INL/CON-24-77172-Revision-0

Securing Solar for the Grid (S2G): SETO Peer Review

March 2024

Megan Jordan Culler, Jake P Gentle, Daniel Alan Ricci

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-24-77172-Revision-0

Securing Solar for the Grid (S2G): SETO Peer Review

Megan Jordan Culler, Jake P Gentle, Daniel Alan Ricci

March 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Securing Solar for the Grid (S2G)

SETO Peer Review

March 26, 2024

Megan Culler
Idaho National Laboratory

INL/CON-24-77172

Securing Solar for the Grid

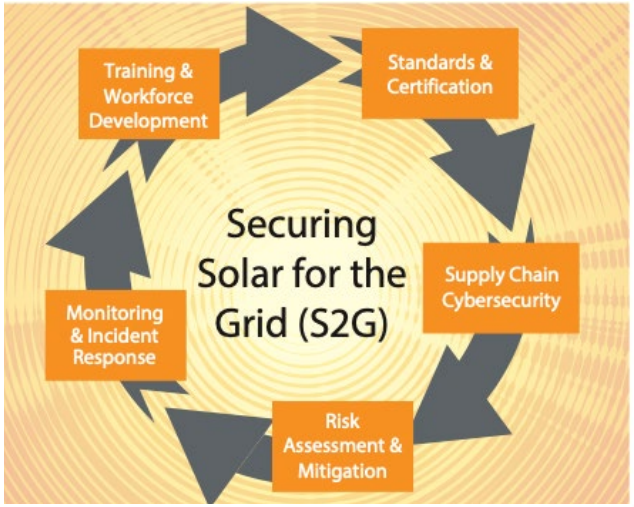
Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Growth of solar penetration along with historical lack of cybersecurity standards and industry awareness drives need for research and deployment-ready solutions

Objectives

- Work with industry to address gaps in solar cybersecurity standards
- Develop tools and resources for cyber risk assessment
- Assess supply chain impacts and mitigations
- Promote training and education for solar stakeholders
- Advance monitoring & incident response capabilities

64 individuals representing 30+ organizations!



Industry Advisory Board Members:

- Trade associations (3)
- Utilities (4)
- Developers (2)
- Manufacturers (3)
- Consultants (5)
- Security Solutions (7)
- Standards Development Organizations (4)
- Regulators (3)
- Other (3)

Lab Coordinating Committee

NREL Transforming ENERGY
Pacific Northwest NATIONAL LABORATORY
Sandia National Laboratories
INL Idaho National Laboratory

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

Research Areas

STANDARDS DEVELOPMENT & BEST PRACTICES

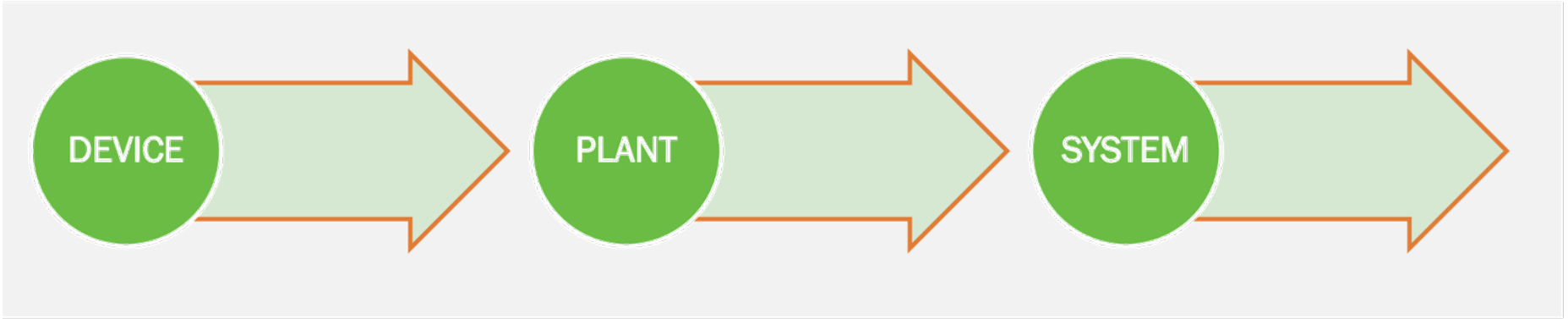
Stakeholder engagement to investigate gaps and develop best practices that can become standards to enable the secure integration of inverter-based resources and DERs.

