Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

The IAB Workshop

will start at

8:30 PDT

SETO: DOE Solar Energy Technologies Office;
INL: Idaho National Laboratory; NREL: National Renewable Energy Laboratory;
PNNL: Pacific Northwest National Laboratory; SNL: Sandia National Laboratories

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Securing Solar for the Grid (S2G)

Workshop and Industry Advisory Board Meeting

Marissa Morales-Rodriguez, DOE Solar Energy Technologies Office
Danish Saleem, National Renewable Energy Laboratory
Scott Mix, Pacific Northwest National Laboratory

September 14, 2023

Project Team: Idaho National Laboratory, National Renewable Energy Laboratory, Pacific Northwest National Laboratory, Sandia National Laboratories

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Workshop Introduction

Danish Saleem, Chair of Laboratory Coordination Committee, NREL
Scott Mix, Vice-Chair of Laboratory Coordination Committee,

Workshop Housekeeping

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

- Rest rooms
- Emergency Evacuation
- Please keep your wristbands on – they are your access into this room and to lunch
- Lunch - Level 2 in Bellini from 12:00 – 1:00 pm
- Afternoon refreshments at 2:00

Agenda

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

8:00	Arrival and Networking	
8:30	Workshop Introduction	Garrett Nilsen, Deputy Director, SETO Guohui Yuan, Program Manager, SETO Marissa Morales-Rodriguez, Technology Manager, SETO
9:00	Keynote Speaker	Elaine Ulrich, DOE Office of Cybersecurity, Energy Security and Emergency Response
9:20	S2G Project Accomplishments BP1 & BP2	Danish Saleem, Chair of Laboratory Coordination Committee, NREL Scott Mix, Vice-Chair of Laboratory Coordination Committee, PNNL
9:50	Networking Break	
10:00	Panel 1: DER Cybersecurity Standards and Certifications	Moderator: Danish Saleem, NREL • Mike Slowinske, UL Solutions • Ryan Quint, North American Electric Reliability Corporation • Tal Homsky, Solar Edge • Bheshaj Krishnappa, Solar Energy Industries Association
11:00	Panel 2: DER Supply Chain Assessment	Moderator: Emma Stewart, INL • Jeffrey Mitchell, INL – Energy Cyber Sense Overview: Engagement with Solar • Ryan Cryar, NREL – DER Digital Supply Chain Gap Analysis • Ron Brash, aDolus – Managing Supply Chain Security Intelligence

Agenda

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

12:00	Lunch and Networking	
1:00	Panel 3: DER Risk Assessments & Mitigation	Moderator: Scott Mix, PNNL • Scott Mix, PNNL – Mitigating Supply Chain Risk for the Solar Industry • Andrew Bartels, Operant Networks – Experience with SD2-C2M2 Assessment • Stephen Bukowski, INL – SolarShield and Industry • Sheri Gribbin, CNK Solutions
2:00	Panel 4: DER Vulnerability Assessments and Analysis	Moderator: Jay Johnson, SNL • Keira Elliott/Jon Hurtado, SNL – Vulnerability Analysis and SOAR • Jennifer Guerra, NREL – DERMS Cybersecurity and Recommendations for Aggregators • Wajid Hassan, LogicFinder – Identifying Vulnerabilities through Penetration Testing and Vulnerability Assessment
3:00	Training and Workforce Development	Megan Culler, INL – CyberStrike StormCloud for Solar
3:15	Networking Break	
3:20	Future Areas of Research & Industry Feedback	
4:20	Workshop Closing	Marissa Morales-Rodriguez

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Workshop Introduction

Garrett Nilsen, Deputy Director, SETO
Marissa Morales-Rodriguez, Technology Manager, SETO
Guohui Yuan, Program Manager, SETO

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Opening Remarks

Garrett Nilsen, Deputy Director, SETO

U.S. DEPARTMENT OF ENERGY

Office of ENERGY EFFICIENCY & RENEWABLE ENERGY

Securing Solar for the Grid Workshop

Garrett Nilsen

Deputy Director, Solar Energy Technologies Office

U.S. DOE-Energy Efficiency and Renewable Energy

Solar Energy Technologies Office

Our mission is to accelerate the advancement and deployment of solar technology in support of an equitable transition to a decarbonized economy no later than 2050, starting with a decarbonized power sector by 2035.

To achieve this mission, solar energy must:

- Be affordable and accessible for all Americans
- Support the reliability, resilience, and security of the grid
- Create a sustainable industry that supports job growth, manufacturing, and the circular economy in a wide range of applications

Solar Hardware Technologies

Photovoltaics (PV)

Utility-Scale PV

Rooftop Solar

Solar + Agriculture

Concentrating Solar-Thermal Power (CSP)

Power Tower CSP

Trough CSP

Thermal Storage

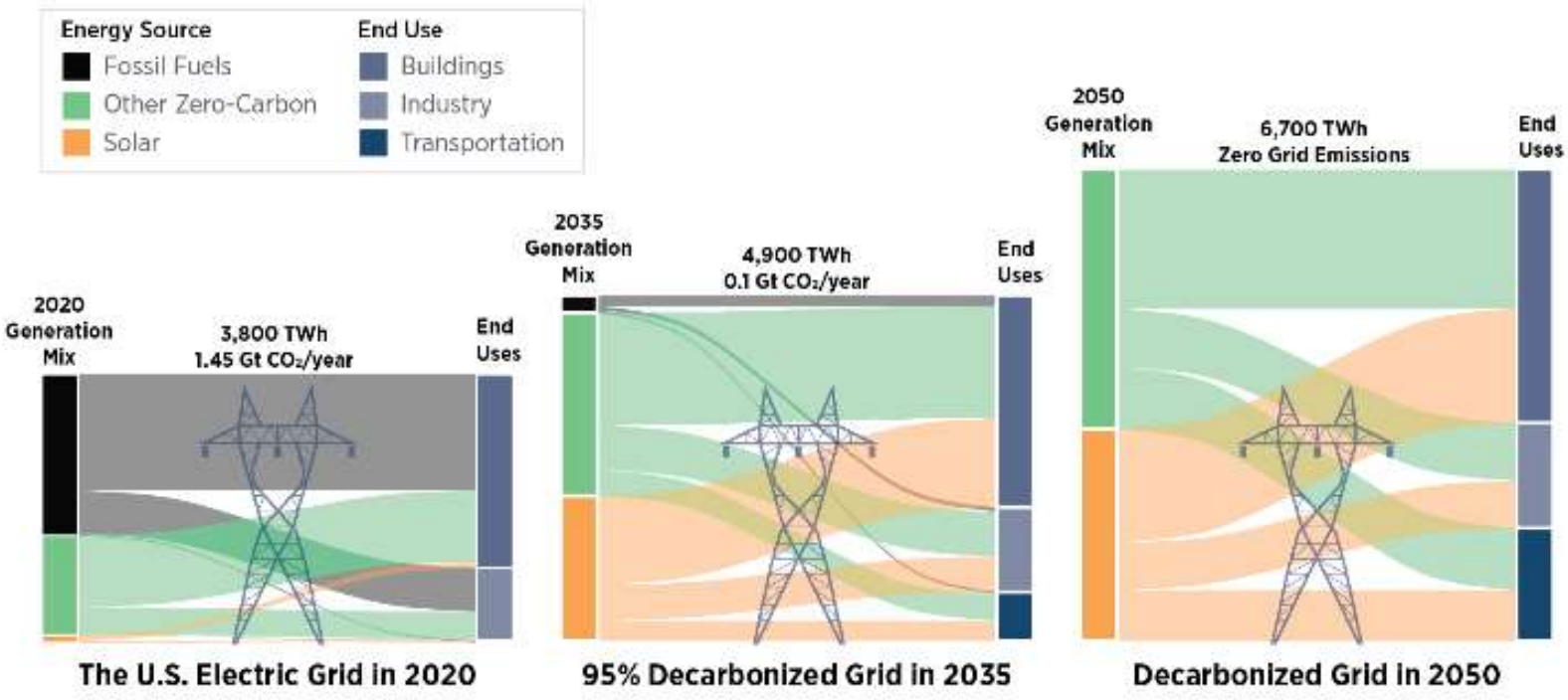
Systems Integration

Energy Storage

Inverters

Sensors

U.S. Energy Mix 2020-2050

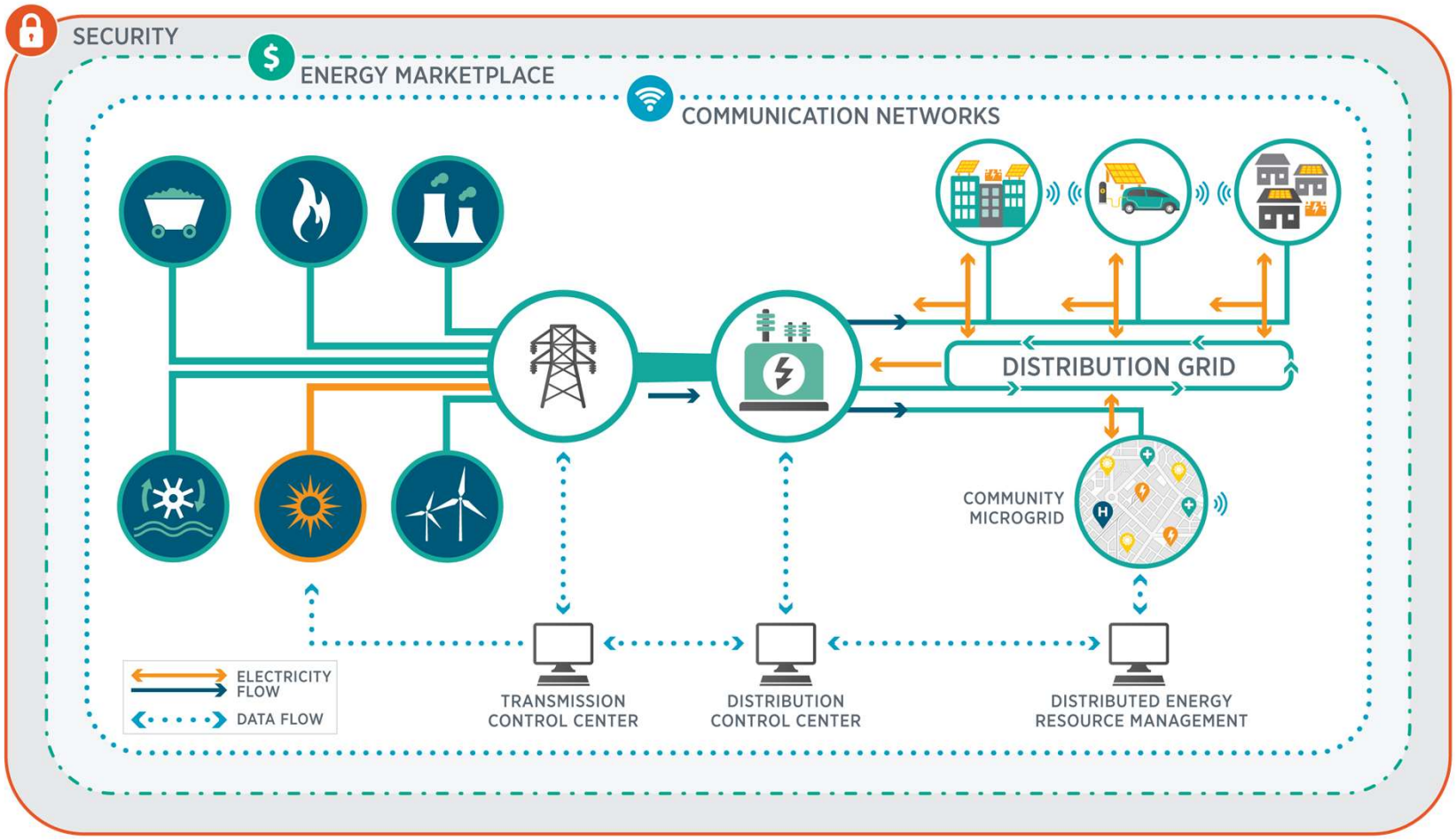


Solar: 3% of electricity demand, 80 gigawatts AC installed

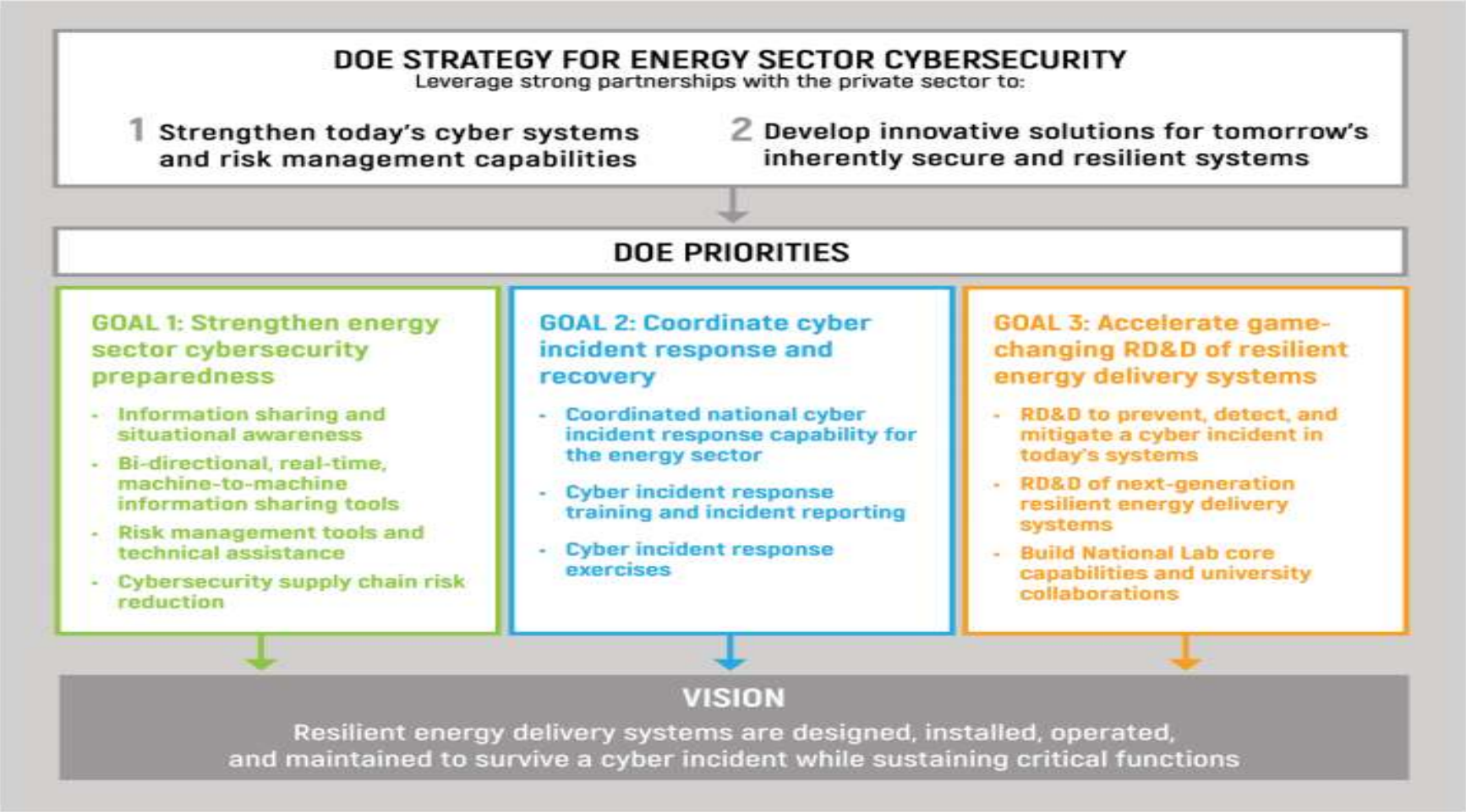
Solar: 40% of electricity demand, 1,000 gigawatts installed

Solar: 45% of electricity demand, 1,600 gigawatts installed 3,000 GW in decarbonized energy system

Just this easy to wrap security around everything?



EERE and SETO Activities Align With DOE's Broader Cybersecurity Strategies



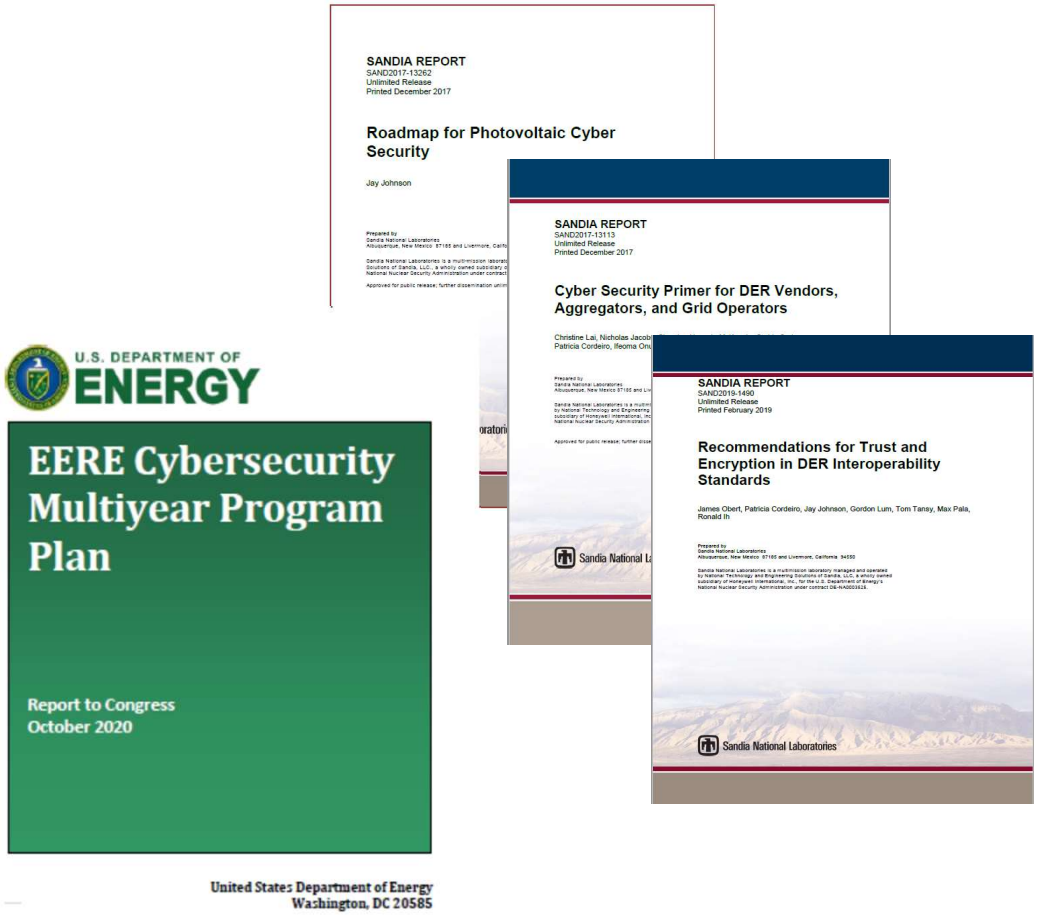
Cybersecurity a Key Challenge and an EERE Priority

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

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

Goal 2: Increase EERE Stakeholder Cybersecurity Awareness

- **2.1 Improve situational awareness.**
- **2.2 Enhance EERE technology cybersecurity maturity.**
- **2.3 Identify opportunities for EERE stakeholder participation in cyber incident response exercises.**

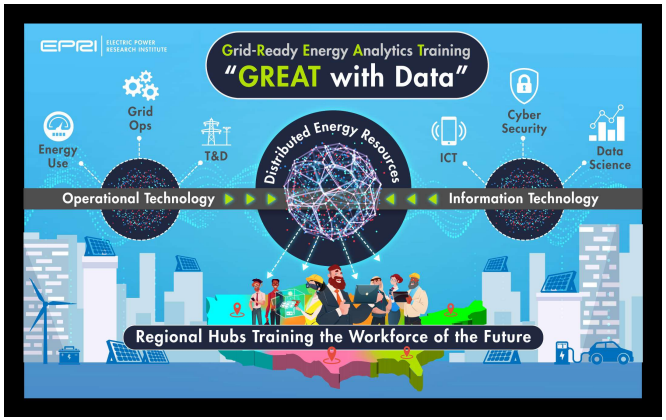


Don’t forget dissemination…

Workforce Development

Broader Grid Communications- EPRI

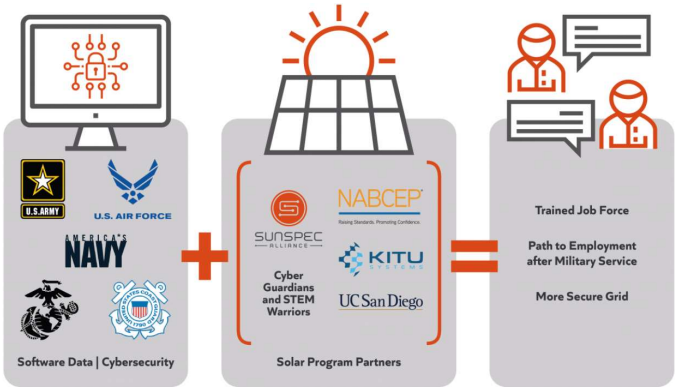
- The *GREAT with Data* initiative I developing and delivering training and education (T&E) materials (both professional and university training) to address issues for merging Grid Operations Technology (OT) and Information Technology (IT).
- Revamp power systems engineering education by leveraging new electric industry R&D and operational experiences



Ends in 2024

Cyber Specific Education- SunSpec

- The Cyberguardians and STEM Warriors project worked to establish a complete learning and career advancement system for veterans, transitioning military personnel and other qualified individuals to enter the DER workforce.



