Integrated Generator-Rectifier Co-Design for Offshore Wind Turbines

Phuc Huynh
Department of Electrical and Computer Engineering

Abstract
The conventional harvesting of offshore wind energy relies on multi-megawatt direct-drive permanent-magnet synchronous generators equipped with full-power-rated active rectifiers. Functional integration of the generator and rectifier has led to the creation of an integrated generator-rectifier system with higher efficiency, reliability and power density. In this architecture, size of the power converter depends on the generator per-unit reactance. In addition, the generator design must be optimized for weight and efficiency to obtain the potential system-level benefits. This work proposes a framework using the generator per-unit reactance as a handshake variable to co-design the generator and power electronics. The design approach enables the reduction of the system weight and conversion losses by 25 % and 61 %, respectively, for a 10-MW system.

Risk Evaluation of Ransomware in Energy Systems

Megan Culler
Department of Electrical and Computer Engineering

Abstract
Ransomware can be a devastating cyberattack with lasting impacts in the form of forensics, lost work time, and reputation damage. The loss of access to critical files or functionality can pose an even bigger threat to energy systems. The last three years have seen a rise in cyberattacks against Industrial Control Systems (ICS), a trend which is expected to continue. While the technical literature has, typically, grouped all ICS ransomware together, the various industries in which ICS are deployed have very different networks, operations and configurations which are quite distinct. In particular, the energy sector often claims that their systems are complex and isolated, making it hard for a ransomware attack to cause actual operational impacts on process control. Nevertheless, the energy sector is often cited as one, in which a successful ICS cyberattack may result in severe impacts. In this presentation, we examine the trends in ICS ransomware attacks over the past four years, categorize the conditions under which ransomware can result in marked operational impacts on energy systems and quantify the ransomware impacts on the energy sector compared to ICS overall. We also explore the potential impacts of ransomware on power systems when different ICS components are attacked. We find that ransomware attacks have risen in proportion with overall ICS cyberattacks. So far, the energy sector has experienced few incidents of ransomware. Among all ICS attacks, 28.2 % of the attacks have had an operational impact on process control. Simulation shows that power grids can continue to operate with the loss of various computing resources over the short term.