Securing Solar for the Grid (S2G): Cybersecurity for Solar Systems

DOE/EERE/SETO Systems Integration Webinar
Marissa Morales-Rodriguez, PhD
Technology Manager (Contractor)

May/2023
Agenda

• Motivation

• Alignment with DOE Activities

• S2G: Securing Solar for the Grid
  – Research Areas
  – Accomplishments
  – Get Engaged!

• Conclusion/Summary
To manage, optimize, and secure the future grid, new technologies, control techniques, and supporting reliability and security standards will be required.
Recent Reports

IEEE Power & Energy Society
December 2022

TECHNICAL REPORT
PES-TR105

Towards Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector

PREPARED BY THE IEEE/NERC Joint Task Force on Security Integration into BPS Engineering Practices

© IEEE (2022) The Institute of Electrical and Electronics Engineers, Inc.

IEEE Power & Energy Society

U.S. DEPARTMENT OF ENERGY
SOLAR ENERGY TECHNOLOGIES OFFICE

Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid

October 2022

Goal 1: Accelerate Cyber Resilience R&D of EERE Operational Technologies

1.1 Improve cybersecurity defenses and resilience.
1.2 Mitigate vulnerabilities
1.3 Next-generation cyber resilient technologies.

Goal 2: Increase EERE Stakeholder Cybersecurity Awareness

2.1 Improve situational awareness.
2.2 Enhance EERE technology cybersecurity maturity.
2.3 Identify opportunities for EERE stakeholder participation in cyber incident response exercises.
EERE and SETO Activities Align With DOE’s Broader Cybersecurity Strategies

DOE STRATEGY FOR ENERGY SECTOR CYBERSECURITY
Leverage strong partnerships with the private sector to:

1. Strengthen today's cyber systems and risk management capabilities
2. Develop innovative solutions for tomorrow's inherently secure and resilient systems

DOE PRIORITIES

GOAL 1: Strengthen energy sector cybersecurity preparedness
- Information sharing and situational awareness
- Bi-directional, real-time, machine-to-machine information sharing tools
- Risk management tools and technical assistance
- Cybersecurity supply chain risk reduction

GOAL 2: Coordinate cyber incident response and recovery
- Coordinated national cyber incident response capability for the energy sector
- Cyber incident response training and incident reporting
- Cyber incident response exercises

GOAL 3: Accelerate game-changing RD&D of resilient energy delivery systems
- RD&D to prevent, detect, and mitigate a cyber incident in today's systems
- RD&D of next-generation resilient energy delivery systems
- Build National Lab core capabilities and university collaborations

VISION
Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions
# S2G: Securing Solar for the Grid

## VISION

Achieving high cybersecurity maturity levels for solar technologies, equipment, supply chains, facilities, as well as the bulk and distribution electric power grids.

## GOAL

Ensure the cybersecurity of electric grids with high penetration levels of solar PV and other DERs.

## APPROACH

A collaborative effort by multiple national labs, DOE offices, and industry to address gaps in requirement standards, best practices, testing and analysis for solar PV and DERs cybersecurity.

## EXPECTED OUTCOMES

Development and dissemination of requirement standards, best practices, equipment testing procedures, assessment tools, as well as education and training materials for cyber defense, posture and maturity tailored to solar technologies.
Securing Solar for the Grid (S2G): Cyber-physical Integrated Approach

Source: RoadmapforPhotovoltaicCyberSecuritySAND2017-132624-10-2018
Project Management Structure

- **SETO** provides project oversight and coordinates with other DOE offices.

- **DOE Coordination**
  - **SETO - Project Manager**
  - **Industry Advisory Board**
  - **Lab Coordination Committee**

- **LCC coordinates for priority discussions**, identifies gaps / issues / barriers, engages with Inter/Intra-lab & external stakeholders

- **PNNL project**
- **NREL project**
- **INL project**
- **SNL project**

- Project PIs responsible for specific tasks.
LCC Activities

- Regularly meet to assess current industry trends and facilitate non-consensus discussion and debate on project priorities.
- Coordinate activities and promotes collaboration with CESER and EERE offices.
- Facilitate Industry Advisory Board meetings. The purpose is to:
  - Gather industry priorities and effectiveness feedback
  - Perform stakeholder engagement to assess industry gaps, issues, and barriers
  - Disseminate project outcomes
  - Perform continuous reprioritization evaluation.
- Facilitate periodic informational webinars, led or supported by the national labs.
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**
### Project Activities

