INL/CON-24-80483-Revision-1

Securing Solar for the Grid (S2G) Cybersecurity for Solar Systems Workshop at RE+: Fall 2024 IAB Meeting

October 2024

Megan Jordan Culler, Krystal M. Pratt, Marissa Morales-Rodriguez, Danish Saleem, Jenna deCastro, Ingrid Rayo, Manimaran Govindarasu, Wajid Hassan, Scott Mix, Daniel Alan Ricci, Brian Lyttle, Emily Hwang, Andrew Plunkett

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

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-24-80483-Revision-1

Securing Solar for the Grid (S2G) Cybersecurity for Solar Systems Workshop at RE+: Fall 2024 IAB Meeting

Megan Jordan Culler, Krystal M. Pratt, Marissa Morales-Rodriguez, Danish Saleem, Jenna deCastro, Ingrid Rayo, Manimaran Govindarasu, Wajid Hassan, Scott Mix, Daniel Alan Ricci, Brian Lyttle, Emily Hwang, Andrew Plunkett

October 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

U.S. DEPARTMENT OF
ENERGY

Office of
ENERGY EFFICIENCY &
RENEWABLE ENERGY

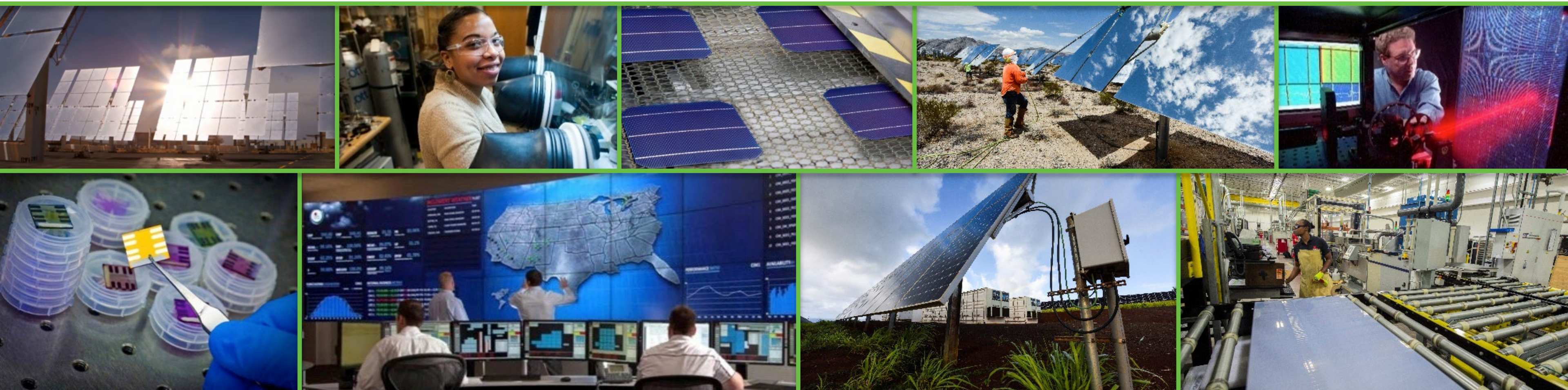
Securing Solar for the Grid (S2G)

Cybersecurity for Solar Systems Workshop at RE+

Fall 2024 IAB Meeting

Lab Coordinating Committee (LCC) Chair: Megan Culler (INL)
LCC Co-Chair: Danish Saleem (NREL)

September/2024

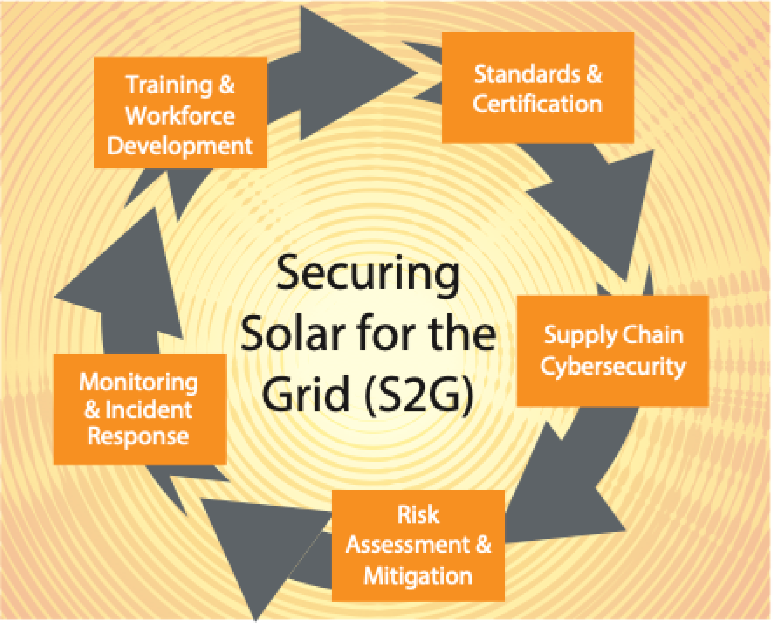


Securing Solar for the Grid

New standards and certifications

Best practice guides and resources

Automated attack surface tools



Securing Solar for the Grid (S2G)

Training & Workforce Development

Standards & Certification

Supply Chain Cybersecurity

Risk Assessment & Mitigation

Monitoring & Incident Response

Risk evaluation and modeling tools

Incident response and vulnerability management

Solar supply chain evaluations

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

Agenda - Morning

Time	Session Title	Location
8:00-8:25	Opening Remarks	211A
8:25-9:15	Cybersecurity for Internet Facing DERs	211A
9:15-9:30	BREAK	Lobby
9:30-9:45	Gaps and Challenge for Solar Energy Cybersecurity	211A
9:45-10:45	Standards Development & Best Practices	211A
10:45-11:15	DER Standards Harmonization	211A
11:15-12:00	Education and Workforce Development	211A
12:00-1:00	LUNCH	204B

Agenda - Afternoon

Time	Session Title	Location
12:00-1:00	LUNCH	204B
1:00-2:00	Cybersecurity Tool Kit	211A
2:00-2:15	BREAK	Lobby
2:15-3:15	Asset and Vulnerability Management	211A
3:15-4:15	Breakout Sessions	211A
4:15-4:30	Closing Remarks	211A

SETO S2G Overview

Dr. Marissa Morales-Rodriguez

U.S. DEPARTMENT OF
ENERGY

Office of
ENERGY EFFICIENCY &
RENEWABLE ENERGY

2024 Workshop Securing Solar for the Grid (S2G)

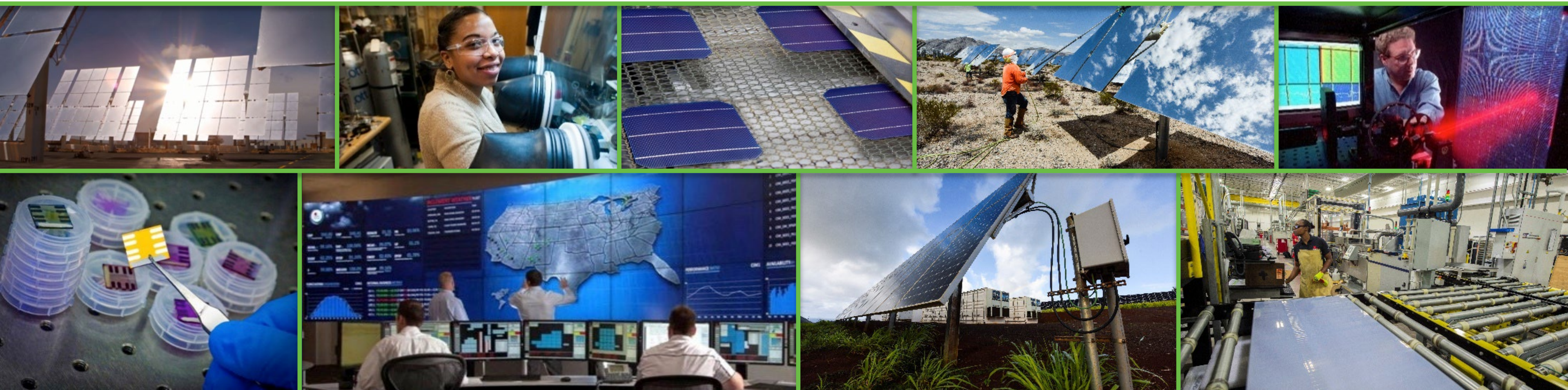
Cybersecurity for Solar Systems

Marissa E. Morales-Rodriguez, Ph.D.

Technology Manager, Solar Energy Technologies Office

U.S. DOE-Energy Efficiency and Renewable Energy

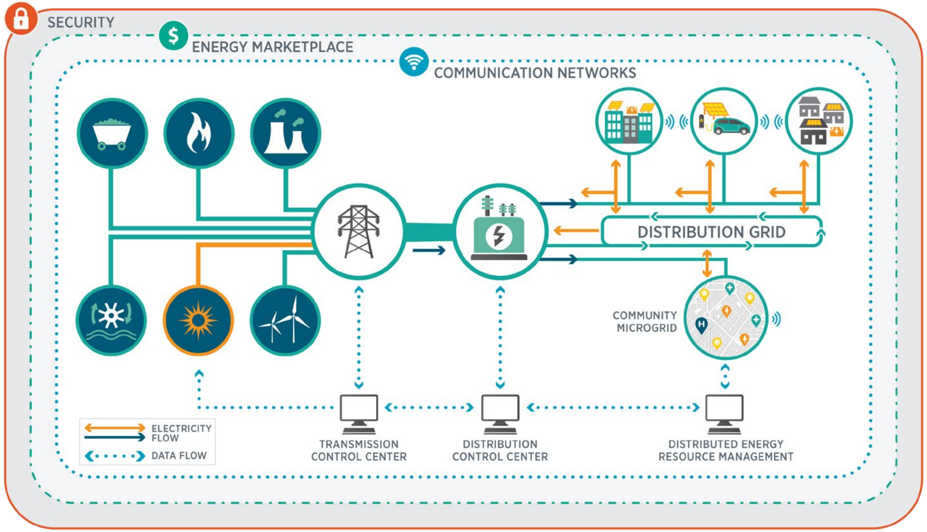
September/2024



SETO Systems Integration Program

The Systems Integration (SI) subprogram supports early-stage research, development, and demonstration (RD&D) of technologies and solutions – focusing on technical pillars **data, analytics, control, and hardware** - that advance the **reliable, resilient, secure and affordable** integration of solar energy onto the U.S. electric grid.

- System Planning
- System Operations
- System and Community Resilience
- Solar and DER Cybersecurity



Achieving 100% Decarbonized Power System

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

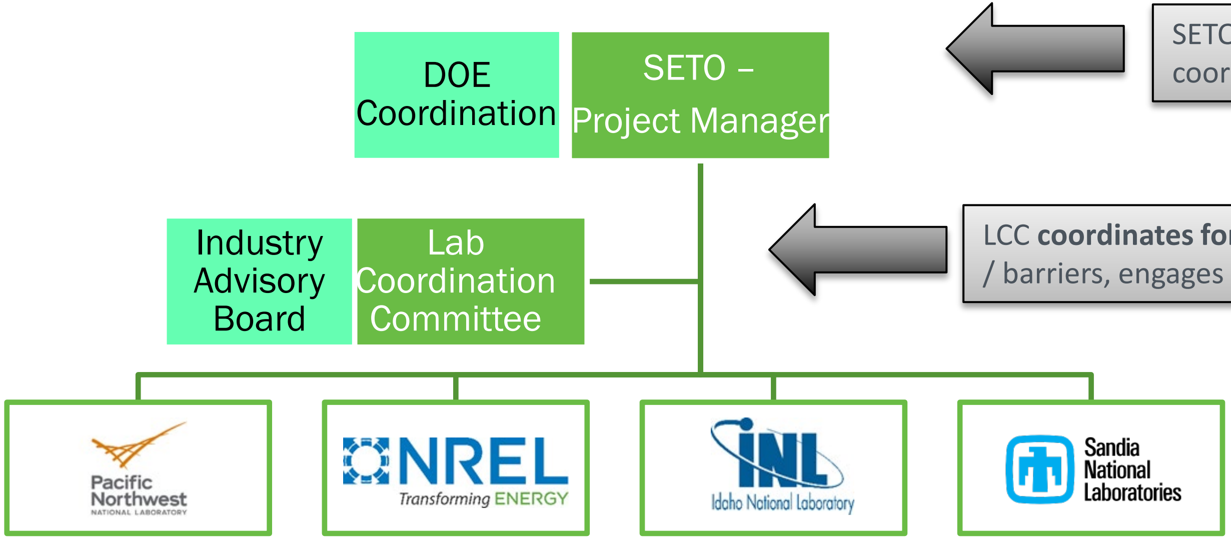
APPROACH

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 **standards' requirements, best practices, equipment testing procedures, assessment tools, as well as education and training materials** for cyber defense, posture and maturity tailored to solar technologies.

S2G Program Management Structure



DOE Coordination

SETO – Project Manager

Industry Advisory Board

Lab Coordination Committee

SETO provides project oversight and coordinates with other DOE offices

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

project PIs responsible for specific tasks

Research Areas

STANDARDS DEVELOPMENT & BEST PRACTICES

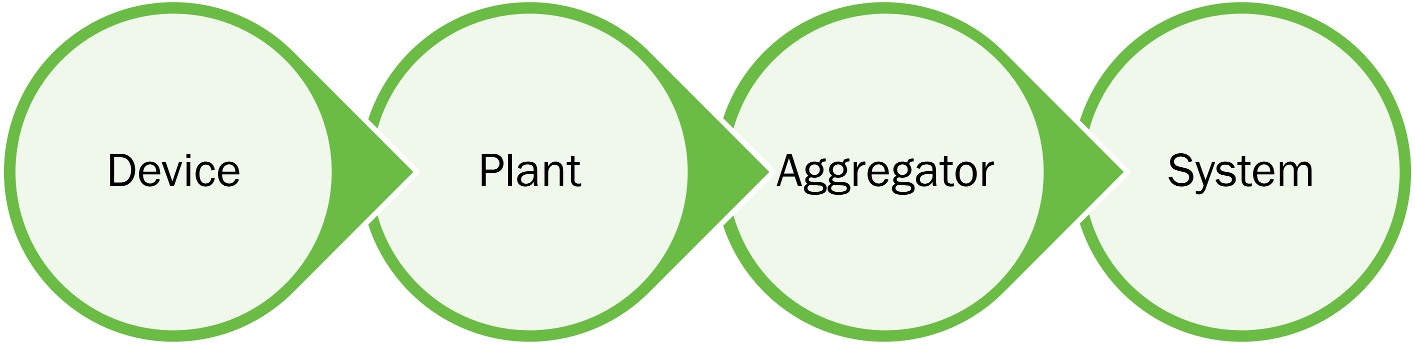
Stakeholder engagement to investigate gaps and develop best practices that can become standards to enable the secure integration of inverter-based resources and DERs.

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.



Device

Plant

Aggregator

System

INCREASING CYBERSECURITY LEVELS OF SOLAR TECHNOLOGIES

Collaboration & Industry Engagement

DOE Cybersecurity, Energy Security, and Emergency Response (CESER)

- CyberStrike StormCloud
- Report "Cybersecurity Considerations for DERs", 2022.
- Supply chain testing prioritization strategy for solar systems.
- GMI project on harmonization of cybersecurity standards.

White House Office of the National Cyber Director

- Priorities for Enhancing the Digital Ecosystem to Support a Secure Energy Future

DOE Energy Efficiency and Renewable Energy (EERE)

- SETO, WETO, and WPTO partnership to develop CyberSHIELD maturity assessment tool for asset operators.

Solar Energy Industries Association (SEIA)

- Outreach and development of training materials based on needs.

National Association of State Energy Officials (NASEO)

- Outreach and development of training materials based on needs.

DHS Cybersecurity and Infrastructure Security Agency (CISA)

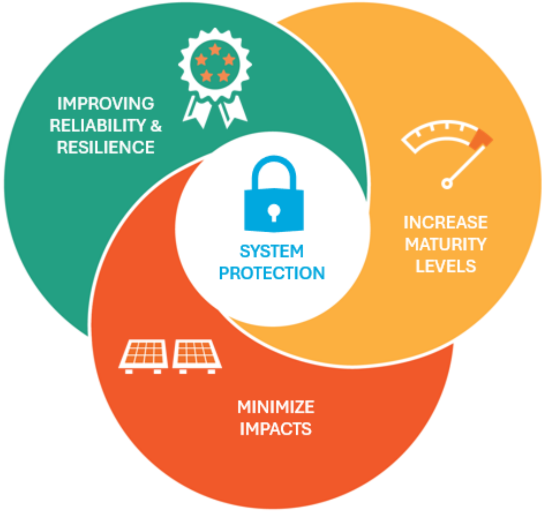
- Coordinated vulnerability disclosure and information sharing.

Underwriters Laboratory (UL)

- DER cybersecurity certification and standards.

North American Electric Reliability Corporation (NERC)

- Reports informing cybersecurity for DER and DER aggregators.



FY22-24 S2G Main Accomplishments

SETO and LCC

- ✓ Industry Advisory Board 60+ members
- ✓ Host two meetings per year
- ✓ Virtual supply chain workshop and report
- ✓ Cybersecurity maturity survey with SEIA
- ✓ Training modules with SEIA and NASEO
- ✓ Report: Roadmap for Solar PV Cybersecurity

Idaho National Laboratory

- ✓ Supply Chain –
- ✓ Workforce Training and Education.
- ✓ PV operator cybersecurity assessment .
- ✓ Reports/Memos: Buy America Guidance for Solar Industry, Confidence in Solar Grid Services.

National Renewable Energy Laboratory

- ✓ Standards - DER Cybersecurity Certification and IEEE 1547.3 Cyber Guide
- ✓ Baseline Reports 10+ .Supply chain gap analysis, Cyber for DER aggregators with NERC, Cyber considerations for DERMs.

Pacific Northwest National Laboratory

- ✓ Solar Vendors Maturity Assessment .
- ✓ Development of cyber scenarios and test models .
- ✓ Standards – UDDEX

Sandia National Laboratory

- ✓ PV operator cybersecurity assessment.
- ✓ Vulnerability Analysis and Disclosure
- ✓ Report. Secure Boot Best Practices, AI Adversary testbed development.
- ✓ Exercises - Incident Response Scenario
- ✓ Tools for Solar IDS with AI/ML – OT Security Orchestration, Automation, and Response (SOAR) .

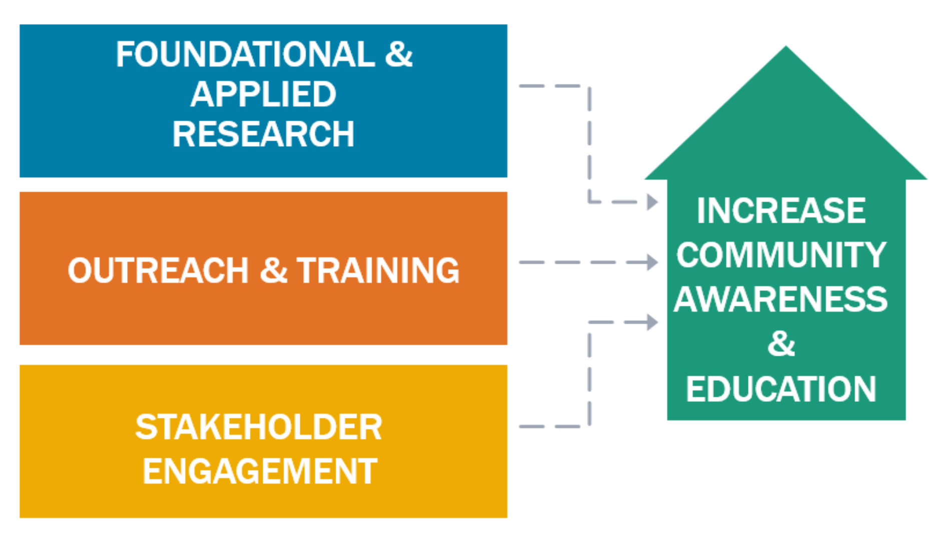
DER Standards

Tools

Training

Summary

- Research efforts are targeting the needs of diverse stakeholders in the solar and DER industry.
- S2G has engaged over 60 industry members to inform research efforts.
- Collaboration is crucial – within DOE program offices and other federal agencies. This approach led to the identification of technical gaps and prioritization of activities.
- DOE and the National Laboratories have developed tools, training and inform standards development to increase cybersecurity maturity levels and raise awareness within the solar and DER community.



FOUNDATIONAL & APPLIED RESEARCH

OUTREACH & TRAINING

STAKEHOLDER ENGAGEMENT

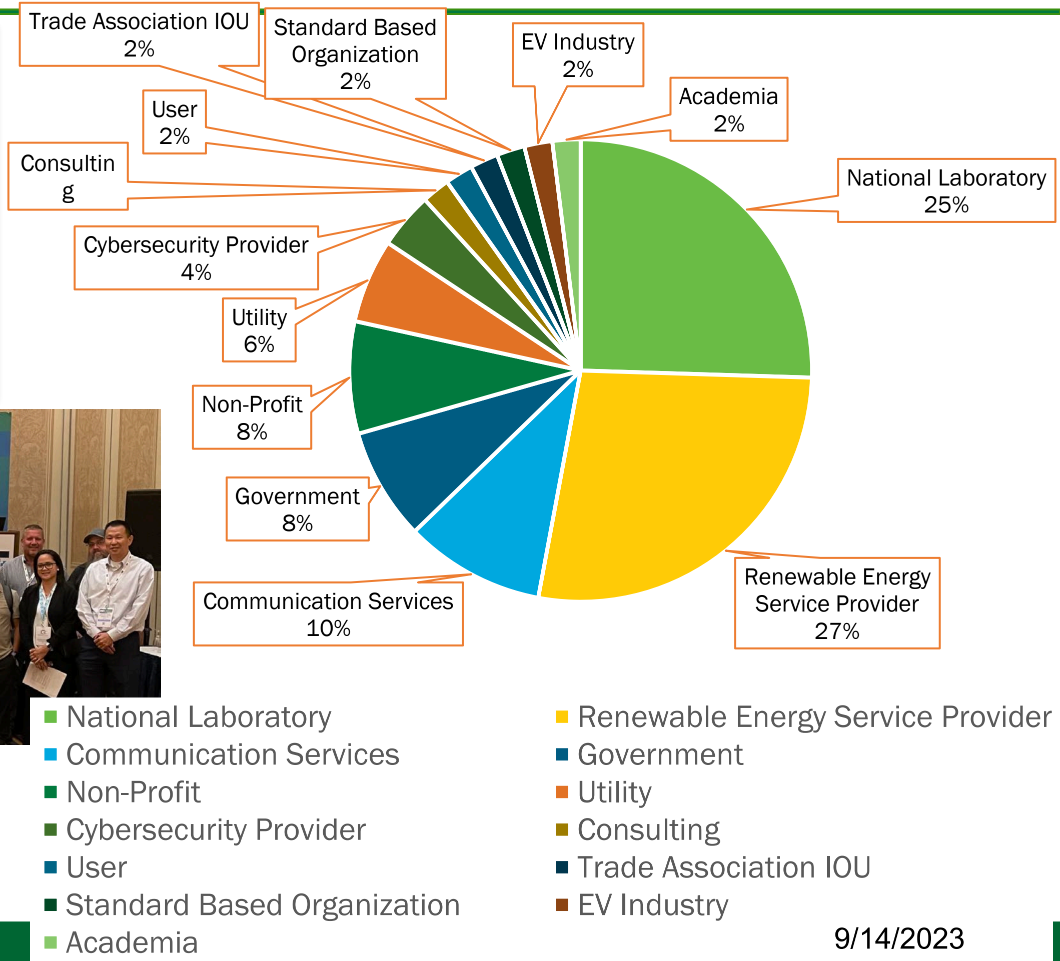
INCREASE COMMUNITY AWARENESS & EDUCATION

SIGN UP NOW:
energy.gov/solar-newsletter

SETO Securing Solar for the Grid (S2G) Workshop at RE+ 2023

Agenda: Cybersecurity for Solar Systems

- Supply chain
- DER Vulnerability Assessments
- Standards and Certifications
- Risk Assessment Tools
- Open Discussion and Industry Feedback



About 75 stakeholders attended our annual workshop

9/14/2023

End of Presentation

Securing Solar for the Grid II (S2G 2): FY25-27

S2G 2 will support R&D to inform and develop cybersecurity standards for solar technologies and distributed energy resources (DERs). S2G works closely with industry to assess the cybersecurity risks of grids with high solar deployment that can impact grid reliability.

GOALS

- **Demonstration and deployment** of cyber-physical monitoring tools to increase solar DER network visibility, detect threats and provide remediation strategies.
- **Establish solar inverter-based resource cybersecurity testing** that considers supply chain and information sharing through stakeholder engagement activities.
- **Refine existing training modules and extending to solar hybrid systems** based on vulnerability assessments.
- Development new frameworks and best-practices guides **to increase DER aggregator maturity levels.**
- **Development and adoption of risk-assessment tools** to inform investments.
- **Inform standards development, harmonization and best practices**.
- **Stakeholder engagement** and collaboration with industry and other DOE offices, including the Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

INL Idaho National Laboratory

NREL Transforming ENERGY

Sandia National Laboratories

Pacific Northwest NATIONAL LABORATORY

S2G 2 FY25-27 Summary of Activities

Research Area	National Lab	Description
Standards and Best Practices	NREL	• Development of material and training to increase awareness and understanding of cybersecurity standards for IBRs and DERs.
	SNL	• Development of best practices to defend against AI/ML cyber incidents.
	PNNL	• Zero-trust reference architecture blueprint, evaluation criteria for commercial and industrial DER-based VPPs
	INL	• Cyber Informed Engineering architectural guide for solar technologies
Tool Kit and Supply Chain	NREL	• DER aggregators risk assessment and cost benefit analysis tool • Consequence-based experimentation on aggregated DERs cyberattacks impact to the grid.
	SNL	• Understand defense and adversary AI/ML implications for network connected IBRs.
	PNNL	• Cybersecurity checklist for commercial, industrial, and residential DER installations. • Supply chain analysis for inverter adjacent technologies.
	INL	• Firmware analysis based on AI/ML • Risk analysis tools and incident response for solar installations including aggregators and VPPs • Inverter HBOM enumeration and catalog in collaboration with CESER
Workforce Developm ent and Training	NREL	• Outreach activities to increase maturity in standards for DERs
	SNL	• Training material on attack scenarios by AI/ML • Monthly webinar series
	PNNL	• Outreach activities on zero-trust architectures for C&I DER-based VPPs
	INL	• Solar Defender focused curriculum development in collaboration with CESER

DIVERSITY

EQUITY

INCLUSION

ACCESIBILITY

Thank you!

marissa.morales-rodriguez@ee.doe.gov

SIGN UP NOW:
energy.gov/solar-newsletter

Enhancing the Digital Ecosystem to Support a Secure Energy Future

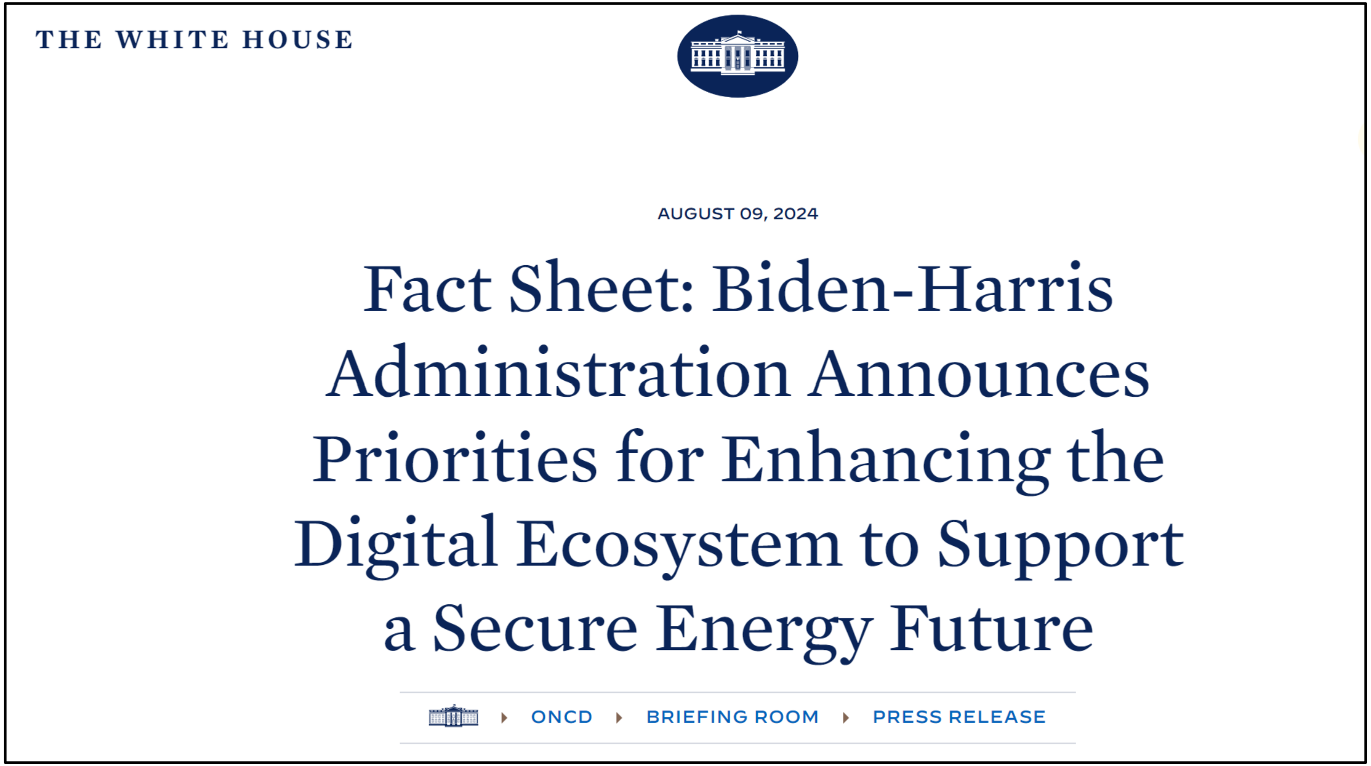
Phoebe Benich
Senior Strategy Advisor
White House Office of the National Cyber Director

Enhancing the Digital Ecosystem to Support a Secure Energy Future

Phoebe Benich, Senior Advisor

Office of the National Cyber Director

September 12, 2024



THE WHITE HOUSE

AUGUST 09, 2024

Fact Sheet: Biden-Harris Administration Announces Priorities for Enhancing the Digital Ecosystem to Support a Secure Energy Future

ONCD ▸ BRIEFING ROOM ▸ PRESS RELEASE

Priorities for Enhancing the Digital Ecosystem to Support a Secure Energy Future

Cybersecurity for Internet Facing DERs

Moderated by:
Bheshaj Krishnappa
(SEIA)

Uri Sadot
(SolarEdge)

Nathan Morelli
(South Australia
Power Network)

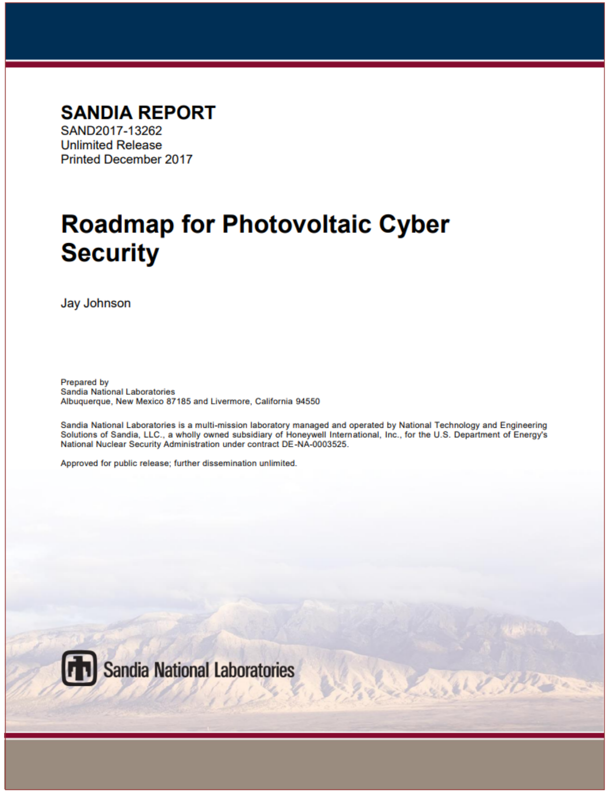
Sara Bavarian
(Tesla)

Michael Brown
(NV Energy)

Plenary Panel

Roadmap for Solar PV Cybersecurity

- **What?**
  - New version of the Roadmap for PV Cybersecurity
  - Near-term, mid-term, and long-term milestones for key cybersecurity focus areas
- **Why?**
  - 2017 version only looked 5 years out
  - Strategy for SETO, targets for labs and industry
- **How?**
  - Lab contributions and industry feedback



SANDIA REPORT
SAND2017-13262
Unlimited Release
Printed December 2017

Roadmap for Photovoltaic Cyber Security

Jay Johnson

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

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

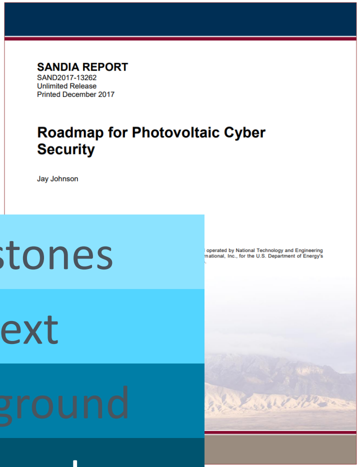
Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Roadmap for Solar PV Cybersecurity

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



SANDIA REPORT
SAND2017-13262
Unlimited Release
Printed December 2017

Roadmap for Photovoltaic Cyber Security

Jay Johnson

operated by National Technology and Engineering
rnational, Inc., for the U.S. Department of Energy's

Vision and Milestones

Broader Context

Technology Background

Motivation & Trends

What can labs do?

