

Cyber-Physical Security and Resilience for Offshore Wind Farms

Jennifer Mielniczek
Safety Engineer
Glückstadt, Germany
j.mielniczek@entrawind.com

Corinna Köpke and Kushal Srivastava
Fraunhofer Institute for High-Speed
Dynamics
Ernst-Mach-Institut, EMI
Efringen-Kirchen, Germany
Corinna.Koepke@emi.fraunhofer.de,
Kushal.Srivastava@emi.fraunhofer.de

Egon Schröder
Offshore Projects
ESC-Systeme GmbH
Leer, Germany
egon.schroeder@esc-systeme.de

Abstract— Offshore wind farms (OWF) are relevant to the grid system and represent a substantial component in the energy transition. Risks such as cyber-physical threats need to be assessed and controlled to protect these infrastructures. In this work, it is aimed to model the relevant cyber and information security components of an OWF and to assess phase-specific risks. The model and risk assessment will be employed to propagate threats and to quantify the systems resilience.

Keywords— *Offshore wind farm, critical infrastructure, cyber-physical security, risk assessment, resilience*

I. INTRODUCTION

In the course of energy transition and the achievement of climate protection goals in Germany, the federal cabinet has passed an amendment to the 2017 Renewable Energy Act (Erneuerbare-Energien-Gesetz- EEG) which come into force on January 1, 2021. With the EEG novella 2021, an increasing trend of offshore wind energy is set: The expansion target for the industry sector is raised to 20 gigawatts for the year 2030 [1]. With this milestone, OWF make another important contribution to the supply of sustainable energy. Due to OWF special marine environmental and system relevance in the context of grid expansion and nuclear phase-out, the industry is facing extended threats which require measures such as permanent cyber-physical security of the assets. In general, cyber experts of the German government emphasize threats such as power outages across Europe caused by cyber-attacks [2]. In December 2015 and December 2016, power failures lasting several hours in Ukraine can be traced back to cyber-attacks [3]. The DNV GL describes the vulnerability of onshore wind farms caused by cyber-attacks which can be benchmarked to OWF [4].

Furthermore, in the sense of the German “Act to Strengthen the Security of Federal Information Technology”, the “Second Ordinance to amend the BSI KRITIS Regulation” comes into force on 01.01.2022. The upcoming amendments through the Federal Office for Information Security are intended to protect the functionality of critical infrastructures (CI or in German KRITIS). It describes, among other themes, the new megawatt (MW) threshold values that classify an asset or system as part of the CI which results in extended cyber security related measures. Within the current published draft bill, it is estimated that after regulation enforcement 150 additional operators will fall under the category ‘service providers for power generation’ with stricter requirements. [5] A transition period of 24 months applies for CI certification. The Federal Association of Wind Farm Operators Offshore (BWO) welcomes the increase of cyber security in sensitive

areas of the German economy, but the “system categories and threshold values” described in Part 3 (1.1.1) of the draft bill are criticized: The threshold value for generating assets is reduced from currently 420MW to 36MW [6]. Also, the Federal Association of Energy and Water Industry (BDEW) evaluated this sharp drop of threshold value as unsuitable. Together with other stakeholders, the BDEW was able to achieve a reduction from 420MW to 104MW instead of the originally planned 34MW [7]. However, the amendment of the regulation shows that cyber and information security is becoming increasingly vital in the field of renewable energies demanding additional security measures.

II. INITIAL ASSESSMENT PREPARATION

Being able to evaluate possible cyber-physical threats, risks, and the resulting measures in the context of resilience, a cyber-physical security assessment is carried out. This assessment requires minimum preparation tasks which starts with the definition of OWF and its’ associated network, followed by the identification and classification of critical components, leading to the requirement of stakeholder involvement. These tasks are not limited to the content described in this section and may be extended or adapted, depending on the application.

A. Definitions

A OWF is a complex system that can be divided into different sections (Fig. 1). Roughly structured, there is initially an offshore and an onshore part. There are the individual wind turbine generators (WTG) as individual components or several subsumed WTG within a so-called string, which are connected to the onshore substation via a converter station, the offshore substation (OSS). These sections or subsections may also belong to different stakeholders such as the windfarm operator (often also in the role of the windfarm owner) or the grid operator. Both, the wind farm operator, and the grid operator, are responsible for their respective systems and therefore the owner of the risk. This not only creates interfaces within the systems, but also between the various owners (owner of the asset), being responsible to manage the risk.