EDUCATION & WORKFORCE DEVELOPMENT

Development of educational modules and training to increase cybersecurity awareness and knowledge within solar stakeholders.

CYBERSECURITY TOOL KIT & SUPPLY CHAIN

R&D of tools to understand cybersecurity posture, risk assessment to inform investments, and device design security & maturity model for cyber supply chain.



INCREASING CYBERSECURITY LEVELS OF SOLAR TECHNOLOGIES

Source: DOE EERE

Accomplishments

Standards Development and Best Practices
Education and Workforce Training
Cybersecurity Tool Kit and Supply Chain

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

INL

CyberSHIELD
- Tuned solar cybersecurity assessment module in CSET
- Malcolm used for asset identification and solar protocol analysis
- Developed materials, websites, and demonstrations to support program and education of CyberSHIELD program for industry

CyberStrike STORMCLOUD
- 6 hardware boxes built
- Over 75 students taken at least some part of the training
- All 8 lab exercises tested in the classroom
- Very positive feedback: 100% would recommend to a colleague
- Promotional video released

Hardware Bill of Materials (HBOMs)
- Developed HBOMs for three different solar inverters
- Each integrated circuit board was broken down into individual components
- Identifiers pulled from components directly or through online research

Codified Attack Surface (CAS)
- Created Structured Threat Intelligence Expression (STIX) bundle for 16 solar inverters and identified vulnerabilities for six of them.
- Scoring for inverters involved vulnerabilities, evidence of flaw remediation, days to update, and market share
- ML scraping in progress to automate analysis

NREL

UL 2941 Cybersecurity Certification
- Co-led the development and publication of UL 2941
- Supported the development of technical committee for UL 2941.
- Leading development of test procedures

IEEE 1547 standard and IEEE 1547.3 cybersecurity guide
- Co-led the development of IEEE 1547.3 as vice chair, now published
- Supporting IEEE 1547 revision as subgroup lead for including cybersecurity in the standard

DER cybersecurity requirements
- Performed correlation of DER cybersecurity requirements from three different sources for CPUC
- Engaging with NERC's SITES and SPIDER working groups

DER Supply chain Cybersecurity
- Performed gap analysis of supply chain cybersecurity for DERs
- Developed supply chain cybersecurity recommendations for Solar

Distributed Energy Resources Management System (DERMS)
- Developed DERMS cybersecurity recommendations for Solar

Collaboration with Standard Development Organizations
- Collaborated with NERC, IEEE, UL, CPUC, NARUC, NASEO, and others to harmonize standard development efforts.
- Hosted FY22 workshop at NREL and supported the planning & coordination of FY23 IAB meetings and workshop.

Accomplishments

Standards Development and Best Practices
Education and Workforce Training
Cybersecurity Tool Kit and Supply Chain

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

PNNL

- **Universal Utility Data Exchange (UUDEX):**
  - Developed information exchange models for Solar DER report
  - Made it available to the UUDEX standardization efforts in IEEE (P2040.103)
- **Secure Design & Development Cybersecurity Capability Maturity Model (SD2-C2M2)**
  - Guided self-assessment of internal processes
  - Design, Build, Test, Integrate, Deploy, Lifecycle domains
- **Cybersecurity Assessments**
  - Completed the Cybersecurity Assessment in DER-rich Distribution Operations
  - Completed one SD2-C2M2 assessment with Operant Networks
  - Scheduled additional assessment for the clean energy industry stakeholders
- **Standard cyber-physical test systems for solar PV/DER**
  - Translate publicly available distribution system models to enable benchmarking of cybersecurity test procedures
  - Completed conversion of three distribution models and validated them in OPAL-RT using ePHASORsim
  - Criticality Levels and Impact Analysis submitted to ISGT 2024
- **Supported Supply chain efforts for Solar product evaluations**