How to adopt?

How to implement?

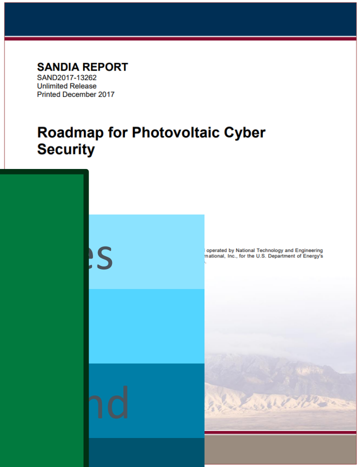
Who’s responsible?

Roadmap for Solar PV Cybersecurity

Contents

- Exe
- Nat
- Sol
- Sol
- Sol
- Standards Development
- Best Practices
- Stakeholder Roles & Industry Targets

We need your input!



SANDIA REPORT
SAND2017-13262
Unlimited Release
Printed December 2017

Roadmap for Photovoltaic Cyber Security

operated by National Technology and Engineering
national, Inc., for the U.S. Department of Energy's

es

nd

s

How to adopt?

How to implement?

Who’s responsible?

Gaps & Challenges for Solar Energy Cybersecurity

Rose

- What has improved?
- What are we doing well?

Bud

- Opportunities
- Emerging trends & technologies

Thorn

- Challenges
- Gaps in research
- Gaps in industry application

Gaps & Challenges for Solar Energy Cybersecurity

Rose

- What has improved?
- What are we doing well?

Bud

- Opportunities
- Emerging trends & technologies

Thorn

- Challenges
- Gaps in research
- Gaps in industry application

Instructions:

- Add a sticky note with your rose, bud, and thorn for solar energy cybersecurity to each board.
- Please sign up if you are interested in being a reviewer for the 2024 Roadmap for Solar PV Cybersecurity

We will resume at 9:40

Standards Development and Best Practices

Moderated by:

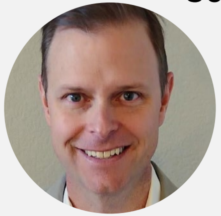
Danish Saleem
National Renewable Energy Laboratory

Panelists

Aung Thant NERC

John Franzino Grid Security, Inc.

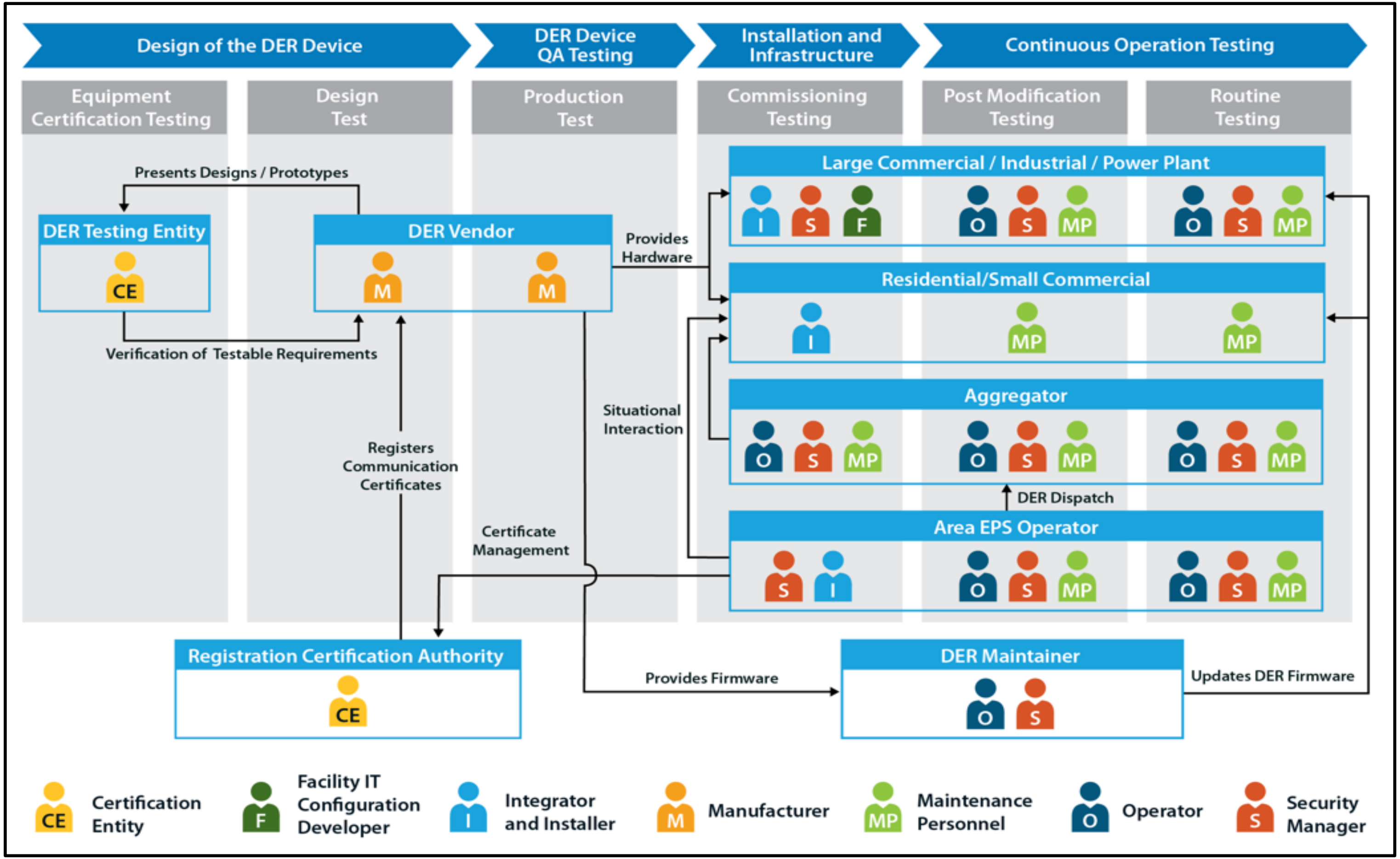
Andre Ristaino ISA



David Benton
Berkshire Hathaway Energy

Mike Slowinske
Underwriters Laboratories

How Recently Developed Standards Would Affect Product Lifecycle & Associated Stakeholders

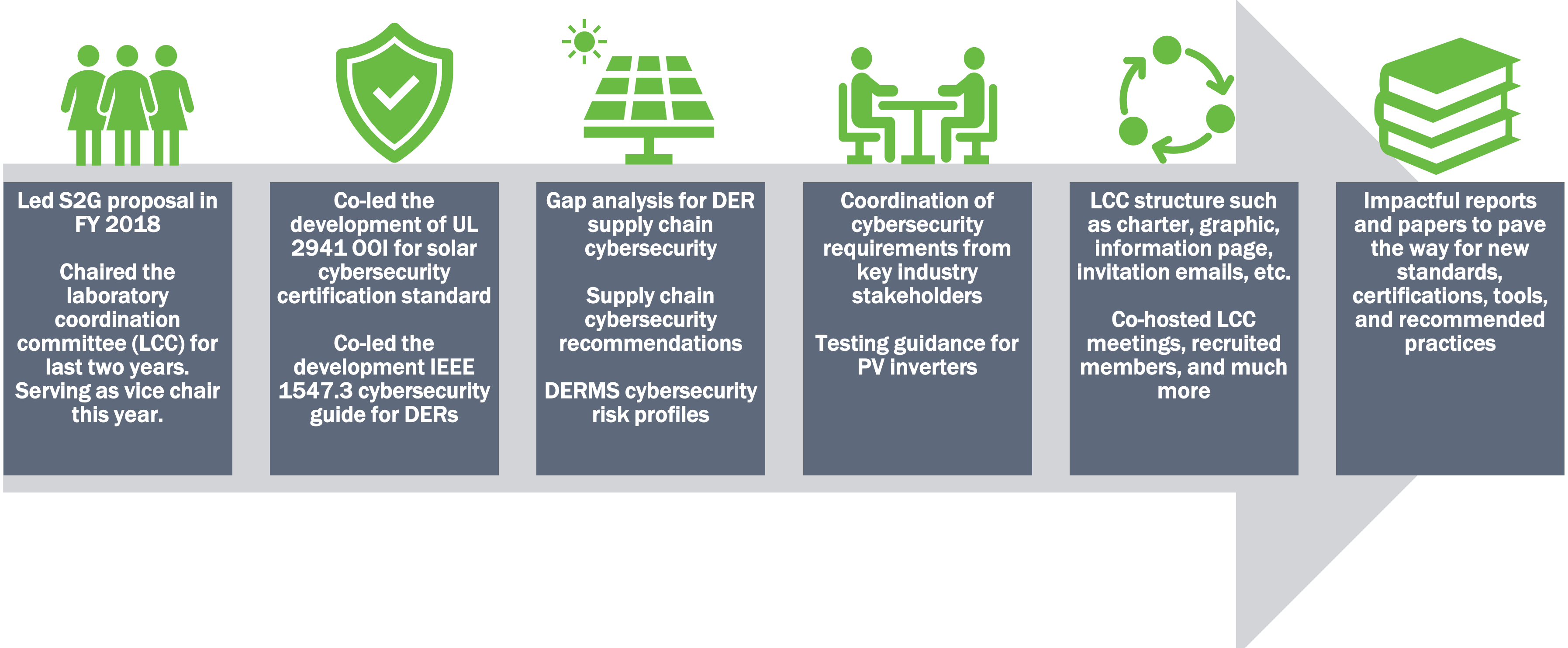


Key Milestones for NREL

Cybersecurity Certification Standard	Cybersecurity Guide for DERs	Solar PV Supply Chain Cybersecurity	DERMS Cybersecurity
Lead the development of a cyber certification standard for solar PV industry	Develop a guide with recommendations for cybersecurity of DERs i.e., IEEE 1547.3	Analyze and document the gaps in the supply chain cybersecurity for DERs	Identify applicable cybersecurity standards and/or guidelines for DERMS
Develop test guidance to support UL 2941 certification standard	Integrate cybersecurity recommendations into IEEE 1547 standard	Publish cybersecurity recommendations for solar PV industry	Identify cybersecurity considerations for DERMS
Support consensus development for UL 2941 among OEMs, utilities, installers, and aggregators		Lead a solar supply chain cybersecurity workshop	Develop cybersecurity risk profiles for DERMS

Through S2G, NREL co-led the development, coordination, and consensus development of 1) cyber certification standard, 2) cybersecurity guide, 3) cyber recommendations for supply chain and 4) DERMS cybersecurity for solar technologies to help secure the clean energy transition.

Impact of NREL’s Work Through S2G



Led S2G proposal in FY 2018

Chaired the laboratory coordination committee (LCC) for last two years. Serving as vice chair this year.

Co-led the development of UL 2941 OOI for solar cybersecurity certification standard

Co-led the development IEEE 1547.3 cybersecurity guide for DERs

Gap analysis for DER supply chain cybersecurity

Supply chain cybersecurity recommendations

DERMS cybersecurity risk profiles

Coordination of cybersecurity requirements from key industry stakeholders

Testing guidance for PV inverters

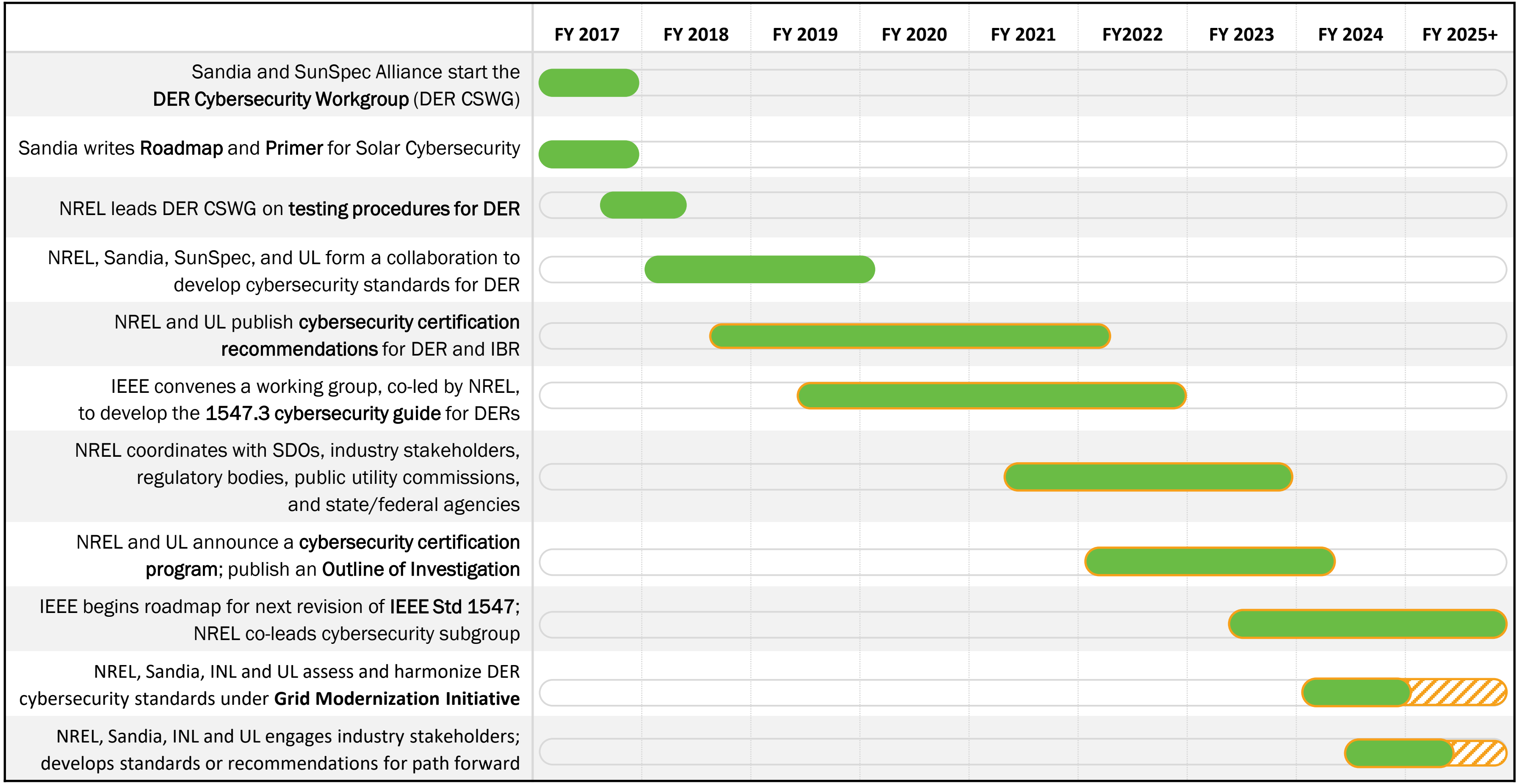
LCC structure such as charter, graphic, information page, invitation emails, etc.

Co-hosted LCC meetings, recruited members, and much more

Impactful reports and papers to pave the way for new standards, certifications, tools, and recommended practices

The project supported a **first of its kind cybersecurity certification standard** that can be used to validate cybersecurity posture of solar PV inverters before deployment and while in the field.

Contribution Towards Standards Development



Sandia and SunSpec Alliance start the **DER Cybersecurity Workgroup** (DER CSWG)

Sandia writes **Roadmap** and **Primer** for Solar Cybersecurity

NREL leads DER CSWG on **testing procedures for DER**

NREL, Sandia, SunSpec, and UL form a collaboration to develop cybersecurity standards for DER

NREL and UL publish **cybersecurity certification recommendations** for DER and IBR

IEEE convenes a working group, co-led by NREL, to develop the **1547.3 cybersecurity guide** for DERs

NREL coordinates with SDOs, industry stakeholders, regulatory bodies, public utility commissions, and state/federal agencies

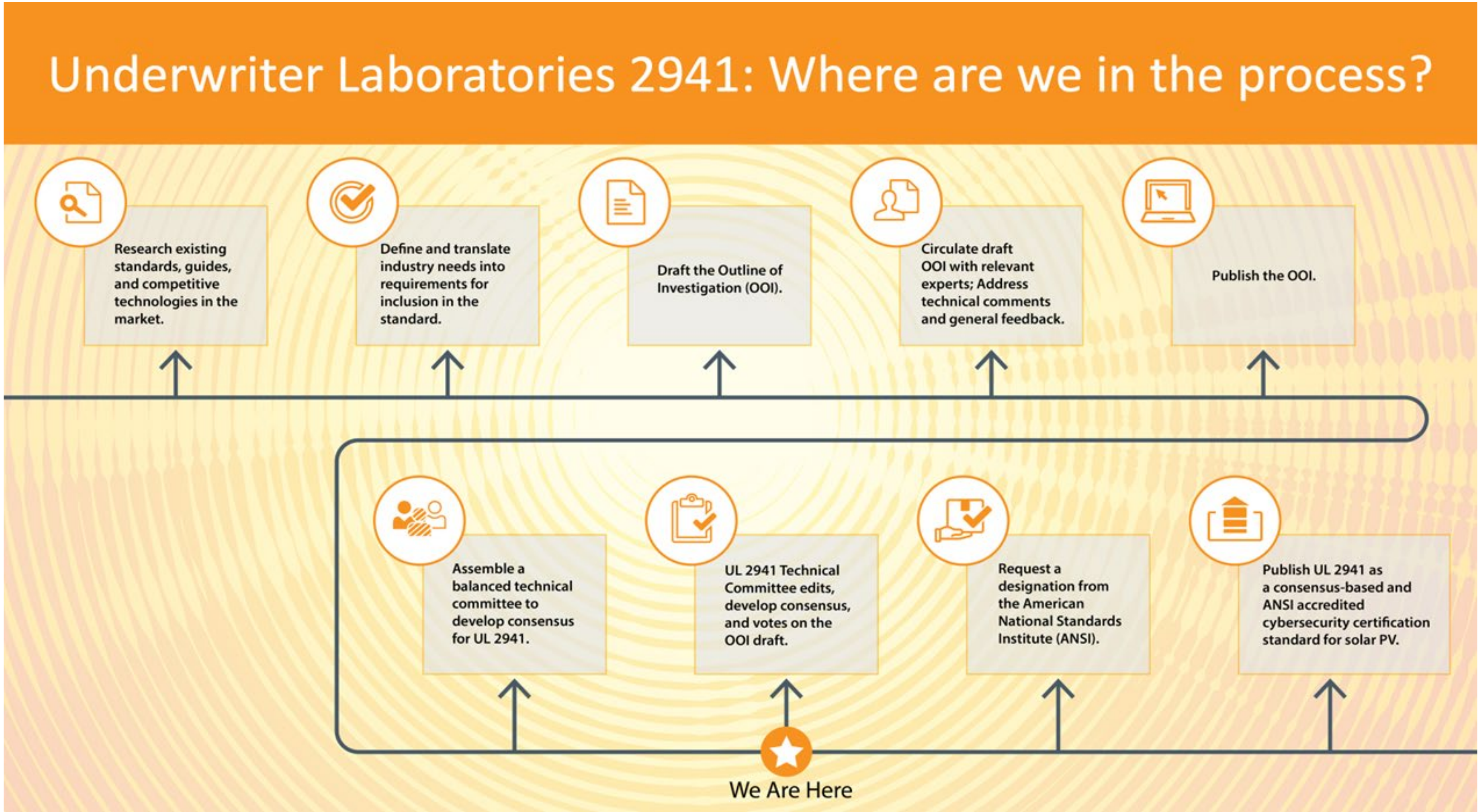
NREL and UL announce a **cybersecurity certification program**; publish an **Outline of Investigation**

IEEE begins roadmap for next revision of **IEEE Std 1547**; NREL co-leads cybersecurity subgroup

NREL, Sandia, INL and UL assess and harmonize DER cybersecurity standards under **Grid Modernization Initiative**

NREL, Sandia, INL and UL engages industry stakeholders; develops standards or recommendations for path forward

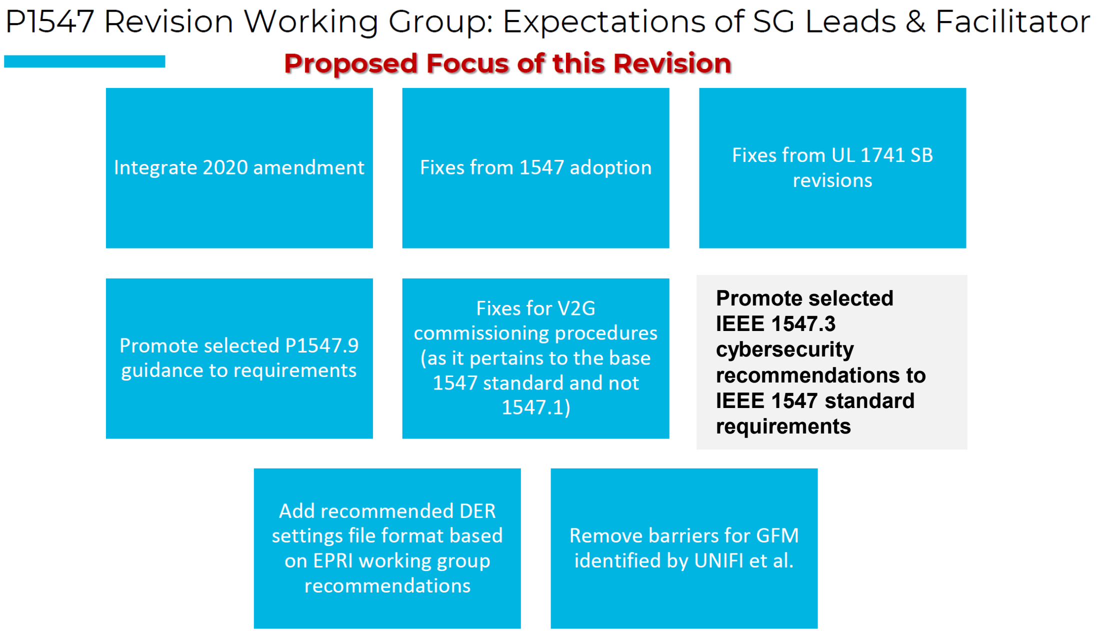
UL 2941: Cybersecurity Certification Standard



Underwriter Laboratories 2941: Where are we in the process?

- Research existing standards, guides, and competitive technologies in the market.
- Define and translate industry needs into requirements for inclusion in the standard.
- Draft the Outline of Investigation (OOI).
- Circulate draft OOI with relevant experts; Address technical comments and general feedback.
- Publish the OOI.
- Assemble a balanced technical committee to develop consensus for UL 2941.
- UL 2941 Technical Committee edits, develop consensus, and votes on the OOI draft.
- Request a designation from the American National Standards Institute (ANSI).
- Publish UL 2941 as a consensus-based and ANSI accredited cybersecurity certification standard for solar PV.

IEEE 1547.3: Cybersecurity Guide for DERs



P1547 Revision Working Group: Expectations of SG Leads & Facilitator

Proposed Focus of this Revision

Integrate 2020 amendment

Fixes from 1547 adoption

Fixes from UL 1741 SB revisions

Promote selected P1547.9 guidance to requirements

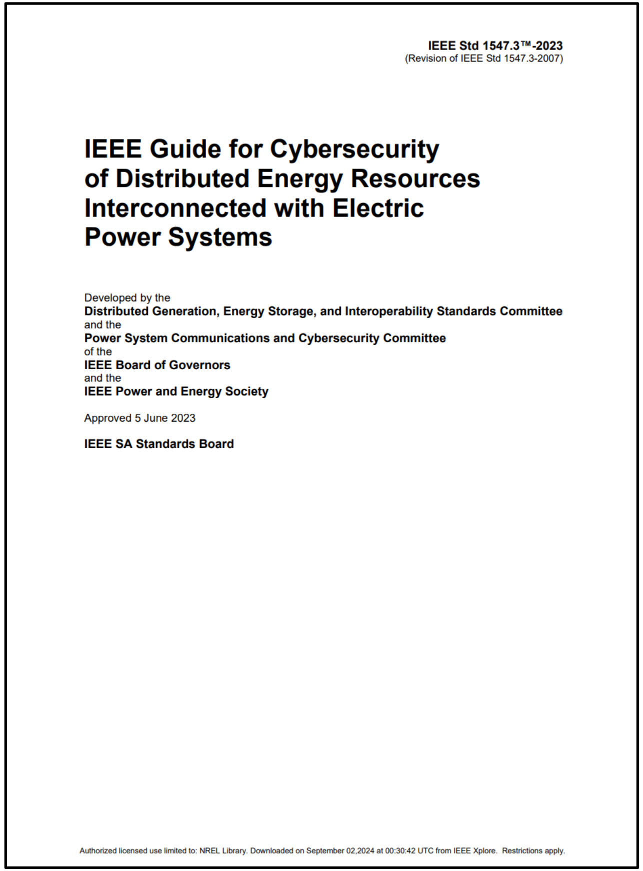
Fixes for V2G commissioning procedures (as it pertains to the base 1547 standard and not 1547.1)

Promote selected IEEE 1547.3 cybersecurity recommendations to IEEE 1547 standard requirements

Add recommended DER settings file format based on EPRI working group recommendations

Remove barriers for GFM identified by UNIFI et al.

- IEEE 1547.3 cybersecurity guide published in December 2023 after being approved by the working group and standards coordination committee
- It was added to the IEEE 1547 standard revision timeline



IEEE Std 1547.3™-2023
(Revision of IEEE Std 1547.3-2007)

IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems

Developed by the
Distributed Generation, Energy Storage, and Interoperability Standards Committee
and the
Power System Communications and Cybersecurity Committee
of the
IEEE Board of Governors
and the
IEEE Power and Energy Society

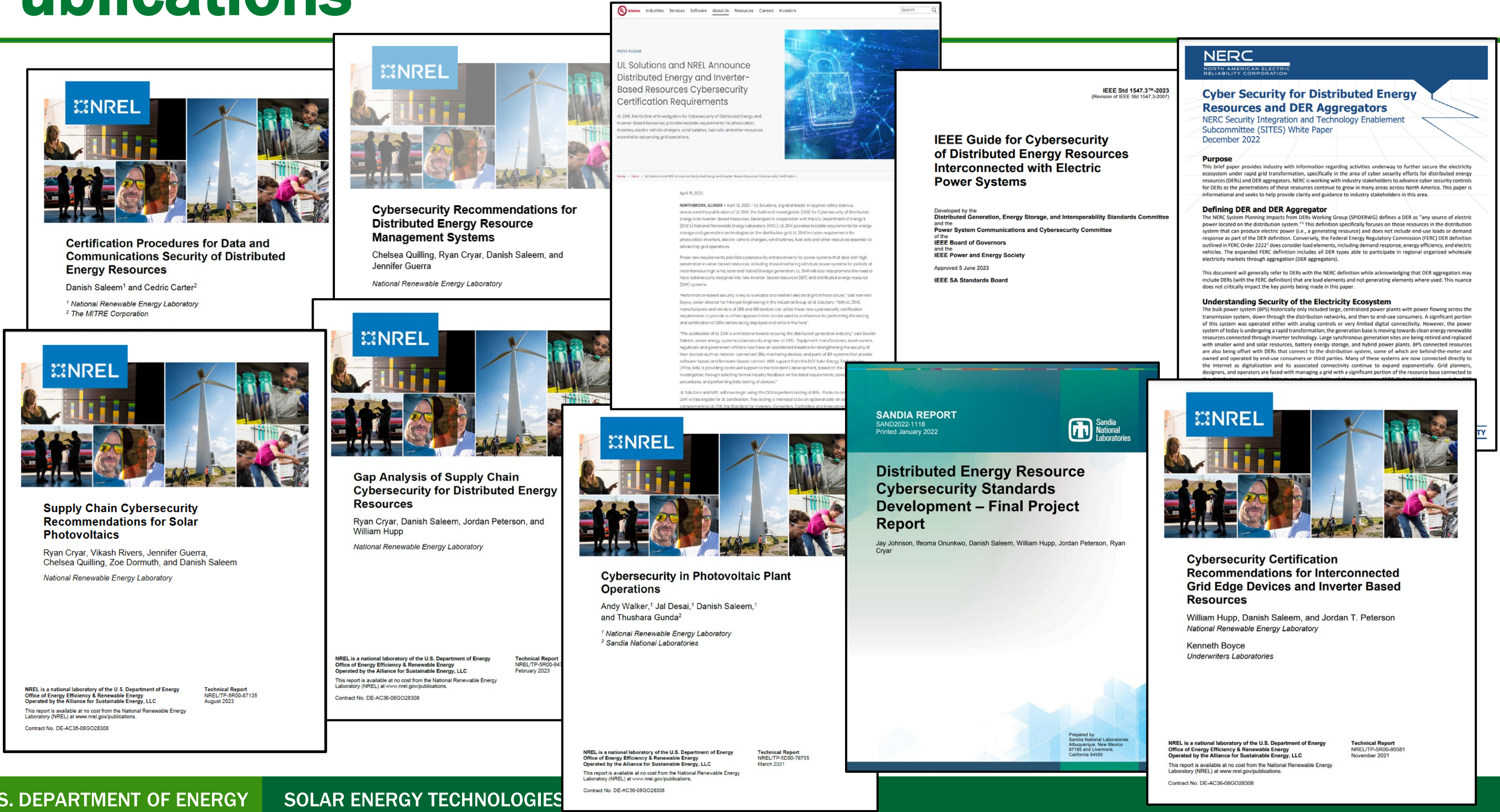
Approved 5 June 2023

IEEE SA Standards Board

Authorized licensed use limited to: NREL Library. Downloaded on September 02,2024 at 00:30:42 UTC from IEEE Xplore. Restrictions apply.

https://ieeexplore.ieee.org/document/10352402/keywords#keywords

Publications



Certification Procedures for Data and Communications Security of Distributed Energy Resources

Danish Saleem[1] and Cedric Carter[2]

[1] National Renewable Energy Laboratory
[2] The MITRE Corporation

Cybersecurity Recommendations for Distributed Energy Resource Management Systems

Chelsea Quilling, Ryan Cryar, Danish Saleem, and Jennifer Guerra

National Renewable Energy Laboratory

Supply Chain Cybersecurity Recommendations for Solar Photovoltaics

Ryan Cryar, Vikash Rivers, Jennifer Guerra, Chelsea Quilling, Zoe Dormuth, and Danish Saleem

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-87135
August 2023

Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources

Ryan Cryar, Danish Saleem, Jordan Peterson, and William Hupp

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-847
February 2023

Industries Services Software About Us Resources Careers Investors Search

PRESS RELEASE

UL Solutions and NREL Announce Distributed Energy and Inverter-Based Resources Cybersecurity Certification Requirements

UL 2941, the Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources, provides testable requirements for photovoltaic inverters, electric vehicle chargers, wind turbines, fuel cells and other resources essential to advancing grid operations.

