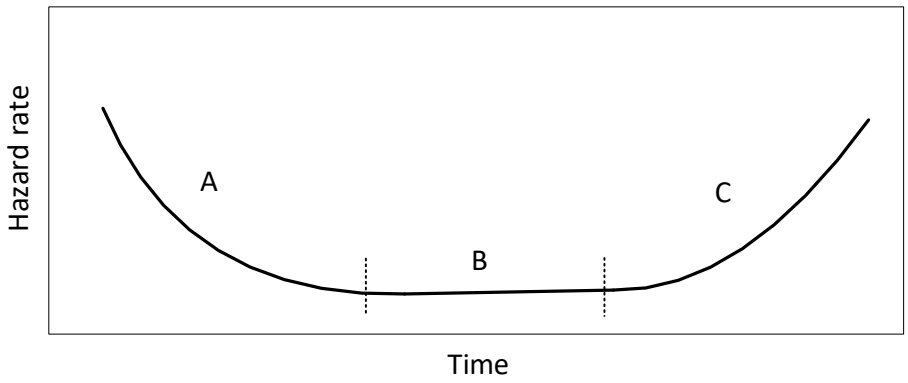

Figure 3: Classical bathtub curve where A, B, and C indicate periods of decreasing, constant, and rising conditional failure rate (i.e. hazard rate).

approach is that the change of a failure behavior is achieved without a need to recalculate the failure time when the behavior is altered.

Our implementation uses the SimEvents library to inform the failure nodes about the stress. The stress factor is sent as a SimEvents entity to a fault node. In Fig. 2, the "Stress factor" input block is green. In this implementation, a global stress factor is used for all nodes that are susceptible to stress. Alternatively, node-specific stress factors could be used. However, this would require validating if the stress events arriving to a node are meant for it. In this paper, the stress factor is used for implementing case 2 on cyber-attack.

3.3. O&M model

Depending on modeling purposes and specific questions a researcher wants to answer, the O&M system could be developed in various ways. Two main issues regarding any representation of reality in a model are time discretization and model complexity. The fact that maintenance results are considered on a system level provides an opportunity to simplify the model structure. We use discrete simulation like in [20]. In our case, the time is discretized with a 1 h interval. The shortest maintenance interval is about four hours including transitions [61]. Therefore, we consider that the 1 h interval is sufficiently accurate for modeling this process.

Our O&M model represents the repairs for failure events produced in the fault library as described in section 3.2.3 and presented in Fig. 2. Therefore, the model only considers corrective maintenance. The input from the fault library is an event description consisting of an OWT number, part number, and failure type. The model has three process paths to depict different interventions as shown in Fig. 4. The names of these paths are based on failure categories in [62].

The model determines the required intervention based on the failure type. The minor repairs path leads to a voyage with a Crew Transfer Vessel (CTV).

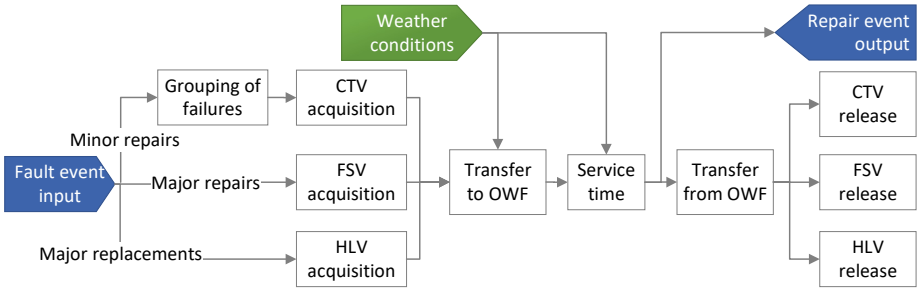

Figure 4: Schematic illustration of the O&M model. The Fault event input and Repair event output connect to channels in fault nodes as shown in Fig. 2.

These are common interventions usually carried out by two to four technicians [18, 21]. Based on the literature, a small CTV is able to carry 12 passengers [21]. Due to varying team sizes and the need for equipment and spare parts to carry out maintenance, it is not clear how many interventions a CTV can support on average. For example, M. Sahnoun et al. assume that each team has their own vessel [18]. We think that this assumption is too restrictive, but we also do not think that the use of the vessels is fully optimized. Therefore, we assume that a small CTV is capable of gathering three teams of three technicians in one voyage. Due to this a dedicated grouping procedure is introduced for such events. The grouping ends under two conditions:

1. when three failures have occurred, or
2. when the maximum time limit for the grouping is reached[3].

Once the grouping procedure ends, the acquisition step obtains the required resources from resource pools. At the moment, the model stores vessels, vessel crew, and technicians in these resource pools.

Major repairs and major replacements are handled by Fast Supply Vessels (FSV) and Heavy Lift Vessels (HLV) respectively. The modeling approach, in these cases, consists of connecting one failure to one vessel that performs the intervention. Such a solution is appropriate due to the complexity of represented repairing operations that may also need large spare parts, e.g. a gearbox or a generator.

Each service voyage consists of three main phases: transfer to the OWF, service time/OWF maneuverings, and transfer from the OWF. The duration of transfers depends on the distance to the OWF and the speed of the used vessel. The simulated service time t_{s_sim} is generated based on a mean service time t_{s_mean} from historical data by adding randomness with a normal distribution filter with equation

$$t_{s\_sim} = t_{s\_mean} + (u * t_{s\_mean})/4, \tag{4}$$

[3]This paper assumes maximum grouping time of 7 days.

where u is a random scalar drawn from the standard normal distribution. After a voyage, the reserved resources are released to resource pools.

The transfer to an OWF and the service can only be conducted if the operation conditions are safe. General constraints of O&M activities are based on regulations, e.g. GOMO [63], and capabilities of the equipment. For example, the vessels have limits on when they can moor to an offshore structure [64, 65].

The adopted O&M limitations vary between countries and companies. In our model, additional inputs are used for determining safe conditions: wind speed s, significant wave height h, temperature (ATMP), and day-night conditions (DN). In this study, we use the same limitations as in [7]: $h < 2.5$ m, $s < 25$ ms^{-1}, and the interventions can only occur during daylight (DN = "true"). In this paper, ATMP parameter is not considered. This is because temperatures below 0 ^{o}C, which stop O&M activities, occur in the German Bight area only several hours per year and usually at night. Wind speed and wave height data are generated by the copula model described in section 3.4. The DN is based on the geographical position of Helgoland: 54^{o} 11' N, 7^{o} 53' E.

We chose this location because the North Sea area is of high interest to the German offshore wind energy industry. The distance from Helgoland to the shore is about the same as most of the German OWFs.

3.4. Copula-based synthetic weather generator

This section provides a summary of the copula-based synthetic weather generation model that is described in more detail in references [8] and [47]. The original motivation came from paper [66] where a copula-based approach was used for modeling weather windows for conducting offshore operations. Paper [47] presented an improved copula-based approach, and paper [8] showed how it can be included in our O&M model.

Our model is based on the copulas library for Python [67] and works as follows. The model uses the Gaussian multivariate class which implements a multivariate distribution by using a Gaussian Copula to combine marginal probabilities estimated using univariate distributions. The class automatically chooses the best-fitting univariate marginal distribution for each dimension. The Copulas library contains the following univariate distributions: Beta, Gamma, Gaussian, Logarithmic-Laplace, Student T, and truncated Gaussian distributions, in addition to Kernel-Density Estimate that uses a Gaussian kernel.

In particular, the intent is to generate time series where the next wind speed s_{n+1} and wave height h_{n+1} would be conditional to the current wind speed s_n and wave height h_n. Generating the random time series is achieved by forming a four-dimensional copula where the dimensions are wind speed s_n, wave height h_n, wind speed change Δs, and wave height change Δh. As the current values are known the particular problem is to generate values Δs, and Δh that are conditional to s_n and wave height h_n. The next values are then calculated with the equations: $s_{n+1} = s_n + \Delta s$ and $h_{n+1} = h_n + \Delta h$.