SNL

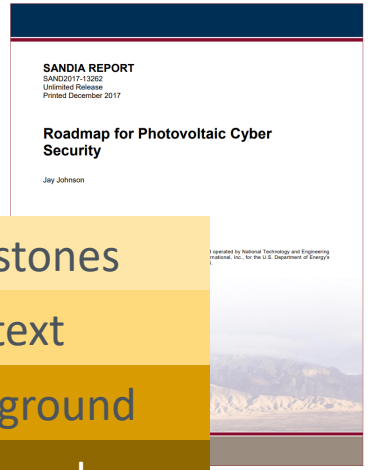
- **Security orchestration, automation, and response for DER**
  - Developed a DER cybersecurity testbed for developing and evaluating a SOAR playbook for DER. Available on git repository.
  - Published chapter in 'Power Systems Cybersecurity' on SOAR for DERs.
- **Published cybersecurity recommendations flyer in collaboration with NERC & SEIA**
  - 58 recommendations covering supply chain management, incident response, threat & vulnerability management, situational awareness, and more.
- **Partnered with Xcel Energy to develop two scenarios for GridEx VII**
  - Story board: Malicious firmware update on residential and community solar installations disables communications to power plant
  - A cyber-attack that changes the power output from a 100 MW PV site
- **Vulnerability Disclosure Best Practices**
  - Define process for disclosing DER vulnerabilities
  - Publish best practices methodology
  - Coordinate with CISA
- **CyTRICS for "clean energy" devices**
  - Identify specific considerations to do PV inverter assessments
- **CyberStrike STORMCLOUD training**
  - Included a virtualized environment and a hardware environment
  - Includes attacks against a single-axis tracker

Roadmap for Solar PV Cybersecurity

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

Contents

- Executive Summary
- National Energy Cybersecurity Efforts
- Solar Energy Technology Landscape
- Solar Cyber Threat Landscape
- Solar Cybersecurity R&D
- Standards Development
- Best Practices
- Stakeholder Roles & Industry Targets



Vision and Milestones

Broader Context

Technology Background

Motivation & Trends

What can labs do?

How to adopt?

How to implement?

Who's responsible?

Recent S2G Events

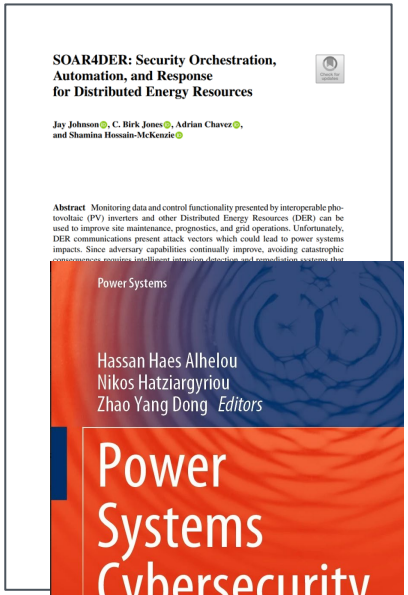
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

- Secure Renewables (June 2023)
- RE+ (Sept. 2023)
  - IAB meeting
  - The State of Cybersecurity for Renewable Energy
  - Creating a 'Cybersecurity Energy Star' for Distributed Generation with Inverter-Based Resources
- IEEE 1547 meeting participation
- Engagement with NERC SITE's and SPIDER working groups
- Energy Transitions Summit (Feb. 2024)
  - CyberStrike STORMCLOUD workshop
  - S2G Panel
  - CyberStrike STORMCLOUD workshop
- 2024 IEEE Innovative Smart Grid Technologies North America (IGST NA) conference (Feb. 2024)
- Spring IAB Meeting (Mar. 2024)

