CIP for Grids with Interconnected DER Systems: Executive Summary

Frances Cleveland, Xanthus Consulting International

Critical Infrastructure Protection (CIP): Resilience and Cyber Security Recommendations for Power System Grids with Distributed Energy Resources (DER) Cyber-Physical Systems. In the energy sector, two key phrases are becoming the focus of international and national policies: "grid resilience" and "cyber security of the cyber-physical grid". Grid resilience responds to the overarching concern: *"The critical infrastructure, the Smart Electric Grid, must be resilient – to be protected against both physical and cyber problems when possible, but also to cope with and recover from the inevitable disruptive event, no matter what the cause of that problem is – cyber, physical, malicious, or inadvertent."*

Resilience of the grid is often associated with making the grid able to withstand and recover from severe weather and other physical events, but resilience should also include the ability of the cyber-physical grid to withstand and recover from malicious and inadvertent cyber events. The "cyber-physical grid" implies that the power system consists of both cyber and physical assets that are tightly intertwined. Both the cyber assets and the physical assets must be protected in order for the grid to be resilient. But protection of these assets is not enough: these cyber and physical assets must also be used in combination to cope with and recover from both cyber and physical attacks into order to truly improve the resilience of the power system infrastructure.

Challenges to Resilience and Cyber Security for Power System Grids with DER. All too often, cyber security experts concentrate only on traditional "IT cyber security" for protecting the cyber assets, without focusing on the overall resilience of the physical systems. At the same time, power system experts concentrate only on traditional "power system security" based on the engineering design and operational strategies that keep the physical and electrical assets safe and functioning correctly, without focusing on the security of the cyber assets. However, the two must be combined: resilience of the overall cyber-physical system must include tightly entwined cyber security technologies and physical asset engineering and operations, combined with risk management to ensure appropriate levels of mitigation strategies.

In particular, distributed energy resources (DER) systems are cyber-physical systems that are increasingly being interconnected to the distribution power system to provide energy and ancillary services. However, distribution power systems were not originally designed to handle these dispersed sources of generation, while DER systems are generally not under direct utility management or under the security policies and procedures of the utilities. Many DER systems provide energy from renewable sources, which are not reliably available at all times. Therefore, the resilience of power systems to even typical disruptions is increasingly at risk as more of these DER systems are interconnected.

Recommendations on Improving Resiliency of Power System Grids with DER. On the other hand, the sophisticated cyber-physical capabilities of smart DER systems could actually improve power system resilience if these smart DER capabilities were properly secure and coordinated with power system management through communications. DER systems can actually compensate for some of the problems they cause, such as riding through temporary spikes and dips in voltage or frequency that could be caused by their fluctuating behavior. Microgrids and the bulk power system can serve as mutual backups during excessive peak loads or during disaster conditions. If both the cyber and the physical components of these DER systems were well designed and implemented with embedded cyber security, and were interconnected and operated using good engineering strategies, they would significantly improve the resilience of the power system.

It is not just the utilities who must take responsibility for achieving this resilience goal. Many stakeholders are involved in the design, implementation, and operation of DER systems, including manufacturers, integrator/installers, users, information and communication technology (ICT) providers, security managers, testing and maintenance personnel, and ultimately utility regulators. However, given this new cyber-physical environment, often these stakeholders do not fully understand or appreciate the types of cyber security and engineering strategies that could or should be used.

***Recommendation*: IEC/TR 62351-12:2016, Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems** *(see https://webstore.iec.ch/publication/24474),* provides detailed discussions and recommended actions. This IEC Technical Report should be recommended by NIST for all stakeholders involved in designing, implementing, and operating DER systems on the grid. Suggestions for improvements of this Technical Report are welcome.