The SunSpec Alliance Cyberguardians and STEM Warriors project will take participants from curriculum enrollment through completion, then help them get hired. Graphic courtesy of SunSpec Alliance.

Completed in 2022

Enabling Solar Cybersecurity Solutions Through State Energy Office and Public Utility Commission Engagement with Private Sector Partners (NASEO/ NARUC)

- Through this project NASEO and NARUC was looking to help protect solar energy infrastructure and the United States' electric grid, at large, against cyber threats by identifying opportunities for State Energy Offices and Public Utility Commissions to pursue policies, plans, and partnerships that support solar cybersecurity.
- NASEO and NARUC is establishing a Solar Cybersecurity Advisory Group, which will be composed of State Energy Officials, Public Utility Commissioners, solar industry stakeholders, cybersecurity experts, utility representatives, and others.
- The advisory group is reviewing existing literature and policy pertaining to solar cybersecurity to identify case studies, industry best practices, and policy precedents that can be built into a series of tools and resources to empower states to support cybersecurity for solar infrastructure within their respective jurisdictions.

Project ends in Q1 2024

Thank you!

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Opening Remarks

Guohui Yuan, Program Manager, SETO

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Opening Remarks

Marissa Morales-Rodriguez, Technology Manager, SETO

U.S. DEPARTMENT OF ENERGY

Office of ENERGY EFFICIENCY & RENEWABLE ENERGY

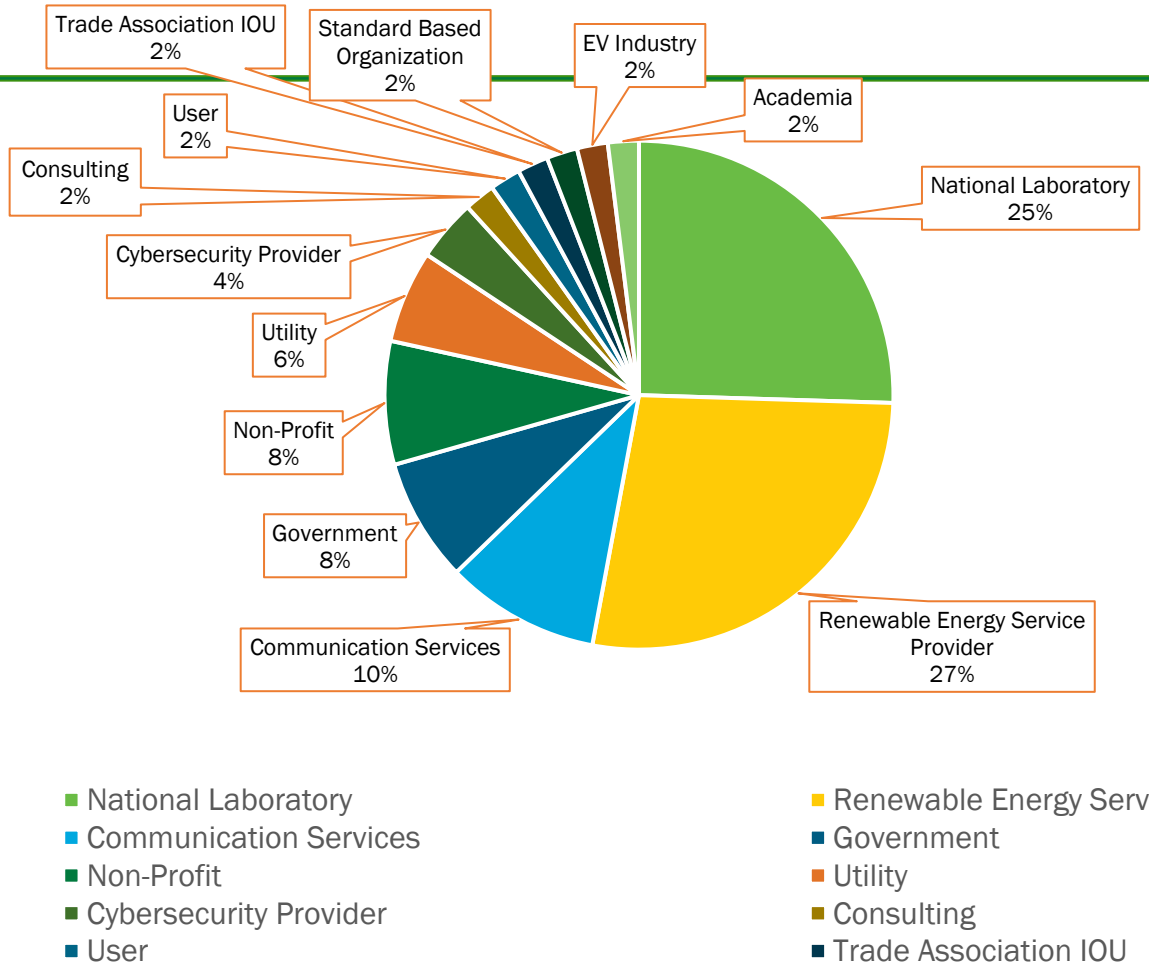
Securing Solar for the Grid (S2G): Our Mission

Marissa E. Morales-Rodriguez, Ph.D.

Technology Manager, Solar Energy Technologies Office

U.S. DOE-Energy Efficiency and Renewable Energy

Welcome!


Trade Association IOU 2%
Standard Based Organization 2%
EV Industry 2%
Academia 2%
User 2%
Consulting 2%
National Laboratory 25%
Cybersecurity Provider 4%
Utility 6%
Non-Profit 8%
Government 8%
Communication Services 10%
Renewable Energy Service Provider 27%
National Laboratory
Renewable Energy Service Provider
Communication Services
Government
Non-Profit
Utility
Cybersecurity Provider
Consulting
User
Trade Association IOU

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

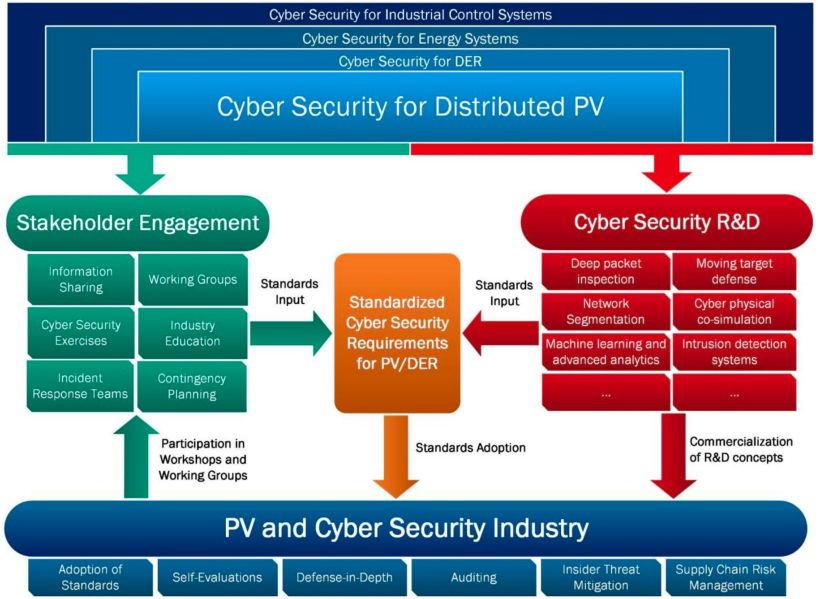
APPROACH

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.

Cyber-physical Approach



Source: Roadmap forPhotovoltaicCyberSecuritySAND2017-132624-10-2018

Research Areas

STANDARDS DEVELOPMENT & BEST PRACTICES

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

EDUCATION & WORKFORCE DEVELOPMENT

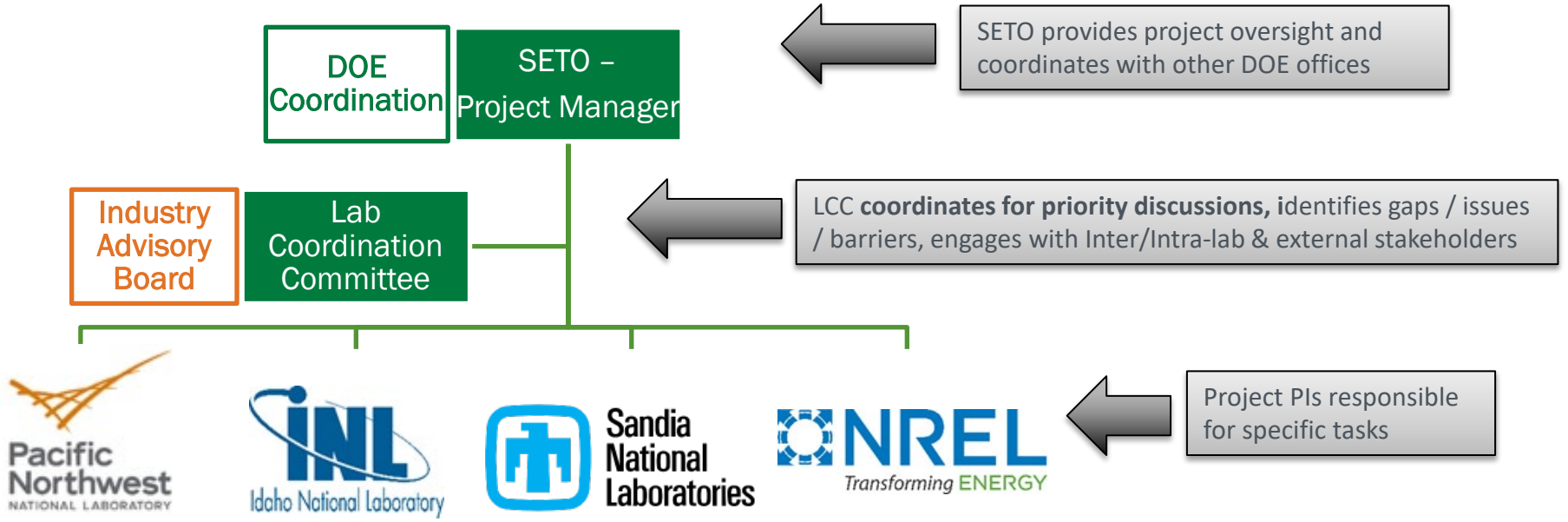
Development of educational modules and training to increase cybersecurity awareness and knowledge within solar stakeholders.

CYBERSECURITY TOOL KIT & SUPPLY CHAIN

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

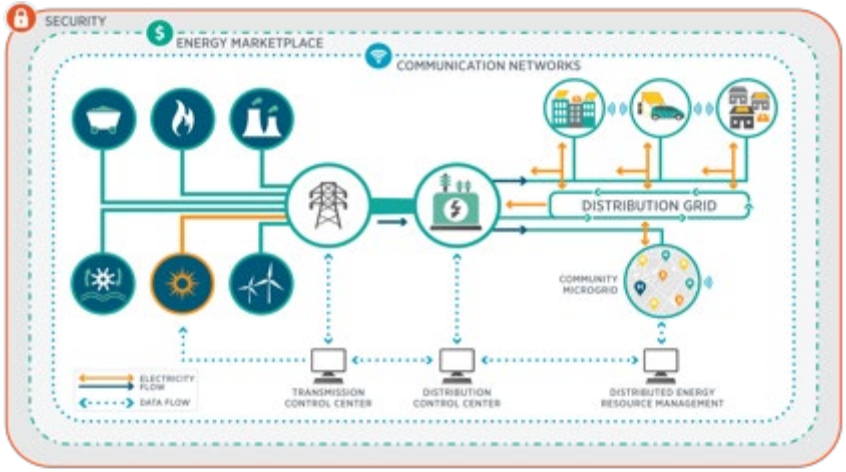
INCREASING CYBERSECURITY LEVELS OF SOLAR TECHNOLOGIES

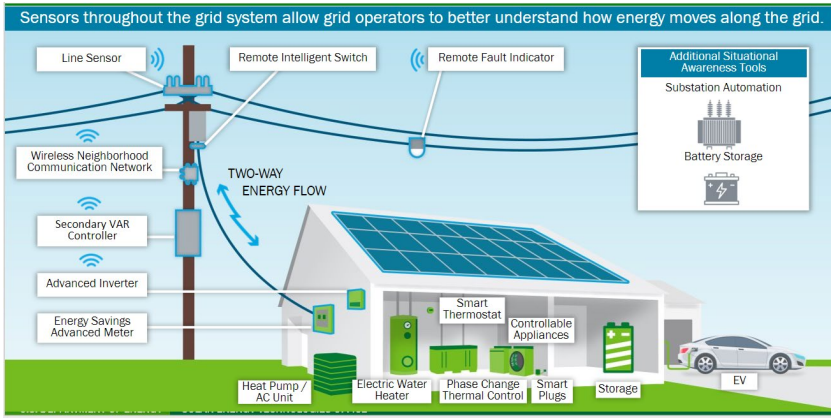
Project Management Structure




To manage, optimize, and secure the future grid, new technologies, control techniques, and supporting reliability and security standards will be required.

DER Integration





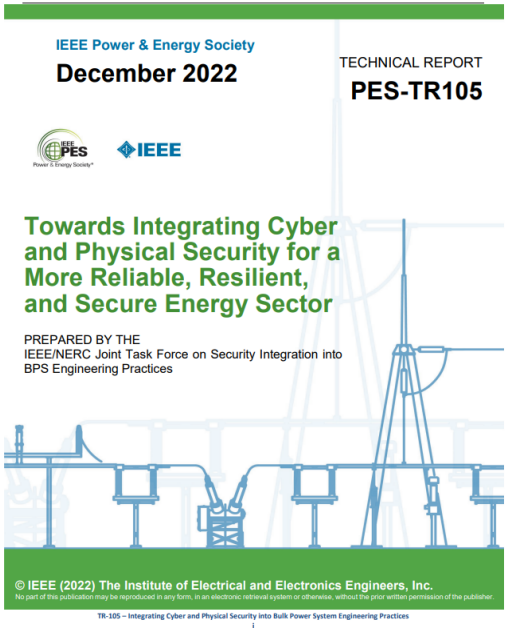
Stakeholders

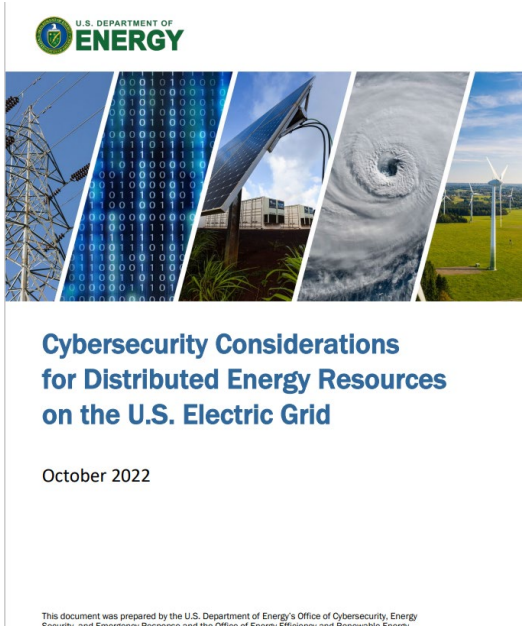
- Manufacturers
- Vendors
- Asset Owners
- Aggregators
- Utilities
- Regulators
- Government

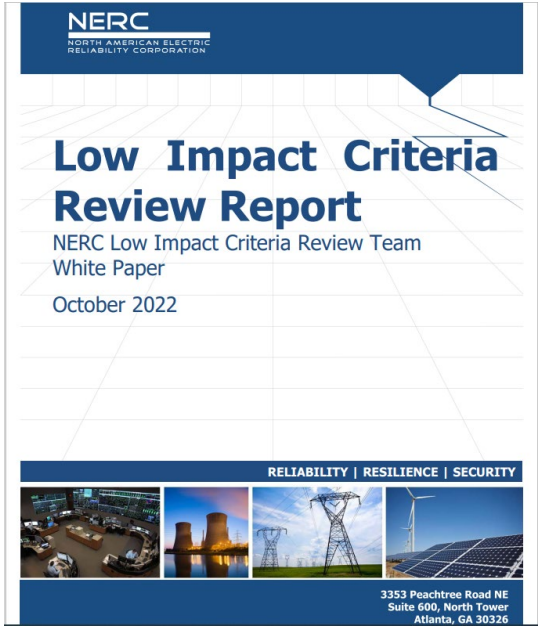
Enabling Technologies

- Cloud Computing
- Artificial Intelligence & Machine Learning
- Digital Twins
- Smart Sensors
- Edge Analytics

