8TH REA SYMPOSIUM EMBRACING RESILIENCE: SCALING UP AND SPEEDING UP
KALMAR, SWEDEN, JUNE 24-27, 2019

# NON-RESILIENT BEHAVIOR OF OFFSHORE WIND FARMS DUE TO CYBER-PHYSICAL ATTACKS

*Nikolai Kulev[1], Albrecht Reuter[2], Oliver Eichhorn[2], Evelin Engler[3], Carl Wrede[1]*

*[1)] German Aerospace Centre, Institute for the Protection of Maritime Infrastructures, Germany; [2)] FICHTNER GmbH & Co. KG, Germany; [3)] German Aerospace Centre, Institute for Communications and Navigation, Germany*

## 1. Introduction

The share of wind power generation is steadily increasing and it reached 20.4% of Germany's power supply in 2018. Thus, wind power is becoming a critical infrastructure with major contributions to power supply and power system grid stability [1]. Consequently, a resilient operation of offshore wind farms (OWFs) is required under normal and disturbed conditions. Resilience stands for the ability of a complex system to proactively and reactively maintain its functionality and performance despite failures or manipulations [2].

Scope of this paper is the investigation of disturbances due to possible cyber-physical attacks on an OWF and the resulting response to them in relation to OWF resilience.

## 2. Functional system model and resilience degrees of a generic OWF

A functional model describes the technical behavior of engineered, cyber-physical systems in relation to the intended task or results of the system. It is a representation of the operation, functionality and performance of the system, e.g. in the form of a block diagram, Fig. 1. The block diagram consists of components performing, according to their technical characteristics, and specified functions on the inputs. Applied to the OWF the components can be grouped into interconnected layers representing the main functional processes: energy conversion (1), data acquisition - control (2)/protection(3), control (4) and protection/maintenance (5).

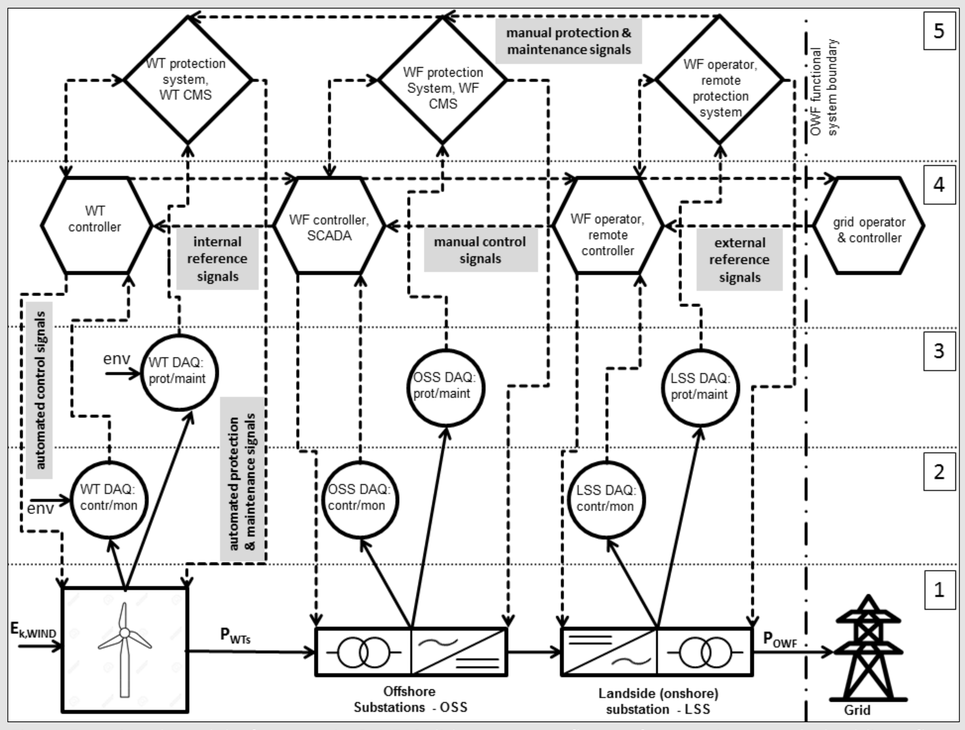


*Fig. 1 Functional model of a generic OWF. Solid arrows are flows of energy/matter, dashed lines flows of signals/data.* DAQ: *data acquisition;* contr/mon*: control and monitoring;* prot/maint*: protection and maintenance;* **$E_{k,WIND}$**: *kinetic energy of the wind;* **$P_{WTs}$**: *electrical energy from the wind turbines;* **$P_{OWF}$**: *electrical energy from the wind farm;* **env**: *influence of the environmental conditions;* WT: *wind turbine;* SCADA: *supervisory control and data acquisition system*; CMS: *condition monitoring system*; CC: *control center*