Fig. 1: Electricity transmission from turbines to offshore substation and finally to the power grid.

Hence, the cyber-physical security assessment requires the definition of an area that is to be assessed. The level of detail of the assessment is decisive for the delimitation of the OWF infrastructure and its network. One way of defining this limitation is to begin with an upper-level assessment, the general assessment. Here, all superior critical components and general risks are assessed, while, if necessary, multiple specific assessments are subsequent carried out. Whereby certain sections of the assessment can be evaluated in more detail. In the following elaboration, a particular case from a general assessment is used to illustrate the cyber-physical security assessment. Within the defined network, assets and components from the offshore and onshore area were considered:

- Assets: turbines, offshore substation, onshore substation,
- Components: offshore controllers, onshore controllers, firewalls, servers, remote technical units (RTU), automatic identification system (AIS), switches, navigational lights.

B. Critical components

Components, which are recognized as been critical to the system, should be acknowledged and evaluated. The identification of critical components is from great interest as they can have an impact on the safety of the system in form of their probability and/or severity.

The BSI-Standard 200-3, which is based on the German IT-Grundschutz modules, defines critical components in general with the following characteristics.

Critical components are:

- confidentiality, integrity, or availability,
- required to be highly protected,
- units which are not pictured by the IT-Grundschutz modules adequately,
- application or operating scenarios which are not covered by the IT-Grundschutzgesetz,
- information threats which are not sufficiently considered,
- additional security safeguards which go over or above the IT-Grundschutz requirements and might be necessary to be implemented. [8]

Critical components are recommended to be risk assessed to evaluate component-specific protection measures. Protection measures imply safety and security measures. Corresponding international norms are the ISO-norms ISO 31000:2018 [9] and ISO 27005:2018 [10], which are within the BSI-Standard 200-3 considered, e.g., risk analysis as part of the risk assessment.

C. Stakeholders

As already stated, the OWF system with its entire IT landscape represents a complex system with various internal and external interfaces. These interfaces can be linked to different stakeholders, who pursue different interests, define different critical components for themselves, identify different threats with their related risks and take different measures from them derive.

It is therefore recommended to take a stakeholder assessment into account with the target of identification and classification of threats, related risks, and further actions [11]. The involvement of stakeholders is depended on the containment of the cyber physical security assessment.

III. CYBER-PHYSICAL SECURITY ASSESSMENT

The identification of these threats is likewise attended by risks that can be subsumed in the form of a risk assessment & risk analysis. As a result of the risk assessment and risk analysis, protection measures can be derived that reduce the risk to an acceptable minimum – as low as reasonably practicable (ALARP) [12]. Finally, these protection measures are connected into the phases of the resilience management.

A. Threats

In the context of risk management, the identification of threats is one initial step needed for a systematic acquisition and collection related to cyber-physical security.

Prior to the assessment of the large number of specific and individual threats, general threats are advised to be summarized. The German BSI Standard 200-3, which is also a guideline for enterprises when it comes to information security risks, has transferred industry-known general threats in 47 so-called elementary threats [13]. Two of the 47 elementary threats are for example ‘malware’ and (cyber-) ‘attack’. So-called core values (C-confidentiality, I-integrity, A-availability) are associated to the individual elementary threat describing the potential damage by the respective threat. In this application, both elementary threats, ‘malware’ and ‘attack’, have according to the BSI Standard 200-3 following recognized core values: C, I, A. Since these threats can be directly or indirectly relevant on a target with an indicated risk of impact on the target, these threats need to be risk assessed.

Consequently, elementary threats can be seen as a guidance for the (general) risk assessment and risk analysis.