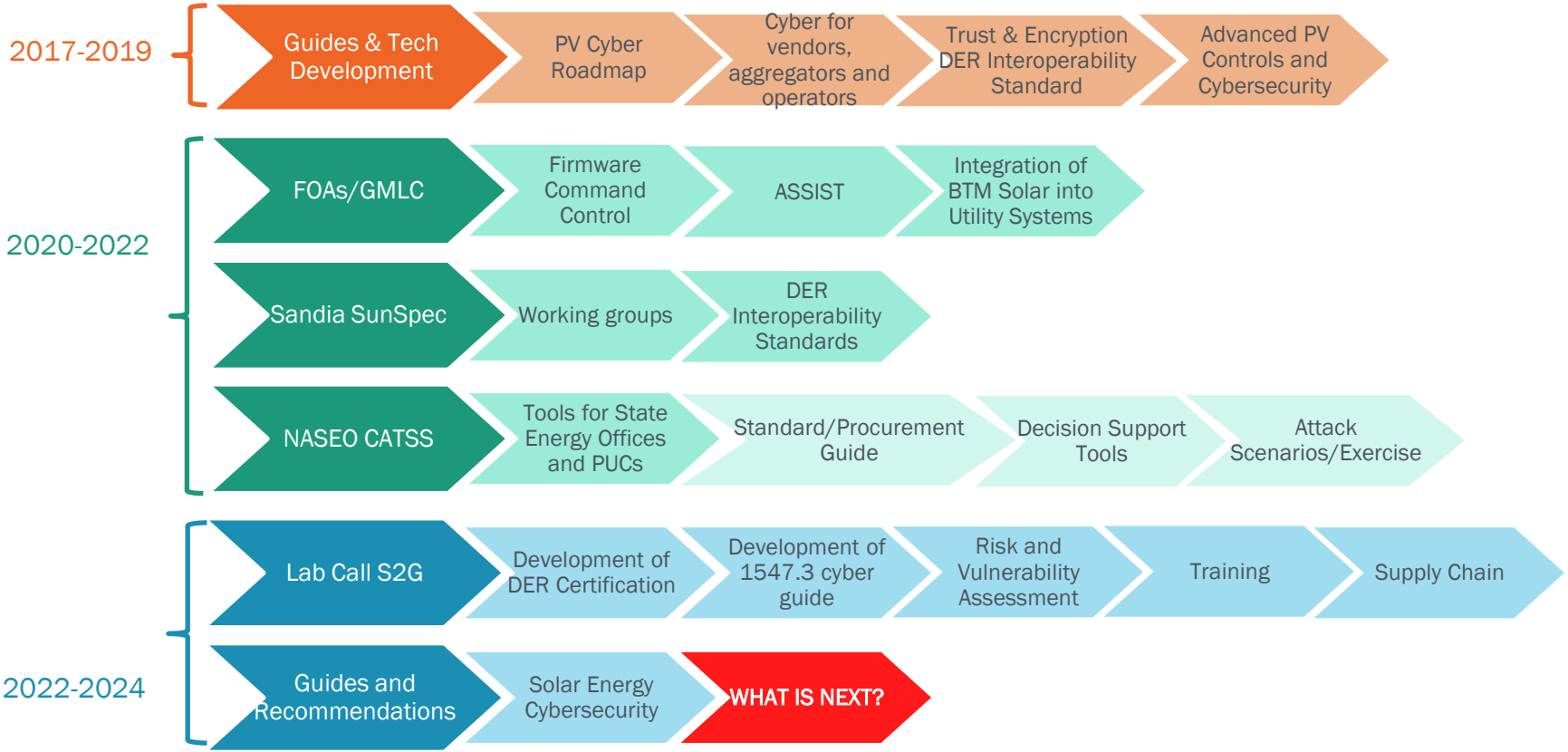
Recent Reports



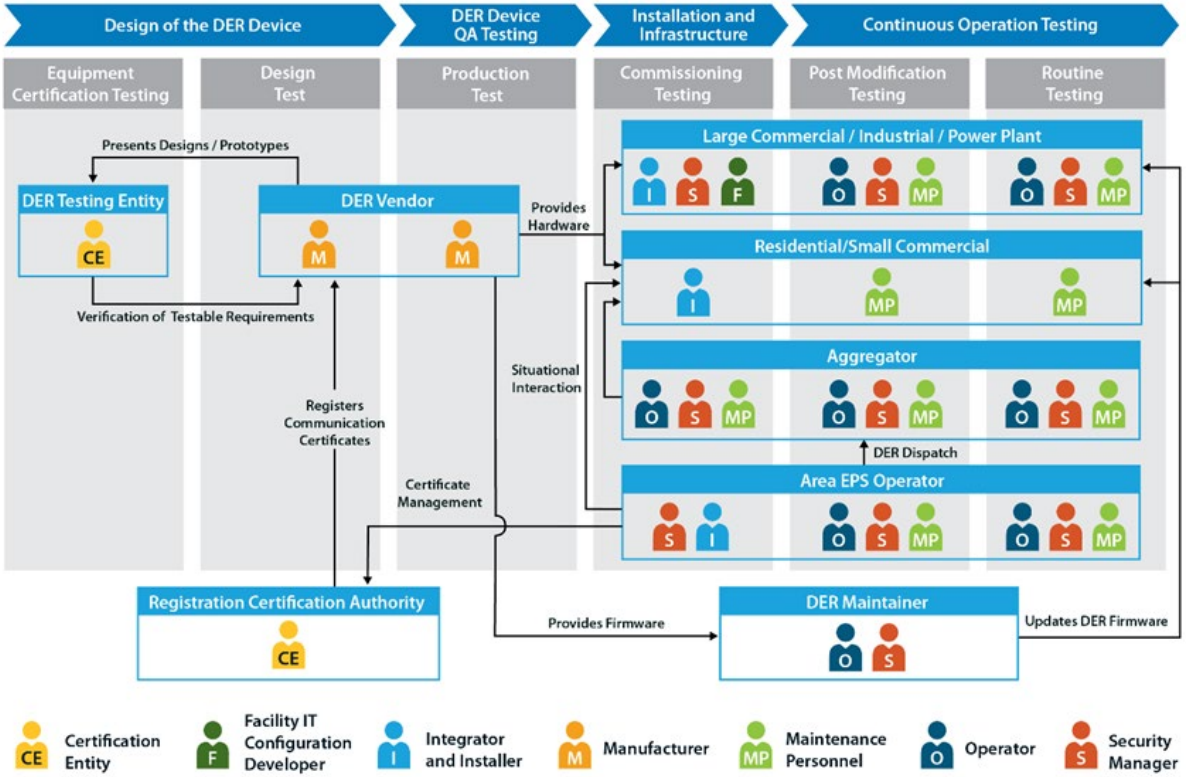




SETO: DER Cybersecurity Efforts



Who is our audience?



Source: NREL

Summary

- The rapid deployment of renewables and distributed energy resources onto the power grid presents new challenges to energy sector cybersecurity.
- A **holistic approach** in information technology (IT) and operation technology (OT) risk management is needed that encompass utility systems with customer owned DER devices and third-party operated systems.
- Need to build **community awareness and information sharing** mechanisms to incorporates equipment standards and vigorous testing, validation, and certification – including global supply chains for products like solar inverters.
- The **DOE and national labs** can provide technical expertise, research and testing capabilities, and funding to support industry
- **Collaboration** is crucial – within DOE program offices, other federal agencies, state and local governments, and industry.

What to expect during the workshop?

- **Networking Activities**
- **Community Building**
- **Discussions:**
  - Research Topics
  - Technical Gaps
  - Next Steps

Thank you!

marissa.morales-rodriguez@ee.doe.gov

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Keynote

Elaine Ulrich, DOE Office of Cybersecurity, Energy Security and Emergency Response

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

Securing Solar for the Grid (S2G) Keynote Speaker

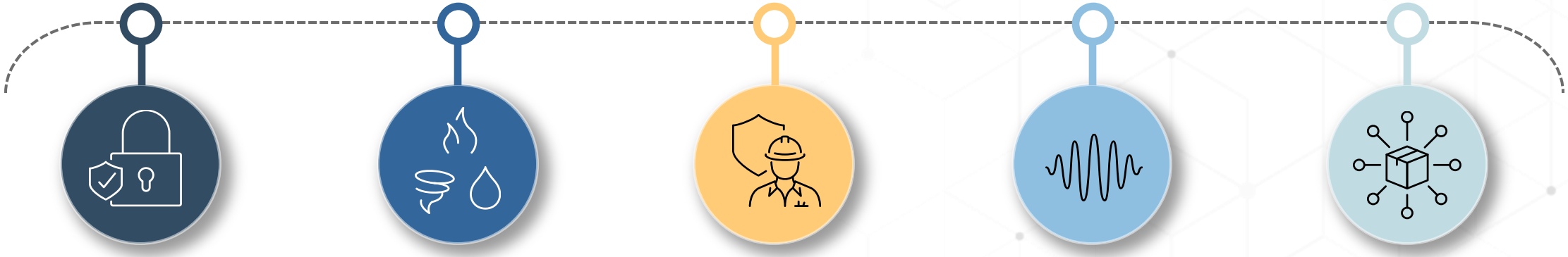
Elaine Ulrich, Preparedness, Policy, and Risk Analysis

September 14th, 2023

CESER Mission

Strengthen the security and resilience of the U.S. energy sector from cyber, physical, and climate-based risks and disruptions.

Evolving Threats to Energy Infrastructure



CESER's Overall Approach

- **What's the risk?**
  - Risk analysis
- **How do you mitigate the risk?**
  - Policies *(National Security Council, States)*
  - Capacity building *(e.g., training, exercises, workforce development)*
  - Cyber and resilience-informed engineering (partnering with other DOE offices, industry)
  - Research and development *(partnering with S3 & S4, industry, academia)*
- **What happens during an emergency?**
  - Respond and restore
  - Execute emergency authorities
  - Leverage tools such as the Strategic Petroleum Reserve
  - Inform short-term and long-term recovery efforts

CESER Structure

Preparedness, Policy, and Risk Analysis

- Energy Security Policy and Partnerships
- Exercises, Training, Workforce Development
- Risk Analysis, Resilience, and Recovery

Risk Management Tools and Technologies

- All-Hazards Tools and Technologies
- Cyber Tools and Technologies

Response and Restoration

- All Hazards Situational Awareness and Analysis
- All Hazards Response Operations
- Response Preparedness and Support

Office of Petroleum Reserves

- Planning & Engineer Office
- Operations & Readiness
- Budget & Financial Management Technologies
- Management & Administration
- Reserve Lands Management
- SPR Project Management

Corporate Business Office

Strategic Communications

Front Office

Collaboration and Coordination is Essential

State, Local, Tribal, and Territorial (SLTT) Governments

NASEO
National Association of State Energy Officials

National Association of Regulatory Utility Commissioners

American Public Power Association

NCSL

NEMA™

NGA
National Governors Association

Energy Government Coordinating Council (EGCC)

Department of Defense

Executive Office of the President

Department of Homeland Security

Transportation Security Administration

Department of Energy

Department of Transportation

United States Coast Guard

Office of the Director of National Intelligence

NASEO NARUC NGA

Industry Councils

ESCC
Electricity Subsector Coordinating Council

Oil and Natural Gas Subsector Coordinating Council

Cybersecurity Capability Maturity Model (C2M2)

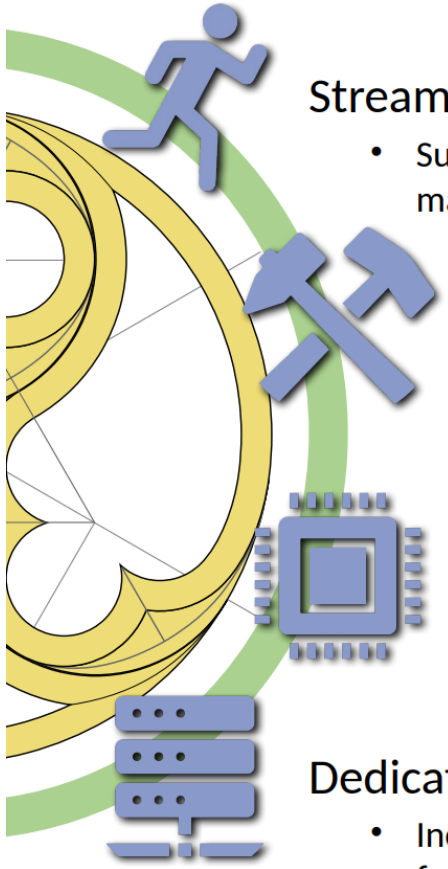
- C2M2 is a free tool to help organizations evaluate their cybersecurity capabilities and optimize security investments.
- The tool uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments.
- An organization can complete a self-evaluation using the C2M2 tools in as little as one day. If requested, DOE can also facilitate a free C2M2 self-evaluation for U.S. Energy Sector organizations. Feel free to email C2M2@hq.doe.gov for more information.

C2M2
Cybersecurity Capability Maturity Model

MALCOLM Tool Suite (INL)

Malcolm

A powerful open-source network traffic analysis tool suite.
https://github.com/idaholab/Malcolm



Streamlined deployment

- Suitable for field use (hunt or incident response) or SOC deployment. Runs in Docker on Linux, macOS and Windows platforms. Provides easy-to-use web-based user interfaces.

Industry-standard tools

- Uses Arkime and Zeek for network traffic capture, Logstash for parsing and enrichment, OpenSearch for indexing and Dashboards and Arkime Viewer for visualization. Also leverages OpenSearch Anomaly Detection, Suricata IDS, YARA, capa, ClamAV, CyberChef and other proven tools for analysis of traffic and artifacts.

Expanding control systems visibility

- Analyzes more protocols used in operational technology (OT) networks than other open-source or paid solutions. Ongoing development is focused on increasing the quantity and quality of industrial control systems (ICS) traffic.

Dedicated sensor appliance

- Includes Hedgehog Linux, a hardened Linux distribution for capturing network traffic and forwarding its metadata to Malcolm.

Exercises and Training

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

U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE PROGRAM

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

U.S. DEPARTMENT OF ENERGY'S
CONQUER THE HILL
PART OF THE CYBERFORCE PROGRAM

Clean Energy Cybersecurity Accelerator (CECA)

- CECA is a technology partnership of federal experts, industry partners in the energy sector, and innovators to accelerate the development of new cybersecurity solutions for the nation's evolving grid.
- The accelerator was launched by DOE and the National Renewable Energy Lab (NREL) to support efforts to modernize the grid, address cybersecurity vulnerabilities, and create a grid that will withstand the transition to a clean energy economy in the effort to reach net-zero emissions by 2050.
- https://www.nrel.gov/innovate/cybersecurity-accelerator.html

Resources and Publications

- National Cyber-Informed Engineering (CIE) Strategy
  - FINAL DOE National CIE Strategy - June 2022_0.pdf (energy.gov)
  - CIE approaches use design decisions and engineering controls to mitigate or even eliminate avenues for cyber-enabled attack or reduce the consequences when an attack occurs.
- DOE Cybersecurity Report Provides Recommendations to Secure Distributed Clean Energy on the Nation's Electricity Grid | Department of Energy
  - Provides recommendations for the DER industry, energy sector, and government to take action and secure current and future systems.

National Cyber Security Strategy

Pillar 4: Invest in a Resilient Future

Strategic Objective 4.4: Secure Our Clean Energy Future

Initiative Number: 4.4.1

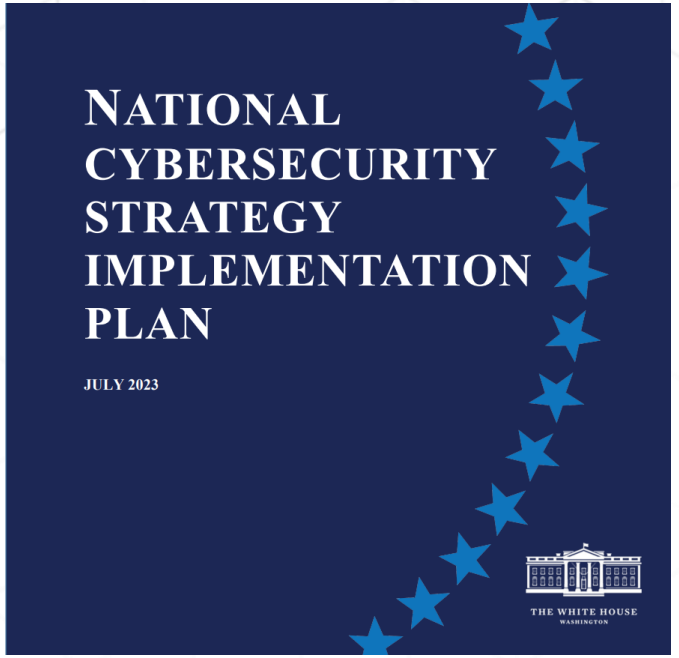
Initiative Title: Drive adoption of cyber secure-by-design principles by incorporating them into Federal projects

Initiative Description

The Department of Energy, working with ONCD and CISA, will work with stakeholders to identify and implement cyber secure-by-design pilot projects, identify economic incentives for cyber secure-by-design, identify needed technology vehicles to apply cyber secure-by-design principles, and measure progress on national implementation of cyber secure-by-design efforts for critical infrastructure.

NCS Reference

DOE, through efforts such as the Clean Energy Cybersecurity Accelerator (CECA) and the Bipartisan Infrastructure Law-directed Energy Cyber Sense program, and the National Labs are leading the government's effort to secure the clean energy grid of the future and generating security best practices that extend to other critical infrastructure sectors. DOE will also continue to promote cybersecurity for electric distribution and distributed energy resources in partnership with industry, States, Federal regulators, Congress, and other agencies.



CESER Announces $39 Million in Clean DER Funding

- On Tuesday, September 12th, 2023, DOE CESER announced $39 million of funding for nine new National Laboratory projects to advance the cybersecurity of DERs.
- The National Laboratory teams aim to improve real-time DER operation data analytics using artificial intelligence (AI)/machine learning (ML) and secure cloud-based solutions for DER applications.
  - The Labs will develop security solutions for current and emerging communication architectures for DER systems and develop innovative, real-time or off-line analysis technologies that secure DER.

Report to Congress on Cybersecurity of Distribution Systems

In support of the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security and Emergency Response (CESER), ***NREL is leading the Infrastructure Bill's Section 40121 Report on Cybersecurity of Distribution Systems***:

A report to Congress that assesses—

(1) priorities, policies, procedures, and actions for enhancing the physical security and cybersecurity of electricity distribution systems, including behind-the-meter generation, storage, and load management devices, to address threats to, and vulnerabilities of, electricity distribution systems; and

(2) the implementation of the priorities, policies, procedures, and actions assessed under paragraph (1), including—

(A) an estimate of potential costs and benefits of the implementation; and

(B) an assessment of any public-private cost-sharing opportunities.