Creating the conditional values Δs and Δh uses the knowledge that the copula is Gaussian and is achieved by transforming the multivariate Gaussian

distribution to a conditional one. For a four-dimensional distribution, the mean values are

$$\bar{\mu} = \begin{bmatrix} \mu_1 & \mu_2 & \mu_3 & \mu_4 \end{bmatrix}^T, \tag{5}$$

and the covariances are

$$\bar{\Sigma} = \begin{bmatrix} \Sigma_{11} & \Sigma_{12} & \Sigma_{13} & \Sigma_{14} \\ \Sigma_{21} & \Sigma_{22} & \Sigma_{23} & \Sigma_{24} \\ \Sigma_{31} & \Sigma_{32} & \Sigma_{33} & \Sigma_{34} \\ \Sigma_{41} & \Sigma_{42} & \Sigma_{43} & \Sigma_{44} \end{bmatrix}. \tag{6}$$

Let us denote that

$$\bar{C} = \begin{bmatrix} \Sigma_{13} & \Sigma_{14} \\ \Sigma_{23} & \Sigma_{24} \end{bmatrix} \begin{bmatrix} \Sigma_{33} & \Sigma_{34} \\ \Sigma_{43} & \Sigma_{44} \end{bmatrix}^{-1}. \tag{7}$$

For a condition that x_3 is normalized s_n, and x_4 is the normalized h_n, a new distribution can be formed where

$$\bar{\mu}^* = \begin{bmatrix} \mu_1 \\ \mu_2 \end{bmatrix} + \bar{C} \left[\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} - \begin{pmatrix} \mu_3 \\ \mu_4 \end{pmatrix} \right], \tag{8}$$

and

$$\bar{\Sigma}^* = \begin{bmatrix} \Sigma_{11} & \Sigma_{12} \\ \Sigma_{21} & \Sigma_{22} \end{bmatrix} - \bar{C} \begin{bmatrix} \Sigma_{31} & \Sigma_{32} \\ \Sigma_{41} & \Sigma_{42} \end{bmatrix}. \tag{9}$$

A new random value pair x_1, x_2 is generated with the conditional distribution. The new values Δs and Δh are formed when the values with the same percentage points are calculated from their univariate marginal distributions. If a new value s_{n+1} or h_{n+1} would be negative, it is set to zero to avoid unrealistic values. The concept is shown in Fig. 5.

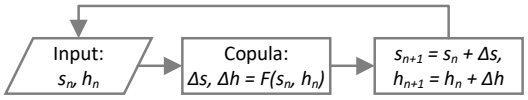

Figure 5: Steps required to calculate the next wind speed and wave height values [8].

Like in our earlier paper [8], we use data from years ERA5 weather dataset [68] to generate synthetic weather data. The ERA5 data set consists of hourly estimates of various weather characteristics and is provided by the European Centre for Medium-Range Weather Forecasts. We use weather data from the years 2019 to 2020 and from a location near Helgoland.

4. Case studies and their results

The ability of the maintenance service to respond to failures is tested in three scenarios that are presented in sections 4.1, 4.2, and 4.3. The first scenario depicts normal operations and acts as a reference for the other scenarios. The second scenario tests how the maintenance service can handle increased failure

rates. We motivate this increase in failure rates with a cyber-attack that makes equipment run with wrong parameters. The third scenario tests the abilities of maintenance services to handle an influx of maintenance tasks that is motivated by a high-impact incident. Fig. 6 illustrates the interactions between failure and maintenance models in these scenarios.

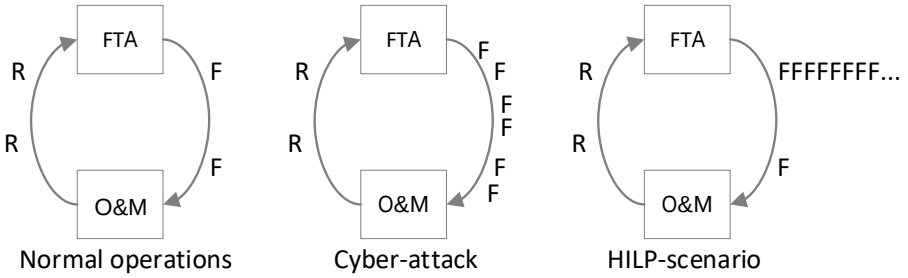

Figure 6: Illustration of the interactions between failure and O&M models for selected cases. The letter "F" stands for failure and "R" for repair. In case 1, during normal operations, failures occur infrequently. In case 2, the cyber-attack significantly increases the failure rates. In case 3, the HILP-scenario causes a high number of simultaneous failures that O&M has to handle.

4.1. Case 1: Normal operations

4.1.1. Case 1 scenario description and modeling

We assume that an OWF consists of 30 OWTs and it has the following assets available to maintain it: 3 CTVs, 1 FSV, 1 HLV, and unlimited availabilities of spare parts, fuel, and personnel. The underlying concept is based on the usage of an external company for maintenance. Table 1 lists the selected inputs for the O&M model.

Table 1: Selected inputs for the O&M model. The fields marked with * are taken from [61].

Name	Value
Number of OWTs	30
Distance to the OWF	50 km
CTV speed	46 km/h
FSV speed	37 km/h
HLV speed	28 km/h
Avg. CTV transition time to/from OWF	1.09 h
Avg. FSV transition time to/from OWF	1.35 h
Avg. HLV transition time to/from OWF	1.79 h
Avg. minor repair time*	6.67 h
Avg. major repair time*	17.64 h
Avg. major replacement time*	116.19 h

We use data from J. Carroll et al. [62] to define the basic failure rates. The data are shown in Table 2 and it has the rates for 19 different components in four categories. As shown in Fig. 4, the categories are used for selecting which kind of vessel is sent to perform the intervention. We combined the categories *"Minor Repair"* and *"No Cost Data"*. So in both cases, a CTV is acquired to maintain the failure. As we are mostly interested in the ability of maintenance to sustain asset integrity, we further combined different components. This leads to a FTA shown in Fig. 7 with three basic event nodes that are connected with an or-gate to the top event. This event depicts a state where the OWT is unavailable due to a failure. The failure rates for basic events are given in

Table 2: Failure rates taken from [62]. Column "Affected by stress" indicates the components that we estimate to have higher failure rates if an OWT is run with the wrong settings.

Category	Major replacement [1/365 d]	Major repair [1/365 d]	Minor repair [1/365 d]	No cost data [1/365 d]	Affected by stress
Pitch / Hyb	0.001	0.179	0.824	0.072	x
Other comp.	0.001	0.042	0.812	0.150	
Generator	0.095	0.321	0.485	0.098	x
Gearbox	0.154	0.038	0.395	0.046	x
Blades	0.001	0.01	0.456	0.053	x
Grease / Oil / Cooling liq.	0	0.006	0.407	0.058	x
Electrical components	0.002	0.016	0.358	0.059	x
Contactor / Circuit breaker / Relay	0.002	0.054	0.326	0.048	
Controls	0.001	0.054	0.355	0.018	
Safety	0	0.004	0.373	0.015	
Sensors	0	0.07	0.247	0.029	
Pumps / Motors	0	0.043	0.278	0.025	x
Hub	0.001	0.038	0.182	0.014	x
Heaters / Coolers	0	0.007	0.19	0.016	x
Yaw systems	0.001	0.006	0.162	0.02	x
Tower / Foundation	0	0.089	0.092	0.004	x
Power supply / Converter	0.005	0.081	0.076	0.018	x
Service items	0	0.001	0.108	0.016	
Transformer	0.001	0.003	0.052	0.009	x

Table 3. Even though reference [62] gives some age-dependent failure rates, we assume constant failure rates. This makes sense as the basic events combine several different component failures and the period of interest is only one or two years long.

To have consistent terminology, our FTAs use the same categories as [62]. Yet, this leads to some confusion. For example, the term "Minor repair" should be understood as a fault requiring a minor repair in the context of FTA. Combining component failures makes the scenario easy to present. However, for a proper analysis, the components should be handled individually. Our model assumes that an item that failed cannot fail again before it is repaired. When different categories are combined there is a chance that more items could fail

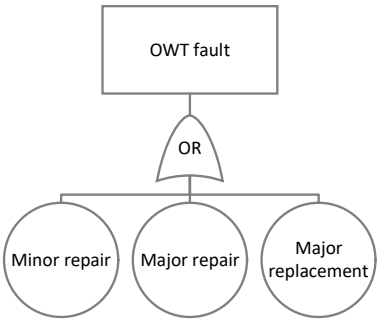

Figure 7: High-level FTA of an OWT.

Table 3: Failure rates for basic events.