Home > News > UL Solutions and NREL Announce Distributed Energy and Inverter-Based Resources Cybersecurity Certification ...

April 18, 2023

NORTHBROOK, ILLINOIS – April 18, 2023 – UL Solutions, a global leader in applied safety science, announced the publication of UL 2941, the Outline of Investigation (OOI) for Cybersecurity of Distributed Energy and Inverter-Based Resources. Developed in cooperation with the U.S. Department of Energy's (DOE's) National Renewable Energy Laboratory (NREL), UL 2941 provides testable requirements for energy storage and generation technologies on the distribution grid. UL 2941 includes requirements for photovoltaic inverters, electric vehicle chargers, wind turbines, fuel cells and other resources essential to advancing grid operations.

These new requirements prioritize cybersecurity enhancements for power systems that deal with high penetration inverter-based resources, including those interfacing with bulk power systems for periods of instantaneous high wind, solar and hybrid/storage generation. UL 2941 will also help promote the need to have cybersecurity designed into new inverter-based resources (IBR) and distributed energy resource (DER) systems.

"Performance-based security is key to a reliable and resilient electrical grid infrastructure," said Kenneth Boyce, senior director for Principal Engineering in the Industrial Group at UL Solutions. "With UL 2941, manufacturers and vendors of DER and IBR devices can utilize these new cybersecurity certification requirements to provide a unified approach that can be used as a reference for performing the testing and certification of DERs before being deployed and while in the field."

"The publication of UL 2941 is a milestone toward securing the distributed generation industry," said Danish Saleem, senior energy systems cybersecurity engineer at NREL. "Equipment manufacturers, asset owners, regulators and government officials now have an established baseline for strengthening the security of their devices such as network-connected IBRs, monitoring devices, and parts of IBR systems that provide software-based and firmware-based controls. With support from the DOE Solar Energy Te

Office, NREL is providing continued support to the Standard's development, based on the

investigation, through soliciting formal industry feedback on the listed requirements, deve

procedures, and performing beta testing of devices."

UL Solutions and NREL will now begin using this OOI to perform testing of IBRs. Products co

2941 will be eligible for UL certification. This testing is intended to be an optional add-on se

complementing UL 1741, the Standard for Inverters, Converters, Controllers and Interconne

IEEE Std 1547.3™-2023
(Revision of IEEE Std 1547.3-2007)

IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems

Developed by the
Distributed Generation, Energy Storage, and Interoperability Standards Committee
and the
Power System Communications and Cybersecurity Committee
of the
IEEE Board of Governors
and the
IEEE Power and Energy Society

Approved 5 June 2023

IEEE SA Standards Board

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security for Distributed Energy Resources and DER Aggregators

NERC Security Integration and Technology Enablement Subcommittee (SITES) White Paper
December 2022

Purpose

This brief paper provides industry with information regarding activities underway to further secure the electricity ecosystem under rapid grid transformation, specifically in the area of cyber security efforts for distributed energy resources (DERs) and DER aggregators. NERC is working with industry stakeholders to advance cyber security controls for DERs as the penetrations of these resources continue to grow in many areas across North America. This paper is informational and seeks to help provide clarity and guidance to industry stakeholders in this area.

Defining DER and DER Aggregator

The NERC System Planning Impacts from DERs Working Group (SPIDERWG) defines a DER as "any source of electric power located on the distribution system."[1] This definition specifically focuses on those resources in the distribution system that can produce electric power (i.e., a generating resource) and does not include end-use loads or demand response as part of the DER definition. Conversely, the Federal Energy Regulatory Commission (FERC) DER definition outlined in FERC Order 2222[2] does consider load elements, including demand response, energy efficiency, and electric vehicles. The expanded FERC definition includes all DER types able to participate in regional organized wholesale electricity markets through aggregation (DER aggregators).

This document will generally refer to DERs with the NERC definition while acknowledging that DER aggregators may include DERs (with the FERC definition) that are load elements and not generating elements where used. This nuance does not critically impact the key points being made in this paper.

Understanding Security of the Electricity Ecosystem

The bulk power system (BPS) historically only included large, centralized power plants with power flowing across the transmission system, down through the distribution networks, and then to end-use consumers. A significant portion of this system was operated either with analog controls or very limited digital connectivity. However, the power system of today is undergoing a rapid transformation; the generation base is moving towards clean energy renewable resources connected through inverter technology. Large synchronous generation sites are being retired and replaced with smaller wind and solar resources, battery energy storage, and hybrid power plants. BPS connected resources are also being offset with DERs that connect to the distribution system, some of which are behind-the-meter and owned and operated by end-use consumers or third parties. Many of these systems are now connected directly to the Internet as digitalization and its associated connectivity continue to expand exponentially. Grid planners, designers, and operators are faced with managing a grid with a significant portion of the resource base connected to

Cybersecurity in Photovoltaic Plant Operations

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

[1] National Renewable Energy Laboratory
[2] Sandia National Laboratories

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5D00-78755
March 2021

SANDIA REPORT
SAND2022-1118
Printed January 2022

Sandia National Laboratories

Distributed Energy Resource Cybersecurity Standards Development – Final Project Report

Jay Johnson, Ifeoma Onunkwo, Danish Saleem, William Hupp, Jordan Peterson, Ryan Cryar

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

Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources

William Hupp, Danish Saleem, and Jordan T. Peterson
National Renewable Energy Laboratory

Kenneth Boyce
Underwriters Laboratories

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-80581
November 2021

Assessment and Coordination of DER Cybersecurity Standards

Principal Investigator: Danish Saleem, National Renewable Energy Laboratory (NREL)

Team Members: Chelsea Neely (NREL), Emily Waligoske (NREL), Kazunori Nagasawa (NREL), Megan Culler (INL), Jordan Waggoner (INL), Chris Lamb (SNL), Jenna deCastro (SNL)

Presented on: 09/12/2024

Project Overview

Outcomes

- DER cyber standards gap analysis
- DER cyber maturity baseline report
- DER cyber standards library
- DER cyber testing methodology
- DER cyber standards advisory group
- Harmonization of cyber requirements and certification programs for DERs

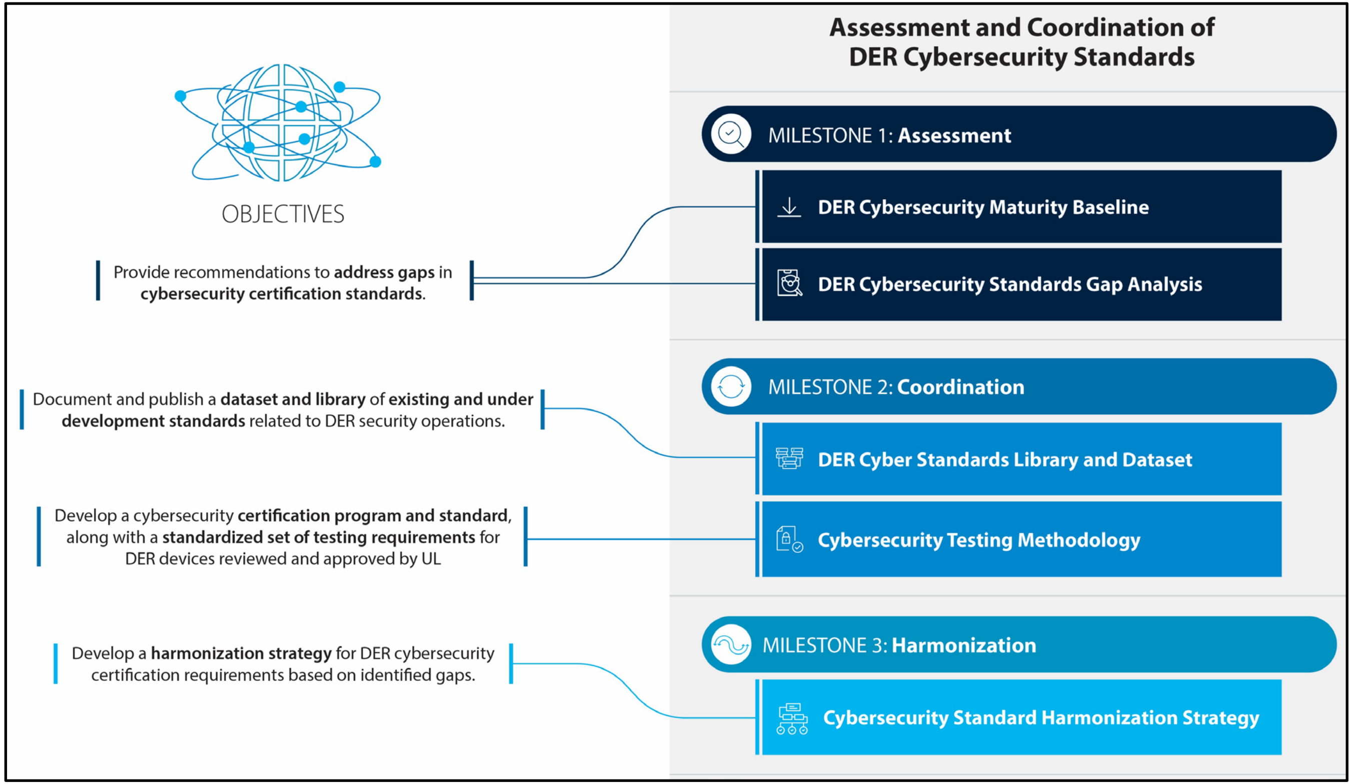
Key Partners

Idaho National Laboratory

Sandia National Laboratories

UL Solutions

solaredge



OBJECTIVES

Provide recommendations to **address gaps** in **cybersecurity certification standards.**

Document and publish a **dataset and library** of **existing and under development standards** related to DER security operations.

Develop a cybersecurity **certification program and standard,** along with a **standardized set of testing requirements** for DER devices reviewed and approved by UL

Develop a **harmonization strategy** for DER cybersecurity certification requirements based on identified gaps.

Assessment and Coordination of DER Cybersecurity Standards

MILESTONE 1: **Assessment**

- **DER Cybersecurity Maturity Baseline**
- **DER Cybersecurity Standards Gap Analysis**

MILESTONE 2: **Coordination**

- **DER Cyber Standards Library and Dataset**
- **Cybersecurity Testing Methodology**

MILESTONE 3: **Harmonization**

- **Cybersecurity Standard Harmonization Strategy**

Defining a DER

What is a distributed energy resource (DER)?

- **Energy resource at the distribution level connected at 20 MW and under:**
  - The types of assets included in this project, but are not limited to, DERs for energy storage, distributed solar, distributed wind, hydrogen fuel cells, building loads, etc.
  - The work in this project also require understanding of supporting technology infrastructure such as demand response, DERMS, and microgrids.
  - Current focus of GMI 2.2 project is wind, solar, storage, hydrogen, and building loads
  - Controllable thermostats, demand response, etc., can be added to the next project cycle

- **Informed by DER definitions from:**
  - NERC, FERC, IEEE 1547-2018, DOE's *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid*, and project 2.2 proposal.

DER Standards Library

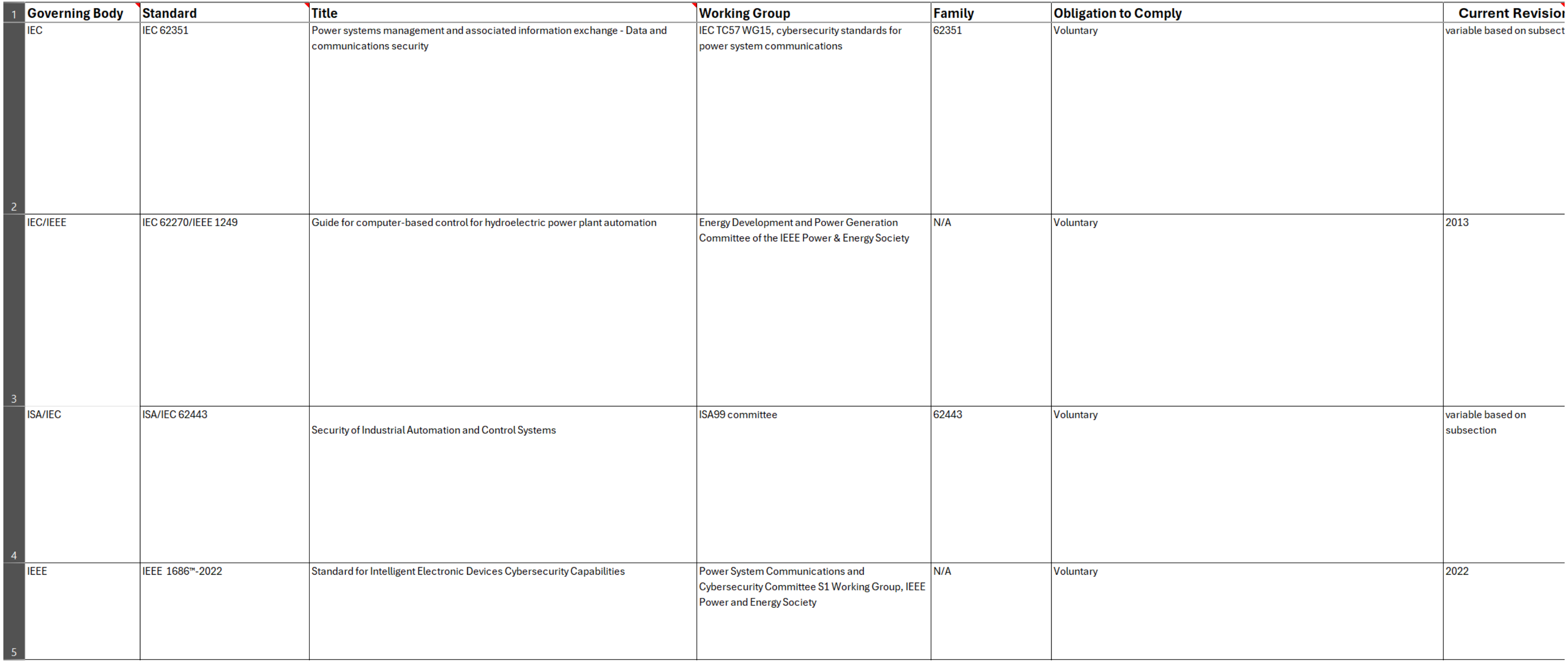
Cybersecurity	Interconnection	Communication	Safety
IEEE 1547.3	IEEE 1547	IEC 61850	UL 1741
UL 2941	IEEE P2800	IEEE 1815 (DNP3)	UL 9540
NIST SP 800-82	IEC TR 62351	Modbus	IEC 62109-1
IEEE P2658	CA Rule 21	IEEE 2030.5	IEEE 2030.2
ISO/SAE 21434	Hawaii Electric Rule 14H	REST	
		Open ADR	

Data Dictionary

- The data dictionary provides uniform identifying information about each standard in the library.
- Categories were chosen based on relevancy to the user of the library and are meant to add value to the library:

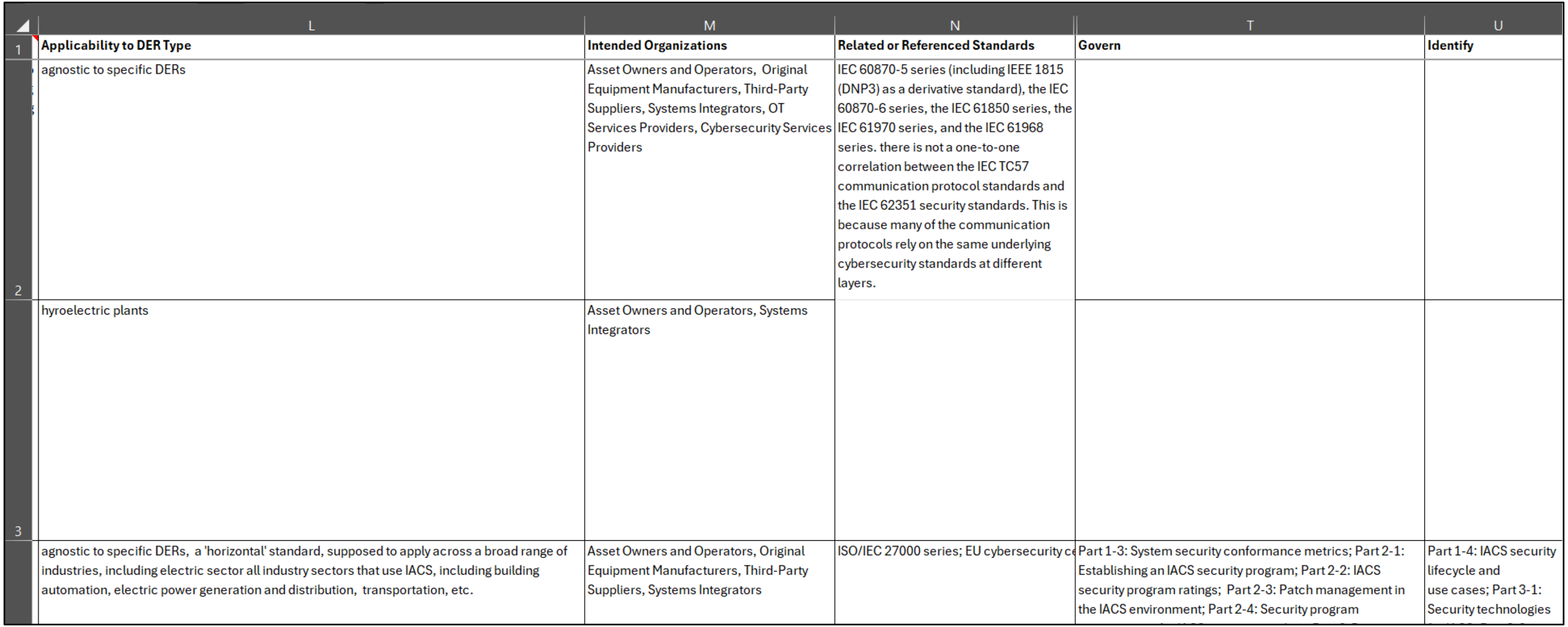
  - Governing body
  - Standard
  - Title
  - Working group
  - Family
  - Obligation to comply
  - Current revision
  - Standard type
  - Geographic scope
  - Functional scope
  - Applicability to DER type
  - Intended organizations
  - Related or referenced standards
  - NIST CSF functions
  - Encryption type
  - Device authentication
  - Key exchange algorithms
  - Accessibility
  - User cost
  - Source/link.

Sample of Database



Governing Body	Standard	Title	Working Group	Family	Obligation to Comply	Current Revisio
IEC	IEC 62351	Power systems management and associated information exchange - Data and communications security	IEC TC57 WG15, cybersecurity standards for power system communications	62351	Voluntary	variable based on subsect
IEC/IEEE	IEC 62270/IEEE 1249	Guide for computer-based control for hydroelectric power plant automation	Energy Development and Power Generation Committee of the IEEE Power & Energy Society	N/A	Voluntary	2013
ISA/IEC	ISA/IEC 62443	Security of Industrial Automation and Control Systems	ISA99 committee	62443	Voluntary	variable based on subsection
IEEE	IEEE 1686™-2022	Standard for Intelligent Electronic Devices Cybersecurity Capabilities	Power System Communications and Cybersecurity Committee S1 Working Group, IEEE Power and Energy Society	N/A	Voluntary	2022

Sample of Database

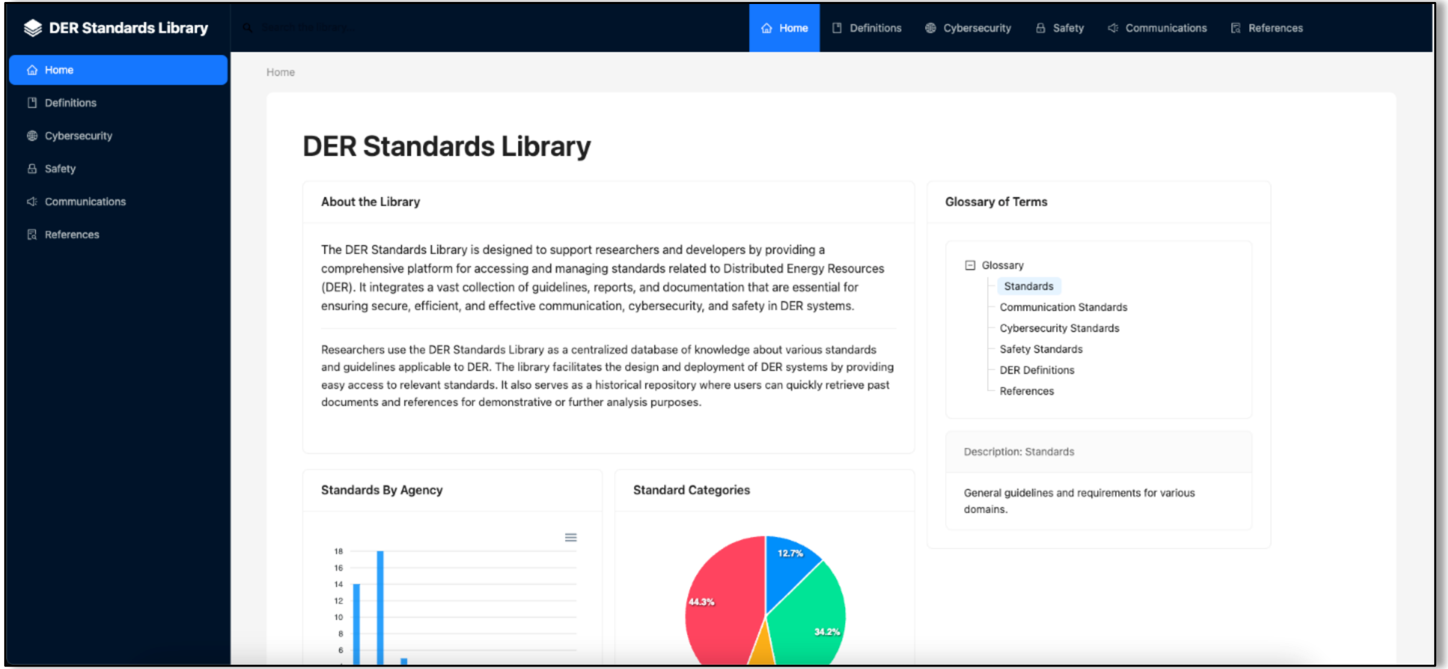


	L	M	N	T	U
1	**Applicability to DER Type**	**Intended Organizations**	**Related or Referenced Standards**	**Govern**	**Identify**
2	agnostic to specific DERs	Asset Owners and Operators, Original Equipment Manufacturers, Third-Party Suppliers, Systems Integrators, OT Services Providers, Cybersecurity Services Providers	IEC 60870-5 series (including IEEE 1815 (DNP3) as a derivative standard), the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. there is not a one-to-one correlation between the IEC TC57 communication protocol standards and the IEC 62351 security standards. This is because many of the communication protocols rely on the same underlying cybersecurity standards at different layers.		
3	hyroelectric plants	Asset Owners and Operators, Systems Integrators			
	agnostic to specific DERs, a 'horizontal' standard, supposed to apply across a broad range of industries, including electric sector all industry sectors that use IACS, including building automation, electric power generation and distribution, transportation, etc.	Asset Owners and Operators, Original Equipment Manufacturers, Third-Party Suppliers, Systems Integrators	ISO/IEC 27000 series; EU cybersecurity c	Part 1-3: System security conformance metrics; Part 2-1: Establishing an IACS security program; Part 2-2: IACS security program ratings; Part 2-3: Patch management in the IACS environment; Part 2-4: Security program	Part 1-4: IACS security lifecycle and use cases; Part 3-1: Security technologies

Web Interface (Beta)

Features under development:

- Look-up
- Keyword search
- Sorting by
- Group by NIST functions
- Compare
- Visualize
- Version history



DER Standards Library

About the Library

The DER Standards Library is designed to support researchers and developers by providing a comprehensive platform for accessing and managing standards related to Distributed Energy Resources (DER). It integrates a vast collection of guidelines, reports, and documentation that are essential for ensuring secure, efficient, and effective communication, cybersecurity, and safety in DER systems.

Researchers use the DER Standards Library as a centralized database of knowledge about various standards and guidelines applicable to DER. The library facilitates the design and deployment of DER systems by providing easy access to relevant standards. It also serves as a historical repository where users can quickly retrieve past documents and references for demonstrative or further analysis purposes.

Glossary of Terms

- Glossary
  - Standards
  - Communication Standards
  - Cybersecurity Standards
  - Safety Standards
  - DER Definitions
  - References

Description: Standards

General guidelines and requirements for various domains.

Standards By Agency

Standard Categories

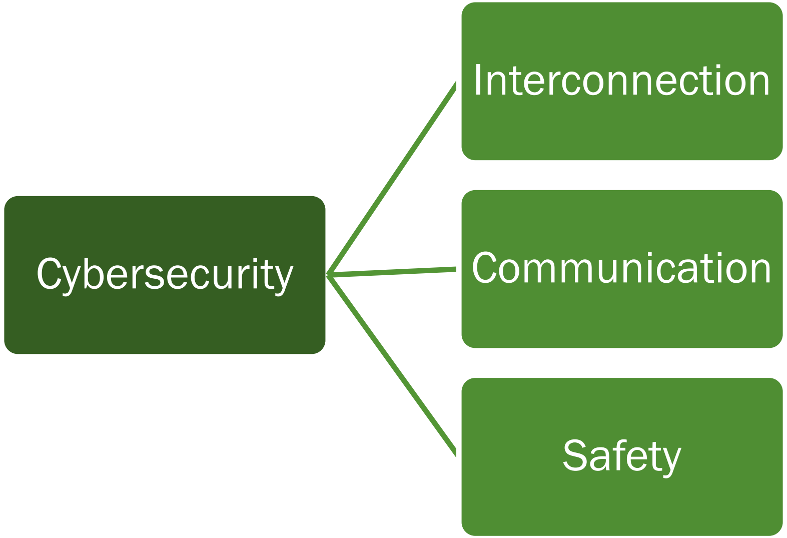
Proposed Approach for Cybersecurity Standards Harmonization

- **What is harmonization?**
  - The adoption of a consistent set of technical requirements that minimize redundant or conflicting standards that may have evolved independently.
    - Through this project, national labs intend to support harmonization for DER cybersecurity standards.

- **Why harmonization?**
  - Conflicting and divergent technical standards make it difficult to implement a cohesive DER cybersecurity policy
  - Diverse standards challenge a sector-wide approach that supports collective defense
  - Due to non-uniform regulations, DER ownership, operation, and maintenance is difficult to effectively manage cybersecurity risk across state lines (e.g., VPPs)
  - Establish guidance for smaller DER owners and operators who don’t have the resources to establish sound cyber controls on their own

Need for Harmonizing DER Cybersecurity Standards

- Few standards directly address cybersecurity for DERs.
- Some broader cybersecurity standards apply.
- Adjacent areas may include cybersecurity requirements.


Cybersecurity
Interconnection
Communication
Safety

Rapidly developing technology

Increasing reliance on DERs for grid reliability

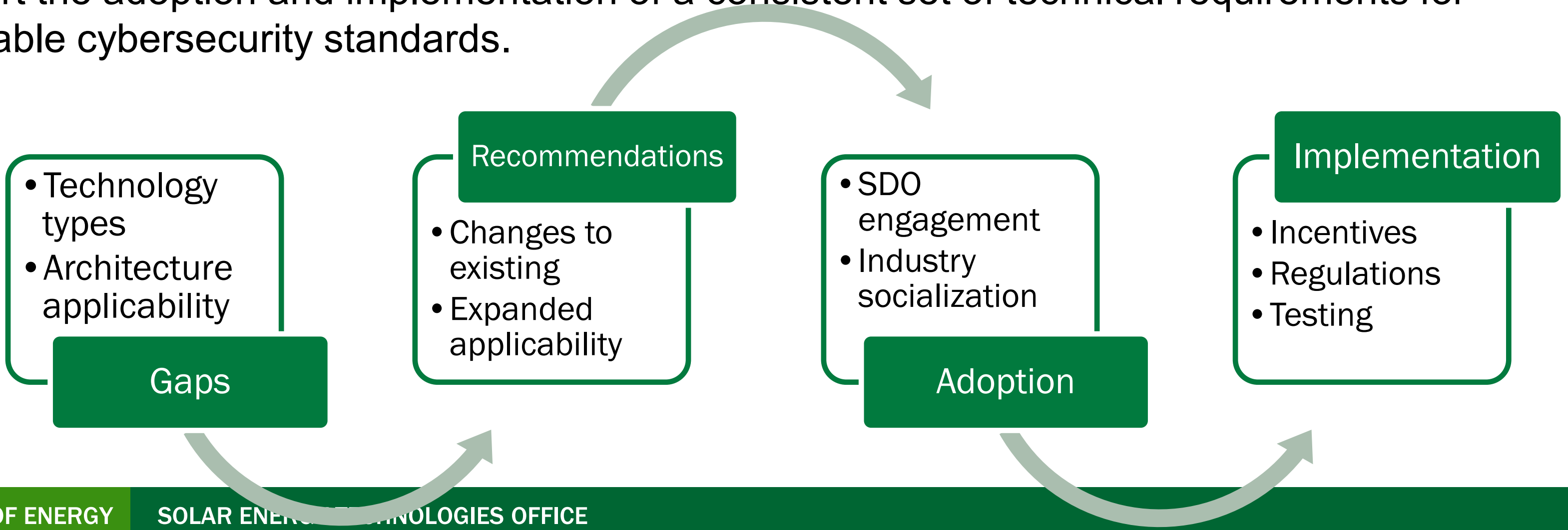
Diverse and complex stakeholder landscape

Non-uniform and/or not regulated policy among 50 states for IOU, co-ops, munis, aggregators or 3rd party

Full benefits of DERs reliant on digitization

How Can Harmonization be Achieved?

- Use the standards library to:
  - Create a one-stop-shop repository to gather and organize standards for reuse in a variety of ways, including the creation of learning modules, training, or testing guidance.
  - Easily share with a wide and diverse group of users.
  - Identify common elements and gaps to develop the harmonization strategy.
- Support the adoption and implementation of a consistent set of technical requirements for applicable cybersecurity standards.



Gaps
- Technology types
- Architecture applicability

Recommendations
- Changes to existing
- Expanded applicability

Adoption
- SDO engagement
- Industry socialization

Implementation
- Incentives
- Regulations
- Testing

Supporting a Harmonization Strategy

- Review, comment, and/or participate in working sessions on drafts of the standards library.
- Promote awareness among policymakers, standards developers, and technology developers of the strategic importance of standards harmonization.
- Help us understand how the implementation of a standards library can improve interoperability with assistive technologies and accelerate the overall progress of DER cybersecurity.
- Support the adoption and implementation of a consistent set of technical requirements for applicable cybersecurity standards.