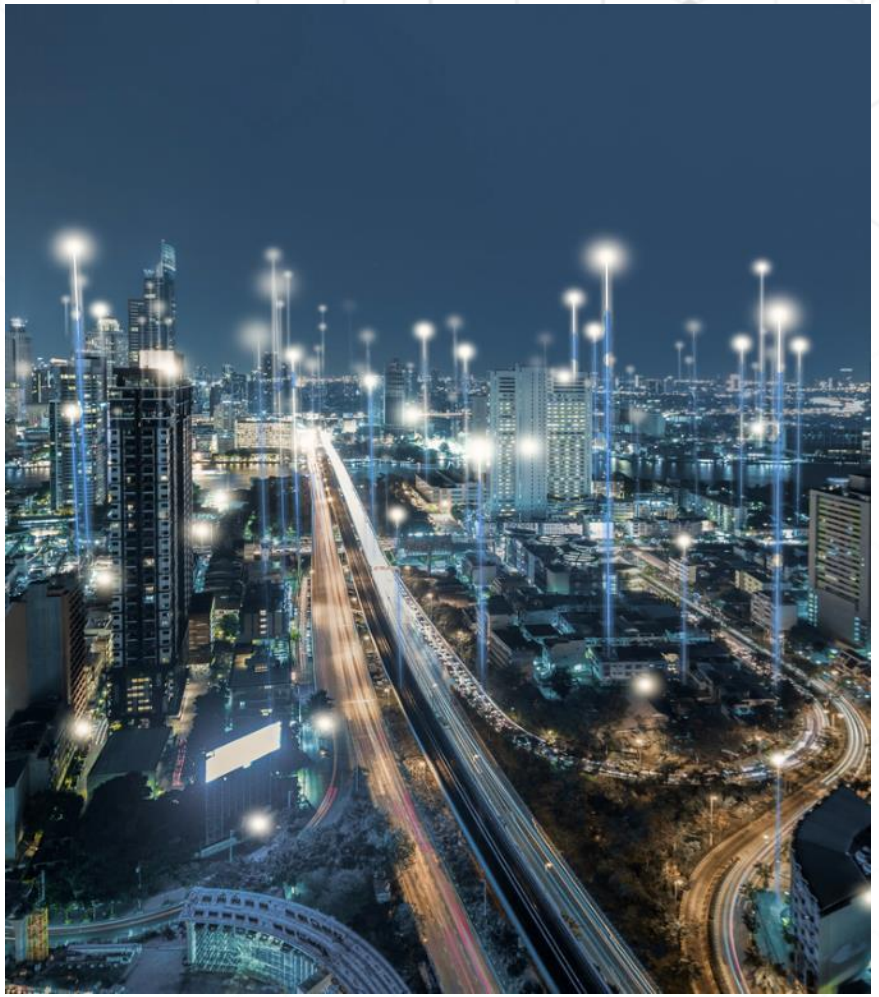
Fundamental Questions

Scope of the Report

- **PRIMARY FOCUS:** Electrical distribution systems, with particular attention paid to future systems in 2030
- Aspects of cybersecurity that are unique to operational technology for distribution systems
- Physical security related to cyber assets.

Relevant Trends

- Avid adoption of digital technology
- Increase in scale of connected devices
- Non-utility devices supporting reliability
- More stakeholders exchanging more information
- Perimeter security model challenged
- Aggregations of DERs and FERC 2222
- More interdependency of critical infrastructures



Technical Contributors

Argonne NATIONAL LABORATORY

BERKELEY LAB

INL Idaho National Laboratory

Lawrence Livermore National Laboratory

NREL NATIONAL RENEWABLE ENERGY LABORATORY

OAK RIDGE National Laboratory

Pacific Northwest NATIONAL LABORATORY

Sandia National Laboratories

PURPOSE Led by NREL, technical contributors are responsible for gathering relevant supporting material, performing analysis, authoring the report, incorporating feedback from the Federal Sponsor Committee and stakeholders, and revising content.

Our Greatest Challenges

- Managing risk and distributing responsibility
- Technology gaps and adoptability
- The size and skill of the cyber workforce
- Diversity of stakeholders in the system

Recommendations Broken Into 5 Pillars

1. Better Quantify Cyber Risk and Equitably Allocate Responsibilities
2. Develop Technology That is Inherently Secure, Scalable, and Easily Adoptable
3. Establish Infrastructure to Unlock Innovation and Support Mission Rehearsal
4. Strengthen the Distribution System Cybersecurity Workforce
5. More Coordination to Support Collective Resilience


ENERGY TRANSITION SUMMIT
Grid Modernization
Creating the modern grid of the future
Clean Energy Cybersecurity
Fostering collaborative security solutions
February 5-8, 2024
Crystal Gateway Marriott
1700 Richmond Hwy, Arlington, VA 22202
U.S. DEPARTMENT OF ENERGY
Led and hosted by the U.S. Department of Energy national laboratories.

Questions?

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

S2G Project Accomplishments
BP1 & BP2

Danish Saleem, Chair of Laboratory Coordination Committee, NREL
Scott Mix, Vice-Chair of Laboratory Coordination Committee, PNNL

Project Team

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

National Laboratory Point of Contacts

- **Idaho National Laboratory (INL):** Jake P. Gentle Jake.Gentle@inl.gov and Stephen A. Bukowski Stephen.Bukowski@inl.gov
- **National Renewable Energy Laboratory (NREL):** Danish Saleem Danish.Saleem@nrel.gov and Ryan Cryar ryan.cryar@nrel.gov
- **Pacific Northwest National Laboratory (PNNL):** Scott Mix scott.mix@pnnl.gov
- **Sandia National Laboratories (Sandia):** Jay Johnson jjohns2@sandia.gov and Chris Lamb cclamb@sandia.gov

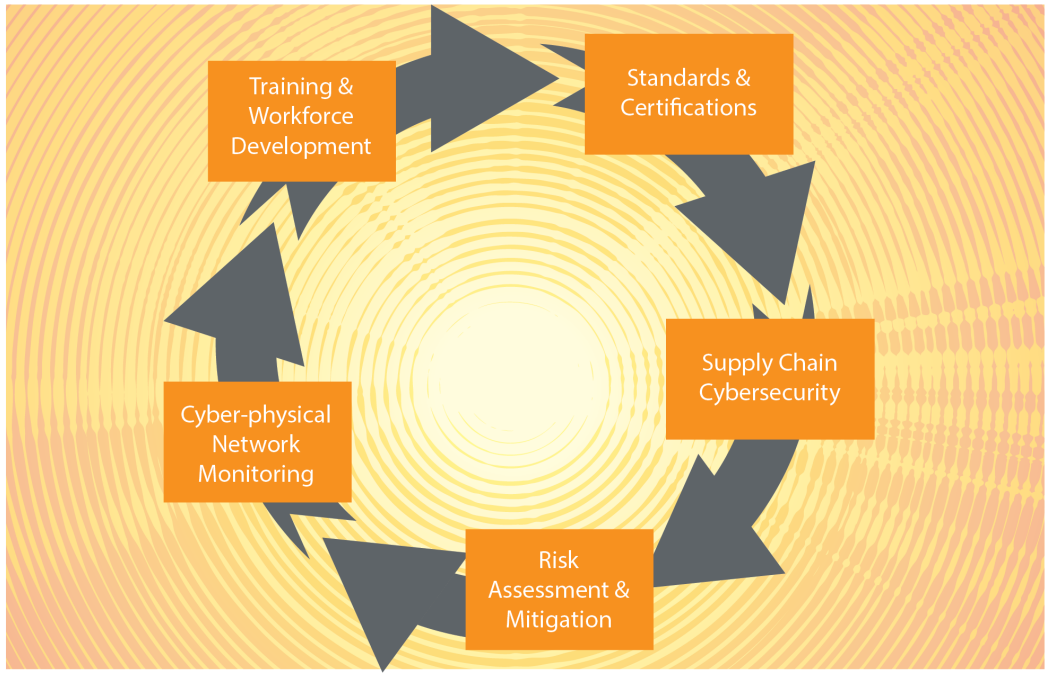
Industry Advisory Board Members

aDolus: Ron Brash	**Fortress:** Tobias Whitney	**NCCOE:** James McCarthy	**SEIA:** Bheshaj Krishnappa
Ampere: Patrick Miller	**GE:** Arvind Tiwari Kumar	**NERC:** Ryan Quint & Larry Collier	**Sense**: Jeremiah Miller
AT&T: Eric Grine	**GridSecurity:** John Franzino	**NERC-CIP:** Lonnie Ratliff	**SEPA:** Aaron Smallwood
AutoGrid Systems: Adam Todorski	**Hitachi Energy:** Steven Kunsman	**Nevermore Security:** Annabelle Lee	**Siemens**: Bruno Paes Leao & Sudeep Vakiti
Axio: David White	**Iowa State Uni:** Manimaran Govinda	**Nexight group**: Cameron Beals	**Solar Edge**: Uri Sadot & Tal Hominsky
Burns & McDonell: Ingrid Rayo	**IREC:** Brian Lydic	**NIST/NCCoE:** Jim McCarthy	**Solectria Solar:** Emily Hwang
CNK solution: Shari Gribbin	**ISA:** Andre Ristaino	**NV Energy**: Michael Brown	**Solv Energy**: Eric Valleton
ConEdison: Thomas Chen & Serena Lee	**Kevala:** Parth Pradhan	**Operant Networks:** Andrew Bartels	**SunSpec:** Tom Tansy
Eaton: Dmitry Ishchenko	**Logic Finder:** Wajid Hassan	**Phillips**: Radhika Chaturvedi	**TVA**: Brad Chadwell
Edison Electric Institute: David Batz	**Mana Group:** Jennifer Jenkins	**PJM:** Eric Hsiah	**UL:** Mike Slowinske & Ken Boyce
Enphase: Adam Rosenstein	**NARUC:** Lynn Costantini	**Savion:** Gizelle Wray	**Veloce Energy:** Salam Bani Ahmed
Florida International Uni: Arif Sarwat	**NASEO:** Kirsten Verclas	**SCE:** Rob Roel	**Xanthus:** Frances Cleveland

DOE Solar Energy Technologies Office

Securing Solar for the Grid (S2G)

- UL Cybersecurity Certification Program
- IEEE 1547.3
- Secure Design Cybersecurity Capability Maturity Model (SD2-C2M2)



- Risk Assessment Methodologies
- Solar Cyberstrike Training and Tool
- Security Orchestration and Vulnerability Analysis

Lab Coordinating Committee

- National Renewable Energy Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories
- Idaho National Laboratory

LCC Chair: Danish Saleem • LCC Vice-chair: Scott Mix • DOE Leader: Marissa Morales-Rodriguez

Industry Advisory Board

aDolus: Ron Brash

Fortress: Tobias Whitney

NCCOE: James McCarthy

SEIA: Bheshaj Krishnappa

Ampere: Patrick Miller

GE: Arvind Tiwari Kumar

NERC: Ryan Quint & Larry Collier

Sense: Jeremiah Miller

AT&T: Eric Grine

GridSecurity: John Franzino

NERC-CIP: Lonnie Ratliff

SEPA: Aaron Smallwood

AutoGrid Systems: Adam Todorski

Hitachi Energy: Steven Kunsman

Nevermore Security: Annabelle Lee

Siemens: Bruno Paes Leao & Sudeep Vakiti

Axio: David White

Iowa State Uni: Manimaran Govinda

Nexight group: Cameron Beals

Solar Edge: Uri Sadot & Tal Hominsky

Burns & McDonell: Ingrid Rayo

IREC: Brian Lydic

NIST/NCCoE: Jim McCarthy

Solectria Solar: Emily Hwang

CNK solution: Shari Gribbin

ISA: Andre Ristaino

NV Energy: Michael Brown

Solv Energy: Eric Valleton

ConEdison: Thomas Chen & Serena Lee

Kevala: Parth Pradhan

Operant Networks: Andrew Bartels

SunSpec: Tom Tansy

Eaton: Dmitry Ishchenko

Logic Finder: Wajid Hassan

Phillips: Radhika Chaturvedi

TVA: Brad Chadwell

Edison Electric Institute: David Batz

Mana Group: Jennifer Jenkins

PJM: Eric Hsiah

UL: Mike Slowinske & Ken Boyce

Enphase: Adam Rosenstein

NARUC: Lynn Costantini

Savion: Gizelle Wray

Veloce Energy: Salam Bani Ahmed

Florida International Uni: Arif Sarwat

NASEO: Kirsten Verclas

SCE: Rob Roel

Xanthus: Frances Cleveland

Want to join our IAB?

S2G IAB Charter

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

1. **Purpose**
The U.S. Department of Energy (DOE) Office of Solar Energy Technology Office (SETO) has funded the project, Securing Solar for the Grid (S2G), to support the development of equipment and communication cybersecurity standards for distributed energy resources (DERs) and inverter-based resources (IBR), and to help establish a national cybersecurity certification standard that could become the reference for the industry. This project will enable national labs to verify and validate the functionalities through laboratory testing before they get standardized, and will help them to accelerate the development, adoption, and implementation of the cybersecurity standards. The project team consists of the National Renewable Energy Laboratory (NREL), Pacific Northwest National Laboratory (PNNL), Sandia National Laboratory (SNL), Idaho National Laboratory (INL), Lawrence Livermore National Laboratory (LLNL), and Lawrence Berkely National Laboratory (LBNL). This project is establishing an industry advisory board (IAB) to solicit feedback and reviews from key industry stakeholders and to provide updates about the project's activities.

2. **IAB Membership**
Membership in the IAB is voluntary and by invitation only. The subject matter experts (SME) can respond to the invitation to both represent their organization and to provide useful feedback on the S2G project. The selected members of IAB will serve in a purely advisory role. DOE reserves the right to review the proposed IAB members and decline individuals who, in their judgment, do not have the background to provide review and guidance. The IAB is expected to have between 15 and 20 members with a mix of electric utilities, equipment manufacturers and vendors, and other interested parties.

3. **Rights**
The IAB members have the right to publicize the fact of their participation in the IAB. They have the right to disseminate work products from the projects, provided that the work products have been cleared for release by the laboratory coordination committee and DOE's SETO office.

4. **Responsibilities**
The IAB members are responsible to attend bi-annually virtual meetings (once every six months) to provide feedback as requested of them and to review the work products (if any). IAB members are also responsible to not disclose their own company's proprietary or other sensitive information during IAB meetings or in their written feedback.

5. **Meetings**
The project team will host bi-annually virtual IAB meetings to solicit the feedback. The IAB members are also encouraged to join the annual in-person continuation review meeting.

6. **Commitment**
The project team estimates that IAB members are not expected to spend more than 2 hours on IAB work every month. The actual time may vary from month to month.

7. **Term of Membership**
The IAB will exist for the duration of the project, which is scheduled to end September 2024. The minimum expected term of IAB membership is one (1) year.

A collaborative effort by national laboratories, DOE solar office, and clean industry stakeholders and SMEs to address gaps in cybersecurity standards and testing requirements, education & workforce development, and supply chain cybersecurity

Accomplishments

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

INL

- **CyberShield**
  - Developed cybersecurity assessment module, and Malcolm tool for Solar industry. Also established public/private partnerships.
  - Developed materials, websites, and demonstrations to support program and education of CyberShield program for industry
- **CyberStrike STORMCLOUD**
  - Completed production of STORMCLOUD hardware box and rolled out training at Secure Renewables ’23
  - ~20 people attended, sharing 8 workstations
  - Feedback mostly positive, but revisions to labs and curriculum ongoing
- **Hardware Bill of Materials (HBOMs)**
  - Developed HBOMs for three different solar inverters
  - Each integrated circuit board was broken down into individual components
  - Identifiers pulled from components directly or through online research
- **Structured Threat Information eXpression (STIX)**
  - Created STIX bundle for 16 solar inverters and identified vulnerabilities for six of them.
  - Scoring for inverters involved vulnerabilities, evidence of flaw remediation, days to update, and market share

NREL

- **UL 2941 Cybersecurity Certification**
  - Co-led the development and publication of UL 2941
  - Supported the development of technical committee for UL 2941.
- **IEEE 1547 standard and IEEE 1547.3 cybersecurity guide**
  - Co-led the development of IEEE 1547.3 as vice chair
  - Supporting IEEE 1547 revision as subgroup lead for including cybersecurity in the standard
- **DER cybersecurity requirements for CPUC**
  - Performed correlation of DER cybersecurity requirements from three different sources for CPUC
- **DER Supply chain Cybersecurity**
  - Performed gap analysis of supply chain cybersecurity for DERs
  - Developed supply chain cybersecurity recommendations for Solar
- **Distributed Energy Resources Management System (DERMS)**
  - Developed DERMS cybersecurity recommendations for Solar
- **Collaboration with Standard Development Organizations**
  - Collaborated with NERC, IEEE, UL, CPUC, NARUC, NASEO, and others to harmonize standard development efforts.
  - Hosted FY22 workshop at NREL and supported the planning & coordination of FY23 IAB meetings and workshop.

Accomplishments (contd.)