B. Risks

As mentioned before, the risk assessment starts with the identification of threats and their respective possible causation or trigger. Affected areas of concerns are classified as four diverse categories: (a) personnel, (b) asset, (c) environment, or (d) organization. Prior to the risk analysis, the risk matrix (definitions of probability and severity) needs to be aligned on - in best case by all stakeholders. Based on the risk matrix, the risk analysis is performed, considering the probability and severity calculation to evaluate the threat and its risk. The risk analysis is recommended to be conducted twice: once without protection measures (initial risk analysis) and once with protection measures (residual risk analysis). Measures need to be evaluated in such a value that the residual risk is acc. to the ALARP principle. In addition, it should be considered that the values or statements (e.g., low, medium, high) of the risk analysis are dependent on the qualitative and quantitative information researched.

In this application the threat identified is a malware attack on the OSS: physical access and malware injection.

TABLE I. SIMPLIFIED DEPICTION OF RISK ANALYSIS WITHOUT PROTECTION MEASURES

Threat	Core Value	Impact (severity x probability) and relevance	Comment
Malware	Confidentiality, availability, integrity.	Direct impact/relevant = high	Application without protection measures
Attack	Confidentiality, availability, integrity.	Direct impact/relevant = high	Application without protection measures

Table 1: The initial risk analysis shows that the threats without additional safeguards are considered with a *high-risk* potential, as the risk cannot be controlled. Possible direct consequences of the risk-impact could be that the malware is (i) slowing down the wind network [14] and (ii) offshore technicians get affected, while physically working on the system, unknowing that the system is under attack. Further, a possible indirect consequence of the risk-impact is linked to (iii) negatively influence of the enterprise's reputation. Thus, the affected areas of concerns are category (a) personnel, (b) asset and (d) organisation. Primarily, the probability of impact is recognised to be much higher for the asset than for personnel or organisation. Still, the severity of the impact on personnel may be critical. This risk evaluation validates that the residual risk must be reduced to an acceptable level. To control the various risks and consequences, protective measures must be taken.

C. Measures

When it comes to the evaluation of protection measures the TOP principle should apply: (T) Technical protection measures to be considered prior to (O) organizational protection measures, while (P) personnel protection measures are considered as the weakest measures (human failure factor).

In the scenario *malware attack on the OSS*, the following measures acc. to the TOP principle have been identified for category (b) asset:

- Restricted access by design (T),
- Individual network segments should be separated from each other and isolated (T),
- Suitable segmentation on the network level (T),
- Adequate key card system (T),
- Only authorised administrators (T),
- Malware analysis and security concept (O),
- Modelling and simulation facilities (O),
- Configuration in such a way that there is no access from outside (O),
- Only enable necessary traffic by specifying protocol and application parameters (O),
- Administration of virtual infrastructure is integrated into the central right management (O),
- Training and awareness of offshore technicians (P).

This list of suggested measures is not limited to. Furthermore, some of the presented measures may also apply for category (a) personnel and/or (d) organisation.

D. Resilience

The risk assessment on elementary threats gives a general overview of potential cyber-physical threats and associated risks. Additionally, affected areas of concerns are identified, consequences of risks are elaborated, and the risk analysis is indicated by the ratio severity/probability. Protection measures for risk mitigation are evaluated and suggested, reducing the remaining risk to an acceptable level.

Risk assessment can be linked to resilience management using e.g., the nine-step resilience management process developed by Häring et al. [15] based on the risk assessment standard ISO 31000:2018 [9]. A key aspect of resilience management is the quantification of infrastructure performance before, during and after any kind of incident. A resilience cycle can be applied that consists of five steps [16, 17, 18]: prepare, prevent, protect, respond, and recover (see Fig. 2). The risk assessment can then be further linked to the resilience cycle by implementing the priorly identified protection measures into the different phases of the resilience management. Reflecting the example of the cyber-physical elementary threat 'malware' and 'attack', the integrated application of resilience management is demonstrated.

Starting position of the resilience management is the trouble-free operation mode of the given system. At this stage, preventive measures as a result of a linked risk assessment are considered (prepare & prevent). An incident also called event or crisis occurs, which disturbs in different ways the trouble-free operation mode. The resilience of the system is the reaction of the impact during (protect) and after (respond) the event/crisis. The reaction is described as the functionality and capability of the system to get back with its own measures into a trouble-free operation mode within a certain timeframe (recover). The circle is closed by the lessons learned from this event and its' implementation into the new starting prepare phase.