The degree of resilience of a power generating system can be related to its system states and the implemented resilience-enhancing measures for prevention, emergency and restoration, Fig. 2 [3, 4]. Proactive measures are intended to avoid disruptive events, to reduce their frequency, or to limit demolitions, whereas the measures for damage containment, recovery and restoration are reactive by nature.

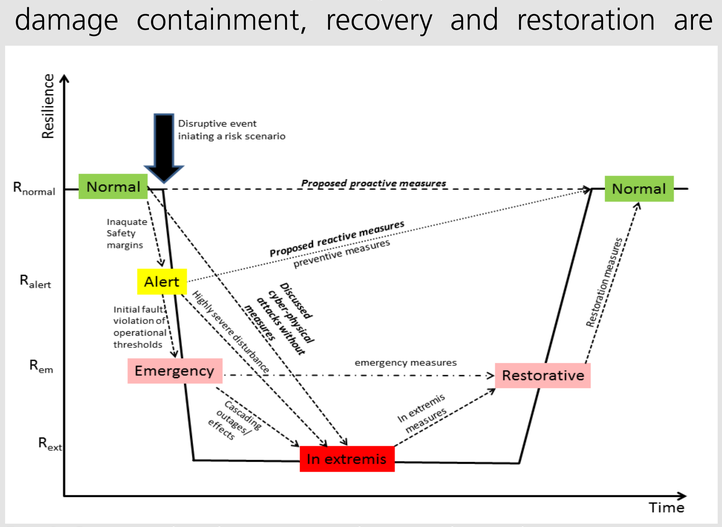


Fig. 2 Conceptual resilience curve relating resilience degree, system states and resilience-enhancing measures of a generic OWF.

## 3. Vulnerability to cyber-physical attacks

By the cyber-physical attack a malicious software is infiltrated within the communication systems of the infrastructure through a physical security weakness. Most of the main functional processes shown in Fig. 1 can be manipulated in this way maliciously [5]. So this vulnerability results also from the IT infrastructure, design of (i) the control system networks and (ii) the controllers within the OWF system.

## 4. Impacts of cyber-physical attacks on the OWF

For our investigation we have developed a full functional model of the WT and the corresponding structures consisting of the relevant cyber-physical systems (Fig. 3 and Fig. 4), a detailed model of the WT part in Fig. 1. Parameters, control and protection signals in the WT control system can be manipulated maliciously so that limit thresholds can be exceeded by far even under normal environmental and power grid conditions. Corresponding chains of effect (propagation of the disturbance initiated by the manipulation) can arise affecting the mechanical (scenario 1 in Fig. 3) or the electrical (scenario 2 in Fig. 4) WT system. Excessive mechanical stresses, electrical and thermal loads can be realized, leading to extreme damage or even destruction of components/subsystems without the possibility of reactive intervention or timely recovery, corresponding to the *In extremis* state in Fig. 2.

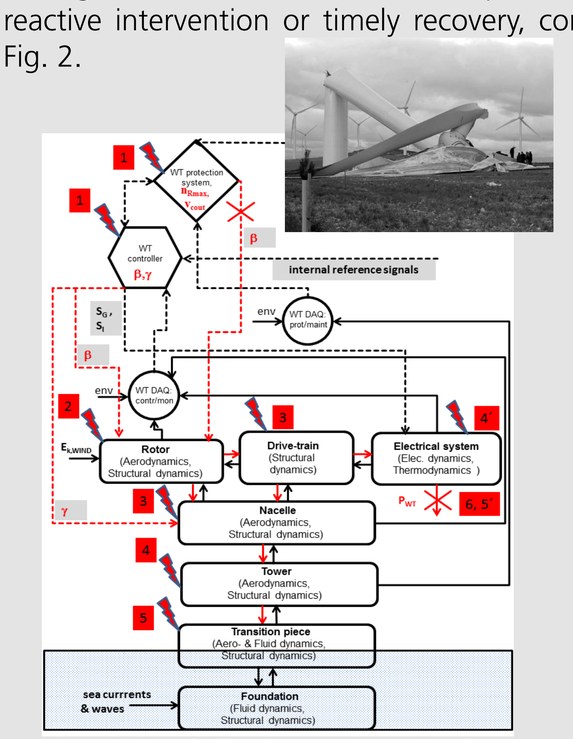


*Fig. 3 Chains of effect by scenario 1. Inlay photo: Comparable natural accident of structural failure and tower collapse of a large onshore WT due the same cause of rotor over-speed [6].*