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

PNNL

- **Universal Utility Data Exchange (UUDEX):**
  - Developed information exchange models for Solar DER report
  - Made it available to the UUDEX standardization efforts in IEEE
- **Cybersecurity Assessments**
  - Completed the Cybersecurity Assessment in DER-rich Distribution Operations
  - Completed one SD2-C2M2 assessment with Operant Networks
  - Scheduled additional assessment for the clean energy industry stakeholders
- **Completed conversion of three distribution models and validated them in OPAL-RT using ePHASORsim**
  - Criticality Levels and Impact Analysis submitted to ISGT 2024
- **Documented examples of determining the R1 Resource Criticality Level for each of the three test models**
  - https://github.com/GRIDAPPSD/CIMHub/tree/feature/SETO/CPYDAR
- **Supported Supply chain efforts for Solar DER product evaluations**

SNL

- **Security orchestration, automation, and response for DER**
  - Developed a DER cybersecurity testbed for developing and evaluating a SOAR playbook for DER.
  - Published chapter in 'Power Systems Cybersecurity' on SOAR for DERs.
- **Published cybersecurity recommendations flyer in collaboration with NERC & SEIA**
  - 58 recommendations covering supply chain management, incident response, threat & vulnerability management, situational awareness, and more.
- **Partnered with Xcel Energy to develop two scenarios for GridEx VII**
  - Malicious firmware update on residential and community solar installations
  - A cyber-attack that changes the power output from a 100 MW PV site
- **Ran 1st CyberStrike STORMCLOUD training for DER cybersecurity at the 2023 Secure Renewables conference**
  - Included both a virtualized training environment and a hardware environment
  - The hardware environment includes attacks against a single-axis tracker

Summary of Lab Participation in Standards

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

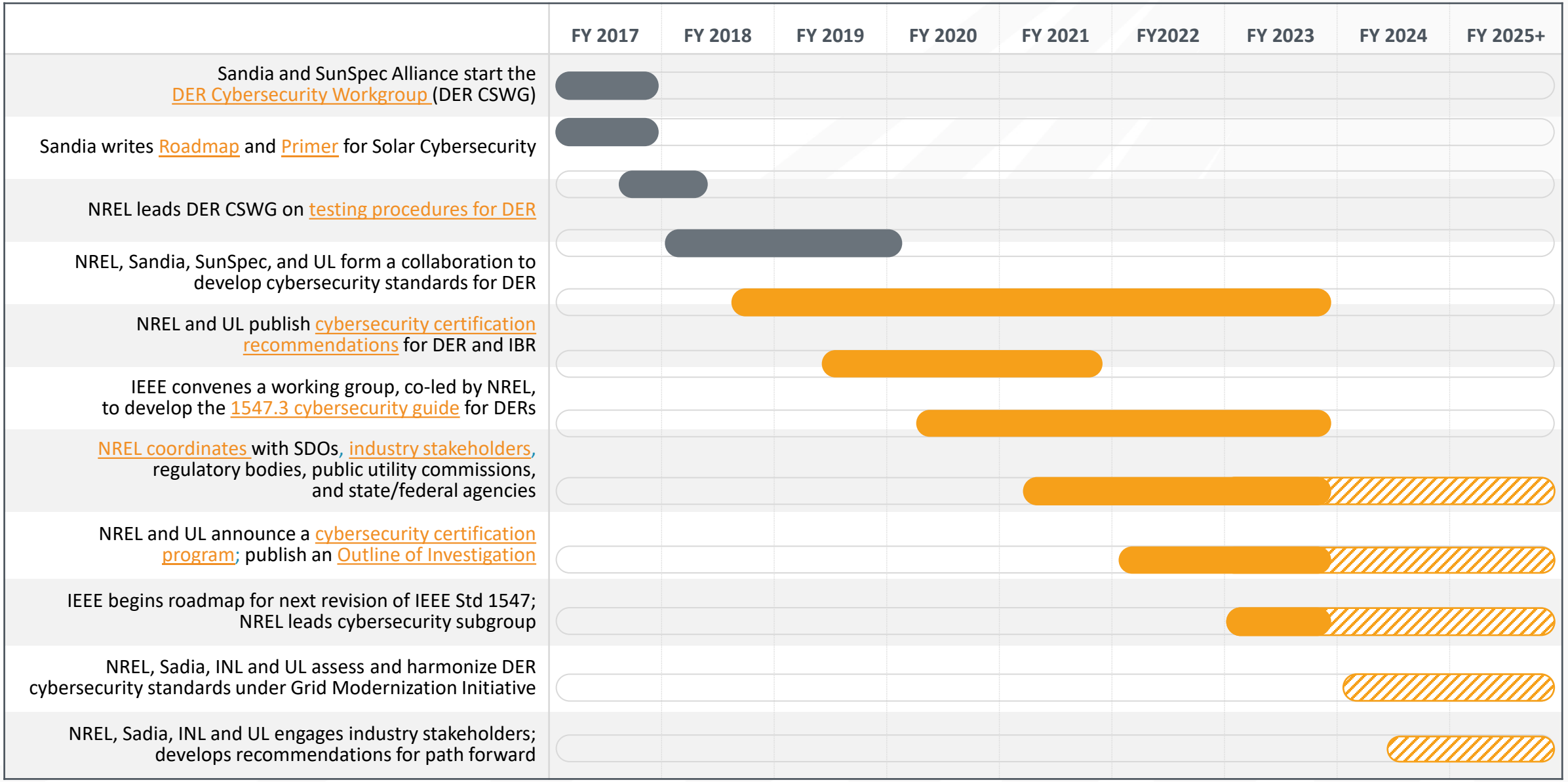
SDO	Standards/Working Groups/Committees	NREL	PNNL	INL	Sandia
UL	UL 2941 cybersecurity certification standard	x			
IEEE	IEEE 1547.3 cybersecurity guide and 1547 standard revision	x			x
IEEE	P2800				x
IEEE	P2030.103 (UUDEX)		x		
IEC	IEC 62351	x			
IEC	IEC 62443		x		
DOE	C2M2 / SD2-C2M2		x		
DOE/DHS	SEI Task Force	x	x	x	x
NARUC/NASEO	Cybersecurity Advisory Team for State Solar	x		x	x
SunSpec	SunSpec-led draft standards			x	x
NERC	RSTC and SPIDERWG	x			

SDO: Standard Development Organization
RSTC: Reliability and Security Technical Committee
SPIDER: System Planning Impacts from DER Working Group

UUDEX: Universal Utility Data Exchange
C2M2: Cybersecurity Capability Maturity Model
SEI: Securing Energy Infrastructure

What's Next in Standards…

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy



S2G Publications

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

- Team made few impactful publications that paved the way for new standards, certifications, tools and recommended practices.
- The publications evaluate impactful tools and resources, address cybersecurity challenges, and provide serve as important resource in the transition to a clean and modern grid.
- Unique opportunity for IAB members to gain deeper level of understanding of emerging cybersecurity solutions, tools, standards and certifications that are shaping the way clean energy energy is integrated and managed.
- Goal is to get IAB feedback and spawn future work based on IAB members needs in DER cybersecurity

S2G Publications (contd.)

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

- Certification Procedures for Data and Communication Security of DERs – https://www.nrel.gov/docs/fy19osti/73628.pdf
- UL Press Release about Cyber Certification for DERs – https://www.ul.com/news/ul-solutions-and-nrel-announce-distributed-energy-and-inverter-based-resources-cybersecurity
- Cybersecurity in Photovoltaic Operations – https://www.nrel.gov/docs/fy21osti/78755.pdf
- Recommendations for Data in Transit Requirements for Securing DER Communications – https://www.osti.gov/servlets/purl/1813646
- Recommendations for Trust And Encryption in DER Interoperability Standard – https://www.osti.gov/servlets/purl/1761841
- Cyber Security for DER and DER Aggregators – https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf
- Gap Analysis of Supply Chain Cybersecurity for DERs – https://www.nrel.gov/docs/fy23osti/84752.pdf
- Supply Chain Cybersecurity Recommendations For Solar Photovoltaics – https://www.nrel.gov/docs/fy23osti/87135.pdf
- Universal Utility Data Exchange (UUDEX): Information Exchange Models for Solar DER - Rev. 1 – https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-34256Rev1.pdf
- Cybersecurity Assessment in DER-rich Distribution Operations: Criticality Levels and Impact Analysis – s*ubmitted to ISGT24*
- Power Systems Cybersecurity: SOAR4DER – https://link.springer.com/chapter/10.1007/978-3-031-20360-2_16
- Privacy And Security Impacts of DER and DER Aggregators – *to be published in October 2023*
- Cybersecurity Recommendations for DERMS – *to be published in Dec 2023*
- Introducing CyberStrike STORMCLOUD – *video to be released publicly in Oct. 2023*

Next Steps

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

- Tools, Assessments and Standards coming up
  - We will send update when published.
- FY24 scope for Securing Solar for the Grid project is under discussion.
  - Reach out for getting actively involved with the projects
- Expectations from IAB members;
  - Ask questions and provide feedback
  - Engage in panel discussions
  - Actively participate in the open discussion later today
- Later today
  - Networking Break
  - Four panel sessions
  - Training and workforce development
  - Industry feedback

Funded by:

SOLAR ENERGY
TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Networking Break

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 1:

DER Cybersecurity Standards and Certifications

Moderator: Danish Saleem, NREL

Mike Slowinske, UL Solutions

Ryan Quint, North American Electric Reliability Corporation

Tal Homsky, Solar Edge, Solar Edge

Bheshaj Krishnappa, Solar Energy Industries Association

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 2:

DER Supply Chain Assessment

Jeffrey Mitchell, INL – Energy Cyber Sense Overview: Engagement with Solar

Ryan Cryar, NREL – DER Digital Supply Chain Gap Analysis

Ron Brash, aDolus – Managing Supply Chain Security Intelligence

Moderator: Emma Stewart, INL

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 2:

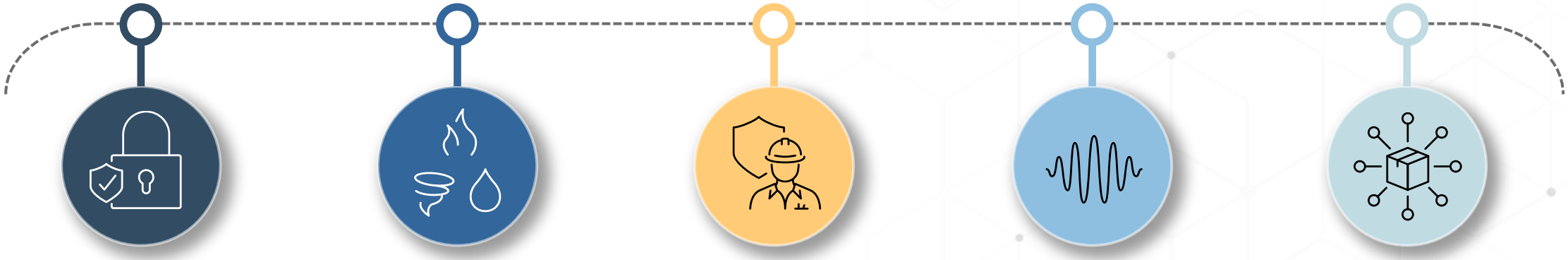
DER Supply Chain Assessment

Jeffrey Mitchell, INL – Energy Cyber Sense Overview: Engagement with Solar

DOE CESER Mission

Strengthen the security and resilience of the U.S. Energy Sector from cyber, physical, and climate-based risks and disruptions.

Evolving Threats to Energy Infrastructure



What Does CESER do?

CESER advances the office's national security mission through:

Risk Assessment — Identifying, analyzing, and prioritizing risks to the Energy Sector.

Risk Mitigation — Developing policies, tools, and technologies and providing technical assistance to mitigate risks to the Energy Sector.

Sector Collaboration — Strengthening the security of U.S. energy systems through enhanced public and private sector collaboration.

Preparedness and Response — Facilitating Energy Sector preparedness, response, and restoration efforts in collaboration with other Federal agencies, the private sector, international partners, and state, local, tribal, and territorial communities.

Energy Supply — Mitigating the impacts of energy supply disruptions on U.S. businesses and consumers.

CESER Divisions

Preparedness, Policy, & Risk Analysis

- Energy Security Policy and Partnerships
- Exercises, Training, Workforce Development
- Risk Analysis, Resilience, and Recovery

Risk Management Tools & Technologies

- All-Hazards Tools and Technologies
- Cyber Tools and Technologies

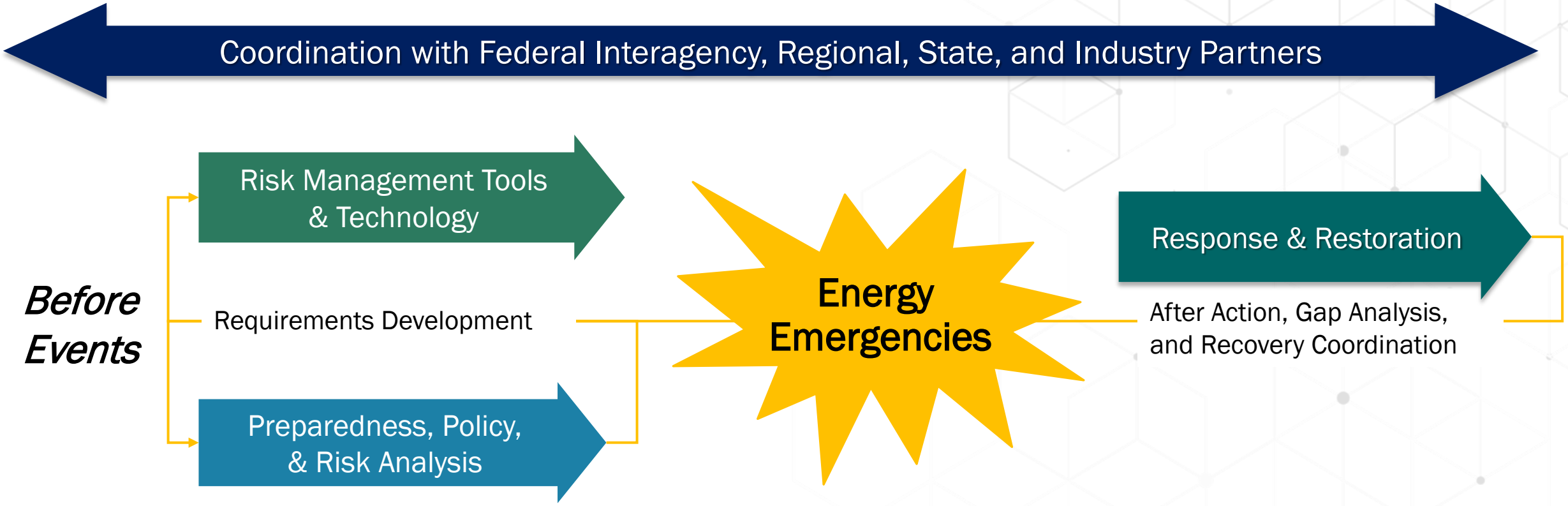
Response & Restoration

- All Hazards Situational Awareness and Analysis
- All Hazards Response Operations
- Response Preparedness and Support

Office of Petroleum Reserves

- Planning & Engineer Office
- Operations & Readiness
- Budget & Financial Management Technologies
- Management & Administration
- Reserve Lands Management
- SPR Project Management

How We Work: Energy Risk Management Timeline



DOE is the ***Sector Risk Management Agency*** for the Energy Sector and the federal coordinating agency for Emergency Support Function (ESF) #12 – Energy

Energy Cyber Sense

Strategic Goal: Establish a national capability for enhancing the cybersecurity and cyber resilience of critical energy infrastructure (including the bulk power system) through:

- Cyber vulnerability testing and forensic analysis
- Illuminating supply chain risks
- Application of classified threat intelligence
- The “engineering-out” of cyber risk through improvements to digital component design, manufacturing, and procurement.

Energy Cyber Sense

- Umbrella program containing multiple Supply Chain Risk Management programs focused on cybersecurity.
- Plans to establish the Energy Sector Industrial Base (ESIB), a voluntary program targeting strategic partnerships with members of the Energy Sector.
  - CESER defines ESIB as the “complex network of industries and stakeholders that spans from extractive industries, manufacturing industries, energy conversion and delivery industries, end of life and waste management industries, and service industries to include providers of digital goods and services.”

Energy Cyber Sense

4 Pillars of Excellence:

Understand Criticality and Provenance

This pillar aims to improve the understanding of impacts from discovered vulnerabilities and illuminate supply chain dependencies within the Energy Sector Industrial Base (ESIB).

Test and Establish Supply Chain Transparency

This pillar aims to enable best-in-class testing, automation of testing, and other tools to scale benefits across the ESIB and illuminate digital supply chain risks for effective decision support in key use cases.

Aid in Application of Standards, Norms, and Best Practices

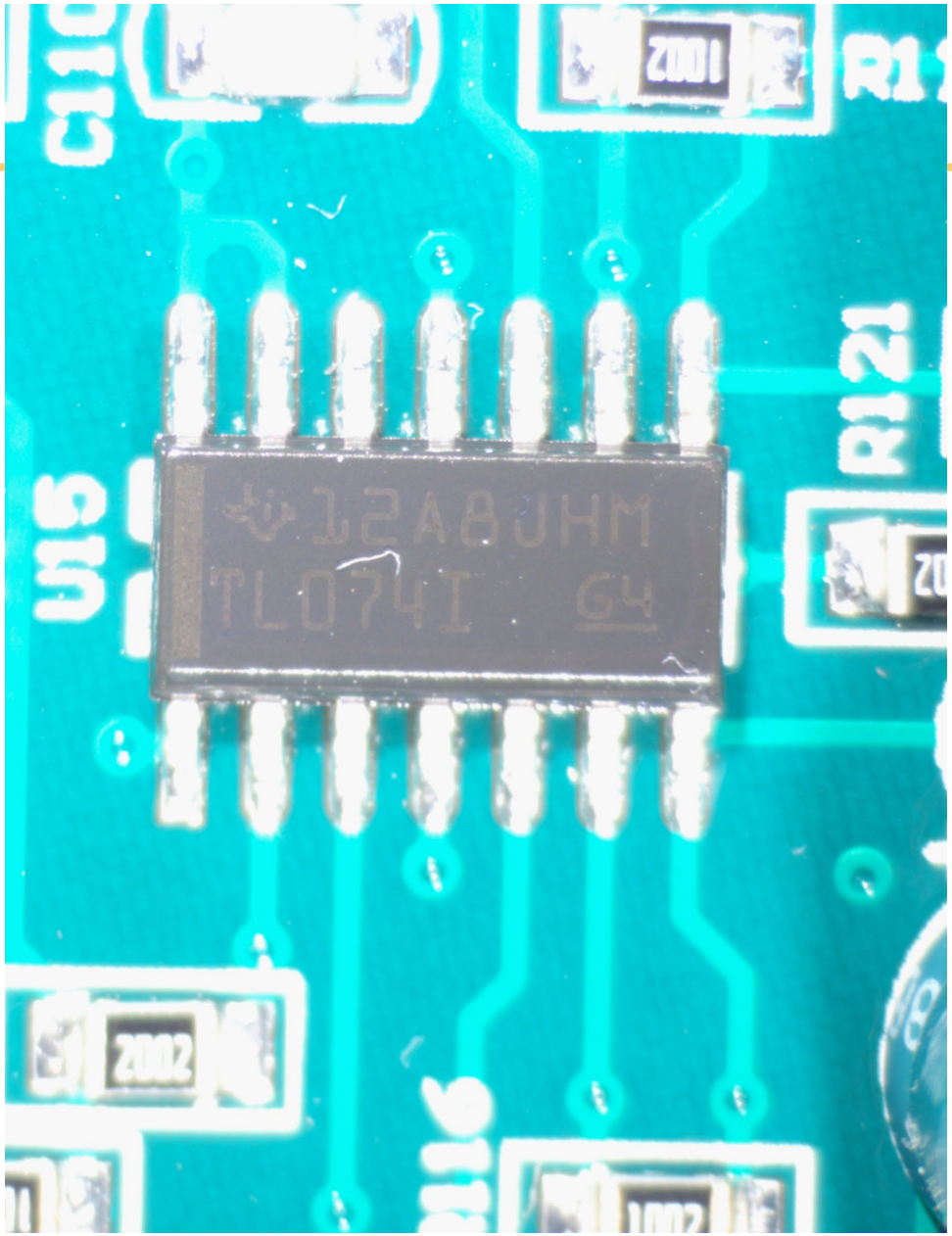
This pillar aims to promote excellence in security standards, norms, and best practices across the ESIB. This effort goes beyond supporting domestic and international standards-setting bodies (e.g., NIST and IEEE) to promote a unity of effort in cybersecurity best practices, lessons learned, and other norms for ICS/OT systems in energy and other critical infrastructure sectors. This pillar includes standardization of reporting and vulnerability disclosure processes.