Education & Workforce Development

Moderated by:
Megan Culler (INL)

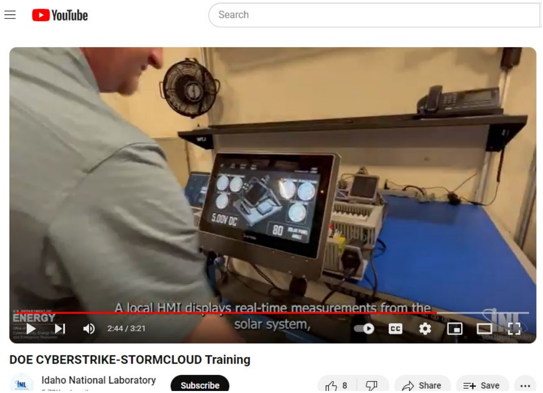
Ingrid Rayo
(Burns &
McDonnell)

Dr. Manimaran
Govindarasu (Iowa
State University)

Wajid Hassan
(Logic Finder)

CyberStrike STORMCLOUD

- **Accomplishments:**
  - Concept development for CESER buy-in
  - 8 hands-on lab exercises developed
  - Custom hardware kits designed and manufactured
  - 8-hour curriculum designed to pair cybersecurity concepts important for solar with real-world events
- **Trainings offered**
  - Half-day rollout at Secure Renewables ‘23
  - Two half-day trainings at DOE Energy Transitions Summit
  - Full-day training offered at 2024 IEEE PES GM
  - Half-day solar training offered at RE+ 24

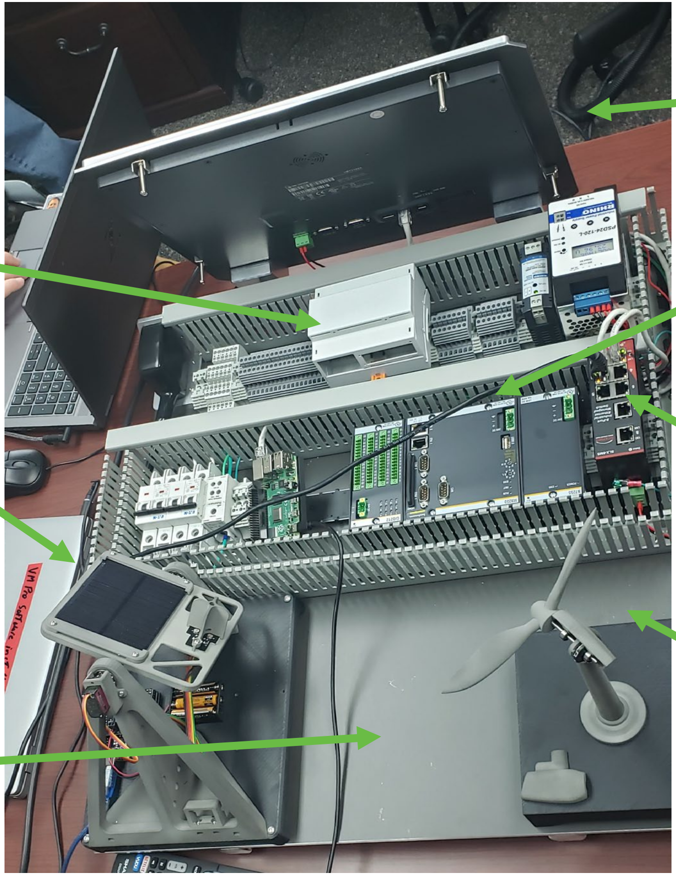


A local HMI displays real-time measurements from the solar system,

DOE CYBERSTRIKE-STORMCLOUD Training

Idaho National Laboratory

CyberStrike STORMCLOUD Training Kit



HMI

Solar “inverter” – Raspberry Pi emulator

Bachmann controller to be used for wind

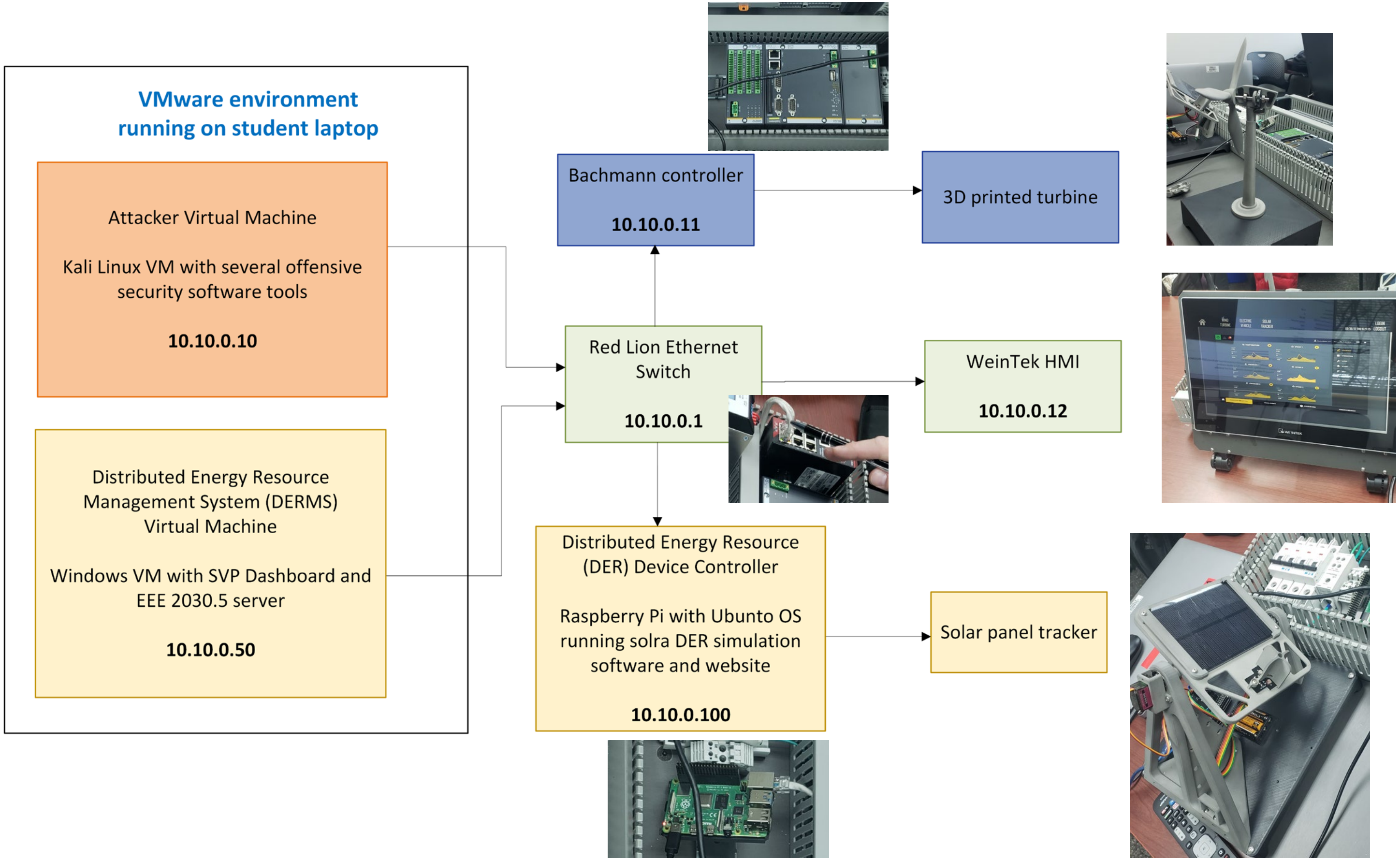
Network switch for the DER system

Single-axis solar

Open platform design to allow wind turbine to blow

Space for EV model

CyberStrike STORMCLOUD Architecture



VMware environment running on student laptop

Attacker Virtual Machine

Kali Linux VM with several offensive security software tools

10.10.0.10

Distributed Energy Resource Management System (DERMS) Virtual Machine

Windows VM with SVP Dashboard and EEE 2030.5 server

10.10.0.50

Bachmann controller

10.10.0.11

3D printed turbine

Red Lion Ethernet Switch

10.10.0.1

WeinTek HMI

10.10.0.12

Distributed Energy Resource (DER) Device Controller

Raspberry Pi with Ubunto OS running solra DER simulation software and website

10.10.0.100

Solar panel tracker

CyberStrike STORMCLOUD Agenda

STORMCLOUD Agenda

MODULE 1
Cyber Kill Chain

MODULE 2
Reconnaissance

MODULE 3
Protecting Critical Functionality

MODULE 4
Cryptology for OT Security

MODULE 5
Web Interfaces for DER

MODULE 6
Applications and APIs

MODULE 7
Data Injection

MODULE 8
Defense

Wrap Up
Conclusion

CyberStrike STORMCLOUD Labs

- Lab 1: Exploring & Exploiting DER Logical Interfaces
- Lab 2: Denial-of-Service
- Lab 3: Firmware Analysis
- Lab 4: Malicious Firmware Update
- Lab 5: Web Exploitation
- Lab 6: Applications and APIs
- Lab 7: Data Injection
- Lab 8: Defense

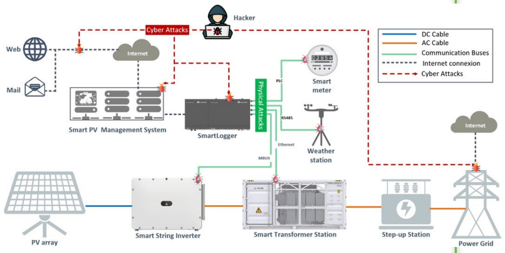
GridEx Storyboard – Solar Scenario

Sandia National Laboratories

Objective: Prepare a NERC/E-ISAC scenario. The scenario shall include a coordinated attack on DER assets.

Deliverable: Story board for how the scenario could be executed at a future event.

Attack Vectors:

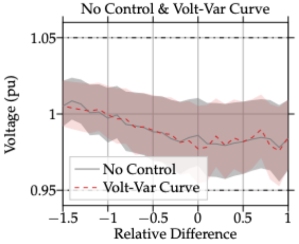


- Internet
- PV Management System Computers
- PV Logging Equipment
- Inverter communications

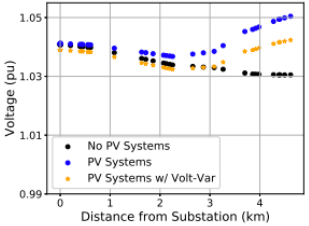
Harrou et al. Cybersecurity of Photovoltaic Systems: challenges, threats, and mitigation strategies: a short survey. Frontiers in Energy Research **2023**, *11*

Potential Impacts:

Small-scale PV found to have little impact on the distribution grid



Large-scale PV at single points on the grid can pose a risk to the distribution grid.



Jones, C.B.; Lave, M.; Reno, M.J.; Darbali-Zamora, R.; Summers, A.; Hossain-McKenzie, S. Volt-Var Curve Reactive Power Control Requirements and Risks for Feeders with Distributed Roof-Top Photovoltaic Systems. *Energies* **2020**, *13*, 4303

Potential Fixes:

Infrastructure:

mechanical

power electronics

Control:

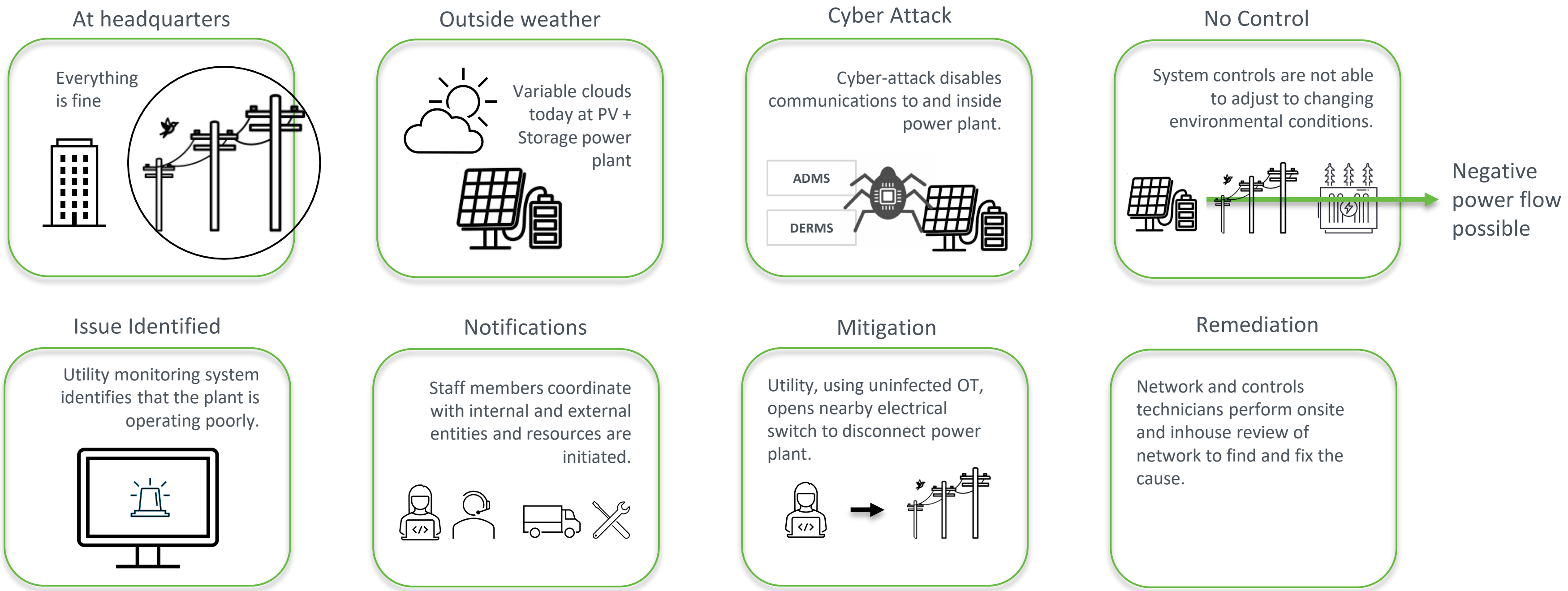
ADMS

DERMS

GridEx Storyboard – Solar Scenario

Sandia National Laboratories

Story board - Example



At headquarters

Everything is fine

Outside weather

Variable clouds today at PV + Storage power plant

Cyber Attack

Cyber-attack disables communications to and inside power plant.

No Control

System controls are not able to adjust to changing environmental conditions.

Negative power flow possible

Issue Identified

Utility monitoring system identifies that the plant is operating poorly.

Notifications

Staff members coordinate with internal and external entities and resources are initiated.

Mitigation

Utility, using uninfected OT, opens nearby electrical switch to disconnect power plant.

Remediation

Network and controls technicians perform onsite and inhouse review of network to find and fix the cause.

Workshops and Webinars

- SEIA Cybersecurity Working Group meetings
- Solar Supply Chain Workshop (Aug. 1, 2024)
- NASEO Energy Security Committee Meetings (upcoming)

Clean Energy Defenders (coming soon)

Objectives:

- Objective 1: Develop an extensible framework to develop curriculum and training modules, establish stakeholders' cohorts, and promote networking among clean energy stakeholders.
- Objective 2: Establish partnerships within stakeholders and DOE offices to support cybersecurity workforce development for clean energy technologies.
- Objective 3: Launch cohorts with tailored training modules for clean energy technologies.

Modules:

- Developing a cyber program
- Reporting requirements and NERC CIP applicability
- ICS4ICS – incident response training
- Threat briefings
- Supply chain management
- OT sensing and SOCs
- Working in cloud environments
- Red team/blue team exercises

Additional DOE and Lab Resources

- Liberty Eclipse
- CyberForce
- OT Defender
- Solar, Wind, & Fire Escape Room
- DOE Cybersecurity Awareness and Training (CSAT)

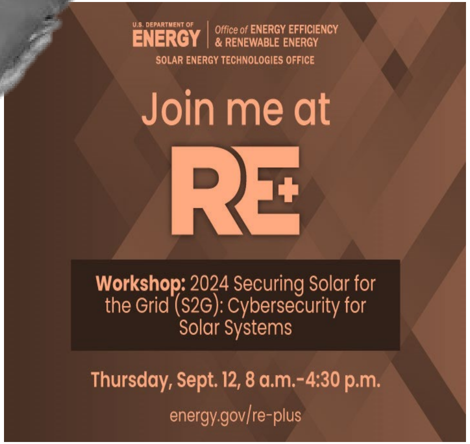
LIBERTY ECLIPSE
U.S. DEPARTMENT OF ENERGY

U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE COMPETITION®
DEFENDING U.S. ENERGY INFRASTRUCTURE

™ Operational Technology Defender Fellowship

1898 & CO
PART OF BURNS & McDONNELL

Education & Workforce Development



U.S. DEPARTMENT OF ENERGY | Office of ENERGY EFFICIENCY & RENEWABLE ENERGY
SOLAR ENERGY TECHNOLOGIES OFFICE

Join me at

RE+

Workshop: 2024 Securing Solar for the Grid (S2G): Cybersecurity for Solar Systems

Thursday, Sept. 12, 8 a.m.-4:30 p.m.

energy.gov/re-plus

Ingrid Rayo, GCIP, GICSP, DHS ILO*, VIRT*
Client Engagement Director
Security & Risk Consulting

281-733-4607

ingrid.rayo@1898andco.com

SAFETY, INCLUSION, & SECURITY MOMENT

EMBRACE DIVERSITY
1898 & CO.

Safety Moment

Cybersecurity 101: Top 5 Tips for Protecting Your Digital Life in 2 Minutes

1 **Strong, Unique Passwords**
15 alpha-numeric, special character.
Consider using a password manager.

2 **Beware of Phishing Scams**
Be vigilant and look out for suspicious emails/messages.
Don’t click on the links from unknown sources.

3 **Mindful about Sharing info**
Information is digital currency. Cybercriminals can use information about you to socially engineer you or your loved ones. Be mindful what you post and who can see it.

4 **Public Wi-Fi**
Avoid using public wi-fi. Use a VPN to encrypt your internet connection and protect your data.

5 **Use Two-Factor Authentication**
Add an extra layer of security by sending codes to your phone to enter with your password.

Stay safe and secure.

Stereotype Threat

- The expectation that one will be judged or perceived based on social identity group membership rather than actual performance and potential.

Techniques to Overcome Stereotype Threat

Feedback to level the playing field

Self-affirmation exercise

MAKE THEM **WORK** FOR IT

1 in 3 Americans experienced cyber crime in the past year.

BURNS McDONNELL

What Should You Do if you fall victim to a cyber crime?

1 **Change All Your Passwords**
Change all of your passwords, as soon as possible, using strong and unique passwords for each account.

2 **Contact Your Financial Institutions**
Important to contact your bank and/or credit card company immediately to report the incident and prevent any further unauthorized transactions

3 **Monitor Your Accounts and Personal Information**
Remain vigilant and monitor your accounts and personal information for any suspicious activity. Consider signing up for a credit monitoring or identify theft protection services to stay ahead of any potential risks.

About Ingrid

CE Director, Security Risk

Ingrid is a technically sophisticated and business-savvy information systems executive with a fast-track pioneering management and NERC Critical Infrastructure Protection (CIP) cyber security compliance career reflecting strong leadership qualifications coupled with "hands-on" re-engineering, troubleshooting, and networking expertise. She is results-driven with expertise envisioning and leading technology-based programs and growth initiatives grounded solidly on NERC CIP, NIST 800, ISO 27000, and corporate business standards. Ingrid drives organizations to maintain focus on achieving a solid sustainable cyber security compliance program while formulating and implementing advanced technology and business solutions to meet a diversity of needs. She demonstrates an ability to build peak-performing teams that are able to deliver large-scale, mission-critical CIP projects and roll-outs on time and under budget. Ingrid has provided technology-oriented advisement for numerous Fortune 500 companies across North America and possesses cross-industry expertise.

EDUCATION

BA, University of Tulsa

Microsoft Certified Systems Engineer, Southern Methodist University, School of Engineering and Applied Sciences (SEAS)

Project Management Professional, Florida Atlantic University

COMPLIANCE INDUSTRY EXPERIENCE

Global Industrial Cyber Security Professional (GICSP) – Analyst 140461 #133

GIAC Critical Infrastructure Protection (GCIP) – Analyst 140461 #75

Certified Information Systems Security Professional (CISSP) Training

Department of Homeland Security (DHS) Infrastructure Liaison Officer (ILO)

State of Texas Incident Response Team

GridEx Design and Planning Team

26 YEARS OF EXPERIENCE

12 Years with Burns & McDonnell

5 Years with IOUs

Driving Success with:

- Advanced Threat Protection Center
- Cyber Informed Engineering
- Governance, Risk, & Compliance
- Incident Response
- Managed Security Services
- NERC Compliance
- Security by Design
- Threat Hunting
- Vulnerability Assessments

1898 & CO.

POSSIBILITIES POWERED BY EXPERIENCE

SOLAR CYBERSECURITY

The intersection of solar energy and cybersecurity is a niche but growing area that requires a blend of skillsets to overcome technology, adoption, and implementation challenges in the field.

CHALLENGES

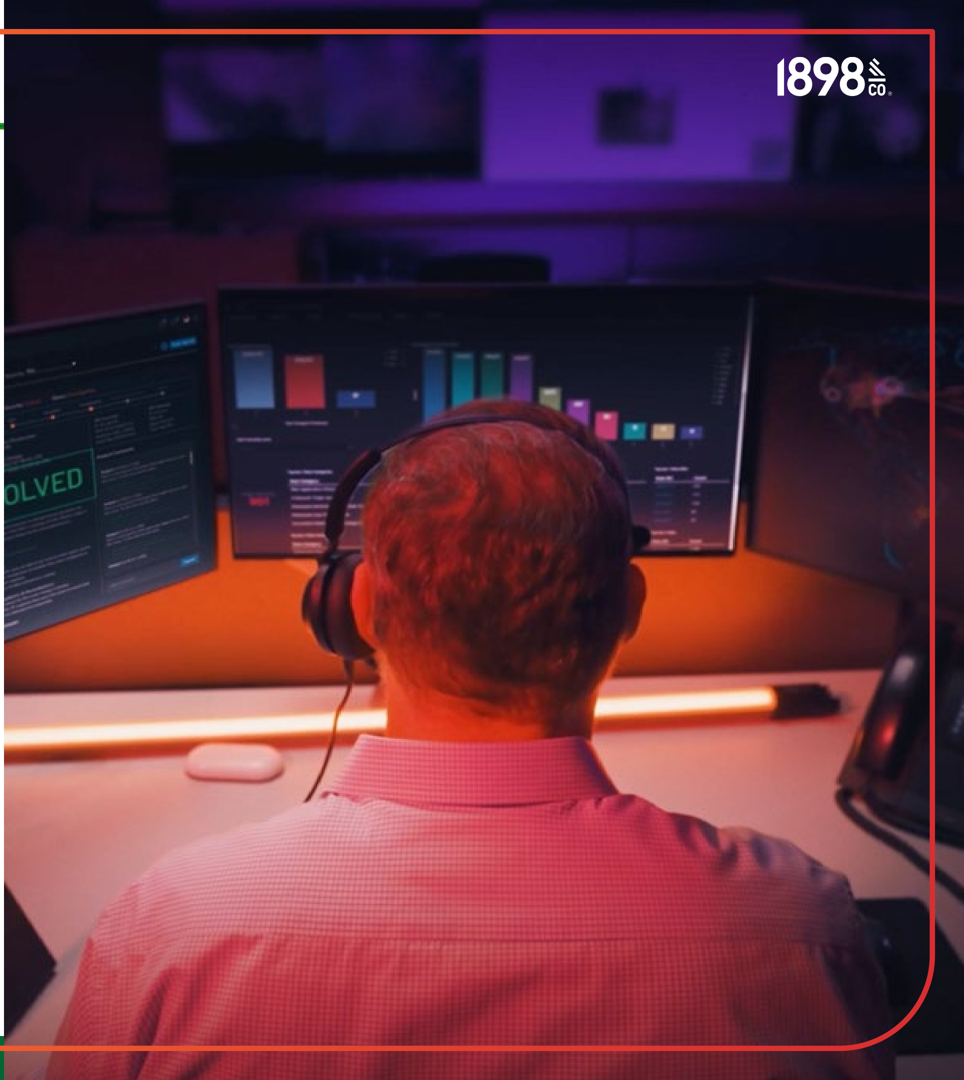
1. Rapid increase of solar installations
2. Technical advancements and functionality of supporting cyber assets
3. Owners, operators, and installers don’t understand the full breath and functionality of all assets in their environment
4. Most implementations are not designed with embedded cybersecurity controls
5. Remote access for management and monitoring is required

SOLAR CYBERSECURITY

The intersection of solar energy and cybersecurity is a niche but growing area that requires a blend of skillsets to overcome technology, adoption, and implementation challenges in the field.

SKILLS NEEDED

1. Inventorying capabilities with proper documentation
2. Understanding cyber asset capabilities
3. Data Flow and Communication understanding
4. In-depth understanding of cybersecurity controls and implementation
5. Network segmentation
6. Securing remote access
7. Patch management
8. Supply chain management
9. Information gathering and sharing
10. Cybersecurity framework implementation



TRUSTED PARTNER

COMPANY OVERVIEW

Global Practice Collaboration

A&F

CDB

PWR

E98

1898 & CO.

GFS

TND

CONVERGENCE OF IT & OT
EVER-INCREASING DATA CREATION & UTILIZATION
NEW ROLE OF THE CUSTOMER
EVOLVING WORKFORCE
INCREASING DEMANDS FOR PERFORMANCE & RELIABILITY
INCREASING SECURITY THREATS & EXPOSURE POINTS
BUSINESS MODEL EVOLUTION

WHO WE ARE

40+ LOCATIONS

including international offices in Canada, England, India, & Mexico

500+ EMPLOYEES

spanning business, cybersecurity, data, digital, engineering, finance, planning, & strategy

25+ YRS. EXPERIENCE

serving critical infrastructure industries

OUR CLIENTS

GOVERNMENT, MILITARY & MUNICIPAL

MANUFACTURING & INDUSTRIAL

OIL, GAS & CHEMICAL

PORTS & MARITIME

POWER

TRANSPORTATION

WATER

BUSINESS STRATEGY & TRANSFORMATION

INDUSTRIAL CYBERSECURITY

ASSET PLANNING & MANAGEMENT

ACQUISITION & DIVESTMENT

1898 & Co. is a business, technology and security consultancy that plans, secures, and optimizes critical infrastructure organizations.

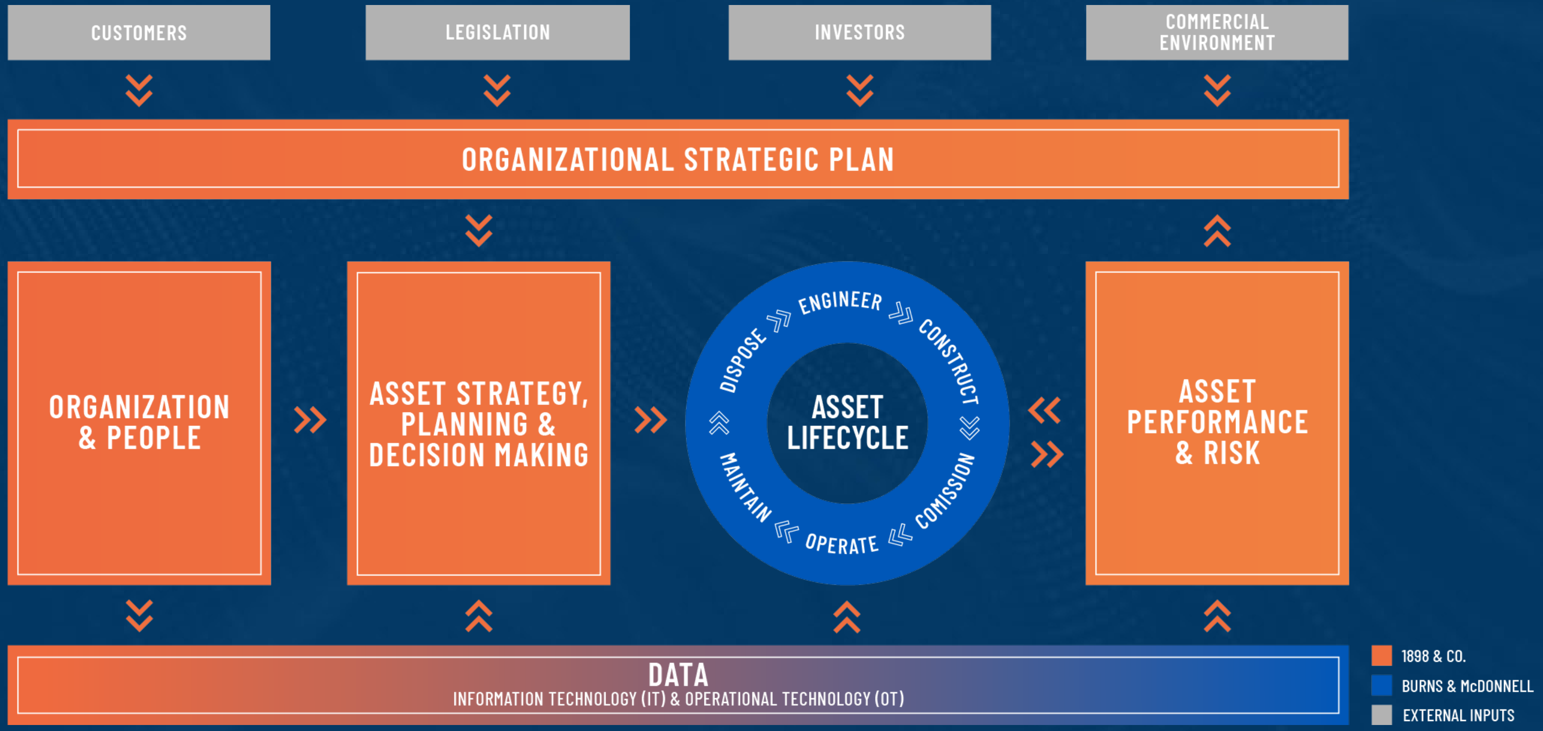
DATA & ANALYTICS

ENTERPRISE TECHNOLOGY

FINANCIAL ANALYSIS

POLICY & REGULATORY

UNIQUELY POSITIONED TO SERVE ASSET-INTENSIVE ORGANIZATIONS...



CUSTOMERS

LEGISLATION

INVESTORS

COMMERCIAL ENVIRONMENT

ORGANIZATIONAL STRATEGIC PLAN

ORGANIZATION & PEOPLE

ASSET STRATEGY, PLANNING & DECISION MAKING

ASSET LIFECYCLE

ENGINEER

CONSTRUCT

COMISSION

OPERATE

MAINTAIN

DISPOSE

ASSET PERFORMANCE & RISK

DATA

INFORMATION TECHNOLOGY (IT) & OPERATIONAL TECHNOLOGY (OT)

🟧 1898 & CO.

🟦 BURNS & McDONNELL

⬜ EXTERNAL INPUTS

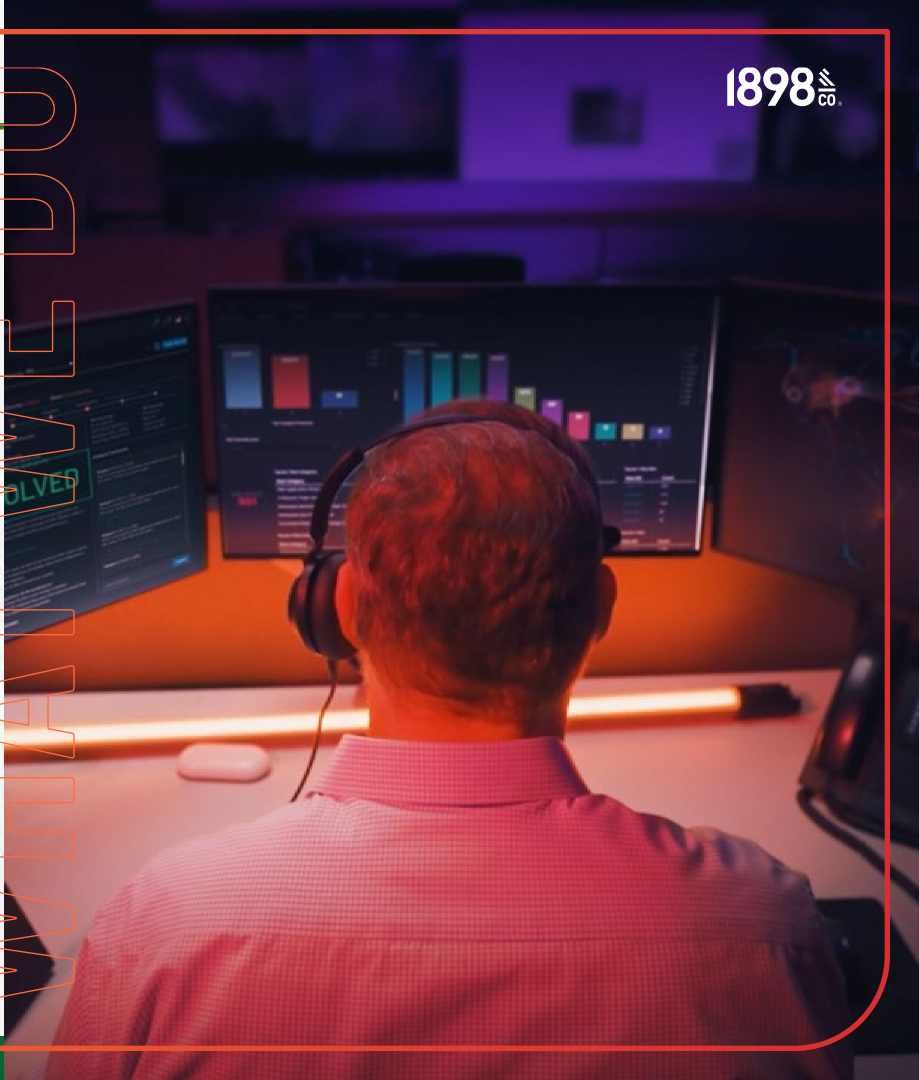
INDUSTRIAL CYBERSECURITY

Keep critical assets secure and operational with a comprehensive portfolio of services from high-level assessments to fully managed security services designed for operational technology applications.

