Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

NREL
Transforming ENERGY

Cybersecurity Guidance for Distributed Energy Resource Management Systems (DERMS)

Securing Solar for the Grid Workshop

September 14, 2023

Principal Investigator: Danish Saleem
Presenter: Jennifer Guerra
Other Contributors: Chelsea Quilling, Ryan Cryar

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Purpose and Audience

- Purpose:
  - Provide cybersecurity guidance and best practices for distributed energy resource management systems (DERMS).
  - Prioritize guidance that is testable and could be adapted for a future standard.
- Audience:
  - Standards organizations
  - DERMS vendors, owners, and operators.

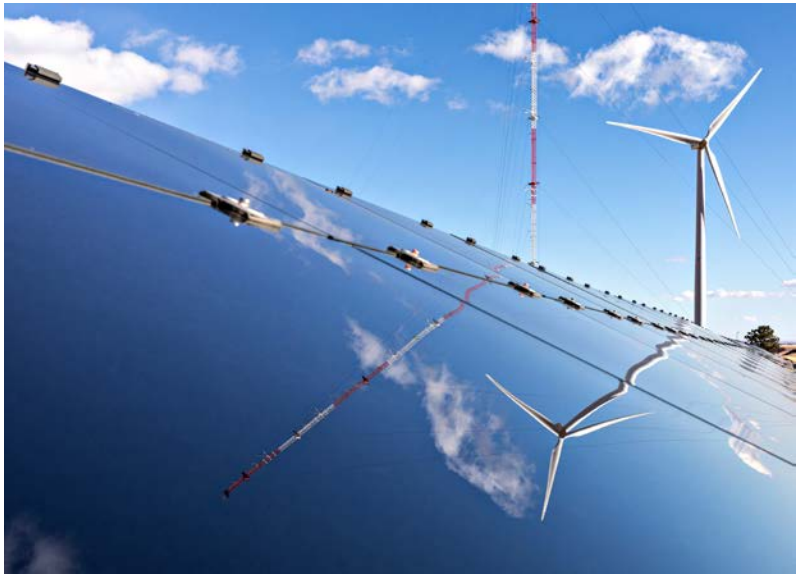

Photo by Werner Slocum, NREL 66364

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Report Outline

- Draft version 2 is in process.
- The aim is to advance cybersecurity best practices for DERMS solutions covering a variety of deployments.
- The focus is on guidance that can be testable as future requirements/standards.
- Applicable standards are outlined.

Table of Contents

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Example Threat Scenarios

Attack Category	Vulnerability	Attack Vector	Impact	Security Violation
Financial Loss	Misconfigured firewall	Compromised communications result in incorrect distributed energy resource (DER) time and forecast data sent to DERMS.	Loss of DERMS real-time load and capacity information; loss of visibility/communications	Integrity Availability
Customer Data Loss	Vulnerabilities in customer wireless network	Intercepted network traffic results in stealth of sensitive customer data, including personally identifiable information and financial information.	Data breach affecting customer data privacy and confidentiality, with potential sale of sensitive data to other malicious actors	Confidentiality Integrity Non-repudiation
Load Shedding/ Outage	Lack of software update testing	Malicious software update includes malware that sends shut-off commands to inverters.	Loss of generation to large numbers of DERs, resulting in the loss of power quality and possibly rolling or cascading blackouts	Integrity Availability
Equipment/ Personnel Safety	Poor user access control/password management	Hijacked remote access issues false command to reconnect equipment to the grid during maintenance/repair.	Damage/injury to equipment and personnel when deactivated DERs unexpectedly start up during maintenance/repair	Integrity Availability Non-repudiation

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Industry/LCC/SETO Involvement

- Completed independent industry peer review process:
  - Reviewed by Eaton and Dominion Energy.
- Reviewed by SNL, INL, PNNL, and SETO
- Organized and rescoped draft to include:
  - Applicability of existing standards to DERMS
  - Specific threat scenarios
  - Cybersecurity roles and responsibilities
  - Categorization of guidance by cybersecurity function, not DERMS function.
- Removed system-level considerations and saved them for future work
- Will continue soliciting industry feedback to improve cybersecurity guidance based on state-of-the-art security practices in today's market.

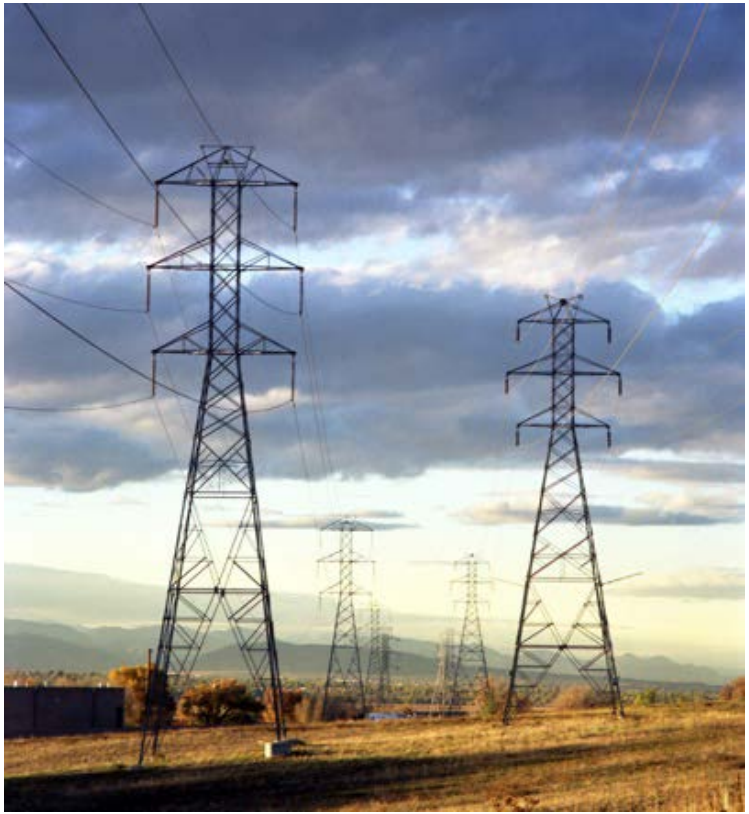

Photo by Werner Slocum, NREL 00001

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Potential Future Work

- Develop system-level cybersecurity guidance for DERMS integration.
- Develop procedures for testing DERMS solutions.
- Coordinate with industry to scope testing for DERMS state-of-the-art capability.
- Develop a report on DERMS cybersecurity testing.

July 11, 2018 – Tami Reynolds, project manager, Cyber-Physical Security Group, and colleague Anuj Sanghvi review the security site assessments that Reynolds has been leading for utility partners. *Photo by Dennis Schroeder, NREL 51929*

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Thank You!

Let’s work together!

Danish.Saleem@nrel.gov
Chelsea.Quilling@nrel.gov
Jennifer.Guerra@nrel.gov
Ryan.Cryar@nrel.gov

NREL/PR-5R00-87289

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 U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office. 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.

NREL
Transforming ENERGY