Fig. 2: Resilience Cycle based on [16,17]

With the systematic assessment of resilience through these phases, a crisis, or an unforeseen event such as a cyber-attack can be mitigated. This process can support the efficient and effective way back into a fault and trouble-free condition – a successful operating OWF.

IV. SIMULATION

A. Model

To predict and quantify the impact of certain cyber-physical threats on OWF systems, the network and connections of relevant IT and information security components (Fig. 3) are represented in a generic OWF infrastructure model. A similar approach can be found in [19].

Different example components of the OWF have been selected to generate a generic OWF infrastructure model (generic graph-based model), i.e., controllers located on- or offshore, firewalls, servers, switches, RTU, turbines, AIS and navigational lights (see also section II-A). Note, the degree of detail is not for every component the same. The components No. 24 to No. 26 represent the Virtual Local Area Network (VLAN) responsible for controlling the navigational lights and components No. 27 to No. 30 are part of the SCADA VLAN. The connections between the components are based on the information flow between them. For example, an RTU collects information about a turbine and forwards this information on a regular basis to the SCADA server.

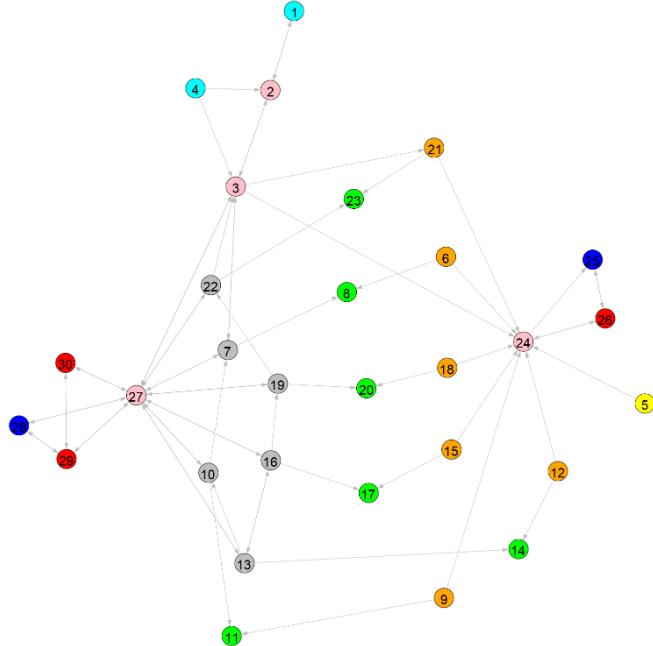


Fig. 3: OWF Model consisting of controllers on- and offshore (light blue), firewall (pink), server (red), remote technical units (grey), turbines (green), AIS (yellow), switches (dark blue), navigational lights (orange).

B. Scenario and Setup

The simulation setup is divided into component properties, threat properties and simulation properties. For the component properties the following applies:

TABLE II. COMPONENT PROPERTIES

Parameter	Value [minutes]
Mean impact delay	5
Standard deviation of the impact delay	1
Mean restoration time	60
Standard deviation of the restoration time	10

The threat properties are chosen with a probability to propagate of 15%. The 100 repeated simulations with 125-time steps (~2h duration) represent the simulation properties.

The scenario considered in the following, is a malware attack on the OSS executed by an intruder that gained physical access. The latter can be achieved by climbing the platform unauthorized or through employees influenced by social engineering. In the past, one prominent example for Cyber-attacks is the malware attack on Maersk in 2017 [20].

C. Impact Propagation

In the following, the scenario has been simulated within the prior established network. In Fig. 4, the potential propagation of the attack is shown. Component No. 4 marked with a red circle is the attacked node. Components No. 2 and No. 3 are the first potential propagation steps (see orange arrows). The Second potential propagation steps are No. 7, No. 21 and No. 24 (see yellow arrows). The impact continues to propagate to all connected nodes until they are all affected. This impact can be delayed by some minutes based on the impact delay times specified in Table II. During that time, the first impacted nodes already start to recover based on their restoration time.