Category	Failure rate [$1/10^4$ h]
Minor repair	0.79
Major repair	0.12
Major replacement	0.03

before the repair is done. In the case of a minor repair, one could argue that the maintenance team may be able to handle multiple minor issues during an intervention to an OWT. However, this may not be true for the other categories, but the situation is less likely as failure requiring major replacements or repairs occur less often.

4.1.2. Case 1 results

Fig. 8 shows the instantaneous availabilities of an OWF during a one year of simulations. It is measured by calculating the number of OWTs available for a given moment and dividing this value by the total number of OWTs. The result shows that the availability stays above 90% the majority of the time. The value is not higher mainly because CTVs wait for three failures to occur before launching a voyage. There are minor disruptions during January, November, and December. These are caused by weather limiting access to the OWF. However, the fact that the OWF availability returns to high value shows that the maintenance assets are sufficient to sustain operations.

We further calculated the averages of 100 rounds of simulations N to produce availability and Mean Time To Repair (MTTR) performance indicators. The mean availability m was 91.2% with a standard deviation s of 0.4%. The average MTTR was 100.7 h with a standard deviation of 5.2 h. The actual mean values μ can be estimated with equation

$$m - 1.96\frac{s}{\sqrt{N}} < \mu < m + 1.96\frac{s}{\sqrt{N}}, \tag{10}$$

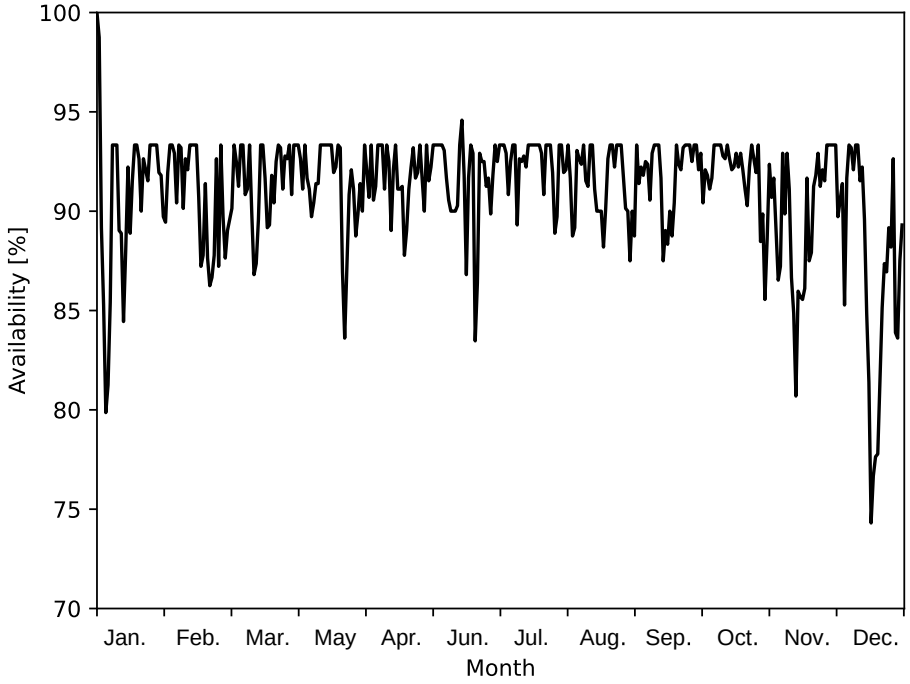

Figure 8: Average daily availability during one year of normal operations simulation.

which gives the 95% confidence intervals. For the availability, the μ is between 91.1 and 91.3%. For the MTTR, the μ is between 99.7 and 101.7 h. The narrow confidence ranges confirm that 100 simulations are sufficient for obtaining accurate estimates.

These results show that case 1 is a credible normal operations scenario. For example, M. Scheu et al. [17] also achieved similar availability in a case with low failure rates. However, their case had more OWTs, longer transit times, and a similar number of vessels. Also, Y. Dalgic et al. show that 90 - 95% availability can be expected in these kinds of simulations [21] and their previous paper further shows that the MTTR is in a range between 100 - 300 h [69].

4.2. Case 2: Cyber attack

4.2.1. Case 2 scenario description and modeling

Stuxnet malware made Iranian centrifuges operate with a too-high speed to cause failures [10]. Similarly, an OWT can be made to operate with a too-high speed by manipulating the pitch angles of the blades and disabling the protection system. A scenario where this manipulation leads to a destruction of an OWT is described in section 4.1.2 in [70]. In our case, we consider a more concealed approach where an attacker wants to hinder operations instead

of causing indisputable damage. Therefore, we assume that as a result of the attack certain failure rates increase.

An attacker needs a path to access the computers to infect them. This is an issue as these computers may not be connected to the internet. For Stuxnet, this may have occurred by infecting a willing or unknowing third party, such as a contractor who perhaps had access to the facility, or an insider [10]. The original infection may have been introduced by a removable drive. In an OWF, multiple stakeholders could cause an infection. J. Staggs et al [71] list attack paths as gaining physical access to an offshore structure and plugging a malicious device; cyber access using a vendor network; cyber access using technician equipment; or cyber access through a compromised supply chain. Several works have been conducted on cyber-attacks. S. Xu et al. considered how to enhance the resilience of renewable systems against malware attacks [72], S. Parvin et al. studied hardware trojans [73], and M. McCarty et al. conducted a cyber-security resilience demonstration for wind energy sites in a simulation environment [74].

In our case, we assume that increasing rotation speed causes higher stresses and vibrations that increase the likelihood of all mechanical failures. We assume that the failure rates increase for categories that are marked as "Affected by stress" in Table 2. In the model, we divided the items into the ones affected in "class A" and not affected in "class N", and formed the basic events for all failure categories. Fig. 9 shows the resulting FTA for an OWT. The increase of failure rates is implemented with the stress factor from Eq. 3. It is set four for the affected class A items when the manipulation starts.

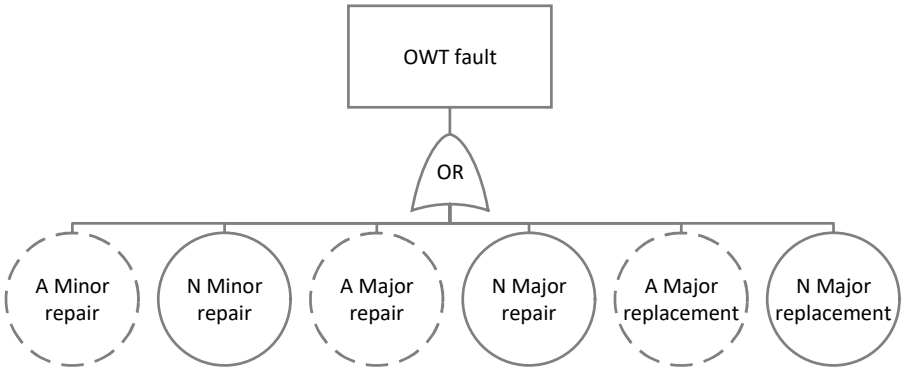

Figure 9: High-level FTA of OWT for the cyber attack case. Compared to Fig. 7, the tree has event classes A and N. Class A events are made more frequent by the stress caused by the cyber attack, while class N events are not.

We do not speculate how the attack was conducted as the main interest is to study the ability of the maintenance to sustain operations. Therefore, we consider a case that would cause the most harm to the operations. We assume that an attacker has infected all the OWTs and starts the attack when the OWF is the hardest to access. In the North Sea, the wind speed and wave heights are higher during the winter. The high wind speed also increases the

OWF's potential for energy production and, at the same time, the need for energy for lighting and heating is the highest. Due to these reasons, we set the manipulation to occur at the start of October.

4.2.2. Case 2 results

Fig. 10 shows availability during a one year of simulations where the failure rate increases at the start of October, due to the stress factor being set four. The effect is not immediately visible as to a certain degree O&M can keep up with the increasing amount of failures. As in case 1, the weather in this specific year prevented maintenance in November and December. Unlike in case 1, this leads to a significant drop in availability. However, in some simulated years, this difference is not as clear as in Fig. 10. Therefore, the authors believe that in some cases the attack would not be immediately recognized.