Resources

https://www.energy.gov/eere/solar/securing-solar-grid-s2g

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


SOAR4DER: Security Orchestration, Automation, and Response for Distributed Energy Resources

Jay Johnson, C. Birk Jones, Adrian Chavez, and Shamina Hossain-McKenzie

Abstract Monitoring data and control functionality presented by interoperable photovoltaic (PV) inverters and other Distributed Energy Resources (DER) can be used to improve site maintenance, prognostics, and grid operations. Unfortunately, DER communications present attack vectors which could lead to power systems impacts. Since adversary capabilities continually improve, avoiding catastrophic

Book Chapter


SANDIA REPORT
SAND20XX-XXXX
Printed March 2020
Sandia National Laboratories

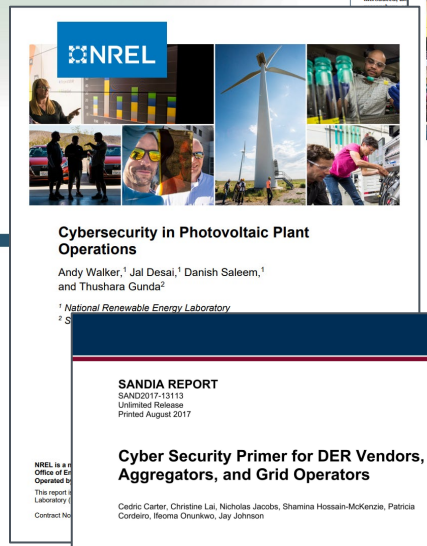
Recommendations for Data-in-Transit Requirements for Securing DER Communications

Ifeoma Onunkwo


Cybersecurity Assessment in DER-rich Distribution Operations: Criticality Levels and Impact Analysis

Manisha Maharjan, Shiva Poudel, Scott R. Mix, and Thomas E. McDermott
Pacific Northwest National Laboratory (PNNL)
Richland, WA, USA
email: manisha.maharjan@pnnl.gov

Abstract—The integration of distributed energy resources (DERs) in distribution networks has become a pivotal strategy for achieving ... optimizing ... erations of ... communication ... cyber threats, ... ensuring secu... challenge. In t... introduced, ... and threats, National Electric Sector Cybersecurity Organization Resource (NESCOR) have presented a threat model

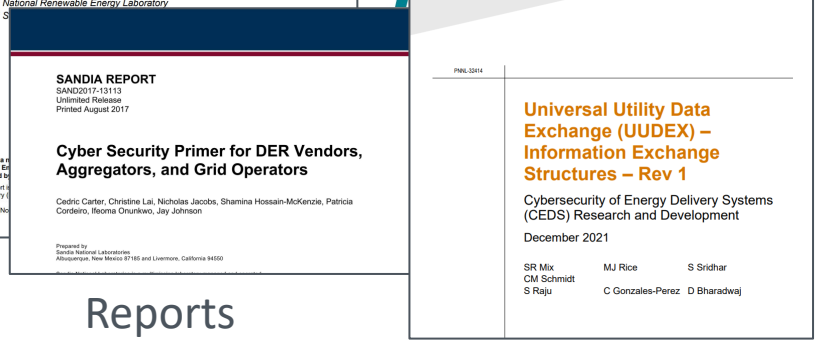


Cybersecurity in Photovoltaic Plant Operations

Andy Walker,[1] Jal Desai,[1] Danish Saleem,[1] and Thushara Gunda[2]

[1] National Renewable Energy Laboratory

Certification Procedures for Data and Communications Security of Distributed Energy Resources


SANDIA REPORT
SAND2017-13113
Unlimited Release
Printed August 2017

Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators

Cedric Carter, Christine Lai, Nicholas Jacobs, Shamina Hossain-McKenzie, Patricia Cordeiro, Ifeoma Onunkwo, Jay Johnson