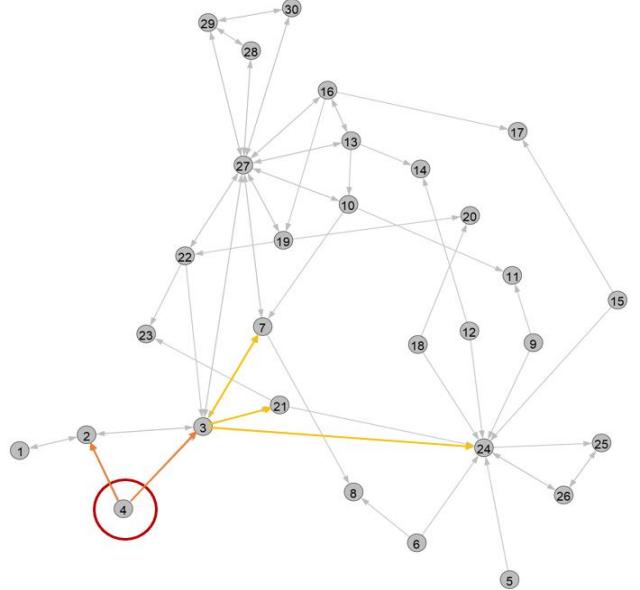


Fig. 4: OWF model with the nodes impacted during the scenario highlighted. First an initial node is attacked (red), the first (orange) and second (yellow) propagation step is shown.

Simulating this impact propagation with the respective impact delays and restoration times repeatedly as a function of times requires the definition of performance measures that can be monitored. Various measures can be defined such as the current performance of the SCADA or navigation light system, the wind farm controller systems with their emergency power control (park shutdown) functionality, the electricity output of the whole OWF or the general connectivity of the nodes in the network. Here, the number of not-impacted nodes normalized with the total number of nodes in the network has been selected as performance measure. This measure might not be the most useful for an OWF operator, nonetheless it represents in an intuitive way how many nodes got impacted and how fast the overall system recovers. The results are represented in resilience curves. For more information on the approach, the impact propagation

technique has been presented for another CI, namely an airport, in [21].

Fig. 5 shows the resilience curve of the above-described scenario. Due to the 100 repeated simulations which are all summarized in one Figure, several slightly deviating curves are presented. The uncertainties arise from the impact delay and the restoration time which are drawn from normal distributions at the beginning of each simulation but also from the probability to propagate given in section IV-B. The malware attack is placed on the node specified in the scenario in time zero. The degradation of the system can be observed from a decreasing number of undisturbed nodes.

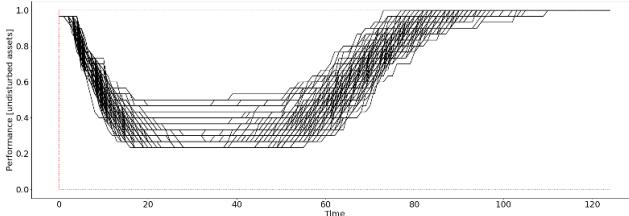


Fig. 5: Resilience curve: Malware attack on the offshore OSS - controller at time zero (red dashed vertical line).

While the system recovers, the number of undisturbed nodes stay relatively constant. From minute 60 to 80 the system returns to its initial functionality and is fully recovered after around 100 minutes. Note, the performance never drops to zero, which depends on the network structure.

Often, one cyber-attack is already enough to damage the system and to interrupt main functionalities. However, also cases of combined attacks exist like a series of cyber-attacks in Vietnam where an airline's website, but also public announcement systems and flight information display systems of several airports were hijacked in 2016 [22]. Inspired by this combined attack, we study in the following a combined attack on the OSS controller and a time-delayed attack on the AIS system. Both attacks are again malware attacks to be able to compare the system behavior to the first scenario presented in Fig. 5.

The results of the combined attack are presented in Fig. 6. In minute 0 the initial attack on the OSS controller takes place and then in minute 60 the second malware attack impacts the AIS. The second attack disturbs the system while still recovering from the first attack. Additionally, the second attack especially leads to an increase in uncertainty which is reflected by the large deviation of resilience curves. The second impact might be smaller but maybe it also leads to severe combined effects and a second drop of performance with the same significance than the first one. This increased uncertainty makes planning and decision making very difficult and thus the definition of mitigation measures to face combined attacks is a big challenge.