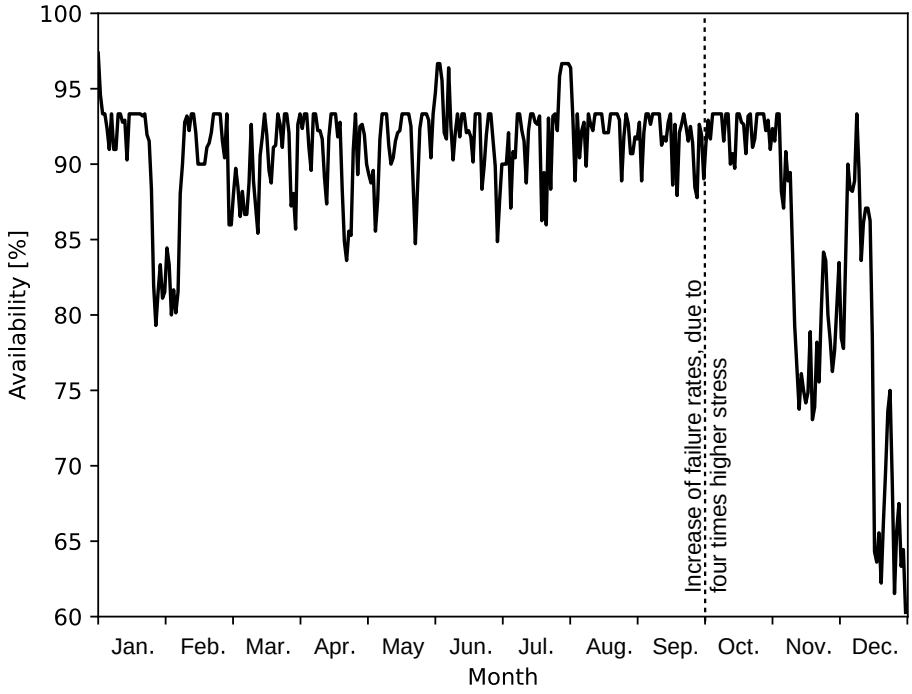

Figure 10: Average daily availability in a simulation of the cyber attack case. The availability starts to decrease in November once the maintenance becomes overwhelmed with tasks.

We again calculated the averages of 100 rounds of simulations to produce availability and MTTR performance indicators. The mean availability was 87.6% with a standard deviation of 1.1%. The MTTR was 102.5 h with a standard deviation of 7.8 h. While the difference to case 1 seems small, the MTTR is higher after the attack. For example, in one case the MTTR was 96.6 h before the attack and 108.9 h after it. Notably, unfinished repairs are

excluded from these values. Therefore, the difference between MTTR before and after the attack is likely higher.

The main purpose of this case is to show how the O&M can handle a higher failure rate. In a more detailed model, the effects of the attack scenario could be slightly different. In the presented simplified model, if a certain type of failure occurs in an OWT, the same type of failure cannot occur again before it is repaired. This assumption leads to a cycle where the O&M starts to increase the availability once enough failures have occurred.

However, if we model individual systems and assume that the attack rapidly ages the systems, the failure rates may only increase over time as was presented in Fig. 3. In that case, the drop in performance would occur later. This behavior is also suggested by B. Le and J. Andrews [75]. As their data shows a significant increase in failure rates only once the equipment has degraded to a critical condition. On the other hand, a cyber-attack has the potential to cause immediate damage [70], if an attacker acts in a more unconcealed manner.

4.3. Case 3: HILP scenario

4.3.1. Case 3 scenario description and modeling

This case represents an incident where a ship collision with an OWT causes a rare 3-phase short circuit. Such an electrical disturbance within an OWF causes transients within its power system dynamics. This means that the power flow of the affected component would be redistributed to other components according to circuit laws, and subsequently redistributed again according to the control and protection actions [70, 76]. These transients include deviations of power flows, frequency, currents, and voltages. Therefore, sufficiently severe disturbances would result in the disconnection of the affected OWTs by corresponding protection actions [70, 76].

The Simscape Electrical Specialized Power Systems was used under the Simulink environment for the quantitative investigation of the HILP disturbance in the OWF model through physical simulation with control and protection logic [77]. The OWF is modeled as a large-scale dynamical multi-domain system, consisting of interacting sub-systems of elements for energy conversion, transmission, measurement, control, and protection. This enables the simulation of the dynamic system response of the whole OWF to disturbances in the different sub-systems, capturing in a detailed manner the system behavior on functional and process levels. In this way, the power system dynamics due to the disturbance are determined quantitatively.

The OWF model with a 25 km AC export cable and individual OWTs with squirrel-cage induction generators (SCIG) were used, as shown in Fig. 11. The model has an array of six OWTs arranged in three strings, shown on the right. Each string contains two OWTs with the corresponding two internal AC cables (each 1 km long). The voltage level within the array is 25 kV. The active power generated (P) by the OWTs is transmitted through the AC export cable to the onshore transformer substation whereas reactive power (Q) flows in the opposite direction. The voltage is raised at the onshore substation to the level of

the onshore grid of 120 kV. After this, the power is fed into the onshore AC grid. A static compensation (STACOM) device is installed at the offshore substation providing stability to the OWT array. This model was introduced in [78] and it is an extension of the one used in [70]. Both of these works [70, 78] study the same HILP scenario and show that if the short circuit duration is long enough all the OWTs will get disconnected and this effect can be scaled.

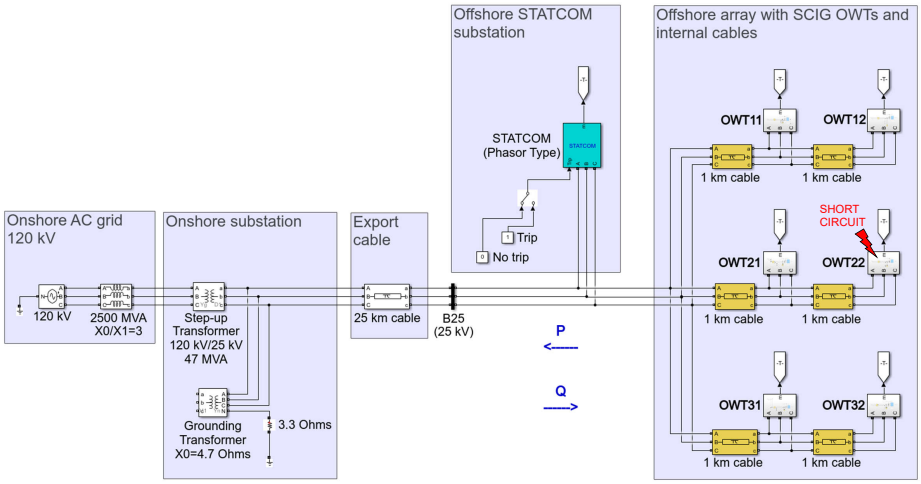

Figure 11: Power system model of the OWF with 6 SCIG OWTs used for HILP scenario investigation. The corresponding short circuit is also indicated.

We assume as a cause for the HILP a severe collision of a ship with an OWT, here OWT22. Such a collision would damage the tower/foundation of the OWT. This would lead to a significant mechanical deformation of the components of the electrical system in the region of the aforementioned structural damage. Such deformations are one of the main causes of the 3-phase short circuits, which are rare in electrical systems. The scenario is modeled in electrical system terms here by applying a 3-phase short circuit (phase-to-ground) at the terminals of OWT22 at $t = 10$ s with a short-circuit duration of 0.099 s.

The short circuit occurs at terminals of OWT22, i.e. on the low voltage side (690 V) prior to the OWT transformer[4]. The result of the simulation of the disturbance is shown in Fig. 12. Prior to the disturbance ($t < 10$ s) the OWF is in a normal operation state expressed by the steady-state curves of the generated power of all OWTs, which overlap due to the identical wind speed value for all OWTs. The occurrence of disturbance perturbs the curves so that all OWTs enter a disturbed operational state for $10 \text{ s} \leq t < 10.13$ s.

The disturbance is so severe that it propagates from the low voltage region at OWT22 through the much higher medium voltage (25 kV) region of the internal

[4]The transformer is not depicted in Fig. 11.