FOCUS AREAS:

- Business Outcome Solutions
- Cybersecurity Executive Advisory Services
- Design, Protect, Optimize

WHAT WE DO



1898 & CO.

Offerings We Provide

Facility Cyber Design

Facility-Related Control Systems and Cyber Design Support and advisory services. Extensive experience in UFC 4-010-06 and UFGS Specifications for Federal Facilities.

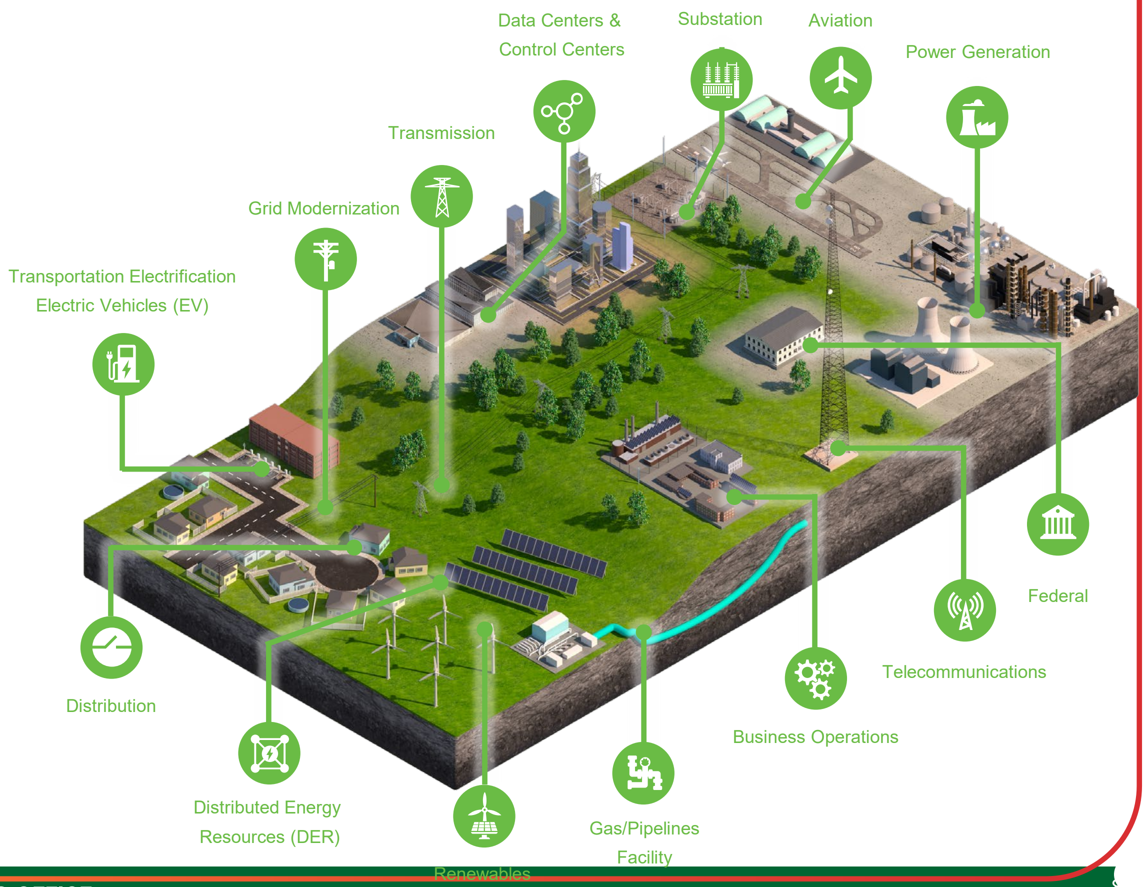
Facility & Cyber Systems Commissioning

Validating the installation, functionality, and performance of physical infrastructure and digital systems, involving testing, documentation, and training to improve reliability and alignment with standards and specifications.
Extensive experience in UFC 4-010-06 and UFGS Specifications.

Accreditation Services / RMF Support

Service delivery model for governance,
risk management, & compliance with DoD required risk management framework.

Assets We Support



1898 & CO℠

PART OF BURNS & McDONNELL

Grid-DER Cybersecurity Education & Training @ Iowa State University

University Education	Industry Training
Curricular Modules	Tutorials and Industry Learning Modules
Hands-on Lab-based Training	Hands-on Lab-based Industrial Training
Testbed-based Projects	Testbed deployments & Demos
Testbed Attack-Defense Exercise	Table-Table Exercise
Attack Modules, Defense Modules, Libraries, Datasets	Testbed-based Attack-Defense Exercise
Research Experimentations	Industry Webinars

Manimaran Govindarasu
Distinguished Professor
Iowa State University

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Acknowledgement - Funding Support

U.S. DOE SETO project DE-EE0008773 (completed)

- Enhancing grid reliability and resilience through novel DER control, total situational awareness and integrated distribution-transmission representation

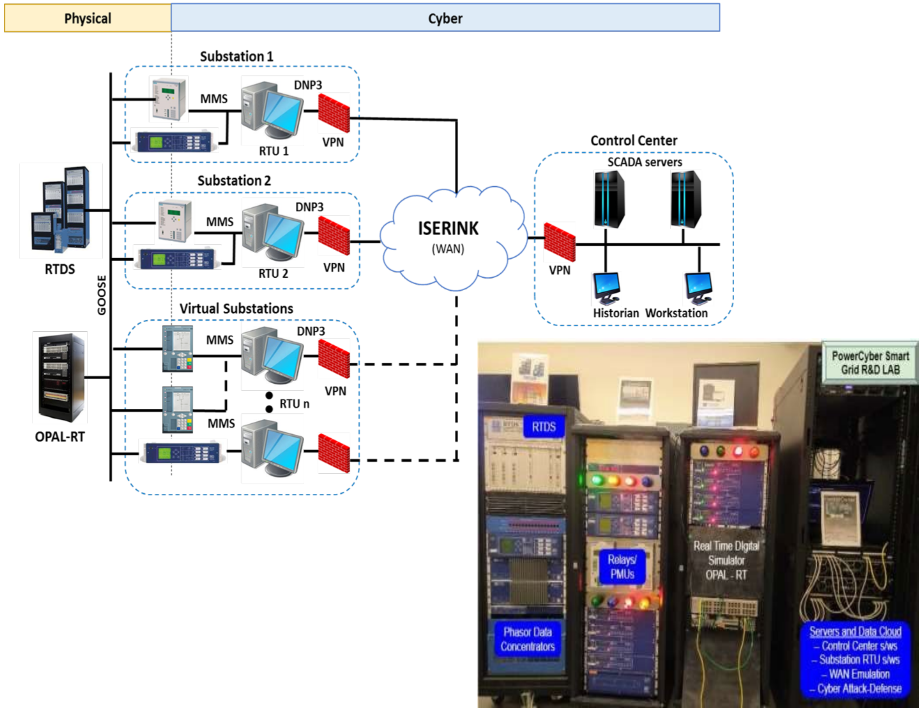
U.S. DOE CESER Award# DE-CR0000040 (ongoing)

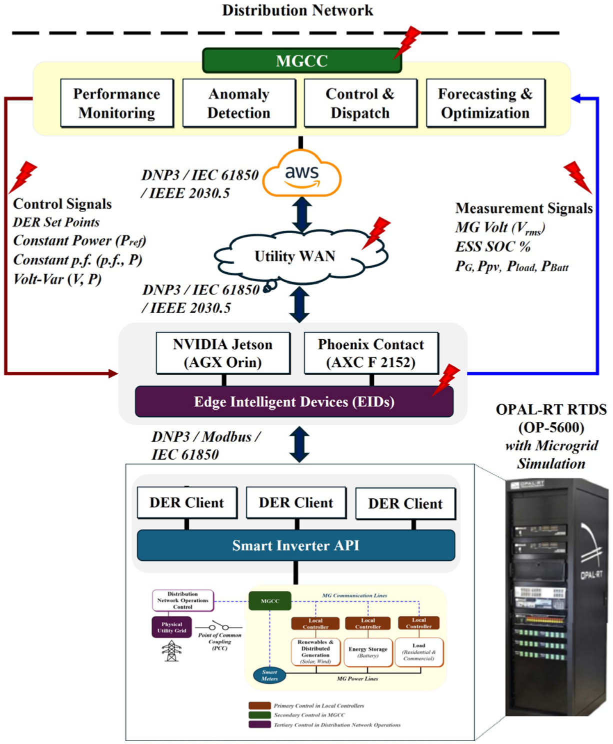
- CyDERMS: Center for Cybersecurity & Resiliency of DERs and Microgrids Integrated Distribution Systems

U.S. DOE CESER Award# DE-CR0000049 (ongoing)

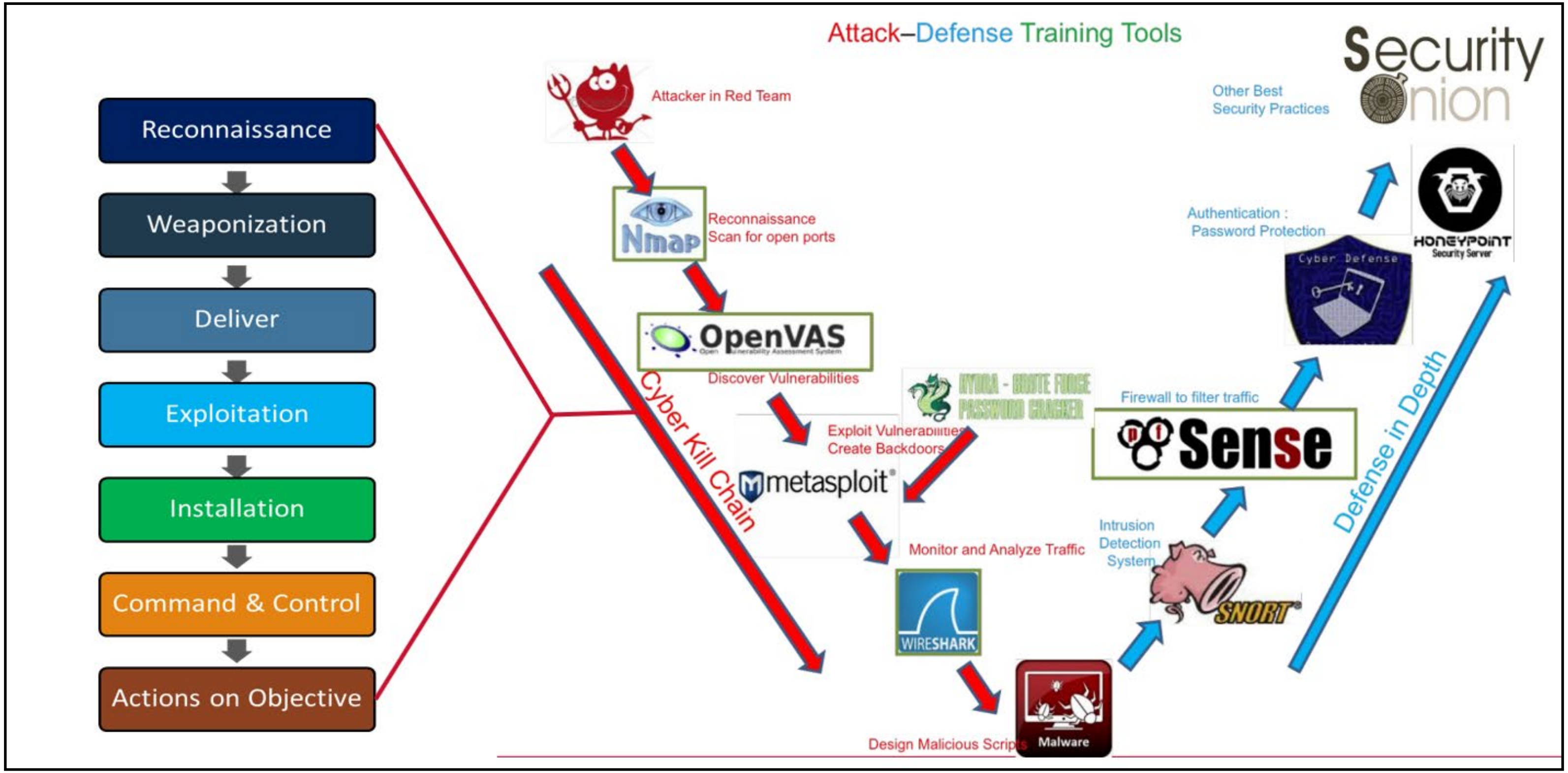
- ZT-CARD: Zero Trust integrated Real-Time Cybersecurity Situational Awareness and Attack Resilience for DER Networks

DER-Microgrid CPS PowerCyber Testbed @ISU




Distribution Network
MGCC
Performance Monitoring
Anomaly Detection
Control & Dispatch
Forecasting & Optimization
Control Signals
DER Set Points
Constant Power (P_{ref})
Constant p.f. (p.f., P)
Volt-Var (V, P)
DNP3 / IEC 61850 / IEEE 2030.5
aws
Utility WAN
DNP3 / IEC 61850 / IEEE 2030.5
Measurement Signals
MG Volt (V_{rms})
ESS SOC %
P_G, P_{pv}, P_{load}, P_{Batt}
NVIDIA Jetson (AGX Orin)
Phoenix Contact (AXC F 2152)
Edge Intelligent Devices (EIDs)
DNP3 / Modbus / IEC 61850
OPAL-RT RTDS (OP-5600) with Microgrid Simulation
DER Client
DER Client
DER Client
Smart Inverter API
Distribution Network Operations Control
Physical Utility Grid
Point of Common Coupling (PCC)
MGCC
MG Communication Lines
Local Controller
Local Controller
Local Controller
Renewables & Distributed Generation (Solar, Wind)
Energy Storage (Battery)
Load (Residential & Commercial)
Smart Meters
MG Power Lines
Primary Control in Local Controllers
Secondary Control in MGCC
Tertiary Control in Distribution Network Operations
OPAL-RT

Attack-Defense Training Modules



Attack–Defense Training Tools

Reconnaissance

Weaponization

Deliver

Exploitation

Installation

Command & Control

Actions on Objective

Cyber Kill Chain

Defense in Depth

Attacker in Red Team

Reconnaissance
Scan for open ports

Discover Vulnerabilities

Exploit Vulnerabilities
Create Backdoors

Monitor and Analyze Traffic

Design Malicious Scripts

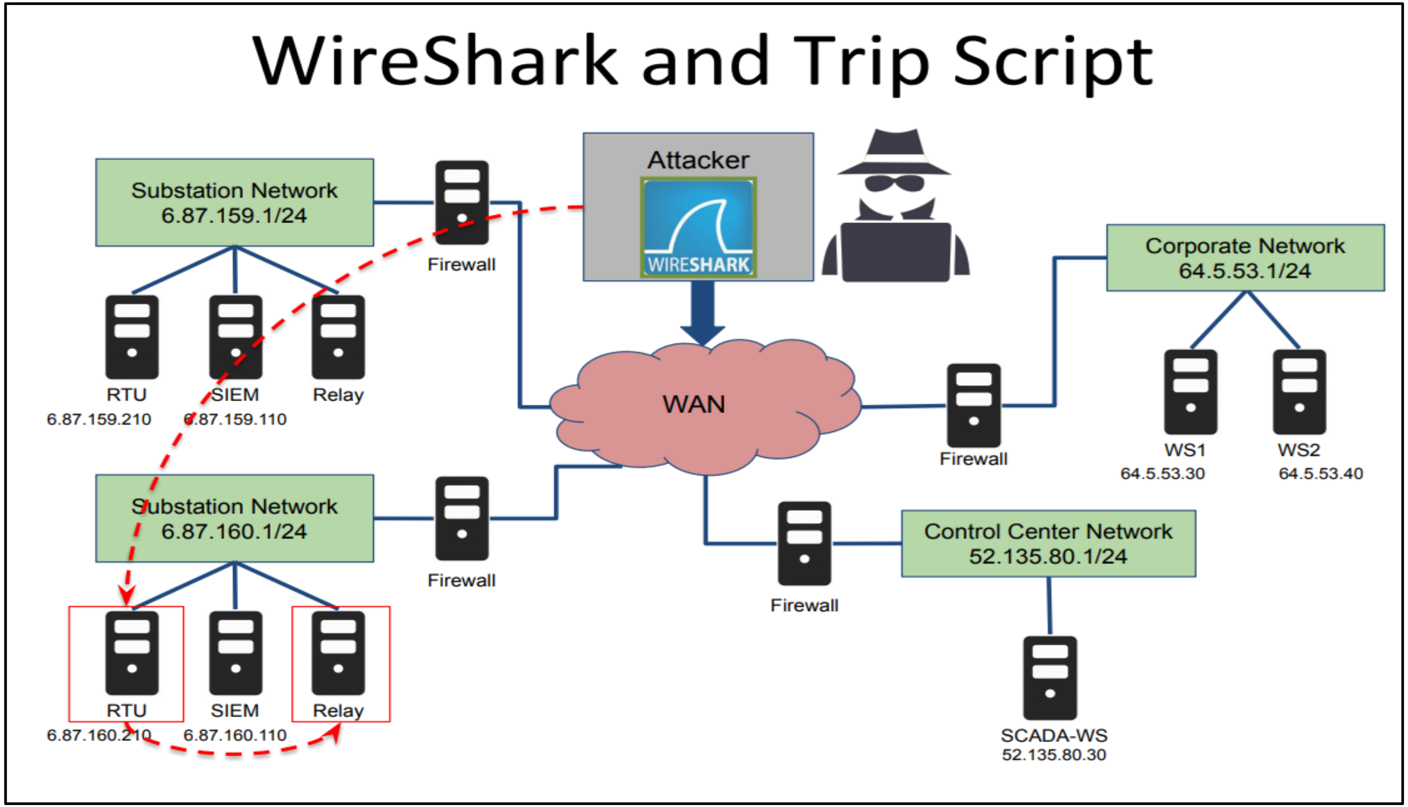
Intrusion
Detection
System

Firewall to filter traffic

Authentication :
Password Protection

Other Best
Security Practices

Sample Testbed-based Training Module



Challenges and Resolutions in Operational Technology (DER) CyberSecurity Workforce Development : Building a Resilient Organization

LogicFinder
Consulting, Development and Training

About me

Wajid is a veteran of IT Industry and an authority on CyberSecurity issues. Wajid is the CEO of LogicFinder and NetworkFort.

Previously he has worked at AT&T, T-Mobile, Amazon, Microsoft and with major governmental agencies on policy and technical positions.

His company LogicFinder has been providing IT, Software, Networking CyberSecurity Solutions to Commercial and Federal Clients .

Mr. Hassan has a Ph.D. in Technology Management and has industry respected certifications CISSP, Cisco Certified Internetwork Experts (CCIE) in Service Provider, Data Center, Security and Routing and Switching.

His current research focus is Zero Trust Architecture, Software Defined Networks, Machine Learning and Data Analytics.

The Growing Cyber Security Challenge in OT Space

Cyberattacks are on the rise, threatening organizations globally.

Addressing these challenges requires a comprehensive approach that includes:

- **Investment in Modern Technology:** Upgrading legacy systems and investing in modern, secure technology.
- **Collaboration and Information Sharing:** Encouraging collaboration and information sharing between IT and OT teams, as well as with industry peers and government agencies.
- **Implementing Best Practices:** Adopting cybersecurity best practices and frameworks, such as the NIST Cybersecurity Framework, to guide security efforts.
- **Regular Assessments and Audits:** Conducting regular security assessments and audits to identify and address vulnerabilities.
- **Enhanced Training and Education**: Providing ongoing training and education for OT personnel to increase cybersecurity awareness and skills.

LogicFinder
Consulting, Development and Training

Employer Perspective

Workforce development for cybersecurity in operational technology (OT) has several aspects

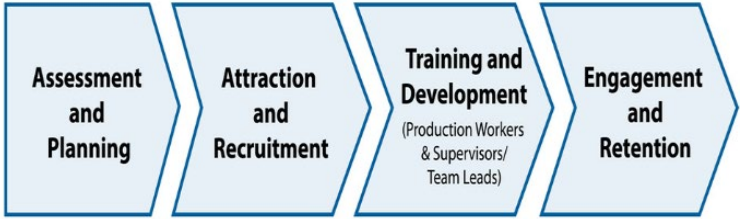
Assessment and Planning

Enhancing organizational performance is a top priority for manufacturers, and achieving this is nearly impossible without a well-trained workforce.

Attraction and Recruitment

A company’s ability to fill open positions is crucial for its long-term success. This involves:

- Developing a hiring plan to attract suitable candidates.
- Creating clear and concise job postings based on job descriptions to market the position effective
- Organizing and executing recruitment activities that reach a diverse range of candidates,
  - including underrepresented groups such as women, minorities, veterans, and displaced workers (DEI)



Assessment and Planning
Attraction and Recruitment
Training and Development
(Production Workers & Supervisors/ Team Leads)
Engagement and Retention

Training and Development

Providing training and skills development is essential for workforce growth and efficiency.

Engagement and Retention

- Engaging and retaining current staff is vital to maximize productivity and reduce turnover.
- Hiring and developing new staff is an investment, and engaging employees helps to maximize that investment.

Challenges for Cybersecurity Workforce Development

- **Skills Gap:** There is a significant shortage of professionals with the specialized skills needed for OT cybersecurity. This includes knowledge of both IT and OT systems, as well as specific cybersecurity expertise.

- **Legacy Systems:** Many OT environments rely on outdated technology that wasn't designed with cybersecurity in mind. This makes it difficult to implement modern security measures and requires specialized knowledge to secure

- **Integration of IT and OT:** The convergence of IT and OT systems creates complexities in defining roles and responsibilities. IT and OT teams often have different priorities and approaches, which can lead to conflicts and gaps in security coverage

- **Economic Constraints:** Budget limitations can hinder the hiring and retention of qualified cybersecurity professionals. Economic uncertainty has led to reduced investment in cybersecurity workforce development, making it harder to fill critical positions

- **Continuous Learning:** The rapidly evolving nature of cybersecurity means that professionals must continually update their skills. This requires ongoing training and development programs, which can be resource-intensive

- **Retention Issues:** Retaining skilled cybersecurity professionals is challenging due to high demand and competitive salaries in the industry. Organizations often struggle to keep their talent, leading to frequent turnover and knowledge loss.

Addressing these challenges requires a multifaceted approach, including investment in education and training, fostering collaboration between IT and OT teams, and creating attractive career paths to retain talent.

Opportunities (Training and Retention)

There are several promising opportunities for workforce development in cybersecurity for operational technology (OT), particularly in the context of Distributed Energy Resources (DERs):

- **CyberForce Competition®:** The Department of Energy's CyberForce Competition® is a hands-on event that engages students in realistic scenarios involving the defense of critical infrastructure, including DERs. This competition helps participants develop practical skills and gain experience in managing cyber-physical threats

- **OT Defender Fellowship:** This program offers specialized training for OT security managers, enhancing their ability to contribute to information sharing between government and industry. It focuses on developing skills necessary to protect critical infrastructure, including DERs

- **Collaborative Training Programs:** Partnerships between educational institutions and industry can create tailored training programs that address the specific needs of OT cybersecurity. These programs can include internships, co-op programs, and collaborative research projects.

Opportunities (Training and Retention)

LogicFinder
Consulting, Development and Training

- **Government Initiatives:** Increased funding and support from government agencies can help develop a skilled cybersecurity workforce. Programs like the National Cybersecurity Strategy aim to create a more secure and resilient energy sector by fostering professional development at the cyber/energy nexus.
- **Professional Development Workshops:** Regular workshops and webinars focused on OT and DER cybersecurity can help professionals stay updated with the latest threats and technologies. These events provide opportunities for networking and knowledge sharing.
- **Interdisciplinary Education:** Combining IT and OT training programs can bridge the gap between these fields, creating professionals who are well-versed in both areas. This is crucial for securing DERs, which often involve both IT and OT components
- **Mentorship Programs:** Establishing mentorship programs can provide guidance and support for individuals entering the field. Experienced professionals can help newcomers navigate the complexities of OT cybersecurity

By leveraging these opportunities, we can build a robust and capable workforce ready to tackle the unique challenges of cybersecurity in operational technology and distributed energy resources.

Resolutions

Addressing the challenges in workforce development for cybersecurity in operational technology (OT), especially for Distributed Energy Resources (DERs), requires a multifaceted approach. Here are some effective strategies:

- **Educational Programs and Competitions:** Initiatives like the Department of Energy's CyberForce Competition® provide hands-on experience in defending critical infrastructure, including DERs.
- **Collaboration Between Academia and Industry:** Partnerships between educational institutions and industry can create tailored training programs that address the specific needs of OT cybersecurity. This ensures that the curriculum is relevant and up-to-date.
- **Continuous Professional Development:** Offering ongoing training and certification programs helps professionals stay current with the latest cybersecurity threats and technologies. This can include workshops, webinars, and online courses focused on OT and DER cybersecurity.
- **Government and Industry Support:** Increased funding and support from government and industry can help develop and retain a skilled cybersecurity workforce. This includes scholarships, grants, and incentives for pursuing careers in OT cybersecurity.
- **Interdisciplinary Training:** Combining IT and OT training programs can bridge the gap between these traditionally separate fields. This helps create professionals who are well-versed in both areas, which is crucial for securing DERs.
- **Mentorship and Networking Opportunities:** Establishing mentorship programs and professional networks can provide guidance and support for individuals entering the field. This helps in knowledge sharing and career development.
- **Focus on Soft Skills:** In addition to technical skills, developing soft skills such as communication, teamwork, and problem-solving is essential. These skills are critical for effectively managing cybersecurity in complex OT environments

DEI approach to DER

JUSTICE40

2024 U.S. Energy & Employment Jobs Report (USEER)

These numbers are not for cybersecurity workforce which would be much lower!

- Veterans accounted for only **9%** of the U.S. energy workforce.
- The energy workforce is younger than average, with 29% of workers **below the age of 30.**
- Latino and Hispanic workers in new energy jobs stand at only **79,000 workers**

Justice40

- **Justice40** establishes the goal that **40%** of the overall benefits of certain federal investments flow to disadvantaged communities (DACs).

- **Justice40** Initiative applies to over **145 Department of Energy (DOE) programs** and to much of the **$62 billion** investment in DOE under the Bipartisan Infrastructure Law.

- We need to start thinking in DOE/CyberSecurity space on how to approach **Justice 40** for Workforce Development funding and a DEI approach to DER.

Diversity , Equity and Inclusion

One of the important aspects of workforce development is Diversity, Equity, and Inclusion (DEI) . It is is crucial for several reasons:

- **Addressing Talent Shortages:** The cybersecurity industry faces a significant talent shortage, with nearly 500,000 open positions in the U.S. alone. Attracting diverse candidates can help fill these gaps.
- **Improving Security Outcomes:** A diverse workforce brings varied perspectives and experiences, which can lead to more innovative solutions and stronger security outcomes.
- **Enhancing Organizational Performance:** Studies have shown that diverse teams perform better and are more effective at problem-solving.
- **Reflecting Global Demographics:** The current demographics in cybersecurity are not representative of the broader population. For example, women make up only 24% of the cybersecurity workforce, and underrepresented groups such as Black and Hispanic professionals are also significantly underrepresented
- **Creating Inclusive Work Environments:** Fostering an inclusive environment where all employees feel valued and supported can improve retention and job satisfaction.
- **Efforts to improve DEI in cybersecurity include:**
  - Recruitment and Retention: Focusing on hiring diverse candidates and providing them with opportunities for growth and leadership
  - Education and Training: Developing programs to educate and train underrepresented groups in cybersecurity skilIS.
  - Policy and Leadership: Implementing policies that promote DEI and ensuring leadership is committed to these values

Case Study - Electric Power company

- We assisted an Electric Power Company with a cybersecurity and infrastructure upgrade project, during which they transitioned 30% of their energy generation to solar.

- In the process, we identified that two of their most pressing challenges are their outdated Operational Technology and their technical staff.

The Need for Workforce Development

- Workforce development leads to a more engaged, skilled, and loyal workforce, aligned with your organization’s mission.

- External recruitment is not sufficient to address the talent shortage.

- Developing internal talent is essential to bridge the cybersecurity skills gap.

Strategic Partnerships for Comprehensive Support

LogicFinder
Consulting, Development and Training

NREL
Transforming ENERGY

INL
Idaho National Laboratory

Booz Allen

DEPARTMENT OF LABOR
UNITED STATES OF AMERICA

Commonwealth Cyber Initiative

Pacific Northwest
NATIONAL LABORATORY

OAK RIDGE
National Laboratory

Brookhaven
National Laboratory

Virginia Values Veterans
Official V3 Certified Company

SKILLSPIRE
YOU ASPIRE, WE INSPIRE

VIRGINIA
TALENT + OPPORTUNITY PARTNERSHIP

APPTEON

DEPARTMENT OF LABOR AND INDUSTRY

EOPA
Elected Officials to Protect America

TheCyberGuild

PWCS
PRINCE WILLIAM COUNTY PUBLIC SCHOOLS
LAUNCHING THRIVING FUTURES

SCIPP INTERNATIONAL™
THE SECURITY AWARENESS CERTIFICATION COMPANY

INTERNATIONAL RESCUE COMMITTEE

Industry Associations

nvtc
NORTHERN VIRGINIA TECHNOLOGY COUNCIL

AFCEA

act-iac
Accelerating Government

MIT HORIZON

Open
WASHINGTON DC

FAIRFAX COUNTY
ECONOMIC DEVELOPMENT AUTHORITY

Lunch Break

- Room 240B
- Please return at 12:55

Agenda - Afternoon

Time	Session Title	Location
12:00-1:00	LUNCH	240B
1:00-2:00	Cybersecurity Tool Kit	211A
2:00-2:15	BREAK	Lobby
2:15-3:15	Asset and Vulnerability Management	211A
3:15-4:15	Breakout Sessions	211A
4:15-4:30	Closing Remarks	211A

Cybersecurity Tool Kit

Moderated by:
Scott Mix (PNNL)

Daniel Ricci (INL)

Dr. Shuchimita
“Shuchi” Biswas
(PNNL)

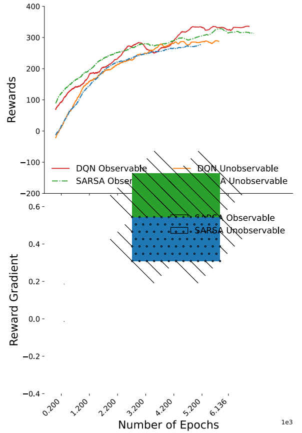
Matthew Hartung
(EDPR)

Artificial Intelligent-Driven Threats (Sandia)

Develop: Artificial Intelligent (AI) Adversary Agents

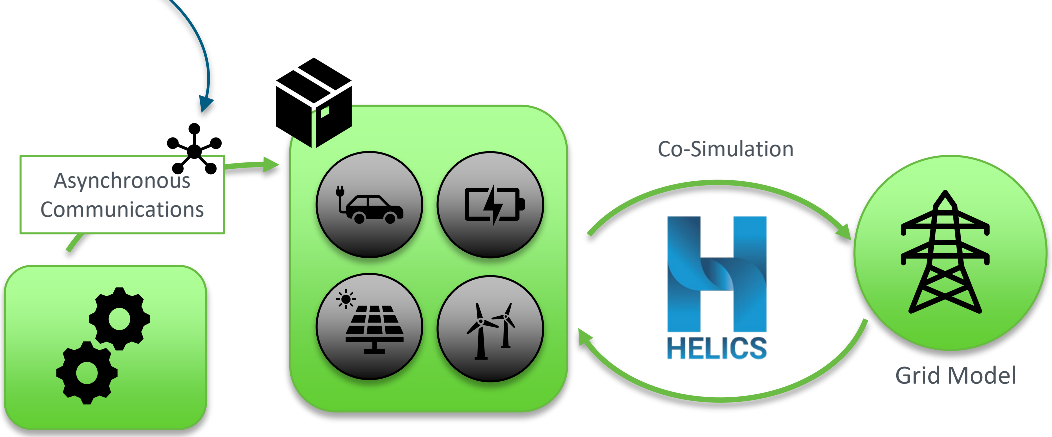
Deploy agents to test AI's capabilities and define best practice for avoiding/stopping threats.