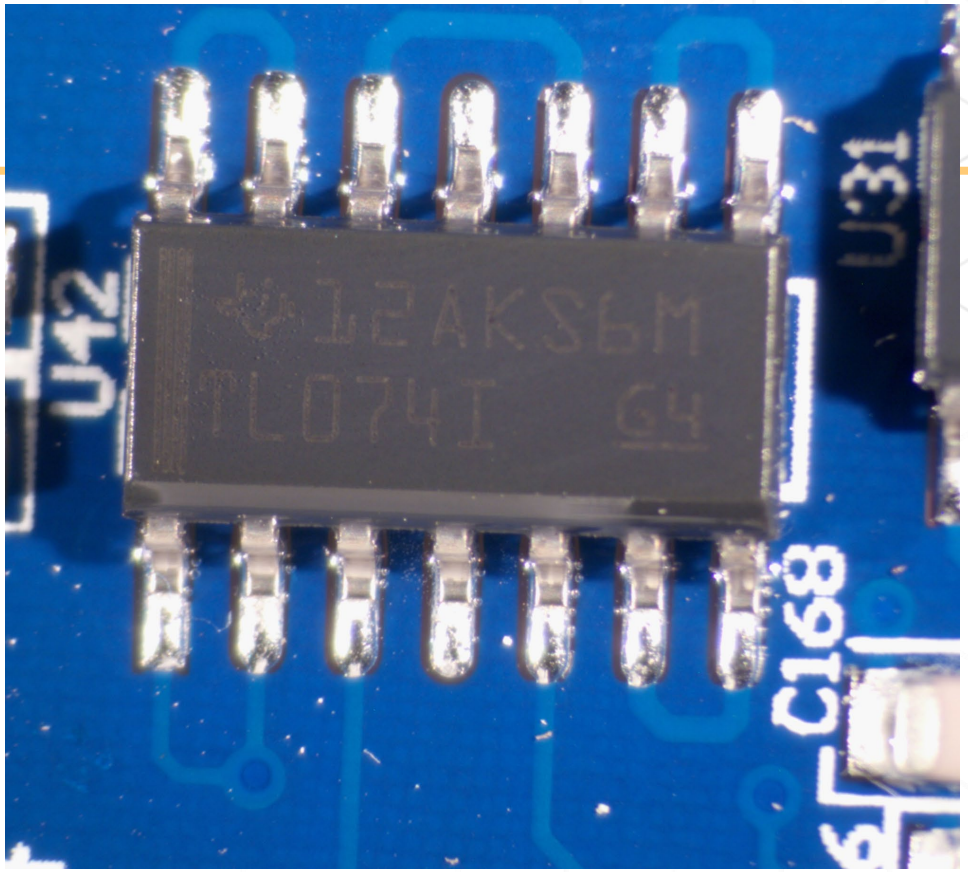
Improve Technology and System Designs (Both Legacy & New)

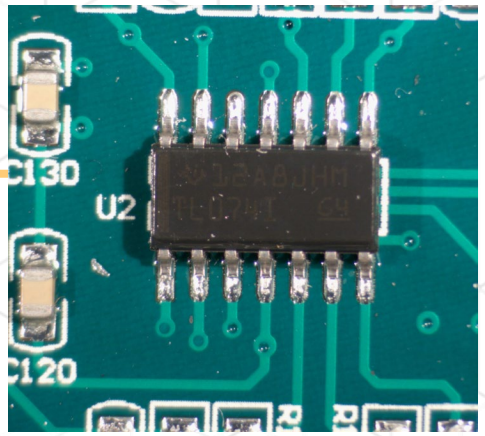
This pillar aims to provide technical assistance to asset owners, manufacturers, system integrators, service providers, and other stakeholders in the ESIB to improve the secure design of technology and systems within ICS/OT.

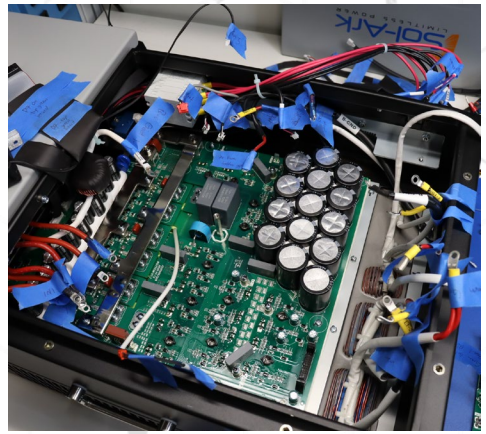
Energy Cyber Sense Collaboration with Solar Energy Technology Office (SETO)

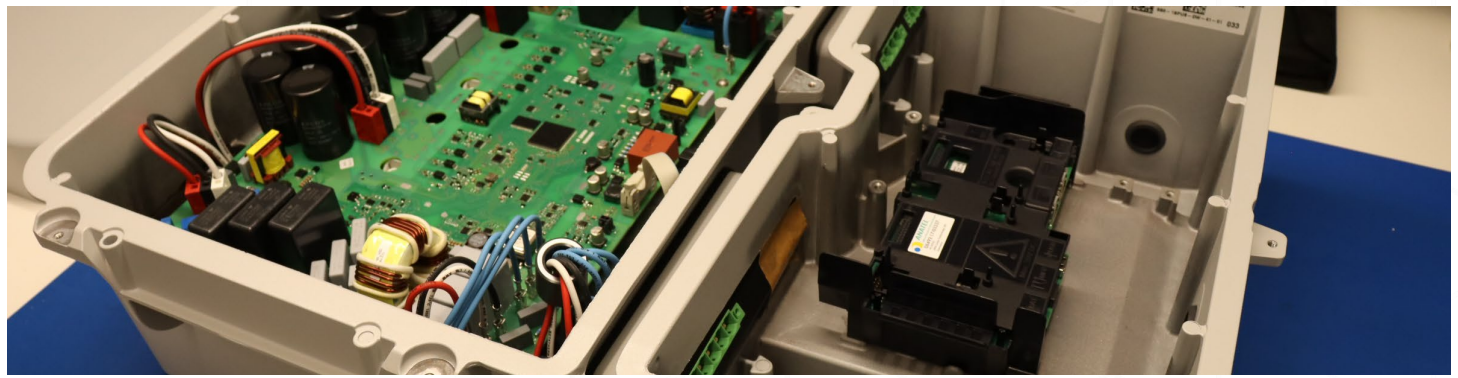
- DOE CESER-sponsored program, focused on supply chain security within the Energy Sector.
  - This SETO tasking is specifically focused on solar devices.
- Develop a hardware bill of materials (HBOM) that includes photos of the system, components, relationships of components, details on each of the components, datasheets on the components, etc.
  - Build a repository, allowing further research.
- Example use cases:
  - Component matching — understanding the components used in both solar devices and other electronics.
  - What are the unique components used in solar devices?
- Understand the physical aspect of the cyber supply chain at the final stage of production.


U16
R121
TL074I
G4


U42
U31
C168
TL074I
G4


C130
U2
C120





Energy Cyber Sense Collaboration with SETO

- Compare components on devices
  - What are the common components across manufacturers?
  - Are there unique components on solar devices, that are unique from other OT devices?
- Research each key component
  - Have we seen this component before?
  - Look for known vulnerabilities / issues on identified components.
- What did we learn?
  - Observations will be shared with CESER and SETO.

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 2:

DER Supply Chain Assessment

Ryan Cryar, NREL – DER Digital Supply Chain Gap Analysis

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

NREL
Transforming ENERGY

DER Digital Supply Chain Gap Analysis

Ryan Cryar, Cybersecurity Researcher

Securing Solar for the Grid Workshop

September 14th, 2023

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

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

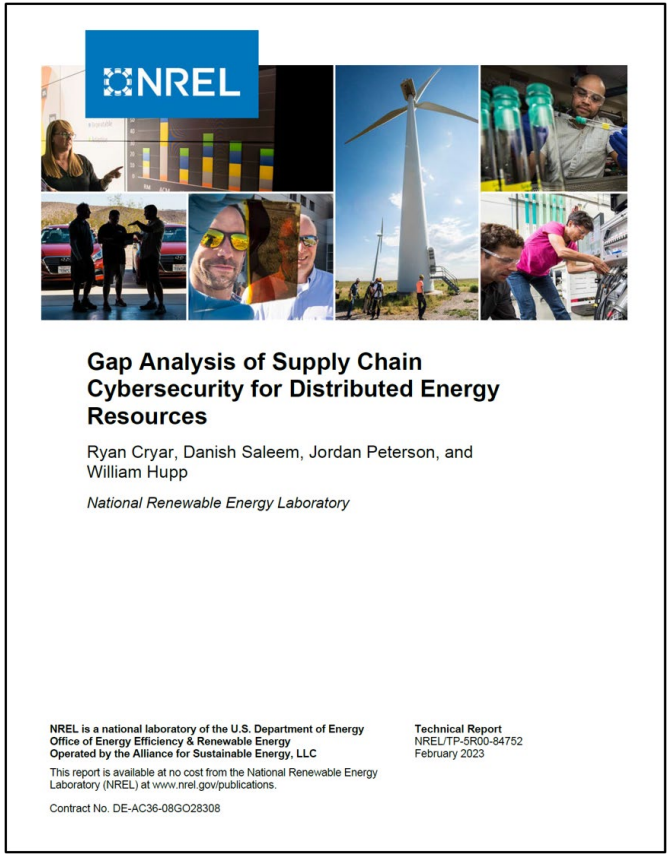
Introduction

- Presidential Executive Order 14017 for supply chain cybersecurity
- This project supported research for supply chain cybersecurity by:
  - Performing gap analysis of current cybersecurity landscape of distributed energy resources (DERs)
  - Creating recommendations for the digital supply chain cybersecurity of solar photovoltaics
  - Engaging with academia, national laboratories, and industry to address and understand digital supply chain challenges.
- Identified future opportunities to engage with industry members through different cybersecurity working groups.

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

Past Work

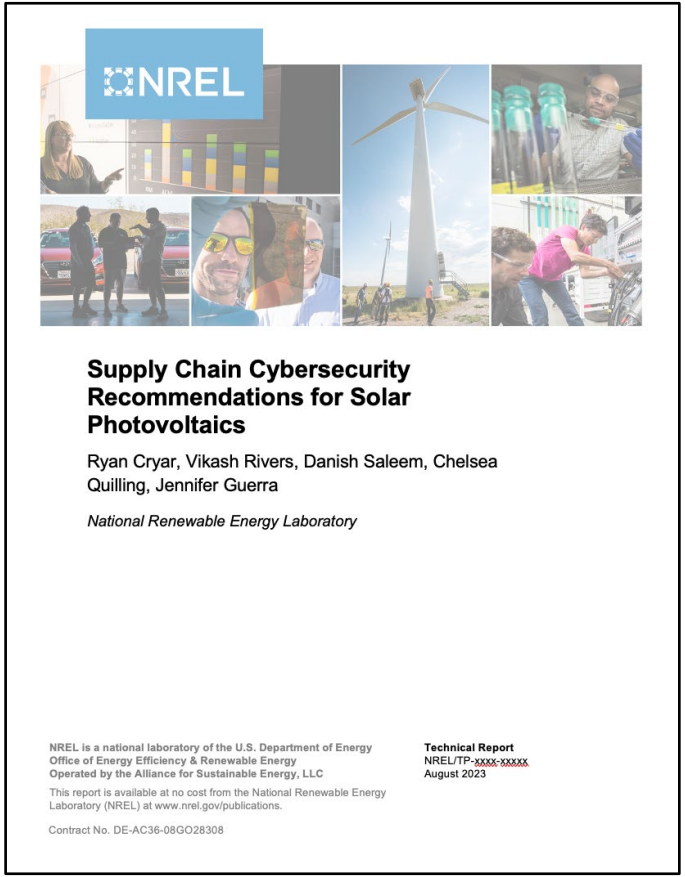
- *Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources*:
  - Addresses the landscape of the digital supply chain
  - Drafts the ideal state of the digital supply chain
  - Provides recommendations to bridge gaps between the current and ideal.
- Challenges stem from areas such as open source, standards, and where to apply best practices.



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

Addressing Recommendations

- Supply Chain Cybersecurity Recommendations for Solar Photovoltaics
  - Follows prior work
  - Addresses practices found and adapted from NERC, NIST, and NATF
  - Provides down-selected recommendations that that could apply to the digital supply chain of solar photovoltaics
  - Focuses on short, clear language that can be testable and quantified
  - Includes recommendations reviewed by academia and national laboratories
- Publication released on NREL website



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

Example Recommendations

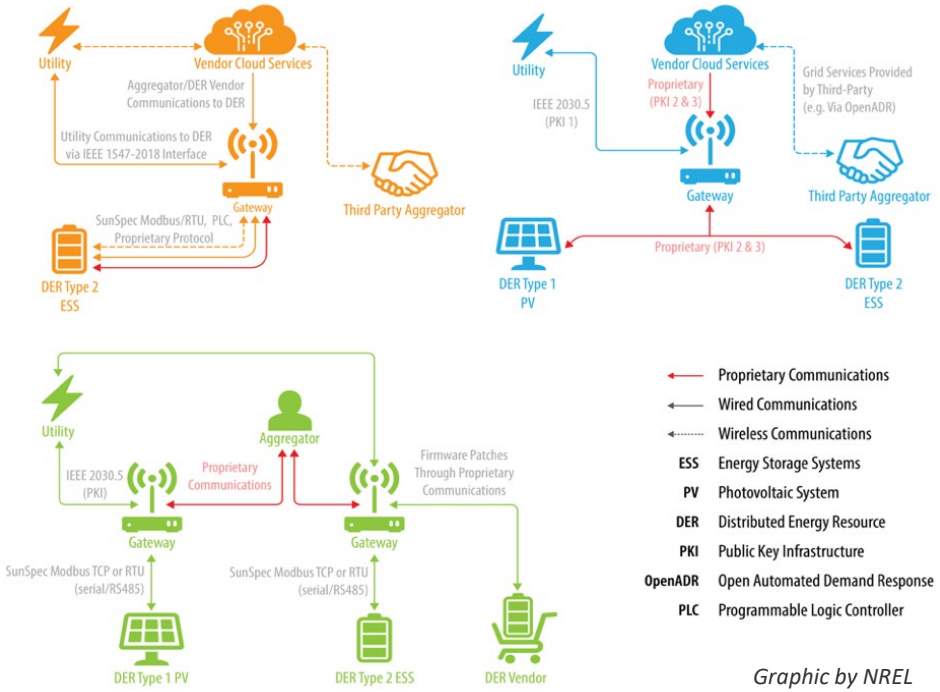
- **Recommendation 30**: Through a secure portal, vendors should provide customers with a vulnerability disclosure report, including the analysis and findings describing the impact that a reported vulnerability has on a product as well as plans to address the vulnerabilities. The vulnerability disclosure report should be signed with a trusted, verifiable, private key that includes a time stamp of the signature. (Adapted from NIST SP 800-161r1 RA-5; NATF Energy Sector Supply Chain Risk Questionnaire RISK-08)

- **Recommendation 31**: Vendors should establish a separate notification channel for customers in case a vulnerability arises that is not included in the vulnerability disclosure report. (Adapted from NIST SP 800-161r1 RA-5; NATF Energy Sector Supply Chain Risk Questionnaire VULN-06, VULN-07)

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

Outcomes of the Reports

- Interest in forming a subgroup on supply chain cybersecurity within SunSpec/Sandia Cybersecurity Working Group
- Engage with industry members to develop more effective recommendations.
- Provide immediate value to industry through recommendations that are testable.
- Gaining visibility into the challenges of the digital supply chain of renewable energy resources.

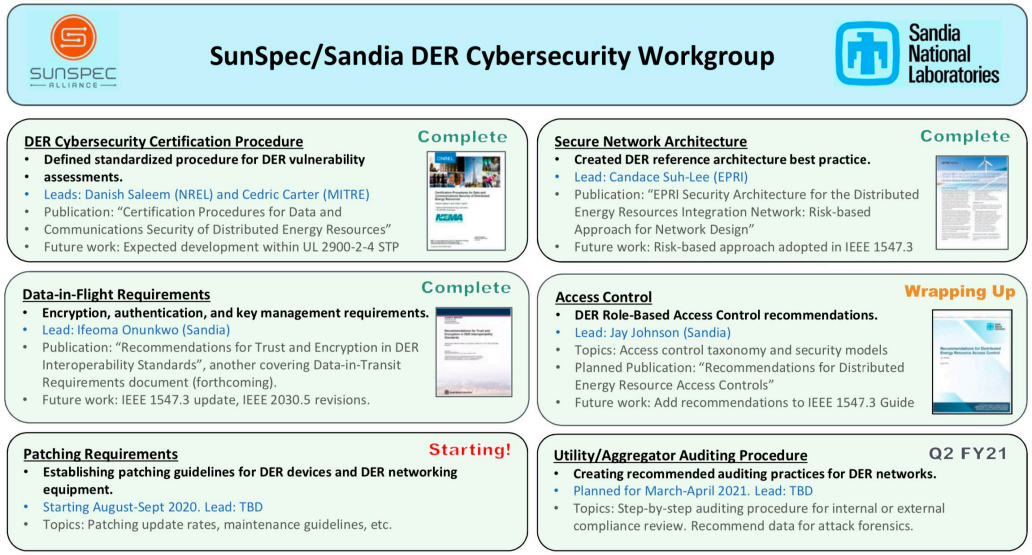


Graphic by NREL

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

Future Work

- By leveraging the SunSpec/Sandia cybersecurity working group to create a subgroup on supply chain cybersecurity, further adapt the recommendations.
- Through this subgroup, to the extent possible, harmonize with other groups, such as SEPA CSWG, CPUC Smart Inverter Working Group, and UL 2941 Technical Committee.
- With this engagement, industry members see immediate value by actively developing recommendations that can be tailored to their own practices.



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

Industry Engagement

- Engagement with industry is prioritized.
- Several working groups are being leveraged to provide balanced feedback among multiple types of stakeholders and participants.
- Additional engagement sources are actively being sought.

Photo by Dennis Schroeder, NREL 22168

Thank You!

Let’s work together!

Ryan.Cryar@nrel.gov

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

NREL
Transforming ENERGY

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

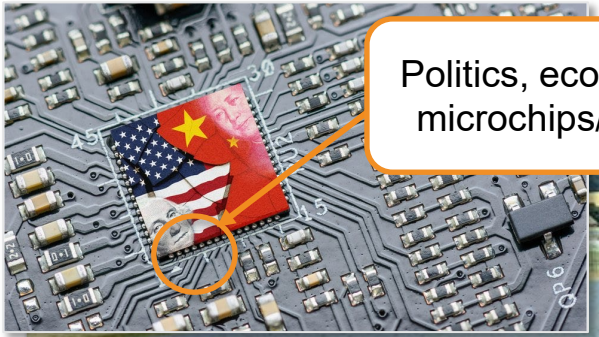
SETO S2G IAB Workshop

Panel 2:

DER Supply Chain Assessment

Ron Brash, aDolus – Managing Supply Chain Security Intelligence

When we think of a supply chain…

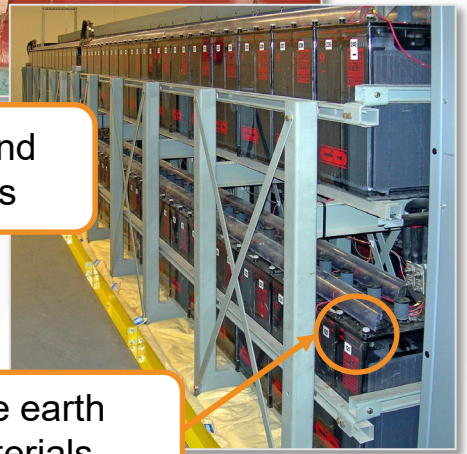


Politics, economics, and microchips/electronics

Inverters, relays, transformers, etc.