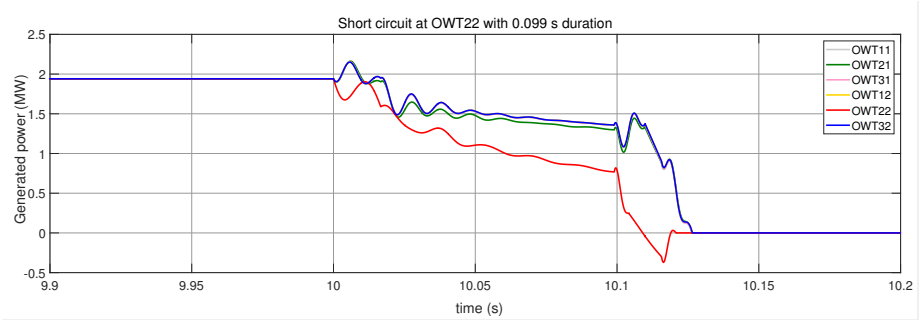

Figure 12: Dynamic response of the OWF to the disturbance.

cables and affects the remaining OWTs. This causes an AC overvoltage that leads the protection systems to disconnect automatically all OWTs. Due to the disconnection, the value of the generated power by all OWTs becomes eventually zero, as shown in Fig. 12. The whole OWF enters to a non-functional state (a service interruption on the OWF level at $t = 10.13$ s).

It was found in [70] that increasing the duration of the short circuit leads to an increased number of disconnected OWTs causing the service interruption of the whole OWF. The presented results here and in [78] confirm these findings. Compared to [70] this paper and [78] assess an OWF model with the double number of OWTs and a string layout. Based on this we assume that a sufficiently long short circuit at a single OWT would lead in a similar way to the disconnection of an OWF with 30 OWTs as considered further here.

The restoration of the original normal operation state of the OWF is modeled in the OWF model described in section 3. Fig. 13 shows the ETA on how the ship collision leads to the tower/foundation damage and the significantly deformed electrical components at OWT22. This deformation causes a short circuit and due to it, all other OWTs need to be inspected and to be manually switched on for achieving normal operation.

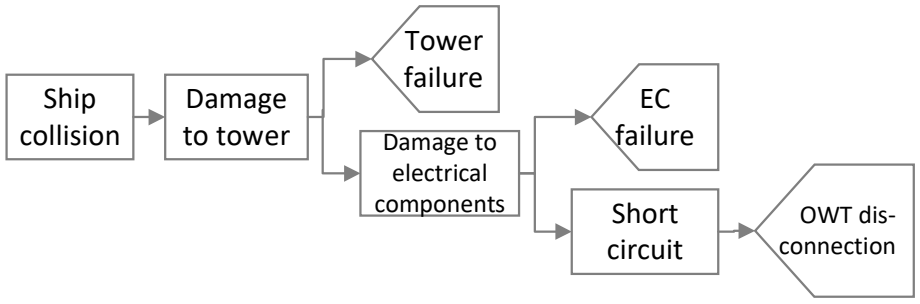

Figure 13: ETA of the HILP scenario where a ship collision leads to major repairs in OWT22 and a short circuit.

710 ETA transfers the faults to FTAs. In OWT22, the failure results in major repair of the foundation and electrical components as shown in Fig. 14. In other OWTs the inspection is considered to be similar to a minor repair in categories used in [62]. The resulting FTA is shown in Fig. 15.

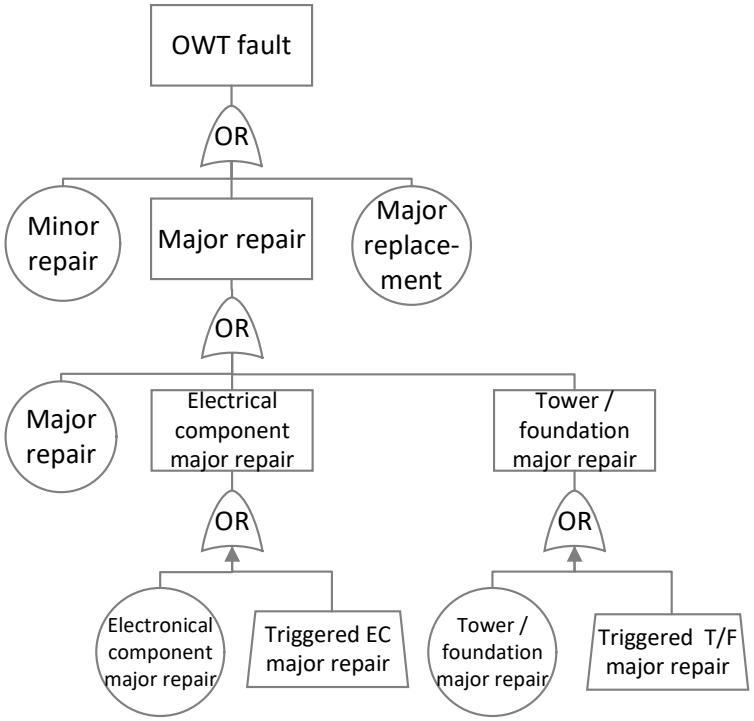

Figure 14: This FTA depicts the OWT where the HILP incident occurs. Therefore, the tower/foundation and electrical components have a triggered failure for major repair in addition to the basic fault node.

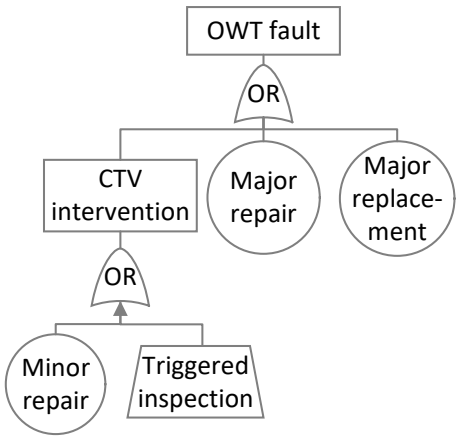

Figure 15: This FTA depicts an OWT that is affected by the HILP incident causing a disconnection that triggers a need for an inspection by a CTV.

4.3.2. Case 3 result

Fig. 16 shows availability during a one year of simulations where the HILP incident occurs during the first half of September. In the shown year, all the failures caused by this incident were repaired 408 h after the incident. The recovery forms a so-called performance based resilience curve, where the availability is regarded as a metric to measure infrastructure performance [79].

We also calculated the averages of 100 rounds of simulations to produce availability and MTTR performance indicators. The mean availability was 89.0% with a standard deviation of 0.4%. The MTTR was 114.6 h with a standard deviation of 5.7 h. On average, the last HILP-related repair was performed 432.5 h after the incident.

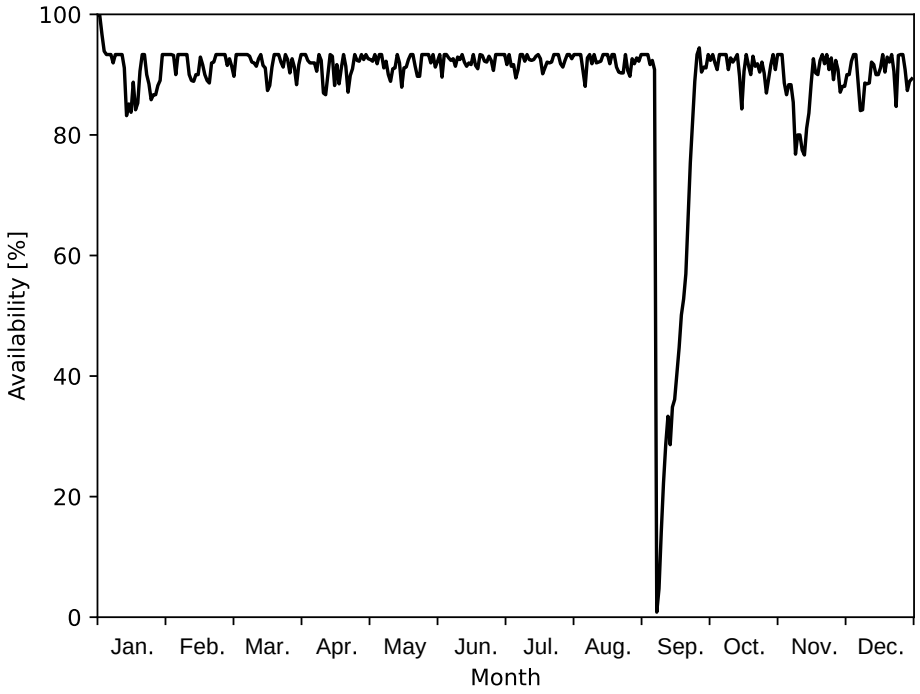

Figure 16: Average daily availability in a simulated year with a HILP incident. The O&M is able to restore the OWF to normal operation availability within a few weeks.