Reinforcement Learning Threat Implementation Experiments



Initial results, from tests in a synthetic environment provide evidence of AI's potential to transverse networks and exploit vulnerabilities in DER devices and networks.

Development, Operate and Share: Cyber-Physical Testbed



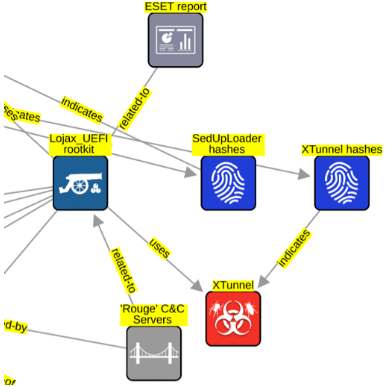
Distributed Energy Resource Management System (DERMS)

Hundreds of Containerized Distributed Energy Resources

Contact:
C. Birk Jones, Ph.D.
cbjones@sandia.gov

Codified Attack Surface with NLP (INL)

Goal: Create an Enduring Life-Cycle Knowledge Base for Solar-Cyber Data Model Using Natural Language Processing (NLP) and Codified Attack Surfaces (CAS)



- Automate Solar Inverter Notional CAS
- Repeatable Scripting Process for Infrastructure CAS
- Integrated into FY23's CAS Enrichment
- Notional Applicability Analysis to Emerging Cyber Threats

Challenges:

- CAS requires manual activity prone to error
- Scrapping data techniques does not handle tables & technical specifications
- Concept of linking Original Equipment Manufacturer (OEM) is complex due to
  - a) Variations in product names, versioning, and releases
  - b) OEM mergers, OEM and product names change

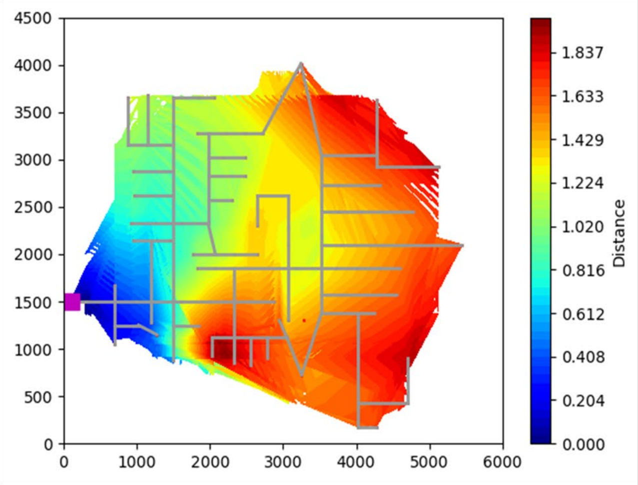
Technologies:

- Graph Data Structures, Graph Analytics, Traversals and Knowledge Base, Data Atom Structures
- Natural Language Processing, Web and/or Document Scrapping of data

Contact:
Rita Foster
rita.foster@inl.gov

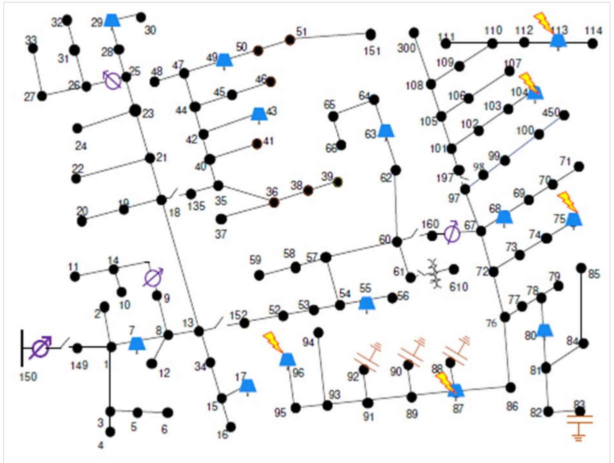
Distribution Model DER Assessments (PNNL)

Solar DER Model Analysis and Assessment



Criticality level of various nodes based on location (distance from substation) and DER injections.

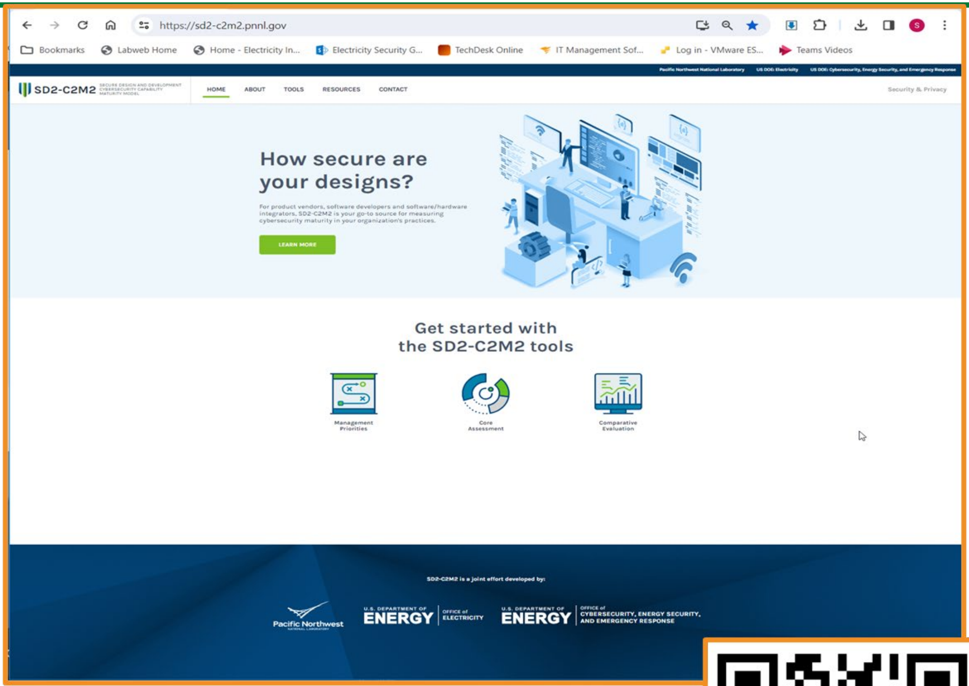
Scan for model information and paper



Most sensitive PVs are located farthest from the substation (i.e., buses 104, 113, 75, 96, and 87).

Contact:
Manisha Maharjan
manisha.maharjan@pnnl.gov

SD2-C2M2 Assessments (PNNL)


https://sd2-c2m2.pnnl.gov
Bookmarks
Labweb Home
Home - Electricity In...
Electricity Security G...
TechDesk Online
IT Management Sof...
Log in - VMware ES...
Teams Videos
Pacific Northwest National Laboratory
US DOE: Electricity
US DOE: Cybersecurity, Energy Security, and Emergency Response
SD2-C2M2
SECURE DESIGN AND DEVELOPMENT CYBERSECURITY CAPABILITY MATURITY MODEL
HOME
ABOUT
TOOLS
RESOURCES
CONTACT
Security & Privacy
LEARN MORE
Management Priorities
Core Assessment
Comparative Evaluation
Pacific Northwest NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY | OFFICE of ELECTRICITY
U.S. DEPARTMENT OF ENERGY | OFFICE of CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

How secure are your designs?

For product vendors, software developers and software/hardware integrators, SD2-C2M2 is your go-to source for measuring cybersecurity maturity in your organization's practices.

Get started with the SD2-C2M2 tools

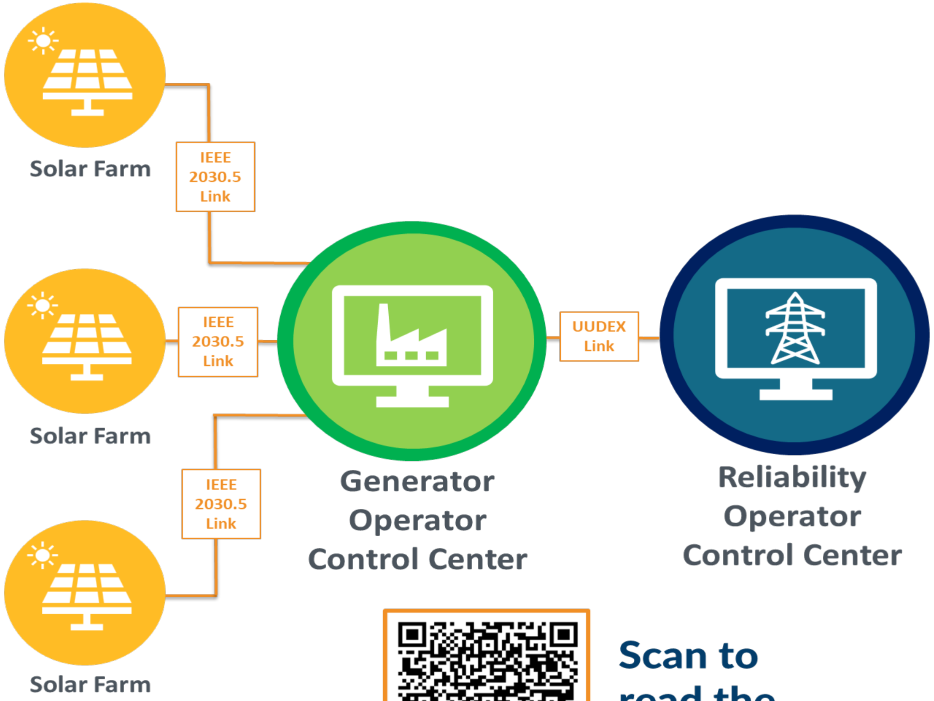
SD2-C2M2 is a joint effort developed by:

Solar Vendor Design and Development Self-Assessments.

Scan QR code to access the tool.

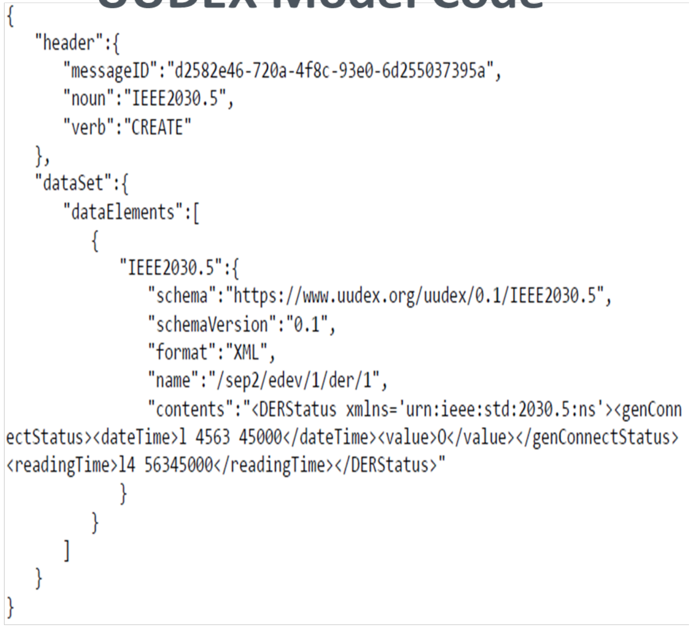
Contact:
Scott Mix
scott.mix@pnnl.gov

UUDEX Models for DER Information Exchange (PNNL)



Scan to read the report

UUDEX Model Code



```
{
   "header":{
      "messageID":"d2582e46-720a-4f8c-93e0-6d255037395a",
      "noun":"IEEE2030.5",
      "verb":"CREATE"
   },
   "dataSet":{
      "dataElements":[
         {
            "IEEE2030.5":{
               "schema":"https://www.uudex.org/uudex/0.1/IEEE2030.5",
               "schemaVersion":"0.1",
               "format":"XML",
               "name":"/sep2/edev/1/der/1",
               "contents":"<DERStatus xmlns='urn:ieee:std:2030.5:ns'><genConn
ectStatus><dateTime>l 4563 45000</dateTime><value>0</value></genConnectStatus>
<readingTime>l4 56345000</readingTime></DERStatus>"
            }
         }
      ]
   }
}
```

Universal Utility Data Exchange (UUDEX) Models for DER Information Exchange.

Contact:
Scott Mix
scott.mix@pnnl.gov

INL Cyber SHIELD-INL CSET for Renewables (INL)

INL Cybersecurity Evaluation and Risk Tool

Key Challenges Targeted

Provide insight and guidance for better-informed risk-based investment decisions for renewable asset owners'/operators' IT and OT cybersecurity programs through Cybersecurity Evaluation Tool (CSET) for Renewable (Open-Source DHS CISA/DOE funded tool for public use)

Key features:

✓ Renewable Sector Focused Capability

✓ Tuned for renewable industry

✓ Identifies gaps in Cybersecurity process and procedures

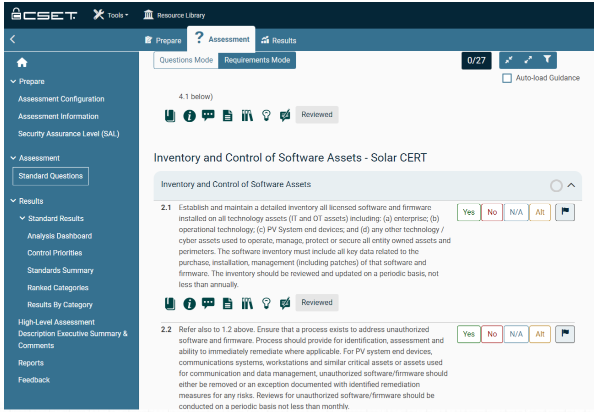
Top 3 Benefits:

1 Guided cybersecurity assessment and risk-based report

2 Map network architecture within the purview of the assessment to control areas to help identify or validate asset owner/operator cyber posture

3 Support cyber program and resource planning to accelerate asset owner/operator Cybersecurity maturity objectives and readiness by providing document templates and process flows to integrate with existing organization configuration management, maintenance, incident response and recovery procedures

CSET Program Assessment



4.1 below)

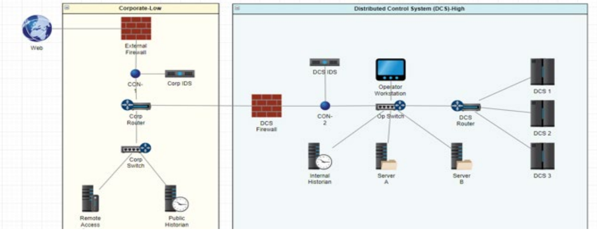
Inventory and Control of Software Assets - Solar CERT

Inventory and Control of Software Assets

2.1 Establish and maintain a detailed inventory all licensed software and firmware installed on all technology assets (IT and OT assets) including: (a) enterprise; (b) operational technology; (c) PV System end devices; and (d) any other technology / cyber assets used to operate, manage, protect or secure all entity owned assets and perimeters. The software inventory must include all key data related to the purchase, installation, management (including patches) of that software and firmware. The inventory should be reviewed and updated on a periodic basis, not less than annually.

2.2 Refer also to 1.2 above. Ensure that a process exists to address unauthorized software and firmware. Process should provide for identification, assessment and ability to immediately remediate where applicable. For PV system end devices, communications systems, workstations and similar critical assets or assets used for communication and data management, unauthorized software/firmware should either be removed or an exception documented with identified remediation measures for any risks. Reviews for unauthorized software/firmware should be conducted on a periodic basis not less than monthly.

CSET Architecture Basics

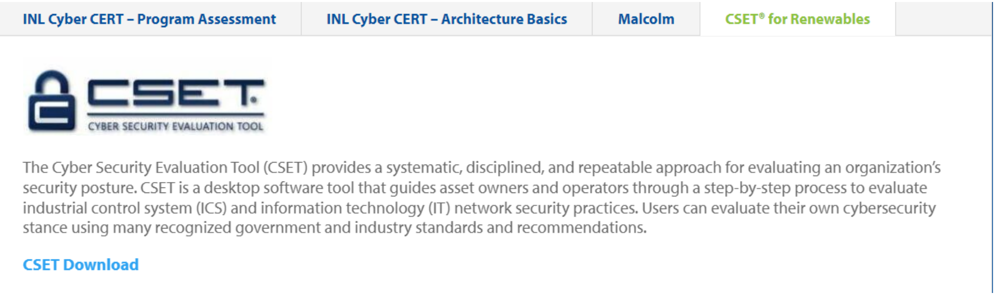


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Network Diagram

What are the Benefits of CSET for Renewables? (INL)

CSET for Renewables

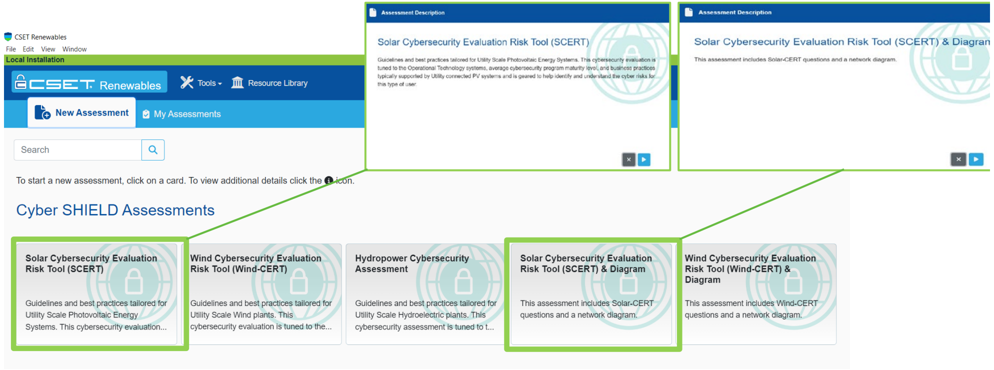


INL Cyber CERT – Program Assessment | INL Cyber CERT – Architecture Basics | Malcolm | CSET® for Renewables

CSET CYBER SECURITY EVALUATION TOOL

The Cyber Security Evaluation Tool (CSET) provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. CSET is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate industrial control system (ICS) and information technology (IT) network security practices. Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations.

CSET Download



To start a new assessment, click on a card. To view additional details click the ⓘ icon.

Cyber SHIELD Assessments

Solar Cybersecurity Evaluation Risk Tool (SCERT)
Guidelines and best practices tailored for Utility Scale Photovoltaic Energy Systems. This cybersecurity evaluation...

Wind Cybersecurity Evaluation Risk Tool (Wind-CERT)
Guidelines and best practices tailored for Utility Scale Wind plants. This cybersecurity evaluation is tuned to the...

Hydropower Cybersecurity Assessment
Guidelines and best practices tailored for Utility Scale Hydroelectric plants. This cybersecurity assessment is tuned to t...

Solar Cybersecurity Evaluation Risk Tool (SCERT) & Diagram
This assessment includes Solar-CERT questions and a network diagram.

Wind Cybersecurity Evaluation Risk Tool (Wind-CERT) & Diagram
This assessment includes Wind-CERT questions and a network diagram.

Assessment Description

Solar Cybersecurity Evaluation Risk Tool (SCERT)

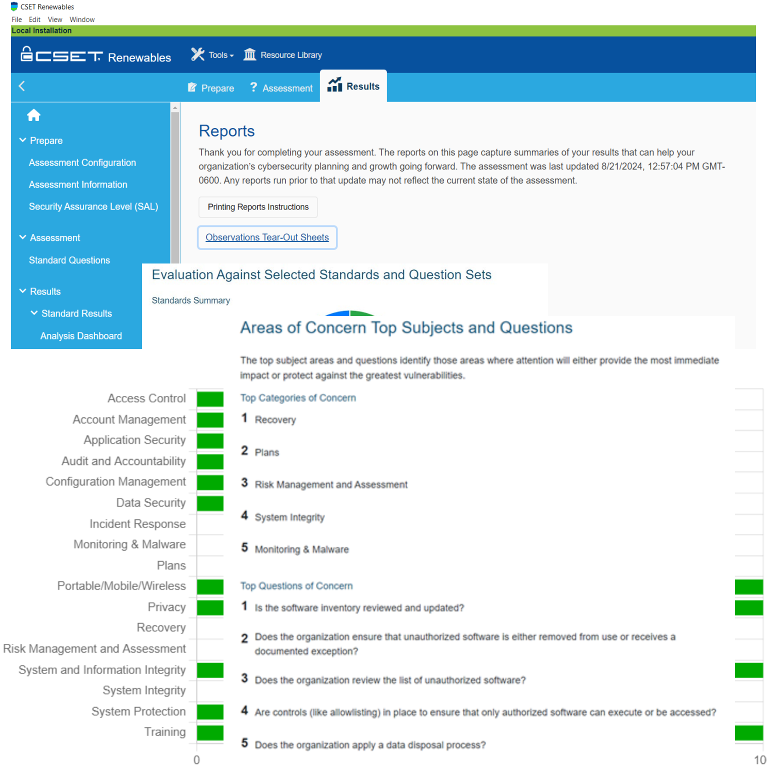
Guidelines and best practices tailored for Utility Scale Photovoltaic Energy Systems. This cybersecurity evaluation is tuned to the Operational Technology systems, average cybersecurity program maturity level, and business practices typically supported by Utility connected PV systems and is geared to help identify and understand the cyber risks for this type of user.

Assessment Description

Solar Cybersecurity Evaluation Risk Tool (SCERT) & Diagran

This assessment includes Solar-CERT questions and a network diagram.

Solar CERT Reports



Reports

Thank you for completing your assessment. The reports on this page capture summaries of your results that can help your organization's cybersecurity planning and growth going forward. The assessment was last updated 8/21/2024, 12:57:04 PM GMT-0600. Any reports run prior to that update may not reflect the current state of the assessment.

Printing Reports Instructions

Observations Tear-Out Sheets

Evaluation Against Selected Standards and Question Sets

Standards Summary

Areas of Concern Top Subjects and Questions

The top subject areas and questions identify those areas where attention will either provide the most immediate impact or protect against the greatest vulnerabilities.

Top Categories of Concern

1 Recovery
2 Plans
3 Risk Management and Assessment
4 System Integrity
5 Monitoring & Malware

Top Questions of Concern

1 Is the software inventory reviewed and updated?
2 Does the organization ensure that unauthorized software is either removed from use or receives a documented exception?
3 Does the organization review the list of unauthorized software?
4 Are controls (like allowlisting) in place to ensure that only authorized software can execute or be accessed?
5 Does the organization apply a data disposal process?

SHIELD–Malcolm (INL)

Asset Interaction Analysis

Key Objectives Targeted

Provide asset owners/operations with initial baseline of assets linked to operational technology (OT) and business processes. Detect and visualize threats and vulnerability identification/analysis for renewable OT environments. Malcolm is an Open-Source tool, initial INL Lab Direct Research Development (LDRD) funded project and sustained by DHS CISA/DOE funding for public use.

Key features:

- ✓ OT Asset to business processes mapping
- ✓ Log collection & analysis tool suite
- ✓ Increases cyber maturity by adding visibility of assets and threats

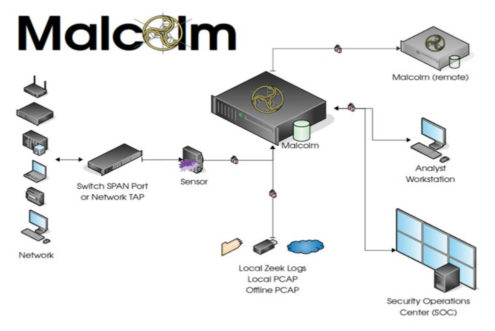
Top 3 Benefits:

1 Better knowledge of assets, clear view of asset risk levels based on devices, protocols, and configurations.

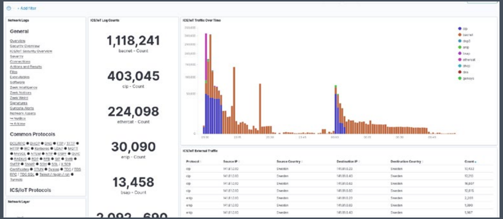
2 Identify potential cyber-attacks, exposed software vulnerabilities, and active exploits impacting assets/devices data through passive monitoring

3 Increases network visibility through dashboard visualization to enable informed decisions and improve operational reliability.

Asset Interaction Analysis
Malcolm
Malcolm Key Benefits & Deployment Overview



Threat Monitoring and Analytics


+ Add filter

Network Logs

General

Overview
Security Overview
ICS/IoT Security Overview
Severity
Connections
Actions and Results
Files
Executables
Software
Zeek Intelligence
Zeek Notices
Zeek Weird
Signatures
Suricata Alerts
Network Assets
↪ NetBox
↪ Arkime

Common Protocols

DCE/RPC ● DHCP ● DNS ● FTP / TFTP ● HTTP ● IRC ● Kerberos ● LDAP ● MQTT ● MySQL ● NTLM ● NTP ● OSPF ● QUIC ● RADIUS ● RDP ● RFB ● SIP ● SMB ● SMTP ● SNMP ● SSH ● SSL / X.509 Certificates ● STUN ● Syslog ● TDS / TDS RPC / TDS SQL ● Telnet / rlogin / rsh ● Tunnels

ICS/IoT Protocols

Network Layer

ICS/IoT Log Counts

1,118,241
bacnet - Count

403,045
cip - Count

224,098
ethercat - Count

30,090
enip - Count

13,458
bsap - Count

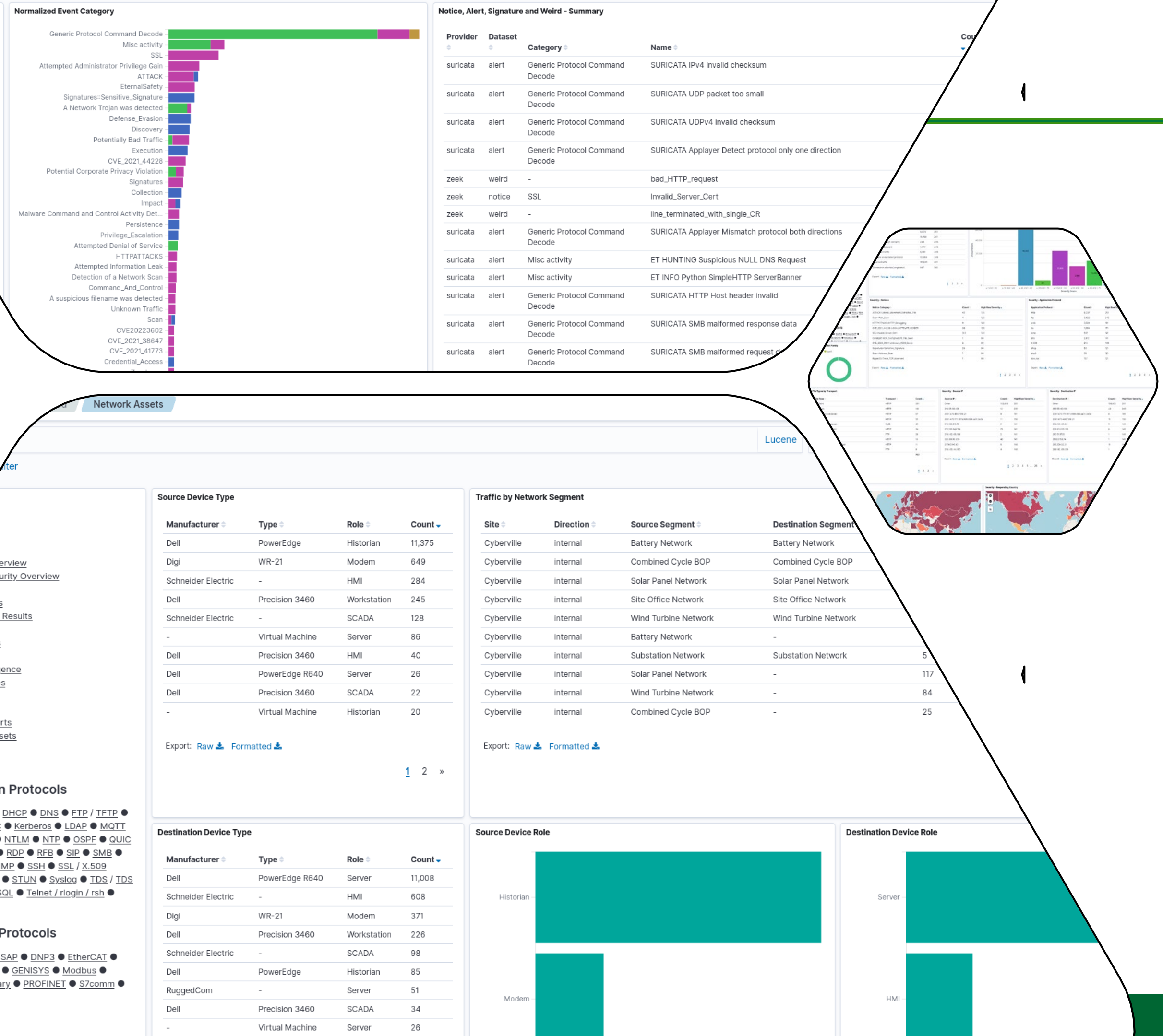
2,092 690

ICS/IoT Traffic Over Time

ICS/IoT External Traffic

Protocol	Source IP	Source Country	Destination IP	Destination Country	Count
cip	141.81.0.10	Sweden	141.81.0.23	Sweden	10,432
cip	141.81.0.10	Sweden	141.81.0.43	Sweden	10,213
cip	141.81.0.10	Sweden	141.81.0.63	Sweden	16,807
cip	141.81.0.10	Sweden	141.81.0.83	Sweden	10,815
enip	141.81.0.10	Sweden	141.81.0.23	Sweden	2,203
enip	141.81.0.10	Sweden	141.81.0.63	Sweden	1,990
enip	141.81.0.10	Sweden	141.81.0.43	Sweden	1,967

How can AIA Benefit You?