Global shipping and logistics

PV panels and components



Rare earth materials

But the *supply chain* – it is broader than you

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Suppliers

- Hardware components
- Hardware-related software
- Software (FOSS, COTS, etc.)

OEMs/Vendors

- Development
  - Cross-BU
  - 1st party dev'
  - Contractors & partners
- MFG
  - Maintenance
  - Iterations*

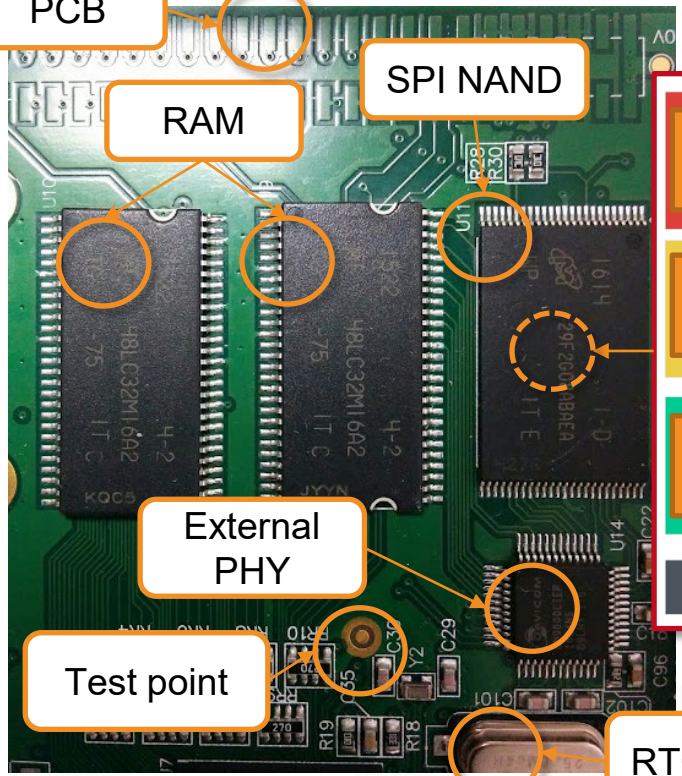
System Integration & Deployment

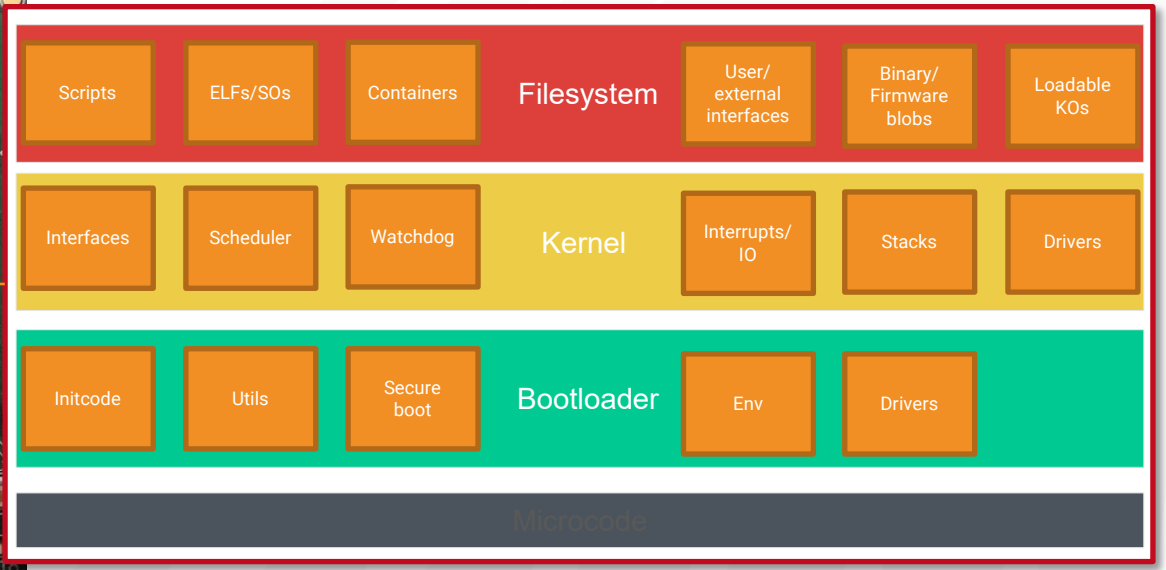
- Design/deployment, FAT, SAT & management
- Parts & maintenance
- Services, connectivity & outsourcing

Asset Owners

- Asset lifecycles
- Third parties, risk, & procurement
- Controls & security
- Compliance, etc.

Real-world case study: industrial gateway device





Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 2:

DER Supply Chain Assessment

Q&A

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Lunch and Networking

Level 2 Bellini

Please be back in the room promptly at 1:00

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 3:

DER Risk Assessments & Mitigation

Scott Mix, PNNL – Mitigating Supply Chain Risk for the Solar Industry

Andrew Bartels, Operant Networks – Experience with SD2-C2M2 Assessment

Stephen Bukowski, INL – SolarShield and Industry

Sheri Gribbin, CNK Solutions

Moderator: Scott Mix, PNNL

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 3:

DER Risk Assessments & Mitigation

Scott Mix, PNNL – Mitigating Supply Chain Risk for the Solar Industry

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G SD2-C2M2 Overview

Securing Solar to the Grid (S2G)

SD2-C2M2 Overview

Fall 2023 Industry Advisory Board

September 14, 2023

PNNL-SA-189881

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

SD2-C2M2 Overview

- Secure Design and Development Cybersecurity Capability Maturity Model – SD2-C2M2
  - Guided self assessment of a manufacturer or developer internal processes for design, development, manufacture, and support of Operational Technology products
  - Assess over 800 Practice Statements for implementation as:
    - Not Implemented (NI), Informally Implemented (II), Documented (D), Formally Implemented (FI)
  - Each Practice Statement assigned a maturity level of:
    - MIL 1 – Basic; MIL 2 – Intermediate; MIL 3 – Advanced

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

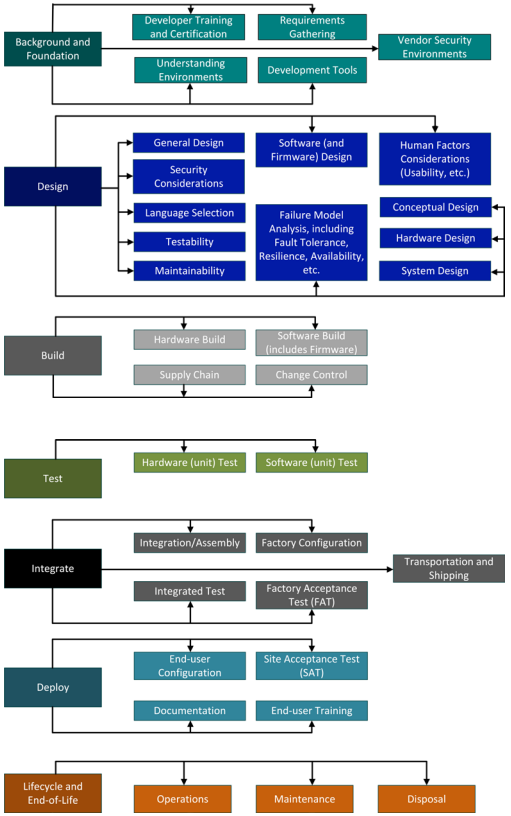
SD2-C2M2 Overview

- Management Selection for desired Maturity Level for broad areas of practices
- Subject Matter Experts respond to Practice Statements
- Tool produces a report summarizing obtained Maturity Levels and identified gaps to achieve desired Maturity Levels

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

SD2-C2M2 Overview

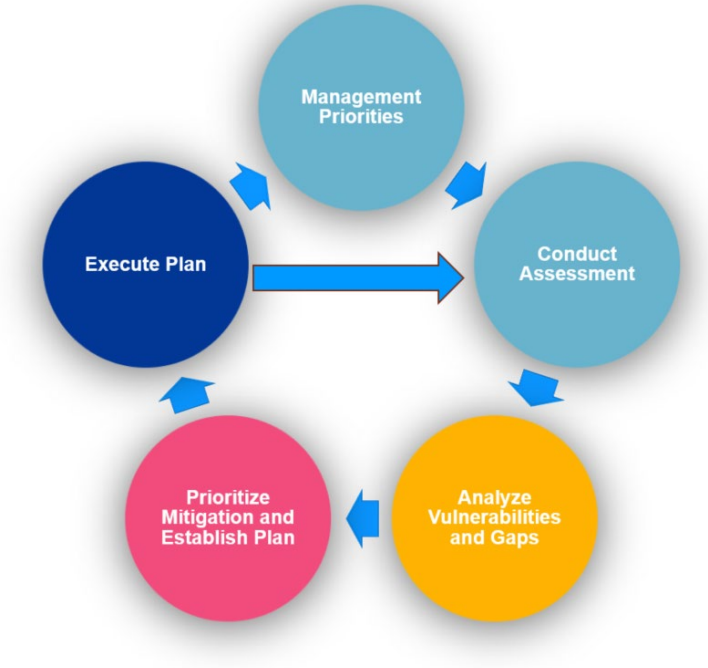
- Domains assessed by the tool:
  - Background and Foundation
  - Design
  - Build
  - Test
  - Integrate
  - Deploy
  - Lifecycle and End of Life



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

SD2-C2M2 Overview

- Tool Workflow:



- Example Results:

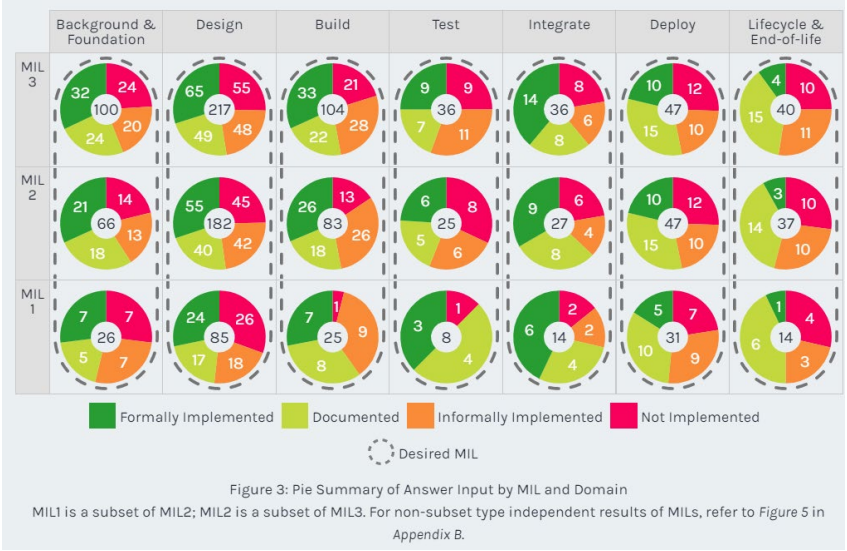


Figure 3: Pie Summary of Answer Input by MIL and Domain

MIL1 is a subset of MIL2; MIL2 is a subset of MIL3. For non-subset type independent results of MILs, refer to *Figure 5* in *Appendix B.*

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 3:

DER Risk Assessments & Mitigation

Andrew Bartels, Operant Networks – Experience with SD2-C2M2 Assessment

OPERANT
NETWORKS

Simplifying cybersecurity and networking for Energy's edge

SETO S2G IAB
2023 Session

SD2-C2M2 Tool Update

Overview: Operant Networks Summary

- A supplier of networking, cyber security, intrusion detection, and remote user access solutions
- Deployed on 10+ GW of renewables and growing
- Secure by Design is mandatory
- An ideal candidate for the SD2-C2M2 program

Using the SD2-C2M2 Tool

~1 year ago: Our initial areas of focus

- ***The tool is comprehensive and applies to all types of large enterprises***
  - Hardware manufacturing, software, quality, documentation, processes
  - ✓ Scales both up and down:
    - ✓ Easily tailored to the types of products an enterprise produces
    - ✓ Management can set capability levels desired and then assess
  - Based on results, assess again and gradually raise capability levels
- ***Interjecting assessments amid business deadlines isn't convenient***
  - ✓ PNNL team was highly informative and supportive
    - 2 initial sessions on how to use the tool and why
  - ✓ Assessment took approximately 8 hours of internal effort
  - ✓ Results are private to your organization, not stored in the cloud

Results of Using the SD2-C2M2 Tool

- ***A clear baseline of capabilities***
  - Capability categories and levels that management sees as critical
  - Assessment of where the capabilities actually are
  - Ability to prioritize initiatives that make the biggest impact on supplier quality
- ***Areas we focused on:***
  - ✓ Expansion of **Secure by Design** initiatives:
    - Continued engineering review of end-to-end security from the very start
    - More quality feedback initiatives, adoption of full automation, CI/CD pipelines
    - SBOM analysis of what we produce and what we consume
    - More capable code vulnerability and CVE analysis at the time of all check-ins
    - Robust technical documentation
- ***Ongoing assessments***
  - Every 6 months, with annual critical capability levels re-baseline

Summary

- ***A small company, but with big impact on our customers' cyber security stance***
  - ✓ Even more focus on **Secure by Design** principles
  - ✓ Additional initiatives for red team testing and results review
  - ✓ Still getting new, impactful products and features to market

- ***Our use of SD2-C2M2 Tool:***
  - Planning to continue assessments ongoing
  - Raising the maturity level of our delivery capabilities

- ***Highly recommend SD2-C2M2 to other suppliers, even if they don't produce security products***

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 3:

DER Risk Assessments & Mitigation

Stephen Bukowski, INL – SolarShield and Industry

Raising the Floor of Cybersecurity in Renewables

INL Cyber Team

Cyber SHIELD for Renewables

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

Cyber SHIELD Overview

Focus is on securing renewable transition. DOE funded program provides tools and resources to entities in support of objective to "raise the cybersecurity floor" across renewable sector

Grid of the Future

Within a decade, renewables will be the leading generation source in our grids. The transition must ensure the future grid is secure. Need to rapidly mature cybersecurity.

Limited Cyber focus to date

Many owner/operators have had little or no focus on developing a cybersecurity program that reflects their risk preferences, generally having limited cyber hygiene.

Changing Regulatory and Business Needs

NERC has identified the changing resource mix and cybersecurity vulnerabilities as the highest risk to reliability of the grid and is making changes to IBR registration and criteria. Insurance is moving burden of proof to insured for cybersecurity program. Litigation claims for poor cyber hygiene escalating.

Renewable sectors are OT centric

Many existing tools have been developed under the focus of Enterprise IT, these applications of cyber controls are for an OT and more specifically renewable environment.

Targeted Support

The Cyber SHIELD initiative leverages multiple robust tools that have been developed under DHS programs. These tools are tuned for use with renewable assets and accommodate any level of cyber maturity with a primary goal of helping owner/operators identify where they are and where to go to improve cyber maturity.

Funded INL – Industry Partnerships

Partner with INL to help improve your cybersecurity maturity, operational reliability, and resiliency

To discuss more or to sign up contact:

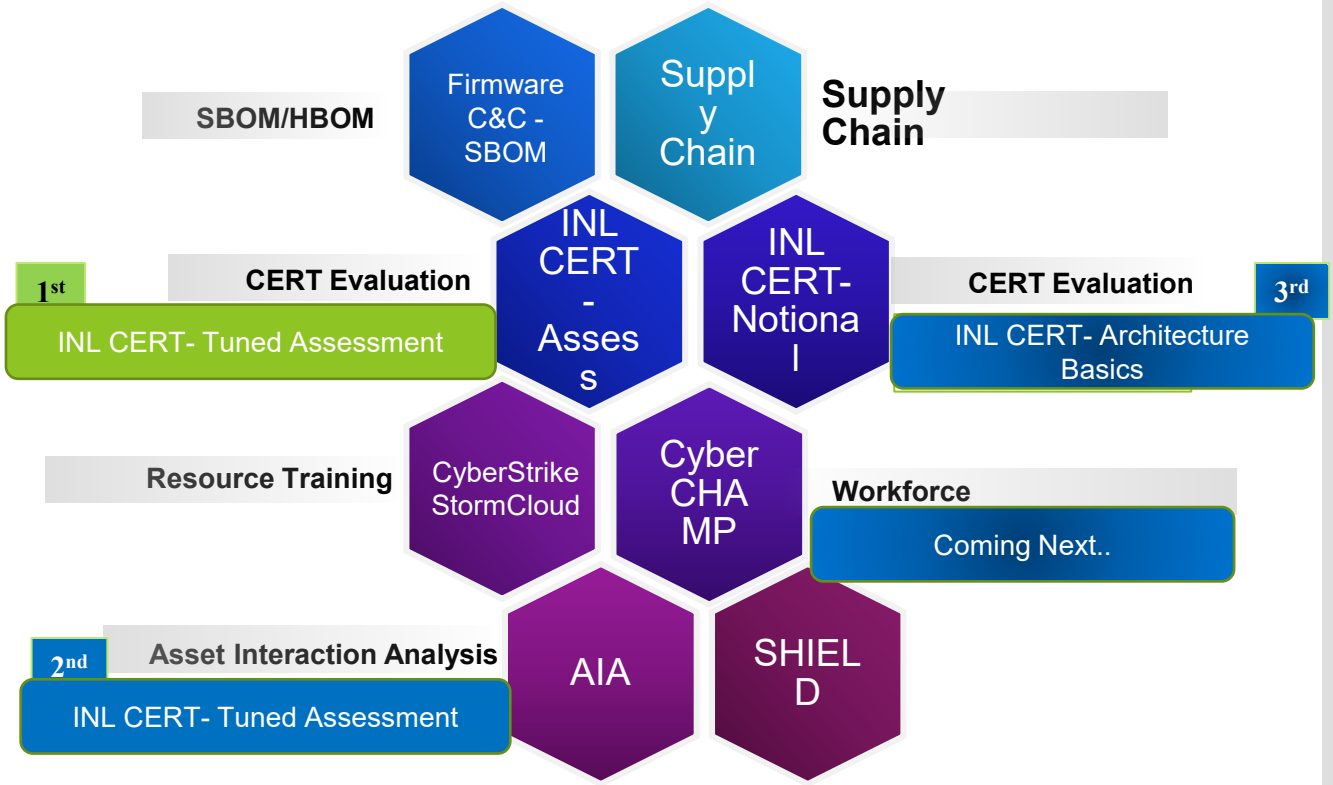
Steve Bukowski at Idaho National Laboratory | stephen.bukowski@inl.gov