5. Discussion

Our approach combines ideas from state-of-art OWF models described in section 2.2 and traditional risk assessment tools. This combination has two main benefits. It allows a more formal description of OWT failures that can be extended to more detailed failure scenarios that are not typically considered in modeling daily O&M activities within OWF. It also responds to criticisms presented in section 2.3, where it was described that traditional risk tools do not correctly depict system restoration. This feature is especially important for modeling system resilience in an offshore environment where the ability to access infrastructure depends on the weather, and availabilities of personnel and equipment. We further believe that this approach of layered state models can be extended to portray additional services within an infrastructure, as suggested in [44].

Section 4 demonstrated the value of this approach in showing that it can be used for describing different disturbance scenarios to study if the maintenance service can sustain or restore OWF availability. These kinds of assessments are in line with ideas from [9] where resilience is presented as the ability of the studied system to maintain functionality and recover, given that one or more adversarial events occur, whether these events are known or not. We believe

that for complex but confined systems, like offshore wind farms, the possible outcomes also have certain limits. A model allows testing system response in different scenarios where the system or the scenario may be novel. This is important for OWF as more of them are planned in new locations and with new configurations. For example, future OWFs may be used for hydrogen production [80].

The issue in these assessments is that a model with a set scenario can only represent a known threat. Work by T. Aven [81] suggests that to prepare for unknown failures one may assess the system from a macro perspective and focus on the major states and consequences. It is unnecessary to know all scenarios that can lead to an undesired state. In this type of assessment, one can assume that the undesired state emerged - whatever the reason. The assessment can focus on making the system able to sustain or restore its functionality and performance following the incident. This is different from attempting to accurately estimate how often this type of state may occur and why.

We similarly believe that system resilience can be assessed by developing exemplary failure scenarios to test the system. In this paper, both test cases assumed certain disturbance scenarios but can be generalized to represent a situation with a high failure rate or multiple simultaneous failures. To a certain degree, one can induce that if a system behaves in a certain way in a test scenario, it will behave similarly in a comparable situation regardless of what caused it. For the sake of modeling, these scenarios must have set failure rates like in case 2 or set faults occurring like in case 3. As these scenario setups are only estimates, in a more thorough analysis one can further conduct an uncertainty assessment by varying these parameters, as it was done in [17]. Presented cases can be seen as testing system's graceful extensibility or brittleness, i.e. are the operations sustained under unexpected stress [82]. These stresses challenge the finite resources reserved for maintaining the system. Costs related to maintenance assets and personnel create an incentive to minimize the amount of them.

Having a system model further enables one to create these test scenarios and compare how a system responds to the incident with different parameters. The change of parameters can e.g. represent a countermeasure that is designed to mitigate a threat. Comparing the initial system performance to the one with a countermeasure provides information on the efficiency of that countermeasure. This information allows assessing how to make the system more resilient and supports the decision on what countermeasures should be introduced. For example, we used our previous model to measure the recoverability of an OWF from an incident with a different number of CTVs [83].

Yet this approach is disputed, as an earlier article by D. Woods has also described unanticipated perturbations being events that call into question the model of competence [84]. In this case, one could argue that considering failures and O&M's ability to handle them could be considered as *"solving the wrong problem"*. However, D. Woods's later article described the abilities to rebound, robustness, and graceful extensibility among concepts of resilience, where robustness is the set of *known* disturbances the system can respond to

effectively [82]. Furthermore, the new CER directive mandates critical entities to conduct risk assessments and take appropriate and proportionate measures to ensure resilience [5]. The focus of the directive is on identified risks. Based on these interpretations, we argue that our approach can provide information on a system's resilience. In our case 2, the increase of failure rate was sufficient to significantly reduce the system availability to a point where the operations would not be sustainable. So, the test proved that at that point the system was not resilient against such an event.

6. Conclusions

The green energy transition and geopolitical risks related to fossil fuels are making the OWFs ever more important for nationwide energy provision. This development combined with the increasing installed power of OWF makes them to be considered as CI and a subject to special attention on their protection and resilience. Section 3 presented a model of an OWF that combined failure and O&M modeling to study how the maintenance service can sustain or recover operations under different stressors.

The fault modeling is based on a cause-consequence tree library for Simulink that was presented in section 3.2. The focus of that section was to present the dynamic features of the library, which are the abilities 1) to change the failure rate during a simulation with a so-called stress factor and 2) to exchange information with the O&M model. This model is described in section 3.3.

In section 4, the model was used for studying OWF availability in three test scenarios. The first scenario depicted normal operations and was used as a reference for other scenarios. The second scenario used a premise of a cyber-attack to show how an increasing failure rate decreases availability. The last scenario presented a HILP incident where the maintenance service must handle a high amount of simultaneous failures. This scenario linked the physical simulation of the energy provision system to the event-driven O&M model of an OWF. In this manner, the OWF operations are considered as a combination of technical and human-technical aspects.

The outcome of this research is an OWF model that was proven to be able to depict different scenarios where OWF operation came under stress. In the future, this model can be used for representing other, more detailed scenarios. The cause-consequence tree library can further be used as a stand-alone tool or as a part of another model for risk and reliability assessments.

Acknowledgments

This paper uses data from Copernicus Climate Change Service information (accessed 2021). Neither the European Commission nor ECMWF is responsible for any use that may be made of the Copernicus information or data it contains.

References

[1] Federal Ministry for Economic Affairs and Climate Action, Overview of the Easter package, Online (2022).
URL https://www.bmwk.de/Redaktion/EN/Downloads/Energy/0406_ueberblickspapier_osterpaket_en.html

[2] IRENA, Future of wind: Deployment, investment, technology, grid integration and socio-economic aspects, White paper, International Renewable Energy Agency (2019).

[3] European Commission, REPowerEU: Joint European action for more affordable, secure and sustainable energy, Press release IP/22/1511, European Commission (2022).

[4] Federal Ministry of the Interior and Community, Zweite Verordnung zur Änderung der BSI-Kritisverordnung, in: Bundesgesetzblat Teil I, no. 63, Bundesanzeiger Verlag, 2021, pp. 4163 – 4187.

[5] European Union, Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Off. J. Eur. Union 65 (2022) 164 – 198.

[6] C. Pursiainen, Critical infrastructure resilience: A Nordic model in the making?, Int. J. Disaster Risk Reduct. 27 (2018) 632 – 641. doi:10.1016/j.ijdrr.2017.08.006.

[7] B. Skobiej, A. Niemi, N. Kulev, F. Sill Torres, Influence of the personnel availability on offshore wind farm maintenance, in: Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15), Research Publishing Services, 2020, pp. 644 – 651. doi:10.3850/978-981-14-8593-0_5735-cd.

[8] B. Skobiej, A. Niemi, Validation of copula-based weather generator for maintenance model of offshore wind farm, WMU J. Marit. Aff. 21 (2022) 73–87. doi:10.1007/s13437-021-00255-x.

[9] T. Aven, The call for a shift from risk to resilience: What does it mean?, Risk Anal. 39 (2019) 1196–1203. doi:10.1111/risa.13247.

[10] N. Falliere, L. O. Murchu, E. Chien, W32.Stuxnet Dossier, White paper Version 1.4, Symantec Corporation (2011).

[11] B. Obama, Critical infrastructure security and resilience, Presidential Policy Directive PPD 21, The White House (2013).

[12] A. Niemi, F. Sill Torres, Evaluation of the proposed European Commission directive on critical entities resilience and its potential to consolidate the

resilience terminology, in: Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022), Research Publishing, Singapore, 2022, pp. 2773 – 2780. doi:10.3850/978-981-18-5183-4_S21-02-213-cd.

[13] C. Pursiainen, E. Kytömaa, From European critical infrastructure protection to the resilience of European critical entities: what does it mean?, Sustain. Resil. Infrastruct. 8 (2023) 85–101. doi:10.1080/23789689.2022.2128562.

[14] OECD, Good Governance for Critical Infrastructure Resilience, OECD Publishing, 2019. doi:10.1787/02f0e5a0-en.

[15] B. Rød, D. Lange, M. Theocharidou, C. Pursiainen, From risk management to resilience management in critical infrastructure, J. Manag. Eng. 36 (2020) 04020039. doi:10.1061/(ASCE)ME.1943-5479.0000795.