<table>
<thead>
<tr>
<th>STANDARDS DEVELOPMENT &amp; BEST PRACTICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>• NREL &amp; UL established requirements for IBR/DER cybersecurity certification</td>
</tr>
<tr>
<td>• NREL published IEEE 1547.3 cybersecurity guide for DERs.</td>
</tr>
<tr>
<td>• NREL conducted initial gap analysis for supply chain cybersecurity.</td>
</tr>
<tr>
<td>• Cybersecurity risk analysis for DERS</td>
</tr>
<tr>
<td>• Cybersecurity requirements for DERMS.</td>
</tr>
<tr>
<td>• Support SDOs working groups</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EDUCATION, WORKFORCE &amp; STAKEHOLDER ENGAGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Leveraging CESER’s Cyber Strike, SNL &amp; INL developed training modules and demonstrations to train solar cyber defenders. Created first 5 lessons for the Solar CyberStrike program, DER Simulator with SunSpec Modbus and IEEE 2030.5 server, and single-axis tracking system.</td>
</tr>
<tr>
<td>• Support the development of cybersecurity requirements for state energy officials (NASEO and NARUC).</td>
</tr>
<tr>
<td>• Engagement with solar vendors for project participation.</td>
</tr>
<tr>
<td>• Industry Advisory Board</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CYBERSECURITY TOOLKIT &amp; SUPPLY CHAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SNL &amp; INL created the Solar Cybersecurity Evaluation and Risk Informed Toolkit (SolarCERT) leveraging DHS’ CSET.</td>
</tr>
<tr>
<td>• SNL Security Orchestration and Automation and Response.</td>
</tr>
<tr>
<td>• PNNL Cyber-Physical Detection and Range (CPYDAR) tool to enable the development, replication and benchmarking of cyber security test procedures for solar PV test system models.</td>
</tr>
<tr>
<td>• PNNL Secure-design &amp; development maturity model and assessment tool for DERs (S2D-C2M2) solar vendors.</td>
</tr>
</tbody>
</table>
S2G: SECURING SOLAR FOR THE GRID
STANDARDS & CERTIFICATIONS
Upcoming Guides & DER Certification Programs

- **Cybersecurity Guidance**
- **DER Certification Programs**
- UL 2941 “Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources”
- SunSpec DER Cybersecurity Certification Program, announced April 28, 2022 (https://sunspec.org/sunspec-cybersecurity-certification-work-group/)
Many Standards and Guides Exist – Why a New One?

The UL cybersecurity certification standard will:

• Build on past work
• Map and leverage security requirements from industry best practices for hardware and software
• Provide an information hub for DER Industry stakeholders
• Establish “security by design”

Note: All these standards serve a different purpose. The UL cybersecurity certification standard will not replace them by any means.
The requirements will provide a single unified approach for testing and certification of DERs in advance of deployment.

The certification will be applicable to generation and energy storage technologies.

UL and NREL are actively developing the OOI.

We will welcome participation from industry.

To receive news and information, please visit UL news.
S2G: SECURING SOLAR FOR THE GRID
RISK ASSESSMENT & MITIGATION
**INL Cyber SHIELD-INL CERT**

**INL Cybersecurity Risk Evaluation Tool**

**Main Goal**
Deliver a standardized, repeatable cybersecurity valuation methodology that is tuned to the needs and characteristics of the renewable industry subsectors and can provide insight and guidance quantitatively to better informed, broader, risk-based investment decisions surrounding renewable IT and OT cybersecurity programs

**Key features:**
- Renewable Sector Focused Capability
- Leverages DHS CSET tool, with multiple years of $$$ investment
- Open-Source and tuned for Solar industry

**Top 3 Benefits:**
1. Guided cybersecurity assessment and risk-based report to enhance cybersecurity programs leveraging established framework tuned for renewable asset sector
2. Design tool to map network architecture and obtain clear view to common design related risks and mitigation options
3. Immediate access to input supporting program and resource planning capabilities to more quickly meet maturity objectives
SHIELD–Malcolm
Asset Interaction Analysis

Main Goal
Links assets to business processes and translates business processes to OT devices. Supports deeper threat and vulnerability identification/analysis for user

Key features:
✓ Malcolm: A first step in asset to business processes mapping
✓ Works with a spectrum of cyber maturity adding capability at their level
✓ Significant investment by others (DHS)

Top 3 Benefits:
1. Get to know what you have, better view of asset level risks - devices, protocols, misconfigurations
2. Helps you identify potential attacks, vulnerabilities, active exploits with more precision specific to your assets/devices
3. Increases visibility into your network to inform decisions and improve reliability

Deploying AIA
INL will deploy hardware (spec’d to multiple environments) and work with your team on installation and configuration for your network
INL will work with your team to identify capture points and configure data collection
INL encourages plant owners and operators to incorporate the capability after engagement

IDAHO NATIONAL LABORATORY
S2G: SECURING SOLAR FOR THE GRID

CYBER-PHYSICAL NETWORK MONITORING
Security Orchestration for DER Equipment

- Sandia developing next-generation **security automation** incorporating multiple data streams and threat intelligence.
- Threat, intrusion detection, and other data is pooled into a Security Information and Event Management (SIEM) application in the **Security Operations Center (SOC)**.
- Detects a variety of DER attacks and **responds quickly** (<30 second response time).
- Automated or human-in-the-loop responses: network topology changes, block IPs, revoke access/certs, modifying VPN/SSH access, etc.