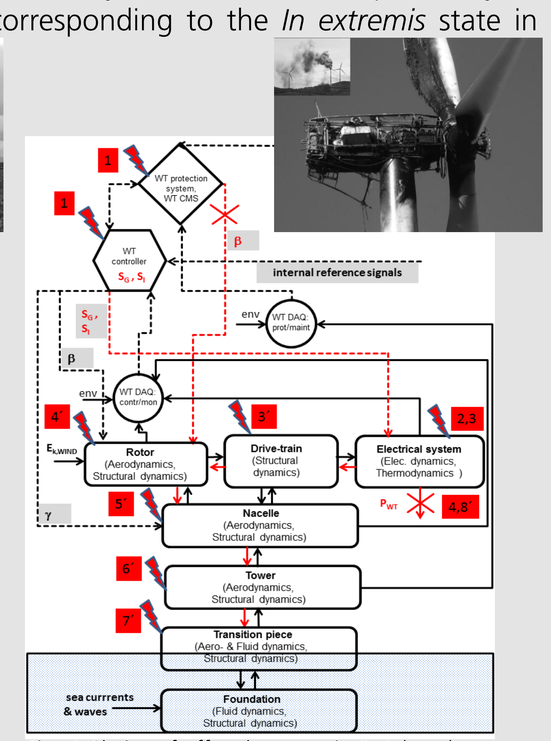


*Fig. 4 Chains of effect by scenario 2. Inlay photo: Comparable natural accident of a burning onshore WT due to the same cause of overheat and fire [6].*

## 5. Measures against cyber-physical attacks

Measures to prevent the cyber-physical attacks described in the previous chapter must take all aspects of the development and impact of the attacks into account. Therefore, both proactive and reactive measures as in Fig. 2 have to be considered, on component level as well as on functional level. Proactive measures include software changes in the layout of the controller Object Dictionaries and in the OPC protocols (must be read-only) regarding the control/protection signals. The physical and the cyber security within the OWF must be generally increased proactively, too, e.g. through motion sensors/CCTV and through authentication/encryption of the OPC protocols. Reactive measures would be the real-time monitoring and analysis of the network traffic between and within the layers of the functional models in Fig. 1 and Fig. 3-4. Apart from this monitoring of the deviations between the real OWF behavior and the simulated model in Fig.1 would indicate abnormal activities.

## 6. Conclusions

We have developed a functional system model of the OWF/WT. Through the model we have investigated the impacts of specific cyber-physical attacks on the OWF. The impacts can affect the OWF/WT functionality and performance extremely and its behavior is clearly non-resilient thereby. The power grid can be severely affected, too. So major security gaps definitely exist concerning the OWF vulnerability to cyber-physical attacks. We have proposed therefore proactive and reactive measures for closing the above gaps which we can evaluate as plausible in qualitative terms based on the proposed functional model.

## References

[1] Thomas Ackermann, ed., *Wind power in power systems*, 2012, John Wiley & Sons Ltd, ISBN 978-0-470-97416-2

[2] International Maritime Organization (IMO): GUIDELINES FOR SHIPBORNE POSITION, NAVIGATION AND TIMING (PNT) DATA PROCESSING, MSC.1/Circ.1575, 16 June 2017

[3] Erik Hollnagel, David D. Woods and Nancy Leveson, *Resilience engineering: concepts and precepts*, Ashgate, ISBN 0-7546-4641-6

[4] Mathaios Panteli and Pierluigi Mancarella, *Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events*, IEEE SYSTEMS JOURNAL, VOL. 11, NO. 3, SEPTEMBER 2017

[5] J. Staggs, D. Ferlemann, S. Shenoi, *Wind farm security: attack surface, targets, scenarios and mitigation*, International Journal of Critical Infrastructure Protection, 17, 2017, 3-14, ISSN 1874-5482

[6] Mario Garcia-Sanz, Constantine H. Houpis, *Wind Energy systems*, 2012, Taylor & Francis Group

Deutsches Zentrum für Luft- und Raumfahrt