[16] M. Hofmann, A review of decision support models for offshore wind farms with an emphasis on operation and maintenance strategies, Wind Eng. 35 (2011) 1–15. doi:10.1260/0309-524X.35.1.1.

[17] M. N. Scheu, A. Kolios, T. Fischer, F. Brennan, Influence of statistical uncertainty of component reliability estimations on offshore wind farm availability, Reliab. Eng. Syst. Saf. 168 (2017) 28–39. doi:10.1016/j.ress.2017.05.021.

[18] M. Sahnoun, D. Baudry, N. Mustafee, A. Louis, P. A. Smart, P. Godsiff, B. Mazari, Modelling and simulation of operation and maintenance strategy for offshore wind farms based on multi-agent system, J. Intell. Manuf. 30 (2019) 2981–2997. doi:10.1007/s10845-015-1171-0.

[19] C. Gutschi, N. Furian, S. Voessner, M. Graefe, A. Kolios, Evaluating the performance of maintenance strategies: A simulation-based approach for wind turbines, in: 2019 Winter Simulation Conference (WSC), IEEE, 2019, pp. 842–853. doi:10.1109/WSC40007.2019.9004681.

[20] E. Byon, E. Pérez, Y. Ding, L. Ntaimo, Simulation of wind farm operations and maintenance using discrete event system specification, Simul. 87 (2011) 1093–1117. doi:10.1177/0037549710376841.

[21] Y. Dalgic, I. Lazakis, O. Turan, Investigation of optimum crew transfer vessel fleet for offshore wind farm maintenance operations, Wind Eng. 39 (2015) 31–52. doi:10.1260/0309-524X.39.1.31.

[22] A. Zitrou, T. Bedford, L. Walls, A model for availability growth with application to new generation offshore wind farms, Reliab. Eng. Syst. Saf. 152 (2016) 83–94. doi:10.1016/j.ress.2015.12.004.

[23] A. Saleh, M. Chiachío, J. Fernández Salas, A. Kolios, Self-adaptive optimized maintenance of offshore wind turbines by intelligent Petri nets, Reliab. Eng. Syst. Saf. 231 (2023) 109013. doi:https://doi.org/10.1016/j.ress.2022.109013.

[24] M. Liu, J. Qin, D.-G. Lu, W.-H. Zhang, J.-S. Zhu, M. H. Faber, Towards resilience of offshore wind farms: A framework and application to asset integrity management, Appl. Energy 322 (2022) 119429. doi:10.1016/j.apenergy.2022.119429.

[25] D. Wilkie, C. Galasso, A probabilistic framework for offshore wind turbine loss assessment, Renew. Energy 147 (2020) 1772–1783. doi:10.1016/j.renene.2019.09.043.

[26] S. Rose, P. Jaramillo, M. J. Small, J. Apt, Quantifying the hurricane catastrophe risk to offshore wind power, Risk Anal. 33 (2013) 2126–2141. doi:10.1111/risa.12085.

[27] A. John, Z. Yang, R. Riahi, J. Wang, A risk assessment approach to improve the resilience of a seaport system using Bayesian networks, Ocean Eng. 111 (2016) 136–147. doi:10.1016/j.oceaneng.2015.10.048.

[28] H. D. Estrada-Lugo, T. Santhosh, M. de Angelis, E. Patelli, Resilience assessment of safety-critical systems with credal networks, in: Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15), Research Publishing Services, 2020, pp. 1199 – 1206. doi:10.3850/978-981-14-8593-0_4192-cd.

[29] C. Heracleous, P. Kolios, C. G. Panayiotou, G. Ellinas, M. M. Polycarpou, Hybrid systems modeling for critical infrastructures interdependency analysis, Reliab. Eng. Syst. Saf. 165 (2017) 89–101. doi:10.1016/j.ress.2017.03.028.

[30] C. Foglietta, S. Panzieri, Resilience in critical infrastructures: The role of modelling and simulation, in: Issues on Risk Analysis for Critical Infrastructure Protection, IntechOpen, 2020, Ch. 1. doi:10.5772/intechopen.94506.

[31] H. Sun, H. Wang, M. Yang, G. Reniers, A STAMP-based approach to quantitative resilience assessment of chemical process systems, Reliab. Eng. Syst. Saf. 222 (2022) 108397. doi:https://doi.org/10.1016/j.ress.2022.108397.

[32] R. Yan, S. Dunnett, Resilience assessment for nuclear power plants using Petri nets, Ann. Nucl. Energy 176 (2022) 109282. doi:10.1016/j.anucene.2022.109282.

[33] R. Yan, S. Dunnett, J. Andrews, A petri net model-based resilience analysis of nuclear power plants under the threat of natural hazards, Reliab. Eng. Syst. Saf. 230 (2023) 108979. doi:10.1016/j.ress.2022.108979.

[34] Z. Tan, B. Wu, A. Che, Resilience modeling for multi-state systems based on Markov processes, Reliab. Eng. Syst. Saf. 235 (2023) 109207. doi:https://doi.org/10.1016/j.ress.2023.109207.

[35] S. Geng, M. Yang, M. Mitici, S. Liu, A resilience assessment framework for complex engineered systems using graphical evaluation and review technique (GERT), Reliab. Eng. Syst. Saf. 236 (2023) 109298. doi:https://doi.org/10.1016/j.ress.2023.109298.

[36] I. Häring, Technical Safety, Reliability and Resilience, Springer Singapore, 2021, Ch. 2, pp. 9–26. doi:10.1007/978-981-33-4272-9_2.

[37] K. Clegg, D. Stamp, J. McDermid, Binding fault logic to system design: A SysML approach, in: Proceedings of the 31st European Safety and Reliability Conference, Research Publishing (S) Pte Ltd., 2021, pp. 880 – 887. doi:10.3850/978-981-18-2016-8_718-cd.

[38] O. Lisagor, T. Kelly, R. Niu, Model-based safety assessment: Review of the discipline and its challenges, in: The Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety, 2011, pp. 625–632. doi:10.1109/ICRMS.2011.5979344.

[39] F. Mhenni, F. Vitolo, A. Rega, R. Plateaux, P. Hehenberger, S. Patalano, J.-Y. Choley, Heterogeneous models integration for safety critical mechatronic systems and related digital twin definition: Application to a collaborative workplace for aircraft assembly, Appl. Sci. 12 (2022) 2787. doi:10.3390/app12062787.

[40] A. Niemi, Modeling future hadron colliders' availability for physics, Ph.D. thesis, Tampere University (2019).

[41] E. Zio, P. Baraldi, E. Patelli, Assessment of the availability of an offshore installation by Monte Carlo simulation, Int. J. Press. Vessel. Pip. 83 (4) (2006) 312–320. doi:10.1016/j.ijpvp.2006.02.010.

[42] F. Chiacchio, J. I. Aizpurua, L. Compagno, S. M. Khodayee, D. D'Urso, Modelling and resolution of dynamic reliability problems by the coupling of Simulink and the stochastic hybrid fault tree object oriented (SHyFTOO) library, Inf. 10 (2019) 283. doi:10.3390/info10090283.

[43] S. Jackson, S. Cook, T. L. J. Ferris, A generic state-machine model of system resilience, INSIGHT 18 (1) (2015) 14–18. doi:10.1002/inst.12003.

[44] E. Engler, M. Baldauf, F. Sill Torres, S. Brusch, Finite state machine modelling to facilitate the resilience of infrastructures: Reflections, Infrastruct. 5 (2020) 24. doi:10.3390/infrastructures5030024.

[45] E. Ruijters, M. Stoelinga, Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools, Comput. Sci. Rev. 15-16 (2015) 29–62. doi:10.1016/j.cosrev.2015.03.001.

[46] Simulink® Getting Started Guide, The MathWorks, Inc., 2022, revised version for Simulink 10.5 (Release 2022a).

[47] A. Niemi, F. Sill Torres, Application of synthetic weather time series based on four-dimensional copula for modeling of maritime operations, in: OCEANS 2021: San Diego – Porto, IEEE, 2022, pp. 1–8. doi:10.23919/OCEANS44145.2021.9705681.

[48] A. de Ruijter, F. Guldenmund, The bowtie method: A review, Saf. Sci. 88 (2016) 211–218. doi:10.1016/j.ssci.2016.03.001.

