Quantitative all-hazard risk assessment of power transmission systems using contingency-constrained optimization

Daniel Jung[1], Ricardo Fernández-Blanco[2], Hugo Calisto[3], Karsten von Maydell[1], Ricardo Bolado Lavín[2]

[1] *German Aerospace Center, Institute of Networked Energy Systems, Oldenburg, Germany*

[2] *European Commission, Joint Research Centre, Petten, Netherlands*

[3] *TEMA – Centre for Mechanical Technology and Automation, University of Aveiro, Campus Universitário de Santiago*

daniel.jung@dlr.de

Abstract

Today's society increasingly depends on a reliable supply of electric energy, leading to the designation of major power transmission systems as "critical infrastructure". These systems are vulnerable to various hazards and threats that can result in the failure of one or multiple components, endangering the stable operation of the system. Due to their inherent complexity, quantitative modeling-based risk assessment is necessary to identify the most critical assets in power transmission systems. Taking into account the time scale on which relevant large-scale crises and their associated restoration processes are taking place, a contingency-constrained direct current optimal power flow approach is proposed, combined with a load shedding procedure to handle cases in which the full demand cannot be served without violating security limits of the system. We compare the contingency-constrained optimization to a standard optimal power flow approach. A step-wise system restoration process is considered, estimating the total energy not served over the whole restoration period. To illustrate the methodology, it is applied to an extension of the IEEE 3-area reliability test system (RTS-GMLC), implemented in DigSILENT PowerFactory. The considered probabilistic scenarios cover two natural hazards and two types of targeted attacks. The results allow for ranking risk events, scenarios, and single assets with respect to their contribution to the global risk.

Topic: Elements of a resilience strategy for energy systems; Energy security issues: system adequacy, cyber-attacks/sabotage, extreme weather events