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*

Abstract
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. 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.
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. The block diagram consists of components performing, according to their technical characteristics, specified functions on the inputs. Applied to the OWF the components can be grouped into several layers representing the main functional processes.
Within this paper we consider the threat of system failures triggered through cyber-physical attacks, based on the vulnerability of the OWFs to such attacks as documented in the literature. Most of the main functional processes can be manipulated maliciously.
The functional model is used to discuss the impacts of different scenarios of cyber-physical attacks and their resulting cascade effects, which may cause a non-resilient behavior of the OFW. Crucial parameters and signals can be manipulated maliciously. Limit thresholds can be exceeded by far even under normal environmental and power grid conditions. 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.
We propose measures on component and functional level for closing the mentioned security gaps to ensure the resilience of the OWF.

Keywords: Offshore Windfarm, Resilience, Safety and Security, Cyber-physical Attacks

ISBN: 978-91-88898-41-8