Cybersecurity Assessment for a Behind-the-Meter Solar PV System: A Use Case for the DER-CF

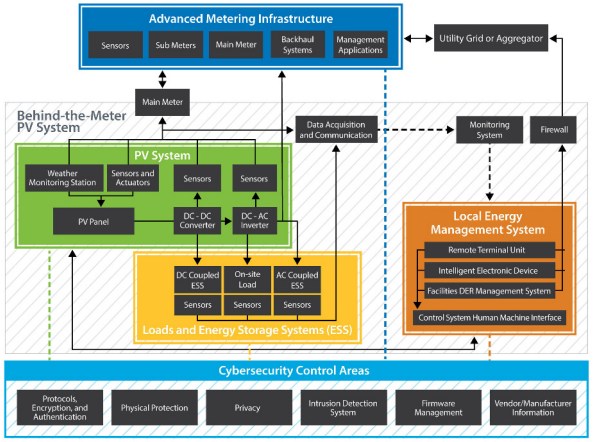
Shuva Paul, Anuj Sanghvi, and Tami Reynolds of the National Renewable Energy Laboratory

The Distributed Energy Resource Cybersecurity Framework

The global energy landscape is shifting toward more cost-effective, cleaner, and sustainable sources. This transition is driven by the increasing adoption of distributed energy resources (DERs), which are rapidly transforming electric grids to achieve energy decarbonization. Solar photovoltaic (PV) systems are integral to this transformation. With more than 90 GW of DERs installed in the United States, including approximately 3 million solar installations, the threat of cyberattacks on this energy infrastructure is important to consider. Cyberattacks on DERs can disrupt energy production and compromise system integrity.

We conducted a cybersecurity risk assessment for behind-the-meter DERs using a solar PV system as a use case of the Distributed Energy Resource Cybersecurity Framework (DER-CF).

DER-CF, developed by the National Renewable Energy Laboratory and funded by the U.S. Department of Energy Federal Energy Management Program, is a free, interactive web tool designed to offer federal facilities an accessible platform for performing self-assessments on both new and existing DER systems. The DER-CF provides system-specific cybersecurity controls to enhance an organization's governance, technical management, and physical security. It generates a prioritized list of action items and offers an interactive dashboard to track progress and highlight areas for improvement.



Architectural Elements

Solar PV systems come in different architectures, including utility-scale and behind-the-meter systems. Common architectural elements include:

- **Inverters and integrated controls:** Convert solar DC power into grid-synchronized AC power, which is critical for system reliability.
- **Data acquisition and control systems:** Employ sensors for comprehensive energy data collection. Security measures, including intrusion detection, are vital.
- **Energy management systems:** Enhance control and economic value by monitoring energy consumption and metering. Cybersecurity is essential to prevent manipulation.
- **Weather monitoring systems:** Vital for optimizing efficiency, weather systems use sensors to gather environmental data. Cybersecurity is necessary to prevent performance impact.
- **Field sensors and actuators:** Monitor data and enhance system efficiency. Unauthorized manipulation affects performance and efficiency.
- **Electronic security perimeter:** Protects infrastructure with electronic borders. Proper configuration is crucial to prevent malware and unauthorized access.

Foundational Controls

The DER-CF includes foundational cybersecurity controls to safeguard DERs against a wide range of cyber threats.

- **Intrusion detection systems:** Vital for detecting unauthorized intrusions and guarding DER systems; proper configuration is key against cyberattacks.
- **Firmware Management:** Critical for security assessments; involves overseeing firmware upgrades, authorizations, and version tracking.
- **Vendor/Manufacturer Information:** Imperative to rely on comprehensive vendor security documentation to minimize external risks and dependencies.
- **Protocols, Encryption, and Authentication:** Crucial for secure equipment communication; emphasizes multi-factor authentication, encryption, and robust logging.
- **Physical Protection:** Boosts equipment security with access control, tamper detection, and contingency planning for physical security incidents.

DER-CF

Conclusion and Future Work

The DER-CF tool is essential for assessing and improving the cybersecurity posture of DER systems. Future work includes developing dynamic assessments, comparative analysis, and integration with zero-trust architectures to ensure a secure and resilient energy infrastructure for the future.

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Federal Energy Management Program. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

Innovative Smart Grid Technologies Latin America 2023
San Juan, Puerto Rico
November 6, 2023
NREL/PO-5R00-87808