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

PNNL-32414

Universal Utility Data Exchange (UUDEX) – Information Exchange Structures – Rev 1

Cybersecurity of Energy Delivery Systems (CEDS) Research and Development

December 2021

SR Mix, CM Schmidt, S Raju, MJ Rice, C Gonzales-Perez, S Sridhar, D Bharadwaj

Reports


SECURING SOLAR FOR THE GRID (S2G)

Advancing Cybersecurity for the Solar Era Quarterly Newsletter

Securing Solar for the Grid (S2G) | Department of Energy

In today's interconnected world, cybersecurity is paramount to ensuring the safety and reliability of our critical infrastructure, including the electric grid. As solar photovoltaic (PV) systems and other distributed energy resources (DERs) proliferate, their integration into the grid presents unique cybersecurity challenges. To address these concerns, the U.S. Department of Energy's Solar Energy Technologies Office (SETO) has launched the Securing Solar for the Grid (S2G) project, a collaborative effort to enhance the cybersecurity of solar technologies and the grid as a whole.

The S2G project brings together leading experts from national laboratories, industry and academia to tackle a wide range of cybersecurity issues, including:

- Developing cybersecurity standards and certifications for DERs to ensure they meet minimum safety and security requirements.
- Creating cyber-physical network monitoring tools to detect and respond to cyberattacks in real time.
- Conducting risk assessments and mitigation strategies to identify and address potential vulnerabilities in solar systems and the grid.
- Providing stakeholder training and education to equip industry professionals and policymakers with the knowledge and skills to protect solar systems from cyberthreats.

The S2G project is committed to ensuring that the solar industry can safely and securely integrate with the grid, enabling the United States to harness the full potential of solar energy while maintaining a resilient and secure electricity system.

Tools for Evaluating & Improving Solar Technologies

CAS Methods Modification

Energy unused is useless energy – at least, that's how a logician like Mr. Spock might see it. From an S2G perspective, this translates into ensuring the end users of solar energy are also considered when developing a comprehensive cyberdefense strategy. With Codified Attack Surfaces (CAS) methods as the vehicle, the S2G design aims to create a cyber-analysis capability at the stakeholder scale, providing indicator and mitigation from existing and evolving cyberthreats. This is a INL product.

SolarSHIELD

Cyberdefense needs in the solar industry are as varied and diverse as the populations the industry serves. Location, hardware, software, data acquisition, collecting connective tissue – all these elements, as well as countless other variables, factor into an effective cyberdefense strategy. Utilizing the groundwork laid by the Cyber Security Evaluation Tool (CSET®) and Malcolm, SolarSHIELD aims to facilitate S2G's goal to deliver standardized, repeatable cybersecurity-evaluation methodology tools to the solar industry.

Standards & Workforce Development

Universal Utility Data Exchange (UUDEX) for Solar Security

The Universal Utility Data Exchange (UUDEX) is a new communication approach for exchanging information between utility control centers. The S2G project supported documenting a method to incorporate solar- and DER-related information exchanges for interchange using the Universal Utility Data Exchange (UUDEX) protocol, which is being converted to an IEEE standard as P2030.103. This task documented the process for exchanging Solar DER information in UUDEX by encapsulating an existing IEEE 2030.5 information packet in a UUDEX wrapper. This is a PNNL product.

CyberStrike STORMCLOUD

Solving the cyberdefense puzzle is a little like solving a Rubik's Cube – training and strategy goes a long way.

Partnering with SNL, INL is refining and focusing the CyberStrike STORMCLOUD training program. STORMCLOUD delivers a solar-focused curriculum and hands-on lab program to help expose cyberdefense professionals to solar energy industry challenges.

The training's target audience is made up of vendors, solar utility owner/operators and, cybersecurity professionals in both the information technology (IT) and operational technology (OT) spheres who are interested in broadening their technical and practical expertise. The platform gives students experience defending solar energy systems from cyberattacks. Course

S2G quarterly newsletter