Normalized Event Category
Generic Protocol Command Decode
Misc activity
SSL
Attempted Administrator Privilege Gain
ATTACK
EternalSafety
Signatures::Sensitive_Signature
A Network Trojan was detected
Defense_Evasion
Discovery
Potentially Bad Traffic
Execution
CVE_2021_44228
Potential Corporate Privacy Violation
Signatures
Collection
Impact
Malware Command and Control Activity Det...
Persistence
Privilege_Escalation
Attempted Denial of Service
HTTPATTACKS
Attempted Information Leak
Detection of a Network Scan
Command_And_Control
A suspicious filename was detected
Unknown Traffic
Scan
CVE20223602
CVE_2021_38647
CVE_2021_41773
Credential_Access

Notice, Alert, Signature and Weird - Summary

Provider	Dataset	Category	Name	Cou
suricata	alert	Generic Protocol Command Decode	SURICATA IPv4 invalid checksum	
suricata	alert	Generic Protocol Command Decode	SURICATA UDP packet too small	
suricata	alert	Generic Protocol Command Decode	SURICATA UDPv4 invalid checksum	
suricata	alert	Generic Protocol Command Decode	SURICATA Applayer Detect protocol only one direction	
zeek	weird	-	bad_HTTP_request	
zeek	notice	SSL	Invalid_Server_Cert	
zeek	weird	-	line_terminated_with_single_CR	
suricata	alert	Generic Protocol Command Decode	SURICATA Applayer Mismatch protocol both directions	
suricata	alert	Misc activity	ET HUNTING Suspicious NULL DNS Request	
suricata	alert	Misc activity	ET INFO Python SimpleHTTP ServerBanner	
suricata	alert	Generic Protocol Command Decode	SURICATA HTTP Host header invalid	
suricata	alert	Generic Protocol Command Decode	SURICATA SMB malformed response data	
suricata	alert	Generic Protocol Command Decode	SURICATA SMB malformed request d	

erview
urity Overview
Results
ence
rts
sets

n Protocols

DHCP ● DNS ● FTP / TFTP ●
● Kerberos ● LDAP ● MQTT
NTLM ● NTP ● OSPF ● QUIC
RDP ● RFB ● SIP ● SMB ●
MP ● SSH ● SSL / X.509
● STUN ● Syslog ● TDS / TDS
SQL ● Telnet / rlogin / rsh ●

Protocols

SAP ● DNP3 ● EtherCAT ●
● GENISYS ● Modbus ●
ary ● PROFINET ● S7comm ●

Source Device Type

Manufacturer	Type	Role	Count
Dell	PowerEdge	Historian	11,375
Digi	WR-21	Modem	649
Schneider Electric	-	HMI	284
Dell	Precision 3460	Workstation	245
Schneider Electric	-	SCADA	128
-	Virtual Machine	Server	86
Dell	Precision 3460	HMI	40
Dell	PowerEdge R640	Server	26
Dell	Precision 3460	SCADA	22
-	Virtual Machine	Historian	20

Export: Raw Formatted

1 2 »

Traffic by Network Segment

Site	Direction	Source Segment	Destination Segment	
Cyberville	internal	Battery Network	Battery Network	
Cyberville	internal	Combined Cycle BOP	Combined Cycle BOP	
Cyberville	internal	Solar Panel Network	Solar Panel Network	
Cyberville	internal	Site Office Network	Site Office Network	
Cyberville	internal	Wind Turbine Network	Wind Turbine Network	
Cyberville	internal	Battery Network	-	
Cyberville	internal	Substation Network	Substation Network	5
Cyberville	internal	Solar Panel Network	-	117
Cyberville	internal	Wind Turbine Network	-	84
Cyberville	internal	Combined Cycle BOP	-	25

Export: Raw Formatted

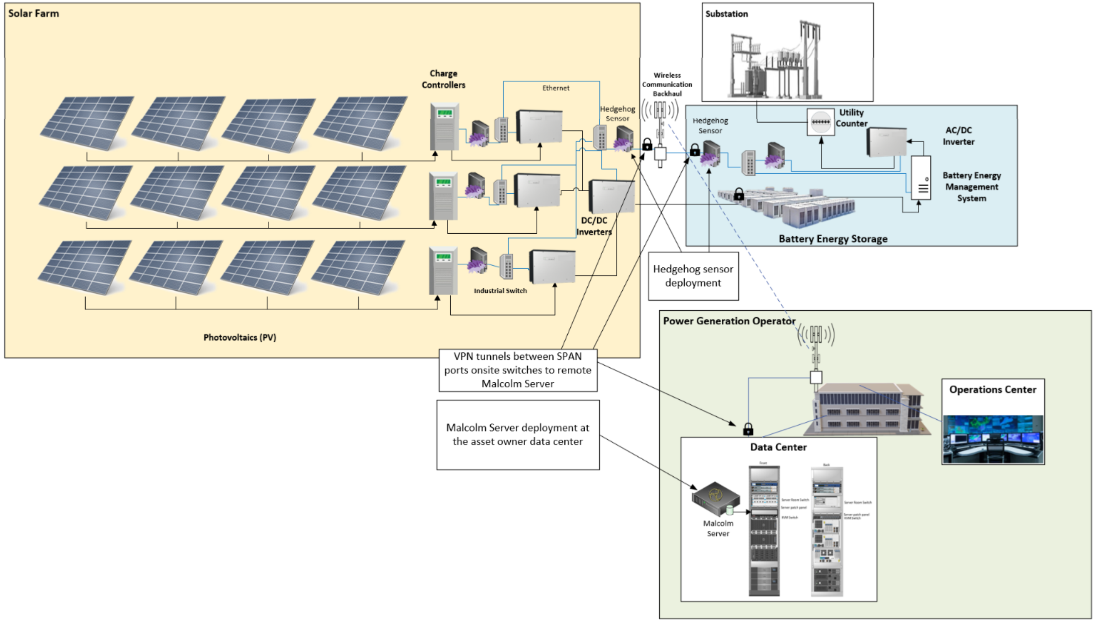
Destination Device Type

Manufacturer	Type	Role	Count
Dell	PowerEdge R640	Server	11,008
Schneider Electric	-	HMI	608
Digi	WR-21	Modem	371
Dell	Precision 3460	Workstation	226
Schneider Electric	-	SCADA	98
Dell	PowerEdge	Historian	85
RuggedCom	-	Server	51
Dell	Precision 3460	SCADA	34
-	Virtual Machine	Server	26

- Get to know your network: Malcolm characterizes traffic by devices and the protocols they use to communicate.
- Understand risks and threats: Malcolm identifies active exploits, potential attacks, and vulnerable devices and protocols.
- Increase visibility: Malcolm highlights inbound, outbound, and internal communications to inform decisions and improve security posture.

Malcolm Deployment for Solar Guide (INL)

- This guide provides detailed instructions for deploying Malcolm in Solar Power Generation systems.
- Deployment process within ICS/OT network architecture
- Configuring network switches and Switched Port Analyzer (SPAN) ports or mirror ports or TAPs
- Best practices for deploying Hedgehog sensors, another critical component in these systems.



Hedgehog sensor deployment

VPN tunnels between SPAN ports onsite switches to remote Malcolm Server

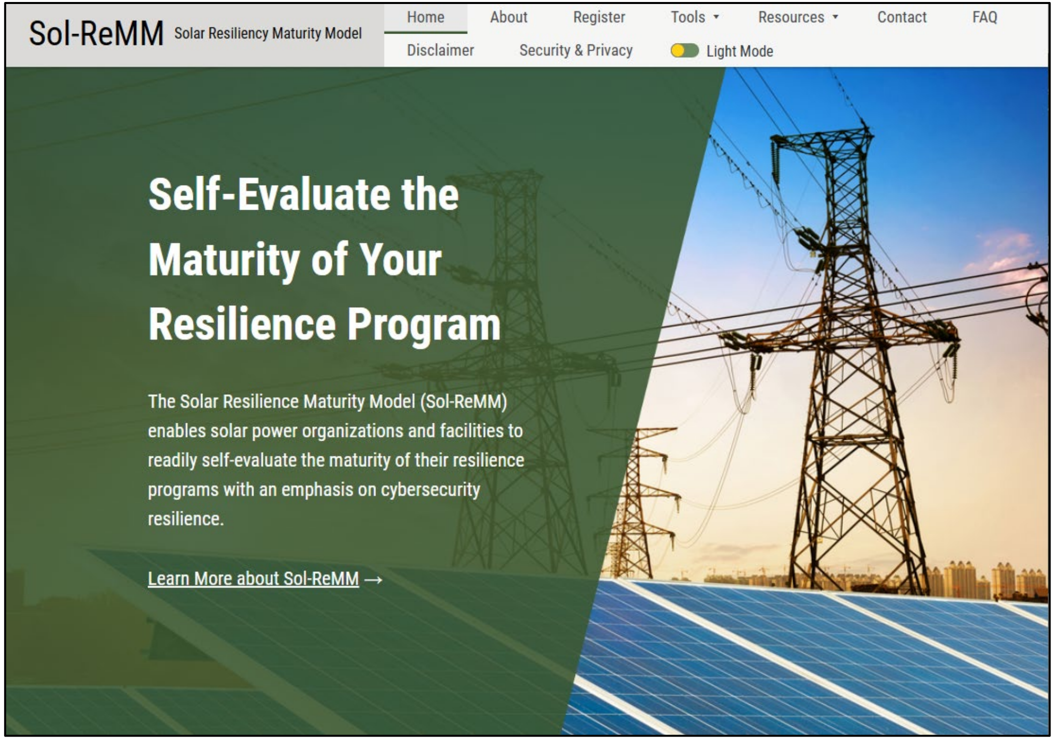
Malcolm Server deployment at the asset owner data center

SHIELD Tools Links (INL)

- CSET Renewable as its own branch: cset-renewables-download.inl.gov
- Malcolm site for industry to interact with dashboards and view functionality: https://training.malcolm.fyi/dashboards
- Malcolm GitHub Site for industry to download and install on local hardware or virtual machine: https://github.com/cisagov/Malcolm
- CyberSHIELD Industry Engagement Website: https://resilience.inl.gov/inlcybershield/
- Email for specific program contacts: CYBERSHIELD@INL.GOV

Sol-REMM

Solar Resiliency Maturity Model



Self-Evaluate the Maturity of Your Resilience Program

The Solar Resilience Maturity Model (Sol-ReMM) enables solar power organizations and facilities to readily self-evaluate the maturity of their resilience programs with an emphasis on cybersecurity resilience.

Learn More about Sol-ReMM →

An easy-to-use free-of-cost tool that allows solar power organizations to:

- self-assess the maturity of resilience programs with an emphasis on cyber-resilience
- identify areas of programmatic strength and weakness
- make risk-based decisions to enhance their resilience program

Public release planned for September 30, 2024

What is a Maturity Model?

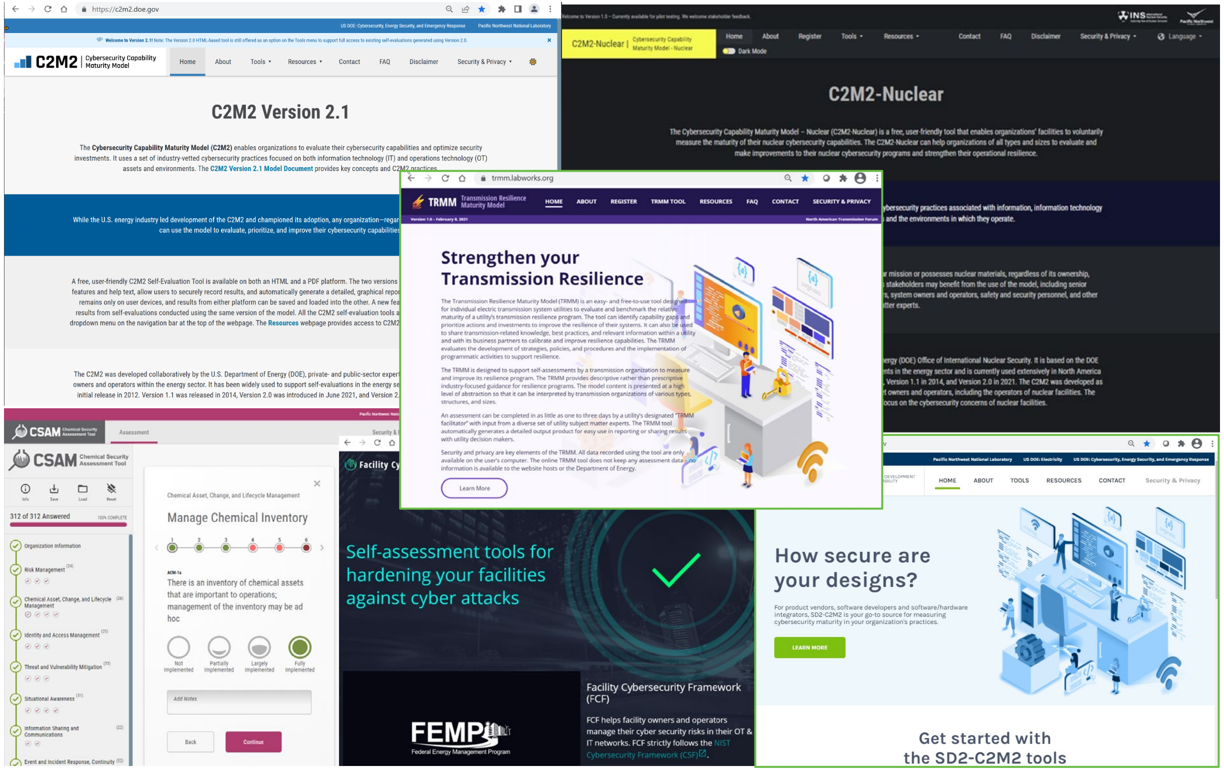
- An organized way to convey a path of experience, wisdom, perfection, or acculturation.

- A Maturity Model tool helps:
  - Exchange program information between SMEs and management
  - Enable benchmarking of program capabilities
  - Enable prioritized actions and investments
  - Share knowledge and best practices

Key Outcome: Help decision makers determine the adequacy of their program and identify potential areas for improvement.

PNNL’s Maturity Models

https://www.pnnl.gov/pnnl-maturity-models


https://c2m2.doe.gov
US DOE: Cybersecurity, Energy Security, and Emergency Response
Pacific Northwest National Laboratory
C2M2 Cybersecurity Capability Maturity Model
Home
About
Tools
Resources
Contact
FAQ
Disclaimer
Security & Privacy

Welcome to Version 2.1! Note: The Version 2.0 HTML-based tool is still offered as an option on the Tools menu to support full access to existing self-evaluations generated using Version 2.0.

C2M2 Version 2.1

The **Cybersecurity Capability Maturity Model (C2M2)** enables organizations to evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments. The C2M2 Version 2.1 Model Document provides key concepts and C2M2 practices

While the U.S. energy industry led development of the C2M2 and championed its adoption, any organization—regar
can use the model to evaluate, prioritize, and improve their cybersecurity capabilities

A free, user-friendly C2M2 Self-Evaluation Tool is available on both an HTML and a PDF platform. The two versions
features and help text, allow users to securely record results, and automatically generate a detailed, graphical repor
remains only on user devices, and results from either platform can be saved and loaded into the other. A new fea
results from self-evaluations conducted using the same version of the model. All the C2M2 self-evaluation tools a
dropdown menu on the navigation bar at the top of the webpage. The Resources webpage provides access to C2M2

The C2M2 was developed collaboratively by the U.S. Department of Energy (DOE), private- and public-sector expert
owners and operators within the energy sector. It has been widely used to support self-evaluations in the energy se
initial release in 2012. Version 1.1 was released in 2014, Version 2.0 was introduced in June 2021, and Version 2.

Welcome to Version 1.0 – Currently available for pilot testing. We welcome stakeholder feedback.
C2M2-Nuclear | Cybersecurity Capability Maturity Model - Nuclear
Home
About
Register
Tools
Resources
Contact
FAQ
Disclaimer
Security & Privacy
Language
Dark Mode

C2M2-Nuclear

The Cybersecurity Capability Maturity Model – Nuclear (C2M2-Nuclear) is a free, user-friendly tool that enables organizations’ facilities to voluntarily measure the maturity of their nuclear cybersecurity capabilities. The C2M2-Nuclear can help organizations of all types and sizes to evaluate and make improvements to their nuclear cybersecurity programs and strengthen their operational resilience.

ybersecurity practices associated with information, information technology
and the environments in which they operate.

r mission or possesses nuclear materials, regardless of its ownership,
stakeholders may benefit from the use of the model, including senior
s, system owners and operators, safety and security personnel, and other
tter experts.

ergy (DOE) Office of International Nuclear Security. It is based on the DOE
nts in the energy sector and is currently used extensively in North America
, Version 1.1 in 2014, and Version 2.0 in 2021. The C2M2 was developed as
t owners and operators, including the operators of nuclear facilities. The
ocus on the cybersecurity concerns of nuclear facilities.

trmm.labworks.org
TRMM Transmission Resilience Maturity Model
HOME
ABOUT
REGISTER
TRMM TOOL
RESOURCES
FAQ
CONTACT
SECURITY & PRIVACY
Version 1.0 – February 8, 2021
North American Transmission Forum

Strengthen your Transmission Resilience

The Transmission Resilience Maturity Model (TRMM) is an easy- and free-to-use tool designed for individual electric transmission system utilities to evaluate and benchmark the relative maturity of a utility’s transmission resilience program. The tool can identify capability gaps and prioritize actions and investments to improve the resilience of their systems. It can also be used to share transmission-related knowledge, best practices, and relevant information within a utility and with its business partners to calibrate and improve resilience capabilities. The TRMM evaluates the development of strategies, policies, and procedures and the implementation of programmatic activities to support resilience.

The TRMM is designed to support self-assessments by a transmission organization to measure and improve its resilience program. The TRMM provides descriptive rather than prescriptive industry-focused guidance for resilience programs. The model content is presented at a high level of abstraction so that it can be interpreted by transmission organizations of various types, structures, and sizes.

An assessment can be completed in as little as one to three days by a utility’s designated “TRMM facilitator” with input from a diverse set of utility subject matter experts. The TRMM tool automatically generates a detailed output product for easy use in reporting or sharing results with utility decision makers.

Security and privacy are key elements of the TRMM. All data recorded using the tool are only available on the user’s computer. The online TRMM tool does not keep any assessment data – no information is available to the website hosts or the Department of Energy.

312 of 312 Answered 100% COMPLETE

- Organization Information
- Risk Management (24)
- Chemical Asset, Change, and Lifecycle Management (26)
- Identity and Access Management (25)
- Threat and Vulnerability Mitigation (33)
- Situational Awareness (31)
- Information Sharing and Communications (22)
- Event and Incident Response, Continuity (52)

Chemical Asset, Change, and Lifecycle Management

Manage Chemical Inventory

1 2 3 4 5 6

ACM-1a

There is an inventory of chemical assets that are important to operations; management of the inventory may be ad hoc

○ Not Implemented ○ Partially Implemented ○ Largely Implemented ● Fully Implemented

Add Notes

Self-assessment tools for hardening your facilities against cyber attacks

Facility Cybersecurity Framework (FCF)

FCF helps facility owners and operators manage their cyber security risks in their OT & IT networks. FCF strictly follows the NIST Cybersecurity Framework (CSF).

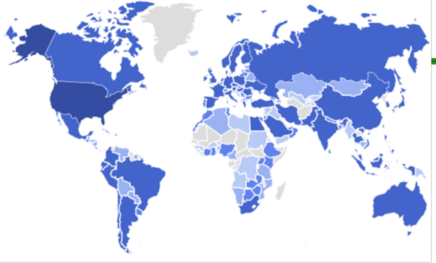
Pacific Northwest National Laboratory
US DOE: Electricity
US DOE: Cybersecurity, Energy Security, and Emergency Response
DEVELOPMENT
ABILITY
HOME
ABOUT
TOOLS
RESOURCES
CONTACT
Security & Privacy

How secure are your designs?

For product vendors, software developers and software/hardware integrators, SD2-C2M2 is your go-to source for measuring cybersecurity maturity in your organization's practices.

Get started with the SD2-C2M2 tools

C2M2 Usage statistics, Aug 2024

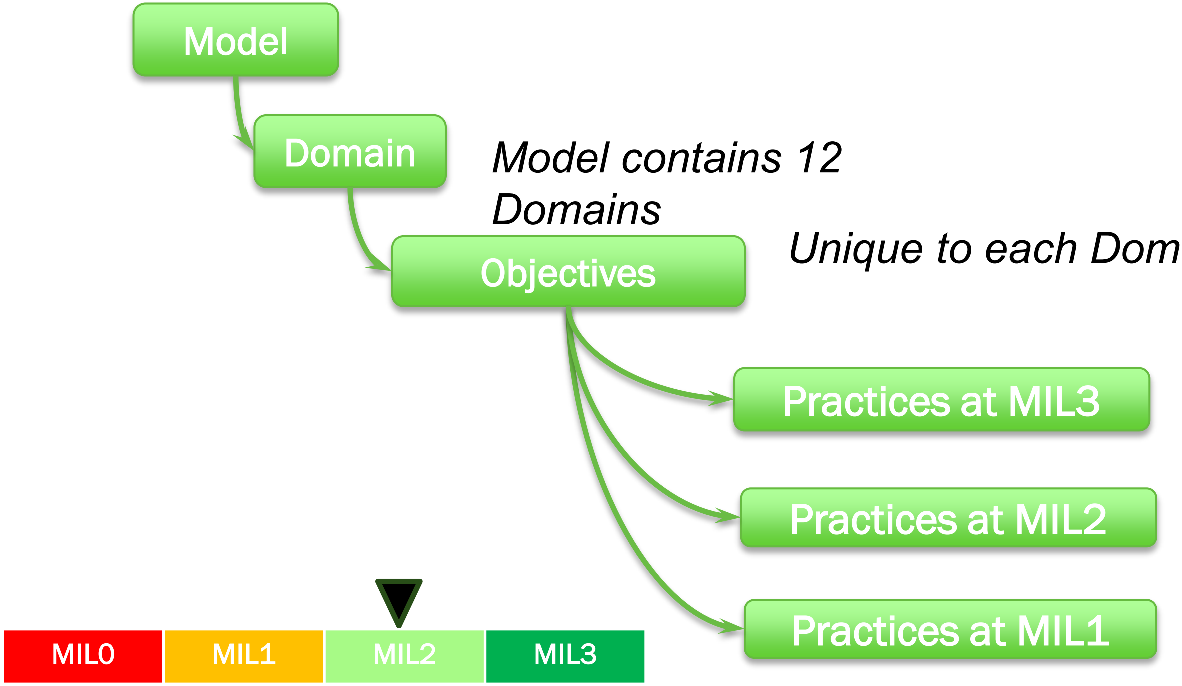


COUNTRY	USERS
United States	10K
India	1.5K
Australia	1.5K
China	1.1K
Canada	1.1K
United Kingdom	1K
Brazil	964

Sponsors:

- DOE CESER
- DOE GDO
- DOE EERE
- DOE SETO
- DOE INS
- DOE FEMP
- State Dept

Organization of the Sol-ReMM



Model

Domain

Objectives

Practices at MIL3

Practices at MIL2

Practices at MIL1

Model contains 12 Domains

Unique to each Domain (3 – 7 per domain)

Objectives are supported by a progression of Practices

MIL0	MIL1	MIL2	MIL3

Maturity Indicator Level (MIL) Scale

Sol-ReMM Domains

- Resilience Program Management
- Asset Inventory Management
- Supply Chain Management
- Threat and Vulnerability Management
- Cybersecurity Architecture
- Asset Configuration and Change Management
- Procurement Process Management
- Risk Assessment and Management
- Workforce Management
- Access and Authorization Management
- Situational Awareness
- Cybersecurity Event and Incident Response

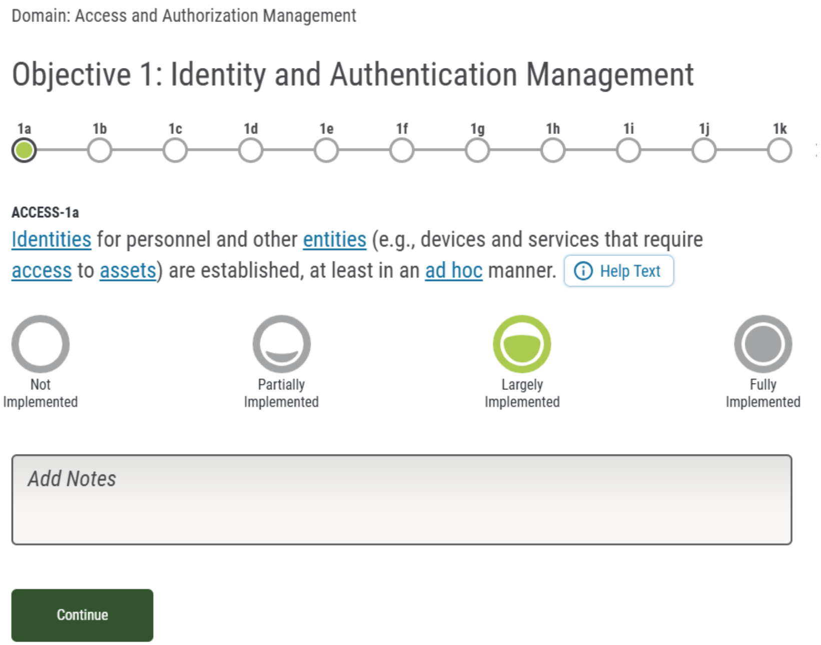
Example Objectives

Cybersecurity Event and Incident Response

1. Detect Cybersecurity Events
2. Analyze Cybersecurity Events and Declare Incidents
3. Respond to Cybersecurity Events and Incidents
4. Address Cybersecurity Resilience in Continuity of Operations
5. Management Activities

Virus Alert!
Warning! Threat detected!
A malicious item has been detected!

Example Practice



Domain: Access and Authorization Management

Objective 1: Identity and Authentication Management

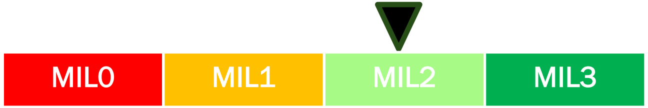
ACCESS-1a

Identities for personnel and other entities (e.g., devices and services that require access to assets) are established, at least in an ad hoc manner. ⓘ Help Text

○ Not Implemented ○ Partially Implemented [✓ Largely Implemented] ○ Fully Implemented

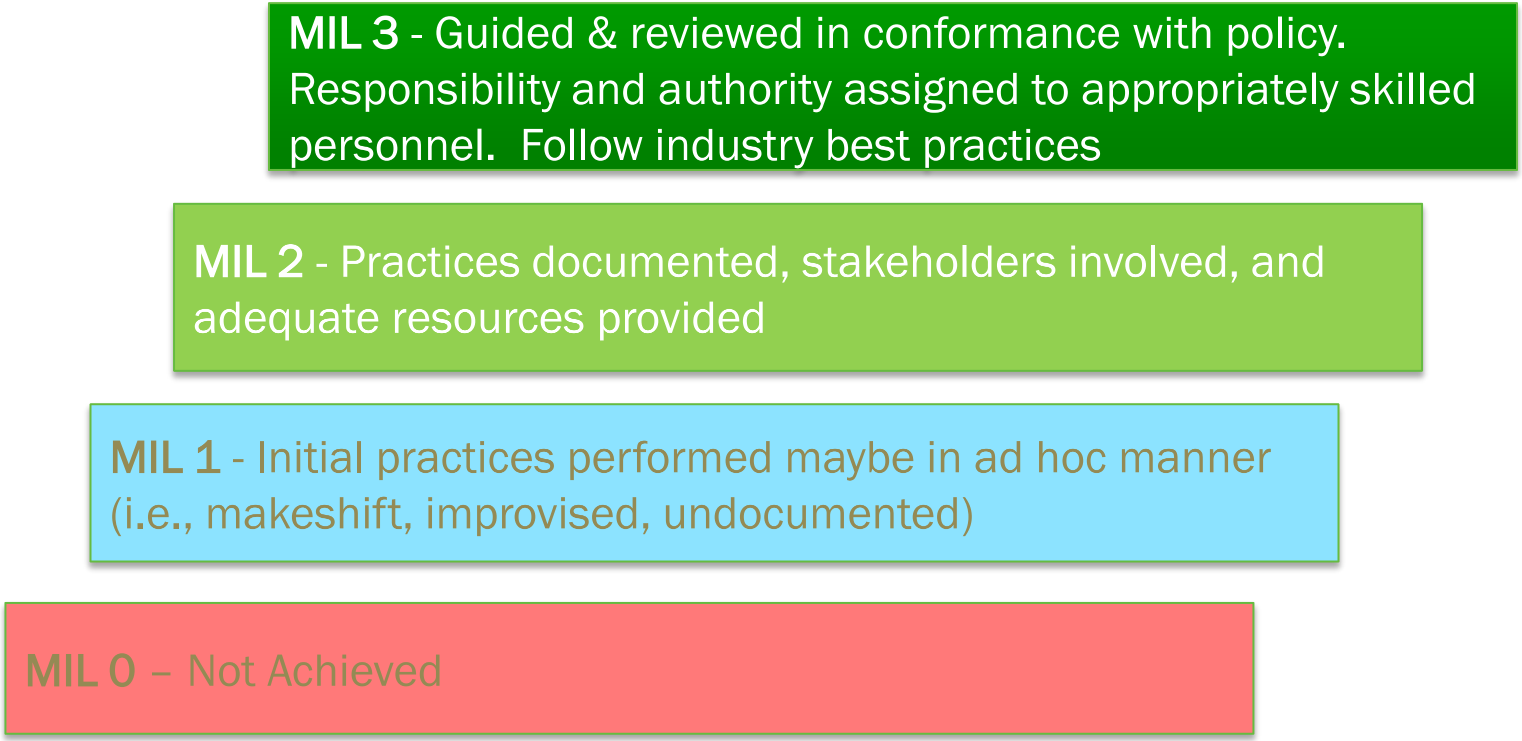
Add Notes

Answer Scale	Implementation Description
Fully Implemented	Complete
Largely Implemented	Complete, but with a recognized opportunity for improvement
Partially Implemented	Incomplete, but there are multiple opportunities for improvement
Not Implemented	Absent, the practice is not performed by the organization



Maturity Indicator Level (MIL) Scale

Maturity Indicator Levels (MIL)

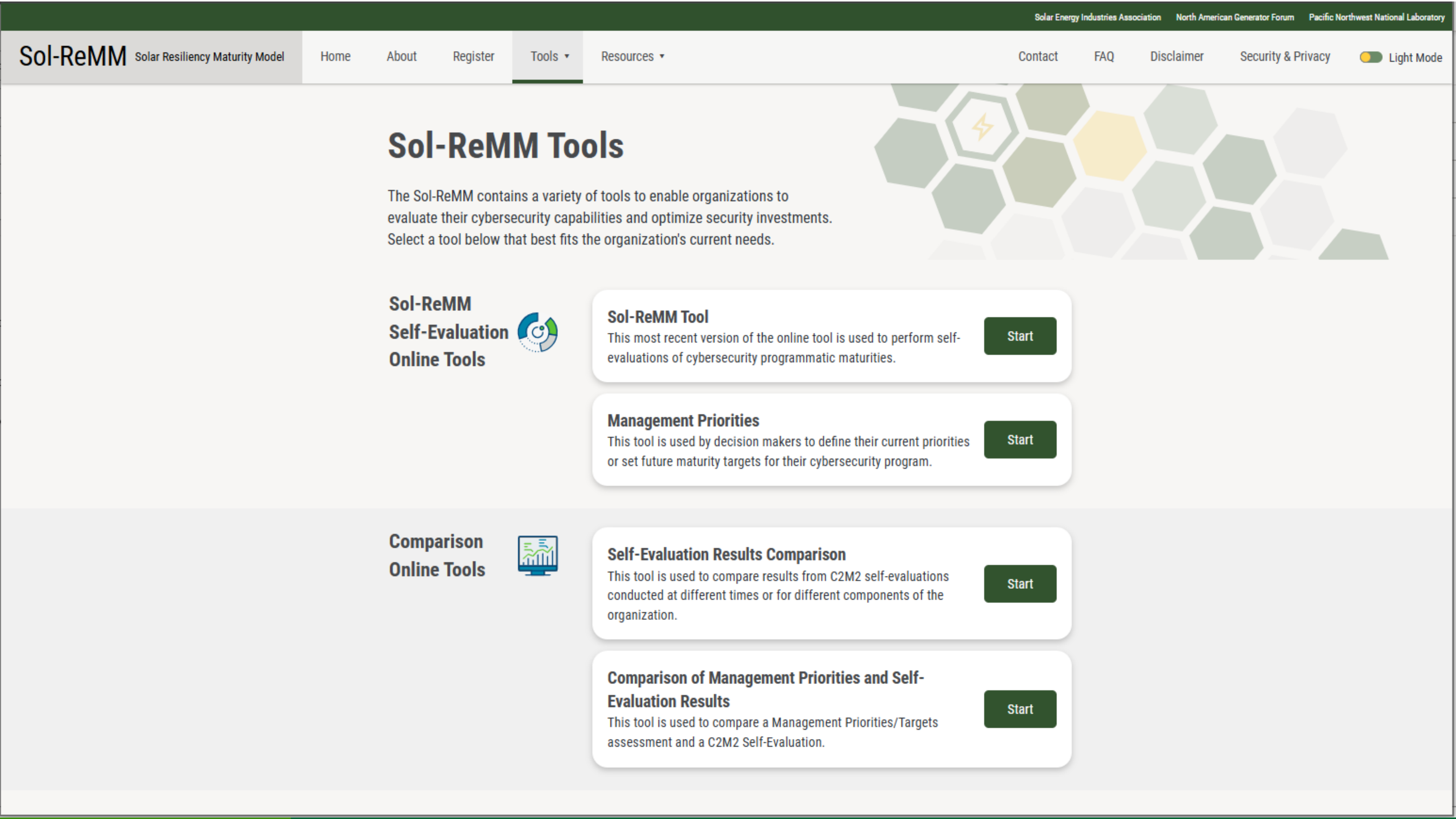


MIL 3 - Guided & reviewed in conformance with policy. Responsibility and authority assigned to appropriately skilled personnel. Follow industry best practices

MIL 2 - Practices documented, stakeholders involved, and adequate resources provided

MIL 1 - Initial practices performed maybe in ad hoc manner (i.e., makeshift, improvised, undocumented)

MIL 0 – Not Achieved


Solar Energy Industries Association
North American Generator Forum
Pacific Northwest National Laboratory
Sol-ReMM Solar Resiliency Maturity Model
Home
About
Register
Tools ▾
Resources ▾
Contact
FAQ
Disclaimer
Security & Privacy
Light Mode

Sol-ReMM Tools

The Sol-ReMM contains a variety of tools to enable organizations to evaluate their cybersecurity capabilities and optimize security investments. Select a tool below that best fits the organization's current needs.