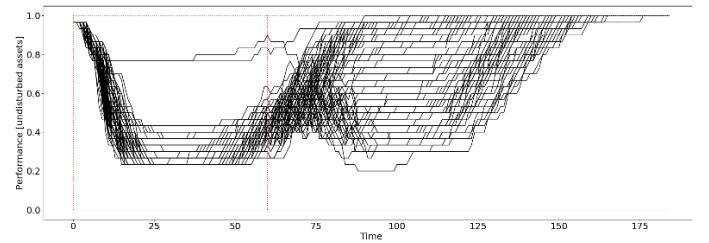


Fig. 6: Resilience curve: Malware attack on (i) the OSS (node 4) in Minute 0 and (ii) the AIS (node 5) in Minute 60.

D. Potential measures

In the simulation, no safety and security measures have been considered. In the following Table III, some potential protection measures from section III-C are discussed and implemented into the different resilience phases where they become effective:

TABLE III. MEASURES IN DIFFERENT RESILIENCE PHASES

Phase	Measure
Prepare	A general and specific cyber-physical security assessment incl. malware analysis followed by a security concept is suggested to be performed with routine review cycles through the OWF development stages.
Prevent	Safeguards e.g., by restricted access by design. Training and awareness of offshore technicians.
Crisis - Malware attack on the OSS: physical access and malware injection	Crisis - Malware attack on the OSS: physical access and malware injection
Protect	Individual network segments should be separated from each other (isolating the attack)
Respond	Troubleshooting by IT system operator / Administration of virtual infrastructure. Determination and Elimination of Malware. Reverse engineering of the malware
Recover	OWF or individual segment back to standard operation mode. Around 80 min with impact delay for single attacks.

In general, this application can be considered as the transition from risk to resilience. Specific protection measures resulting from the risk assessment are connected into the different phases of the resilience process. The link between both processes provides conclusions about the quality of the protection measures and their influence on resilience and the risk impact.

V. CONCLUSION

Offshore Wind is recognized as an expanding industry: With the EEG novella 2021, the expansion target from 20 gigawatts for the year 2030 is set. This decision not only increases the relevance of the offshore wind industry, but also the potential for dangers and their associated risks. In addition, the "Second Ordinance to amend the BSI KRITIS Regulation" recognizes the field of renewable energies as important: With the increasing decentralization and shutdown of large generating units, the systemic relevance of further plants such as OWF assets require stricter cyber and information security measures.

In this context cyber-physical security as a complex system requires ongoing assessments for its effectiveness: Continuous improvement and monitoring of safeguards. Security should always be test benched. Requirements from permits that were up to date e.g., 10 years ago must be adapted and request by the approver of the permit. In addition, network plans need to be updated.

In particular, the development of technology with regards to IT security should be considered. This represents a special challenge because the progress of technology development is difficult to predict.

Nevertheless, systems should be placed and chosen in such a way that improvements can be made. This also applies to the O&M phase. It should be noted here that systems could become more maintenance intensive. For example, hardware may be out of date and replacement parts may no longer be available.

Further development of cyber-physical security standards is necessary not only by the governmental body, but also by the industry itself. This could improve the knowledge transfer between the different industries and the offshore specific application. All of this would also require cyber-physical security response training.

In this paper, a single Cyber-attack on example OWF systems as well as a combined attack scenario have been discussed and simulated with a graph-based approach. It was found that the potential impact of a single attack can be estimated and thus predicted but combined attacks lead to situations with large uncertainties which make a reliable prediction nearly impossible with the suggested methods.

This finding leads to the conclusion that in a world with more and more sophisticated attack scenarios such as hybrid, cyber-physical and combined threats more robust approaches need to be developed and uncertainties need to be quantified through data collection and simulation.

ACKNOWLEDGMENT

The authors like to thank the reviewers of the abstract and conference participants for the appreciated comments that helped to improve the quality of this paper.