[49] D. Nielsen, O. Platz, B. Runge, A cause-consequence chart of a redundant protection system, IEEE Trans. Reliab. R-24 (1975) 8–13. doi:10.1109/TR.1975.5215314.

[50] W. E. Vesely, F. F. Golberg, N. H. Roberts, D. F. Haasl, Fault Tree Handbook, U.S. Nuclear Regulatory Commission, 1981.

[51] International Electrotechnical Commission, International electrotechnical vocabulary (IEV) - Part 192 Dependability, International standard 60050-192:2015, IEC (2015).

[52] F. Chiacchio, J. I. Aizpurua, L. Compagno, S. M. Khodayee, D. D'Urso, Modelling and resolution of dynamic reliability problems by the coupling of Simulink and the stochastic hybrid fault tree object oriented (SHyFTOO) library, Inf. 10 (2019) 283. doi:10.3390/info10090283.

[53] E. Patelli, S. Tolo, H. George-Williams, J. Sadeghi, R. Rocchetta, M. de Angelis, M. Broggi, OpenCossan 2.0: an efficient computational toolbox for risk, reliability and resilience analysis, in: Proceedings of the joint ICVRAM ISUMA UNCERTAINTIES conference, 2018.

[54] E. Patelli, System reliability analysis, Computation of the system reliability based on a fault tree analysis of random heterogeneous media, Internal Working Report No. 3-56, Institute of Engineering Mechanics in Leopold Franzens University (2009).

[55] K. Aslansefat, G. Latif-Shabgahi, M. Kamarlouei, A strategy for reliability evaluation and fault diagnosis of autonomous underwater gliding robot based on its fault tree, Int. J. Adv. Electron. Comput. Sci. 1 (2014) 4 – 10.

[56] A. Chovanec, J. Bucha, Simulation of FTA in Simulink, Reliab. Risk Anal. Theory Appl. 1 (2008) 35 – 41.

[57] B. Bertsche, Reliability in automotive and mechanical engineering, Springer-Verlag, 2008, Ch. 2.2.3, pp. 41–42. doi:10.1007/978-3-540-34282-3_2.

[58] P. Del Moral, S. Penev, Stochastic processes: From applications to theory, CRC Press, 2016, Ch. 4.1, pp. 71 – 73. doi:10.1201/9781315381619.

[59] SimEvents® Getting Started Guide, The MathWorks, Inc., 2022, revised version for Simulink 10.5 (Release 2022a).

[60] L. Felsberger, B. Todd, D. Kranzlmüller, Cost and availability improvements for fault-tolerant systems through optimal load-sharing policies, Procedia Comput. Sci. 151 (2019) 592–599. doi:10.1016/j.procs.2019.04.080.

[61] J. Carroll, A. McDonald, D. McMillan, Failure rate, repair time and unscheduled O&M cost analysis of offshore wind turbines, Wind Energy 19 (2016) 1107 – 1119. doi:10.1002/we.1887.

[62] J. Carroll, A. McDonald, O. Barrera Martin, D. McMillan, R. Bakhshi, Offshore wind turbine sub-assembly failure rates through time, in: European Wind Energy Association annual conference and exhibition. 2015. (EWEA 2015), Vol. 1, WindEurope, 2015, pp. 207–217.

[63] O. S. Andersen et al., Guidelines for Offshore Marine Operations (GOMO), GOMO work group, 2020.

[64] G. Katsouris, L. Savenije, Offshore wind access 2017, Tech. Rep. ECN-E-16-013, ECN (2016).

[65] Outer Continental Shelf National Center of Expertise (OCSNCOE), Introduction to offshore supply vessels, Tech. rep., United States Coast Guard (2020).

[66] G. Leontaris, O. Morales-Nápoles, A. Wolfert, Probabilistic scheduling of offshore operations using copula based environmental time series – An application for cable installation management for offshore wind farms, Ocean Eng. 125 (2016) 328–341. doi:10.1016/j.oceaneng.2016.08.029.

[67] Copulas python library, accessed June 2021.
URL https://sdv.dev/Copulas/

[68] H. Hersbach, B. Bell, P. Berrisford, G. Biavati, A. Horányi, J. Muñoz Sabater, J. Nicolas, C. Peubey, R. Radu, I. Rozum, D. Schepers, A. Simmons, C. Soci, D. Dee, J. Thépaut, ERA5 hourly data on single levels from 1959 to present, Copernicus Climate Change Service (C3S) Climate Data Store (CDS), 2018. doi:10.24381/cds.adbb2d47.

[69] Y. Dalgic, I. Dinwoodie, I. Lazakis, D. McMillan, M. Revie, Optimum CTV fleet selection for offshore wind farm O&M activities, in: Safety and Reliability: Methodology and Applications, CRC Press, 2014, pp. 1177 – 1186. doi:10.1201/b17399-167.

[70] N. Kulev, F. Sill Torres, Simulation of the impact of parameter manipulations due to cyber-attacks and severe electrical faults on offshore wind farms, Ocean Eng. 260 (2022) 111936. doi:10.1016/j.oceaneng.2022.111936.

[71] J. Staggs, D. Ferlemann, S. Shenoi, Wind farm security: attack surface, targets, scenarios and mitigation, Int. J. Crit. Infrastruct. Protect. 17 (2017) 3–14. doi:10.1016/j.ijcip.2017.03.001.

[72] S. Xu, H. Tu, Y. Xia, Resilience enhancement of renewable cyber–physical power system against malware attacks, Reliab. Eng. Syst. Saf. 229 (2023) 108830. doi:https://doi.org/10.1016/j.ress.2022.108830.

[73] S. Parvin, M. Goli, F. Sill Torres, R. Drechsler, Trojan-D2: Post-layout design and detection of stealthy hardware trojans - A RISC-V case study, in: ASPDAC '23: Proceedings of the 28th Asia and South Pacific Design Automation Conference, Association for Computing Machinery, 2023, p. 683–689. doi:10.1145/3566097.3567919.

[74] M. McCarty, J. Johnson, B. Richardson, C. Rieger, R. Cooley, J. Gentle, B. Rothwell, T. Phillips, B. Novak, M. Culler, B. Wright, Cybersecurity resilience demonstration for wind energy sites in co-simulation environment, IEEE Access 11 (2023) 15297–15313. doi:10.1109/ACCESS.2023.3244778.

[75] B. Le, J. Andrews, Modelling wind turbine degradation and maintenance, Wind Energy 19 (2016) 571 – 591. doi:10.1002/we.1851.

[76] W. Kröger, E. Zio, Vulnerable Systems, Springer London, 2011. doi:10.1007/978-0-85729-655-9.

[77] Simscape^{TM} Electrical^{TM} User's Guide (Specialized Power Systems), The MathWorks, Inc., 2022, revised for Version 7.8 (Release 2022b).

[78] N. Kulev, F. Sill Torres, Investigation of high-impact low-probability disturbances in offshore wind farms, in: European Workshop on Maritime Systems Resilience and Security 2022 (MARESEC 2022), Zenodo, 2022. doi:10.5281/zenodo.7149239.

[79] C. Poulin, M. B. Kane, Infrastructure resilience curves: Performance measures and summary metrics, Reliab. Eng. Syst. Saf. 216 (2021) 107926. doi:10.1016/j.ress.2021.107926.

[80] G. Calado, R. Castro, Hydrogen production from offshore wind parks: Current situation and future perspectives, Appl. Sci. 11 (2021) 5561. doi:10.3390/app11125561.

[81] T. Aven, How some types of risk assessments can support resilience analysis and management, Reliab. Eng. Syst. Saf. 167 (2017) 536–543. doi:10.1016/j.ress.2017.07.005.

[82] D. D. Woods, Four concepts for resilience and the implications for the future of resilience engineering, Reliab. Eng. Syst. Saf. 141 (2015) 5–9. doi:10.1016/j.ress.2015.03.018.

[83] B. Skobiej, A. Niemi, N. Kulev, F. Sill Torres, Resilient recovery features of offshore wind farm with maintenance service, in: 2021 Resilience Week (RWS), 2021. doi:10.1109/RWS52686.2021.9611808.

[84] D. D. Woods, Essential characteristics of resilience, in: Resilience Engineering Concepts and Precepts, CRC Press, 2006, pp. 21–34. doi:10.1201/9781315605685-4.