Sol-ReMM Self-Evaluation Online Tools

Sol-ReMM Tool

This most recent version of the online tool is used to perform self-evaluations of cybersecurity programmatic maturities.

Management Priorities

This tool is used by decision makers to define their current priorities or set future maturity targets for their cybersecurity program.

Comparison Online Tools

Self-Evaluation Results Comparison

This tool is used to compare results from C2M2 self-evaluations conducted at different times or for different components of the organization.

Comparison of Management Priorities and Self-Evaluation Results

This tool is used to compare a Management Priorities/Targets assessment and a C2M2 Self-Evaluation.

Asset & Vulnerability Management

Moderated by:
Birk Jones (Sandia)

Brian Lyttle
(Idaho National Laboratory)

Emily Hwang
(Yaskawa Solectria Solar)

Andrew Plunkett
(AES Energy)

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Supply Chain Cybersecurity Principles

Securing Solar to the Grid Workshop

12 Sep 2024

Supply Chain Cybersecurity Principles for Suppliers

Impact-Driven Risk Management
Embed consideration of impacts, specifically including those in your own upstream supply chains, throughout the entire systems engineering lifecycle, seeking to manage risks to functions that are aided by digital technologies.

Framework-Informed Defenses
Incorporate appropriate principles and practices from recognized cybersecurity frameworks into the design of your organization's defenses of its critical functions, infrastructure, and information.

Cybersecurity Fundamentals
Follow relevant domain-specific regulations and international standards, and consider secure and cyber-informed engineering and design principles, to produce products and deliver services with appropriate security features and controls.

Secure Development & Implementation
Use a secure systems development lifecycle process informed by internationally accepted frameworks and standards to encourage adequate security practices throughout an offering's lifecycle.

Transparency & Trust Building
Provide appropriate information to your end users and the public regarding your cybersecurity posture, interoperability, product security, testing methods, independent verifications, and software and hardware composition of your products.

Implementation Guidance
Provide hardening and secure implementation guidance to end users, including transparent information on default settings and behaviors that must be changed or managed in implementation.

Lifecycle Support & Management
Provide appropriate product support, including security patches and mitigations, from transaction through the announced end of lifecycle support.

Proactive Vulnerability Management
Maintain a vulnerability management process—aligned to industry best practices and applicable coordinated vulnerability disclosure processes—for the responsible handling and coordinated disclosure of vulnerabilities.

Proactive Incident Response
Develop and maintain appropriate incident response plans for incidents within your own environments and when supporting end users in responding to incidents involving your products or services.

Business & Operational Resilience
Continually improve your organization's practices and offerings by identifying and implementing adaptations informed by observations, insights, and lessons learned from ongoing operations, end-user experiences, and incident response.

Supply Chain Cybersecurity Principles for End Users

Impact-Driven Risk Management
Embed consideration of impacts, specifically including those in your own upstream supply chains, throughout the entire systems engineering lifecycle, seeking to manage risks to functions that are aided by digital technologies.

Framework-Informed Defenses
Incorporate appropriate principles and practices from recognized cybersecurity frameworks into the design of your organization's defenses of its critical functions, infrastructure, and information.

Cybersecurity Fundamentals
Follow relevant domain-specific regulations and international standards, and consider secure and cyber-informed engineering and design principles, to employ products and services in a secure manner, taking into account accumulated technical and security debt.

Secure Development & Implementation
Engage with suppliers to understand the security features and controls of their offering to ensure they are adequate for your intended purpose or identify necessary compensating controls.

Transparency & Trust Building
Include contractual language for those terms, conditions, and testing requirements that will influence your security outcomes, and which you are able and willing to enforce.

Implementation Guidance
Develop and maintain appropriately secure operating environments, following suppliers' hardening and secure implementation guidance.

Lifecycle Support & Management
Conduct business planning and provide resources to acquire, maintain (including patch management and fixes recommended by the supplier), and replace equipment through its lifecycle, considering continued availability of supplier technical support.

Proactive Vulnerability Management
Maintain a risk-informed vulnerability management process that aligns with the supplier's published process for coordinated disclosure of vulnerabilities discovered through use of their products.

Proactive Incident Response
Proactively coordinate supplier support during response to incidents involving their products or services.

Business & Operational Resilience
Continually improve your organization and its practices by adaptation from observations, insights, and lessons learned from ongoing operations, supplier experiences, and incident response.

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response

Cyber Labeling Research Project

Securing Solar to the Grid Workshop

12 Sep 2024

DOE’s Cyber Labeling Research Project

- “U.S. Cyber Trust Mark” program initiated in 2023 to be led by FCC to “help Americans more easily choose smart devices that are safer and less vulnerable to cyberattacks.”[1]
- **FCC will decide implementation details**
  - If implemented, participation would be voluntary and available to energy sector vendors.
- **DOE to research how a Cyber Trust Mark could apply to Industrial IoT**
  - Energy products focus
  - How best present information about security features?
  - Labs developing proof-of-concept label
- Output: recommendations for content of label, and ability to verify/validate label contents.

[1] https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/

Who is involved?

- Funded by Bipartisan Infrastructure Law, via DOE CESER[2]
- **Industry: feedback from five volunteer vendor partners with inverter and smart meter products**
- The public: seeking feedback from broader audiences (auditors, other vendors, the “general public”)

INL
Idaho National Laboratory
70 YEARS OF SCIENCE & INNOVATION

NREL
NATIONAL RENEWABLE ENERGY LABORATORY

Lawrence Livermore
National Laboratory

Sandia
National
Laboratories

OAK RIDGE
National Laboratory

Pacific Northwest
NATIONAL LABORATORY

Early Takeaways and Processes

- Assessed 19+ standards/recognized research/legislation pertaining to labeling, privacy, and security for IoT and IIoT
  - Key takeaway: **no existing standard or labeling regime adequately addresses privacy and security concerns applicable to energy sector ICS technologies** such as smart meters and inverters.
- Consulted with policy and technology experts from 5 volunteer vendors, both in 1-1 interviews and group workshops
  - Key takeaway: any label for energy IIoT should be **informational** (displaying disclosures about security and privacy measures) **rather than assessment or certification-based** (displaying a rating or seal of approval), **due to the context-dependent and highly variable nature of security** in these environments.
- Developed initial label mockup data-request form for use in pilot.
- Seeking public comment via website:

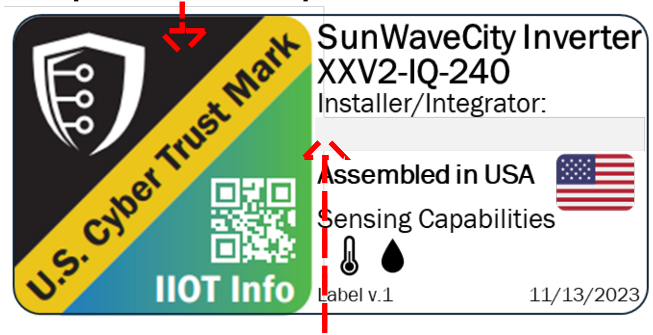
https://energy.sandia.gov/programs/electric-grid/cyber-security-for-electric-infrastructure/cyber-labeling-research-initiative/

Requested Data for an IIoT Cybersecurity Label

Category	Justification
Label Metadata	Provides context to understand the label and can be used to validate authenticity.
Identifying Information	Tells us what the label applies to and, in some cases, serves for data integrity.
Certifications and Standards	Demonstrates reciprocity with other standards, provides information about what efforts the vendor has gone through to build a product to a certain standard, and helps consumers make sense of the label.
Policies	Allows access to important information, demonstrate how companies meet legal requirements, set expectations, and enable consumer choice.
Interfaces	Provides awareness of what you need to protect, what you need to be aware of to enable protection, and what “normal” looks like to enable anomaly detection.
Data Protection	Provides knowledge of what the system is doing to protect the information or data generated or transmitted.
System Composition	Demonstrates depth of knowledge about the product and serves an accountability function.
Security Controls	Demonstrates what the vendor is doing to prioritize security, reduce attack surface, and seek external validation for processes. Disclosing this information serves an accountability function and provides some consumer choice in configurability.
Authentication	Tells the user if there is authentication, how it is enforced, and who has control of the system. A user can make an informed assessment about whether it is effective.
Security Updates	Gives the consumer clear instruction on how to keep the device secure, as well as information related to how long the device will remain secure, and what to expect when vulnerabilities are identified.
Data Sharing	Helps a consumer understand who has access to their data, what data is collected, where and why it is accessed, and whether they have control over data sharing. It also helps them to understand whether the device is compliant with local data sharing laws and regulations.

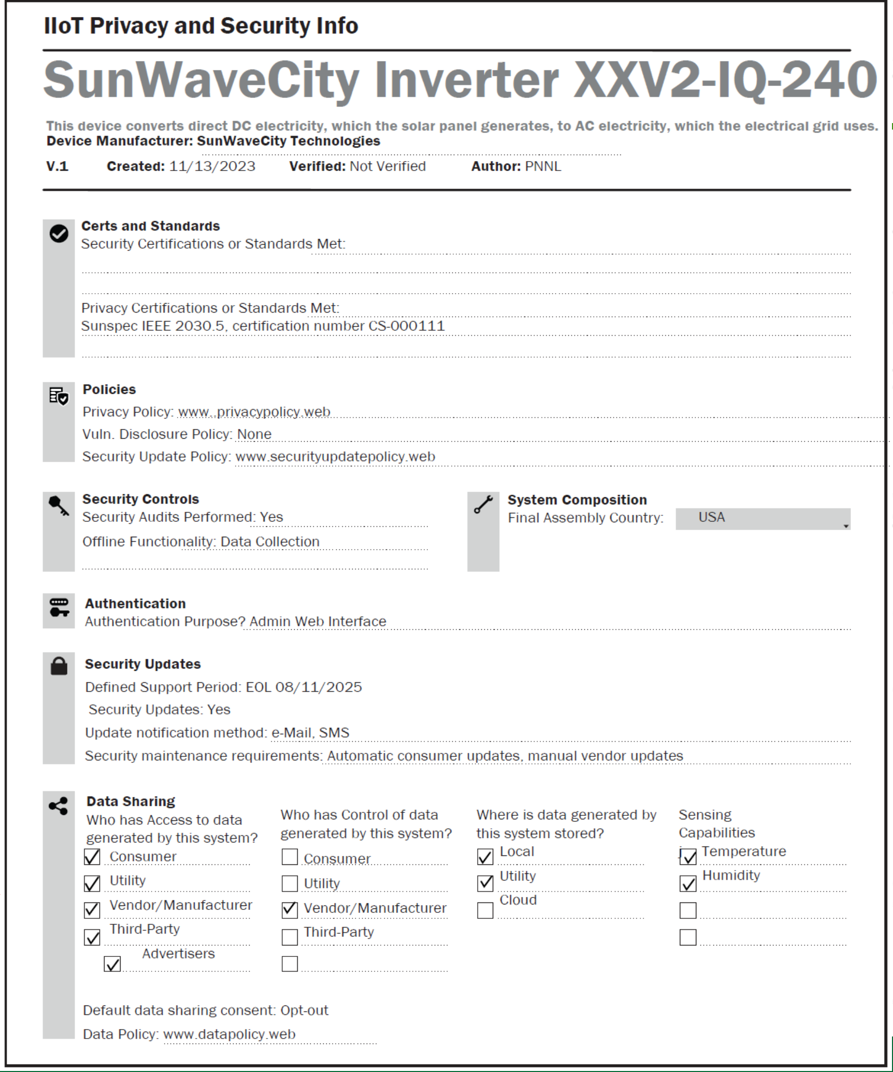
Mock Label for Comment

Sample sticker to be placed on product or product manual



*Installer/Integrator space will likely be removed, per guidance from industry.

Information sheet (hosted online) could be expanded in digital form
to reveal additional details



IIoT Privacy and Security Info

SunWaveCity Inverter XXV2-IQ-240

This device converts direct DC electricity, which the solar panel generates, to AC electricity, which the electrical grid uses.
Device Manufacturer: SunWaveCity Technologies

V.1 **Created:** 11/13/2023 **Verified:** Not Verified **Author:** PNNL

Certs and Standards
Security Certifications or Standards Met:

Privacy Certifications or Standards Met:
Sunspec IEEE 2030.5, certification number CS-000111

Policies
Privacy Policy: www..privacypolicy.web
Vuln. Disclosure Policy: None
Security Update Policy: www.securityupdatepolicy.web

Security Controls
Security Audits Performed: Yes
Offline Functionality: Data Collection

System Composition
Final Assembly Country: USA

Authentication
Authentication Purpose? Admin Web Interface

Security Updates
Defined Support Period: EOL 08/11/2025
Security Updates: Yes
Update notification method: e-Mail, SMS
Security maintenance requirements: Automatic consumer updates, manual vendor updates

Data Sharing

Who has Access to data generated by this system?
☑ Consumer
☑ Utility
☑ Vendor/Manufacturer
☑ Third-Party
☑ Advertisers

Who has Control of data generated by this system?
☐ Consumer
☐ Utility
☑ Vendor/Manufacturer
☐ Third-Party
☐

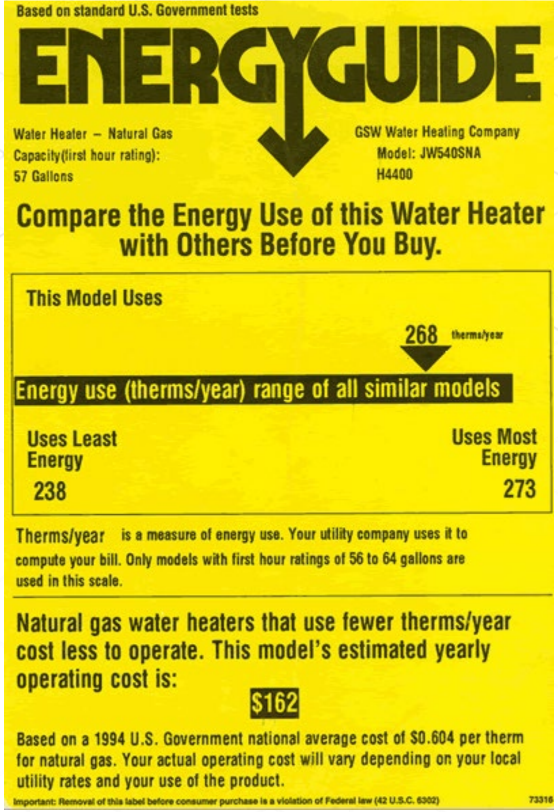
Where is data generated by this system stored?
☑ Local
☑ Utility
☐ Cloud

Sensing Capabilities
☑ Temperature
☑ Humidity
☐
☐

Default data sharing consent: Opt-out
Data Policy: www.datapolicy.web

Recommendation: Cyber Trust Guide

- **Cyber Trust "Guide" may be considered to allow vendors to communicate about their security features even if they do not meet or cannot demonstrate compliance with the NIST baselines.**
  - Further incentivizes information sharing and transparency.
  - Broadens the participation pool (more flexible and accessible way to get involved).
  - Allows consumers to make informed decisions based on what they need to be secure in their own environments.
- **These recommendations aim to build on the NIST baselines in a way that will provide more value and meaning in OT spaces.**



Based on standard U.S. Government tests

ENERGYGUIDE

Water Heater – Natural Gas
Capacity (first hour rating):
57 Gallons

GSW Water Heating Company
Model: JW540SNA
H4400

Compare the Energy Use of this Water Heater with Others Before You Buy.

This Model Uses

268 therms/year

Energy use (therms/year) range of all similar models

Uses Least Energy
238

Uses Most Energy
273

Therms/year is a measure of energy use. Your utility company uses it to compute your bill. Only models with first hour ratings of 56 to 64 gallons are used in this scale.

Natural gas water heaters that use fewer therms/year cost less to operate. This model's estimated yearly operating cost is:

$162

Based on a 1994 U.S. Government national average cost of $0.604 per therm for natural gas. Your actual operating cost will vary depending on your local utility rates and your use of the product.

Important: Removal of this label before consumer purchase is a violation of Federal law (42 U.S.C. 6302)

73316

Claim Verification

Claim verification: process of demonstrating that the data an entity provides to obtain a cyber label is truthful and accurate.

Not intended to demonstrate the effectiveness or security of any given implementation.

The research team is documenting:

- Benefits and limitations of four potential verification processes
- Level of expertise required to verify the data fields for the draft label
- High-level cost/effort estimates for verification options

Path Forward

- Continue exploring alignment with and opportunities to build upon NIST recommendations and baselines.
- Continue collaboration with vendor partners using proof-of-concepts to understand and document challenges associated with disclosing various types of information.
- Confirming industry's ability to conduct Claim Verification

Seeking Your Feedback

- Your opportunity to comment!
  - https://energy.sandia.gov/programs/electric-grid/cyber-security-for-electric-infrastructure/cyber-labeling-research-initiative/
- What data elements are most important?
- Is this too difficult to implement or use?
- Is the label useful? Why / why not?

YASKAWA SOLECTRIA SOLAR

Manufacturer of PV Inverters

SOLECTRIA HEADQUARTERS – THE HISTORIC RIVERWALK BUILDING ca 1905

YASKAWA SOLECTRIA SOLAR

ABOUT THE COMPANY

- **Solectria Renewables, LLC** established in 2005

NOW IN OUR 20th YEAR!

- Transitioned its name to **Yaskawa Solectria Solar** (YSS) after acquisition by **Yaskawa America, Inc.** (YAI) in 2014.

NOW 10 YEARS WITH YASKAWA!

- **Yaskawa Solectria Solar** headquarters is located in the historic Riverwalk woolen-mill buildings in Lawrence, MA (ca 1905)

YASKAWA SOLECTRIA SOLAR

ABOUT THE COMPANY

- **Solectria Renewables, LLC** established in 2005

NOW HEADING INTO OUR 20th YEAR!

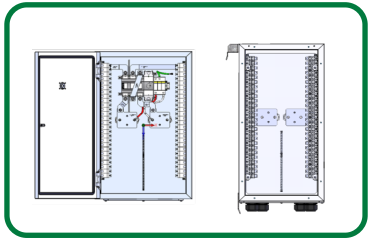
- Transitioned its name to **Yaskawa Solectria Solar** (YSS) after acquisition by **Yaskawa America, Inc.** (YAI) in 2014.

NOW 10 YEARS WITH YASKAWA!

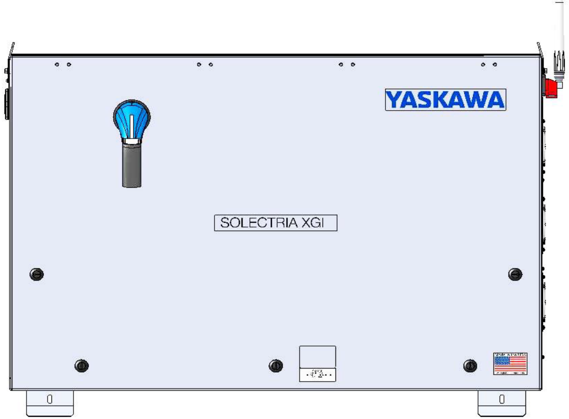
- **Yaskawa Solectria Solar** headquarters is located in the historic Riverwalk woolen-mill buildings in Lawrence, MA (ca 1905)
- **Yaskawa Solectria Solar** XGI 1500 inverters are Made in the USA using global components, at YAI's assembly plant in Buffalo Grove, IL. Combiners are made in Oak Creek, WI.

Solectria XGI® 1500 Product Family

MADE IN THE USA
With U.S. and Global Components

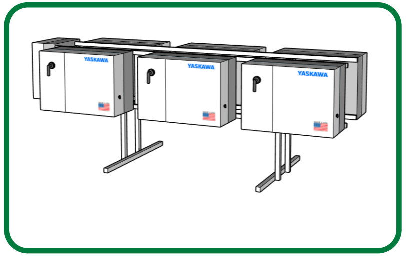


DC String Combiners

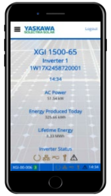


TÜVRheinland

UL 1741 SB



Pre-assembled Solutions



XGI 1500-65
Inverter 1
1W17X2458720001

14:34

AC Power
51.54 kW

Energy Produced Today
325.66 kWh

Lifetime Energy
3.33 MWh

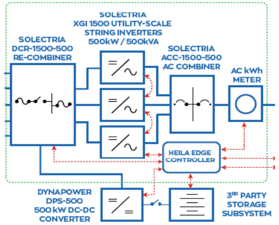
Inverter Status

XGI-00-006 3 | 14:34

Advanced Communications

250kW
225kW
200kW
175kW
166kW
150kW
125kW

Multiple Power Ratings



DC Coupled Energy Storage

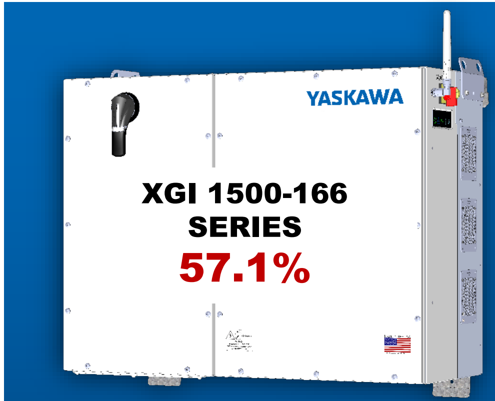
Supply Chain

- Yaskawa America, Inc is a voluntary certified member of the Customs Trade Partnership against Terrorism program since 2009.
- Single vendor issues

CTPAT

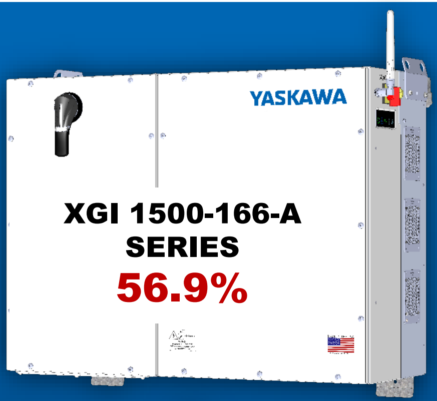
YOUR SUPPLY CHAIN'S STRONGEST LINK.

XGI 1500 – DOMESTIC CONTENT



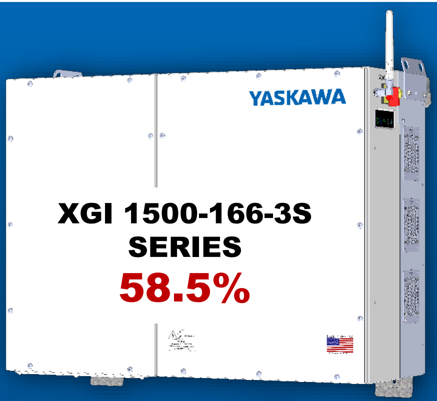
XGI 1500-166 SERIES

57.1%



XGI 1500-166-A SERIES

56.9%



XGI 1500-166-3S SERIES

58.5%

20 YEARS
SOLAR INVERTERS
MADE IN THE USA

XGI 1500-250 SERIES

51.9%

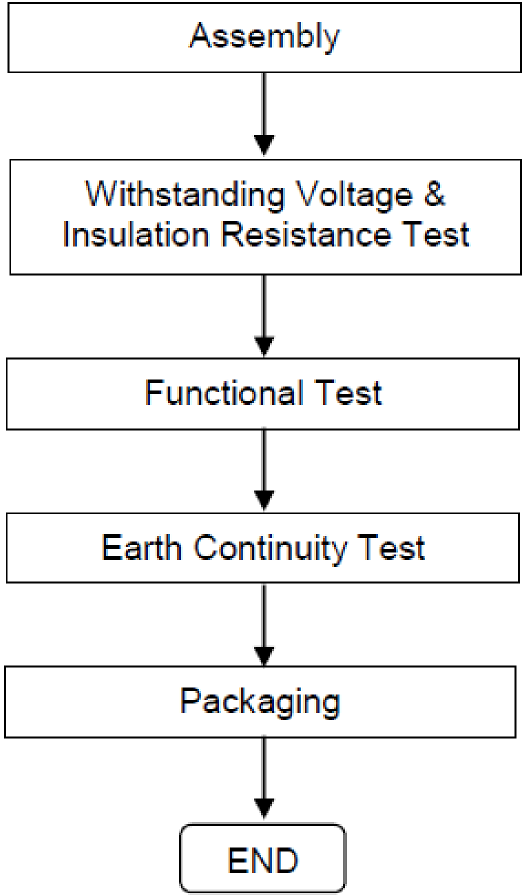
XGI 1500-250-DCG SERIES

53.7%

Solectria XGI 1500 Test Process

Every inverter is 100% tested

- **Software Test:** Including Rev#, checksum, etc
- **Insulation Resistance Test:** Ensure that there is adequate resistance between our terminals & ground.
- **Withstand Test:** Ensure there is no leakage current between terminals and ground
- **Functional Test:** Performed by Automated Test Equipment. Inverters must pass all tests to be shipped. Serial numbers and test results are recorded.
- **Earth Continuity Test:** ensure that the points that should be continuously connected to are.



Assembly

Withstanding Voltage & Insulation Resistance Test

Functional Test

Earth Continuity Test

Packaging

END

Solectria XGI ® - Mitigating Field Vulnerabilities

Baked into the Design

- Software and firmware developed in-house – does not cross country boundaries
- Physical Security: No buttons on the inverter itself
- All communications to and from inverter encrypted
- Monitoring Product: Cloud servers all on domestic servers with redundant backup
- Portal: Encrypted tunnel access and Two Factor Authentication
- Changeable password
- Continually monitor for new vulnerabilities and have a plan

PV Asset and Vulnerability Management

RE+ 2024

Andrew Plunkett

Cyber Security Senior Engineer For OT

AES Corporation

What is AES

Large international energy company with presence in US, South America, Eurasia

200+ power generation sites, T&D in Indianapolis, Dayton, El Salvador

Supply power ~22 Million people

Major push in recent years to decommission fossil fuel plants, develop renewables

5 Keys to OT Asset Vulnerability Management

Vendor Security Program – A program to buy products and services from vendors with strong cyber security programs

Asset Management Program – Know what assets you have so that you can protect them, vendor/product/version, location/IP address

Threat Intel Program – A way to be made aware of critical vulnerabilities in assets you own

Vulnerability Discovery – A technical way of discovering vulnerabilities on assets in your environment

Vulnerability Remediation Program – A process for tracking and remediating vulnerabilities

Vendor Security Program

Have a vendor onboarding process that takes cyber security into account

General idea of their cyber security program, do they even have one?

ISO 27001, SOC 2, BitSight

History of breaches/vulnerabilities, how many, how severe, how they were handled/communicated

Asset Management Program

Automated or manual entry, usually combination of both

Schedule regular updates, tie to change management

Easier if you have a standard deployment, network architecture and vendor/products

Have all sites use the same asset database system

Threat Intel Program

One way to tie vulnerabilities to assets

Identify critical vulnerabilities that are currently being exploited, severe/high risk

Tailor intel feed to assets/environment/industry

Vendor communication about security vulnerabilities/patches, usually goes to operations team

Vulnerability Discovery

Tool to discover assets and vulnerabilities on the network

Active scanning/Authenticated – better results but greater risk to operations

Passive listening – less accurate/detailed results, but safer to operations

Both are hindered by OT network segmentation

Vulnerability Remediation Plan

Have a process for managing vulnerabilities

Detailed information about asset, vulnerability, and risk

Discuss with stakeholders to develop remediation plan

Deploy suggested remediation, mitigation, or exception

Have a centralized system that can track the whole process and is used for all assets, risk decision, manage communication, history, status

Breakout Sessions

1. Risk quantification
2. Risk mitigation and tools
3. Devices and vulnerabilities
4. Risk valuation
5. Risk governance

Instructions:

- Pick 3 topics of interest to discuss.
- Each rotation will last 15 minutes.
- Last 10 minutes will be used for report outs from each facilitator.

Securing Solar for the Grid II (S2G 2): FY25-27

S2G 2 will support R&D to inform and develop cybersecurity standards for solar technologies and distributed energy resources (DERs). S2G works closely with industry to assess the cybersecurity risks of grids with high solar deployment that can impact grid reliability.

GOALS

- **Demonstration and deployment** of cyber-physical monitoring tools to increase solar DER network visibility, detect threats and provide remediation strategies.
- **Establish solar inverter-based resource cybersecurity testing** that considers supply chain and information sharing through stakeholder engagement activities.
- **Refine existing training modules and extending to solar hybrid systems** based on vulnerability assessments.
- Development new frameworks and best-practices guides **to increase DER aggregator maturity levels.**
- **Development and adoption of risk-assessment tools** to inform investments.
- **Inform standards development, harmonization and best practices**.
- **Stakeholder engagement** and collaboration with industry and other DOE offices, including the Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

INL Idaho National Laboratory

NREL Transforming ENERGY

Sandia National Laboratories

Pacific Northwest NATIONAL LABORATORY

S2G 2 FY25-27 Summary of Activities

Research Area	National Lab	Description
Standards and Best Practices	NREL	• Development of material and training to increase awareness and understanding of cybersecurity standards for IBRs and DERs.
	SNL	• Development of best practices to defend against AI/ML cyber incidents.
	PNNL	• Zero-trust reference architecture blueprint, evaluation criteria for commercial and industrial DER-based VPPs
	INL	• Cyber Informed Engineering architectural guide for solar technologies
Tool Kit and Supply Chain	NREL	• DER aggregators risk assessment and cost benefit analysis tool • Consequence-based experimentation on aggregated DERs cyberattacks impact to the grid.
	SNL	• Understand defense and adversary AI/ML implications for network connected IBRs.
	PNNL	• Cybersecurity checklist for commercial, industrial, and residential DER installations. • Supply chain analysis for inverter adjacent technologies.
	INL	• Firmware analysis based on AI/ML • Risk analysis tools and incident response for solar installations including aggregators and VPPs • Inverter HBOM enumeration and catalog in collaboration with CESER
Workforce Development and Training	NREL	• Outreach activities to increase maturity in standards for DERs
	SNL	• Training material on attack scenarios by AI/ML • Monthly webinar series
	PNNL	• Outreach activities on zero-trust architectures for C&I DER-based VPPs
	INL	• Solar Defender focused curriculum development in collaboration with CESER

DIVERSITY

EQUITY

INCLUSION

ACCESIBILITY

Thank you!

marissa.morales-rodriguez@ee.doe.gov

SIGN UP NOW:
energy.gov/solar-newsletter

Additional Slides

QUESTIONS