REFERENCES

- [1] Gesetzentwurf der Bundesregierung, "Gesetz zur Änderung des Erneuerbare-Energien-Gesetzes und weiterer energierechtlicher Vorschriften.", 01.01.2021.
- [2] Gebauer, M. "Cyber-Abwehrzentrum warnt vor Stromausfall in ganz Europa". Spiegel Netzwerk, 24.08.2018.
- [3] Schönbohm, A. BSI-Magazin, pp. 24-25, January 2018 [Mit SicherheitIndustrial Control Systems in der Industrie 4.0, p. 24, 2018].
- [4] Freudenberg, W. K. "Why windfarms need to step up cyber security". Offshore Industry (2018) Issue 5: 69-71.
- [5] Referentenentwurf, Zweite Verordnung zur Änderung der BSI-Kritisverordnung, Federal Ministry of Interior, Building and Community, 22.04.2021.
- [6] Kurzstellungnahme zur Änderung der zweiten Verordnung der BSI-Kritisverordnung, Bundesverband der Windparkbetreiber Offshore e. V. (BWO).
- [7] <https://www.bdew.de/energie/zweite-aenderungsverordnung-der-bsi-kritisverordnung-verabschiedet/> 19.08.2021.
- [8] Vinnem, J.-E., "Offshore Risk Assessment vol 1", Third Edition, Springer-Verlag, p.79, London 2014.
- [9] Risk management – guidelines. Standard, International Organization for Standardization, Geneva, CH (2018)
- [10] Information technology- Security techniques – Information security risk management. Standard, International Organization for Standardization, Geneva, CH (2018)
- [11] Federal Office for Information Security (BSI), "BSI-Standard 200-3: Risk Analysis based on IT Grundschutz" Version 1.0, pp. 5-6, 2017.
- [12] Vinnem, J.-E., "Offshore Risk Assessment vol 2", Third Edition, Springer-Verlag, p.642, London 2014.
- [13] Federal Office for Information Security (BSI), "BSI-Standard 200-3: Risk Analysis based on IT Grundschutz" Version 1.0, pp. 11-12, 2017.
- [14] U.S. Department of Energy, "Roadmap for Wind Cybersecurity", Office of energy efficient & renewable energy, p. 15, 2020.
- [15] Häring, I., Sansavini, G., Bellini, E., Martyn, N., Kovalenko, T., Kitsak, M., Vogelbacher, G., Ross, K., Bergerhausen, U., Barker, K., Linkov, I.: Towards a generic resilience management, quantification and development process: General definitions, requirements, methods, techniques and measures, and case studies. Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht pp. 21-80 (2017)
- [16] Edwards, C.: Resilient Nation, London: Demos 2009.
- [17] Thoma, K., ed. Resilien-Tech:» Resilience by Design «: a strategy for the technology issues of the future. Herbert Utz Verlag, 2014.
- [18] Hiermaier, S., Hasenstein, S., Faist, K.: Resilience Engineering-how to handle the unexpected. In: 7th REA Symposium. p. 92 (2017)
- [19] Queiroz, C., A. Mahmood, and Z. Tari. "SCADASim—A framework for building SCADA simulations." IEEE Transactions on Smart Grid 2.4 (2011): 589-597.
- [20] Gronholt-Pedersen, J., "Maersk says global IT breakdown caused by cyber attack", <https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19IINO>, 2017, accessed on 2021-07-15.
- [21] Köpke, C., K. Srivastava, L. König, N. Miller, M. Fehling-Kaschek, K. Burke, M. Mangini, I. Praca, A. Canito, O. Carvalho, F. Apolinario, N. Escravana, N. Carstengerdes, T. Stelkens-Kobsch 2021 Impact Propagation in Airport Systems, CPS4CIP 2020, LNCS 12618, 1-16, doi : https://doi.org/10.1007/978-3-030-69781-5_13.
- [22] Viet Nam News, "Chinese hackers attack VN's airports and Vietnam Airlines' website", <https://vietnamnews.vn/society/300416/chinese-hackers-attack-vns-airports-and-vietnam-airlines-website.html>, 2016, accessed on 2021-07-15.