---

**SOC Maturity Levels**

**MANUAL (Defensive Position)**
- Prealert and alert originated (e.g., DDoS)
- Detailed network design and implementation
- Endpoint and repairing system locality
- Limited centralized log data
- Security information generally gathered by host
- Manual threat hunting, forensics, & incident response

**ADVANCED ANALYTICS (Data Focused)**
- Data aggregation and prioritization
- Use of powerful SIEM with backward data fusion and analytics
- IDS/IPS logging, anomaly, & chain
- Web application thread scanning with deep packet inspection
- Endpoint detection and response (EDR)

**AUTOMATION (Integration Enforced)**
- SIEM with automated playbooks for incident handling
- Machine learning, software-defined networking (SDN)
- Automated incident response protocols
- Ongoing monitoring & SIEM

**PREDICTION (Resilience Expected)**
- Adversary simulation with tactics, techniques, & procedures
- Automated incident response protocols
- SOC playbooks generation based on threat intelligence
- Dynamic defense using AI and machine learning

---

**SOAR Process**

1. Analyze ports being scanned
2. Calculate packets/second for each IP
3. Get IP details from ES
4. Get Modbus Quickdraw-Snort alerts
5. Get SSH login attempts
6. Check for changed IP address/MAC pairing

**Automated Response Playbook**

- Unauthorized access detected
- Reboot?
- No: Unauthorized Client?
- Yes: Reboot?
- No: DOS Attack?
- Yes: Reboot?
- No: Golden image of DER Modbus settings

---

**Sandia Testbed**

**DER Site**

**Attacker with physical or logical DER site access**

**DER 10.1.2.31**

**Pyranometer 10.1.2.231**

**Attack System 10.1.2.45**

**BITW IDS 10.1.2.34**

**Query Event logs from ES**

**Query Snort logs from ES**

**Query Watchdog alerts from ES**

**Query Snort logs from ES**

**Query Snort logs from ES**

**Query Snort logs from ES**

**Query Snort logs from ES**

**Query Snort logs from ES**

---

**U.S. DEPARTMENT OF ENERGY**

**SOLAR ENERGY TECHNOLOGIES OFFICE**

21
Intrusion Detection and Mitigation for Photovoltaics

Sandia is developing solar-specific Security Operations Centers (SOCs) with intrusion detection and automated mitigation:

- Cyber-physical approach uses network and power system data to detect attacks.
- Adaptive Resonance Theory establishes detection thresholds for physical attacks with online learning.

Physical DER data

Active Power

Reactive Power

Grid Voltage

Abnormal | Normal
S2G: SECURING SOLAR FOR THE GRID

Workforce Development & Training
Training solar cyber defenders

• Sandia is creating a new renewable energy cybersecurity CyberStrike training program for solar inverters, EV chargers, and wind systems.

• 8-hour classes with lectures (slides) and exercises
  • Virtual machine environment for hands-on training without hardware
  • Implementing a hands-on training with hardware including a single axis solar tracker.

• Hardware prototypes have been designed and are being prepared for production.
S2G: SECURING SOLAR FOR THE GRID

Supply Chain
Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2)

SD2-C2M2 Model Architecture

Assessment Workflow

1. Management selects desired MIL for each practice objective.
2. SMEs respond to individual Practice Statements.
3. SMEs and management review responses.
4. Management prioritizes gaps and establishes a plan to remediate them.
5. SMEs execute the remediation plan.
6. Re-evaluate to determine if gaps have been addressed (with or without re-assessment of Management priorities).
• Establish a framework for DER supply chain cybersecurity
• Engage industry for assessments
• Create open-source software guidance
• Establish a testing and certification ecosystem for DER software supply chain cybersecurity
• Address the issue of lacking standards for DER supply chain cybersecurity
• Form working groups for best practices
In Conclusion

- The rapid deployment of renewables and distributed energy resources onto the power grid presents new challenges to energy sector cybersecurity.

- A holistic approach in information technology (IT) and operation technology (OT) risk management is needed that encompass utility systems with customer owned DER devices and third-party operated systems.

- Need to build community awareness and information sharing mechanisms to incorporates equipment standards and vigorous testing, validation, and certification – including global supply chains for products like solar inverters.

- The DOE and national labs can provide technical expertise, research and testing capabilities, and funding to support industry.

- Collaboration is crucial – within DOE program offices, other federal agencies, state and local governments, and industry.
S2G: SECURING SOLAR FOR THE GRID

End of Presentation