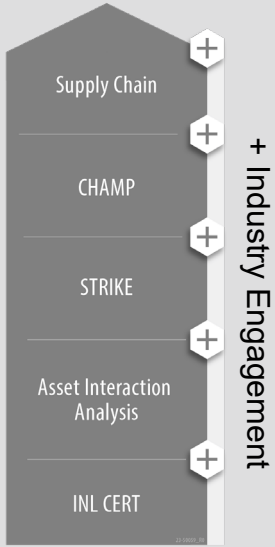
IDAHO NATIONAL LABORATORY

INL - Cyber SHIELD

***S**ecurity through **H**ardware **I**ntegration, **E**ducation, and **L**ayered **D**efense*

Raising the Floor on Cybersecurity for grid scale renewables





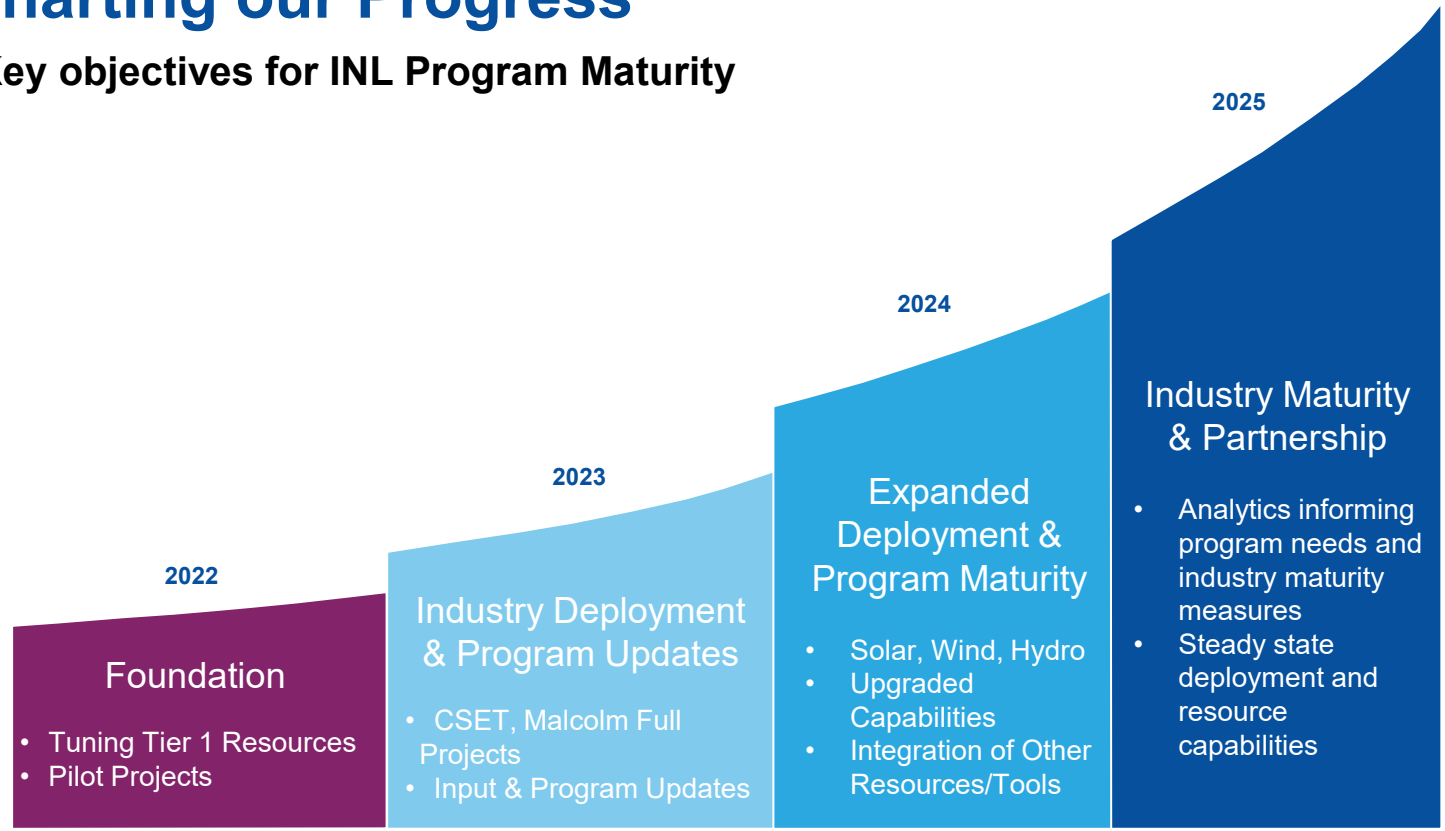
Cyber SHIELD Industry Resources

Leveraging INL Resources to Mature Renewable Sector Cybersecurity Posture and Risk Mitigation Capabilities

Phase I Unstructured	Phase II Reactive	Phase III Evolving	Phase IV Proactive	Phase V Optimized
"The impact of control failures is just a cost of doing business."	**"We have minimum controls and address security risks reactively, as they arise"**	**"We are better but still learning how to consistently and effectively execute"**	**"Understanding and managing emerging security risks is everyone's job."**	**"Strong security programs make us a better company, paving the way to improved performance."**
• No or limited defined processes or controls • Siloed and inconsistent practices • Business areas follow different paths to reconcile control issues • No systems in place to track key controls • Approaches are tactical • No processes in place to measure performance	• Processes and controls are defined but not formally documented • Performance management is centralized (where applicable) but lacks central leadership • Limited or no proactive efforts or coordination • Manual or limited performance testing • Limited engagement from key stakeholders • External relationship management is siloed, inconsistent and reactive	• Executing controls are defined and many are formally documented • Basic governance is in place to support a programmatic management of execution • Buy-in from leadership and all business areas • Adequate resources and staffing to execute controls • Technology solutions are available, but ad-hoc and limited • Ownership of controls generally established	• Centralized leadership to set vision and objectives, central program management, design and implementation • Controls are structured, planned and formally documented • Governance and accountabilities are clearly defined • Controls performance is actively measured with ability to anticipate risks and exposures • Program and controls are integrated as part of annual risk management processes • A combination of standard and custom-developed tools • Performance reporting	• Processes and controls are formally defined and documented, coordinated across organizations and strategically designed • Programmatic approach to training and communications to offer complete visibility across the enterprise • Formal quality assurance controls. Performance is regularly audited for consistent execution • Failures are evaluated and lessons learned are implemented and shared as part of extent-of-condition • Governance and oversight programs are robust, formally structured, centrally led and managed • Technology solutions integral part of all processes
Practices in the domain are not being performed as measured by responses to the relevant cyber framework questions in the domain	All practices that support the goals in a cyber framework domain are being performed as measured.	All specific practices are not only performed but are also supported by planning, defined stakeholders, and relevant standards and guidelines. All practices are performed, planned and have basic governance infrastructure in place to support.	All practices are performed, planned, managed, monitored and controlled	All practices in a cyber framework domain are performed, planned, managed, measured and consistent across all constituencies within an organization who have a vested interest in the performance of the practice
Recommended Cyber Shield Resources ✓ Cyber CERT – Basic Assessment ✓ Cyber CERT – Diagram Essentials ✓ Cyber Champ 	***Recommended Cyber Shield Resources*** ✓ Cyber CERT – Basic Assessment ✓ Cyber CERT – Diagram Essentials ✓ Cyber Champ ✓ Malcolm – Initial Deployment 	***Recommended Cyber Shield Resources*** ✓ Cyber CERT – General Cyber Hygiene ✓ Cyber CERT – Managed Diagram ✓ Cyber Champ ✓ Malcolm – Managed Deployment 	***Recommended Cyber Shield Resources*** ✓ Cyber CERT – Full Framework Assessment ✓ Cyber CERT – Advanced Diagram ✓ Cyber Champ ✓ Malcolm – Advanced Deployment 	***Recommended Cyber Shield Resources*** ✓ Cyber CERT – Full Framework Assessment ✓ Cyber CERT – Advanced Diagram ✓ Cyber Champ ✓ Malcolm – Advanced Deployment 

Charting our Progress

Key objectives for INL Program Maturity



Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 3:

DER Risk Assessments & Mitigation

Sheri Gribbin, CNK Solutions

-

Risk Management:
Leveraging Enterprise Risk Management to Improve Operational & Cyber Risk Mitigation

Risk Mitigation – Start with the Basics
Enterprise Risk Management (ERM)

MOODY'S ANALYTICS

WHITEPAPER

SEPTEMBER 2023

The impact of cyber security management practices on the likelihood of cyber events and its effect on financial risk

Authors

Alejandra Caro Rincon, Associate Director
Alejandra.CaroRincon@moodys.com

Gustavo Ordóñez, Senior Director
Gustavo.Ordonez@moodys.com

Contact Us

Americas
+1.212.553.1658
clientservices@moodys.com

Europe
+44.20.7772.5454
clientservices.emea@moodys.com

Asia (Excluding Japan)
+85 2 2916 1121
clientservices.asia@moodys.com

Japan
+81 3 5408 4100
clientservices.japan@moodys.com

Abstract

The rapid digitization of the economy and businesses' significant reliance on IT infrastructure has thrust cybersecurity to the forefront of risks to be actively managed. This trend has prompted investors, market participants, consumers, and regulators to address this emerging risk with greater urgency. Understanding a company's financial and technological exposure to cyber threats can help these market participants better prepare for potential cyber events and related financial losses. This study focuses on exploring the connection between a firm's cybersecurity management practices and the probability of a cyber event occurring. This study also examines the financial impact of these events by analyzing losses recorded over the 12-month period following a cybersecurity incident, and its potential effect on credit risk.

Our findings demonstrate a strong relationship between the quality of cybersecurity practices and the probability of a reported cybersecurity event. Certain industries, such as Finance, Healthcare, and Technology exhibit relatively higher risk of cyber related financial losses. Likewise, larger companies face an elevated risk of security events compared to smaller ones. This study also illustrates the significant negative effects of cyber incidents on firm value, with severe events leading to persistent negative equity returns over a 12-month period. Our findings demonstrate the potentially material financial implications of cyber risk, and highlight the importance of cybersecurity in a complete integrated risk assessment framework.

"This trend has **prompted investors, market participants, consumers, and regulators** to **address** this emerging risk **with greater urgency**. Understanding a company's **financial and technological exposure to cyber threats** can help these market participants better prepare for potential cyber events and related financial losses."

https://www.moodysanalytics.com/-/media/whitepaper/2023/the-impact-of-cyber-security-management-practices.pdf

ERM Assessment Sample (Simple View)

Enterprise Risks

Enterprise Risk Management (ERM)

- Financial Risks
- Legal Risks
- Operational Risks
- Safety Risks
- Cybersecurity Risks
- Supply Chain Risks

Cyber IT Risks

Products & Services Risks

- Assets (Firmware, Hardware, Software)
- Services
- Vendors / Supply Chain

Business & Operational Risks

- Legal & Regulatory Risk
- Operation & Asset Location
- Program Implementation
- Processes & Controls

Cyber OT Risks

Products & Services Risks

- Assets (Firmware, Hardware, Software)
- Services
- Vendors / Supply Chain

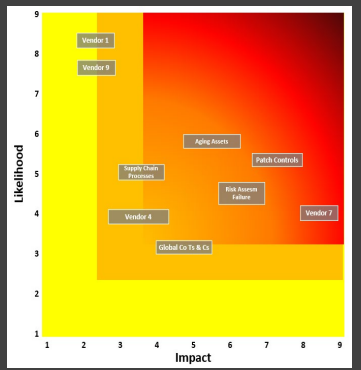
Business & Operational Risks

- Legal & Regulatory Risk
- Operation & Asset Location
- Program Implementation
- Processes & Controls

Enterprise Risk Management

Quarterly Assessment

Cyber Security Results

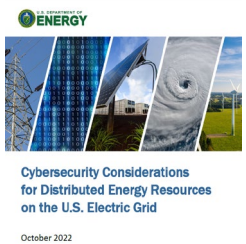


All Inputs are Illustrative

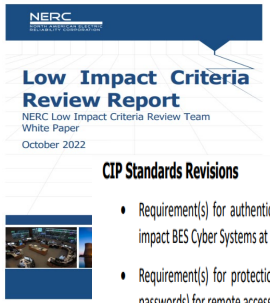
Consider distinctions with New Assets/Build & Legacy or Existing Assets

The Missing Risk Inputs: Regulatory & Legal

FERC, NERC, Federal Legislative and State Pressure

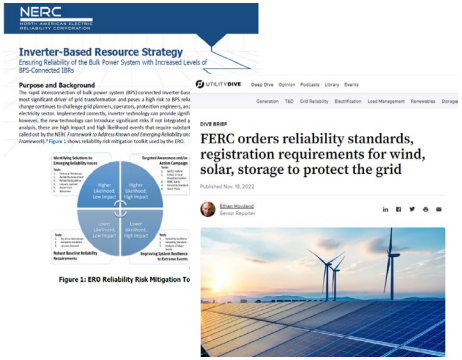


"DOE Cybersecurity Report Provides Recommendations to Secure Distributed Clean Energy on the Nation's Electricity Grid" ~DOE CESER October 6, 2022



CIP Standards Revisions

- Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for protection of user authentication information (e.g. combinations of usernames and passwords) for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.



"we find that unregistered IBRs connected to the Bulk-Power System, regardless of size and transmission or sub-transmission voltage, that in the aggregate have a material impact on Bulk-Power System performance should be registered."
-

NERC IBR Registration Work-Plan

Generator Owner – Inverter-Based Resource (GO-IBR):

Owners of IBRs which have aggregate nameplate capacity of less than or equal to 75 MVA and greater than or equal to 20 MVA interconnected at a voltage greater than or equal to 100 kV; or

Owners of IBRs which have aggregate nameplate capacity of greater than or equal to 20 MVA interconnected at a voltage less than 100 kV.

Insurance Policy and Commercial Litigation Trends – No more wiggle room

CIP-003-9FERC Approves Extending Risk Management Practices to Low-Impact Cyber Systems

CNK Solutions Corp
1325 G Street NW
Suite 500
Washington, DC 20005

cnksolutionscorp.com

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 3:

DER Risk Assessments & Mitigation

Q&A

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 4:

DER Vulnerability Assessments and Analysis

Keira Elliott/Jon Hurtado, SNL – Vulnerability Analysis and SOAR (Security Orchestration Automation and Response)

Jennifer Guerra, NREL – DERMS Cybersecurity and Recommendations for Aggregators

Wajid Hassan, LogicFinder – Identifying Vulnerabilities through Penetration Testing and Vulnerability Assessment

Moderator: Jay Johnson, SNL

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 4:

DER Vulnerability Assessments and Analysis

Keira Elliott/Jon Hurtado, SNL – Vulnerability Analysis and SOAR (Security Orchestration Automation and Response)

Sandia National Laboratories

Exceptional service in the national interest

Vulnerability Analysis and SOAR (Security Orchestration Automation and Response)

Fall 2023 Workshop and Industry Advisory Board Meeting

14 September 2023

Keira Elliott, Jon Hurtado, Sandia National Laboratories

Team: Jay Johnson, Will Vining, George Fragkos, Sherry Mitchell, Brian Wright

SAND2023-12607PE

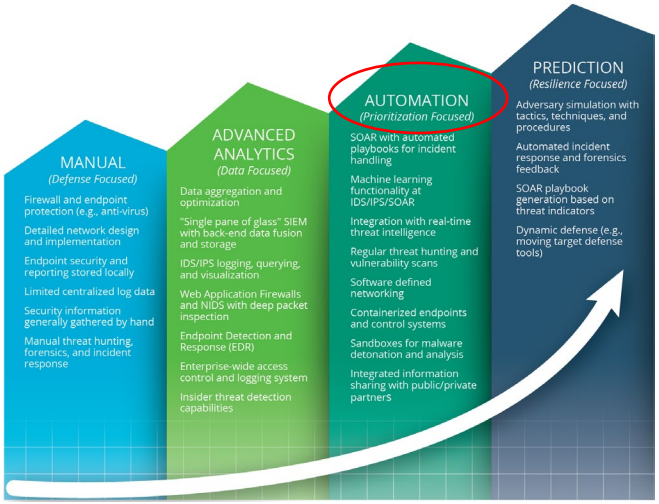
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

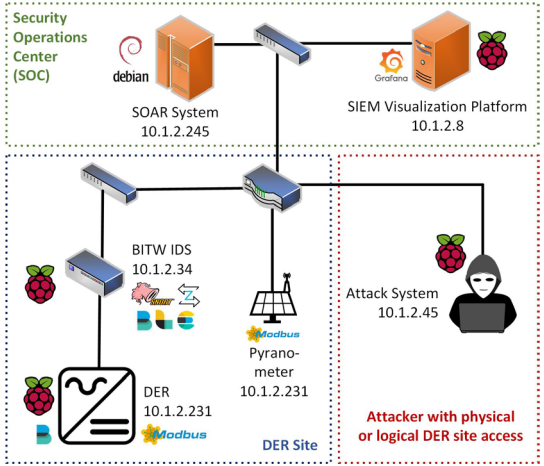
NNSA

Security Orchestration for DER Equipment

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



SOC Maturity Levels

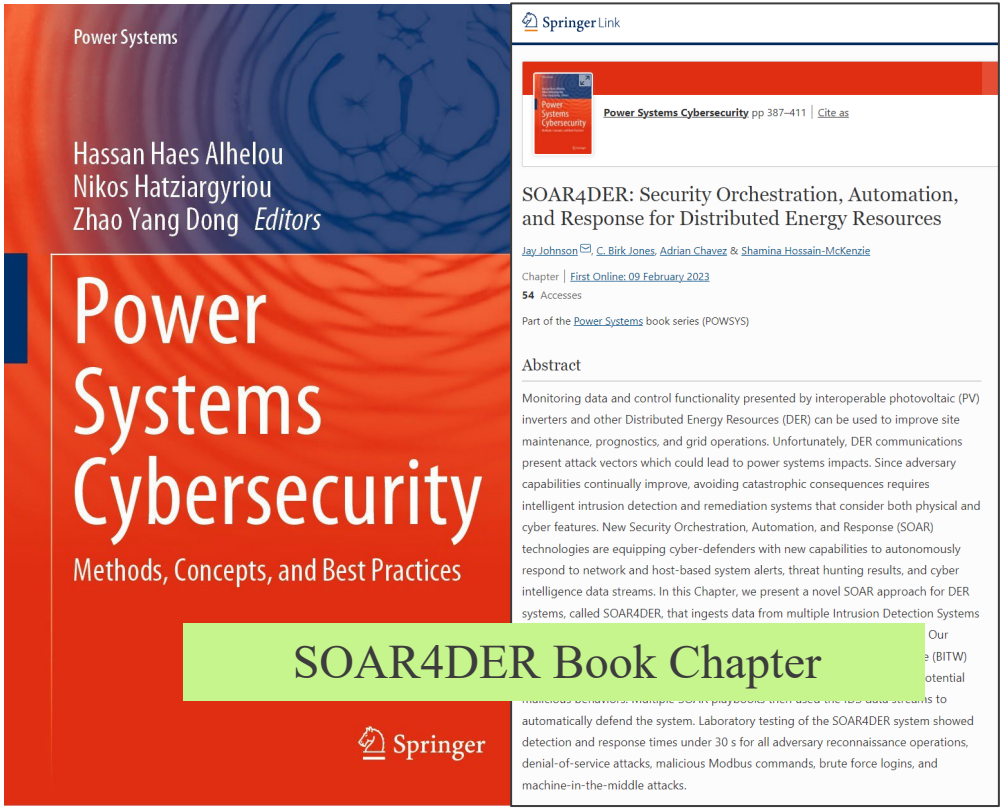


Sandia Testbed

Automated Response Playbook

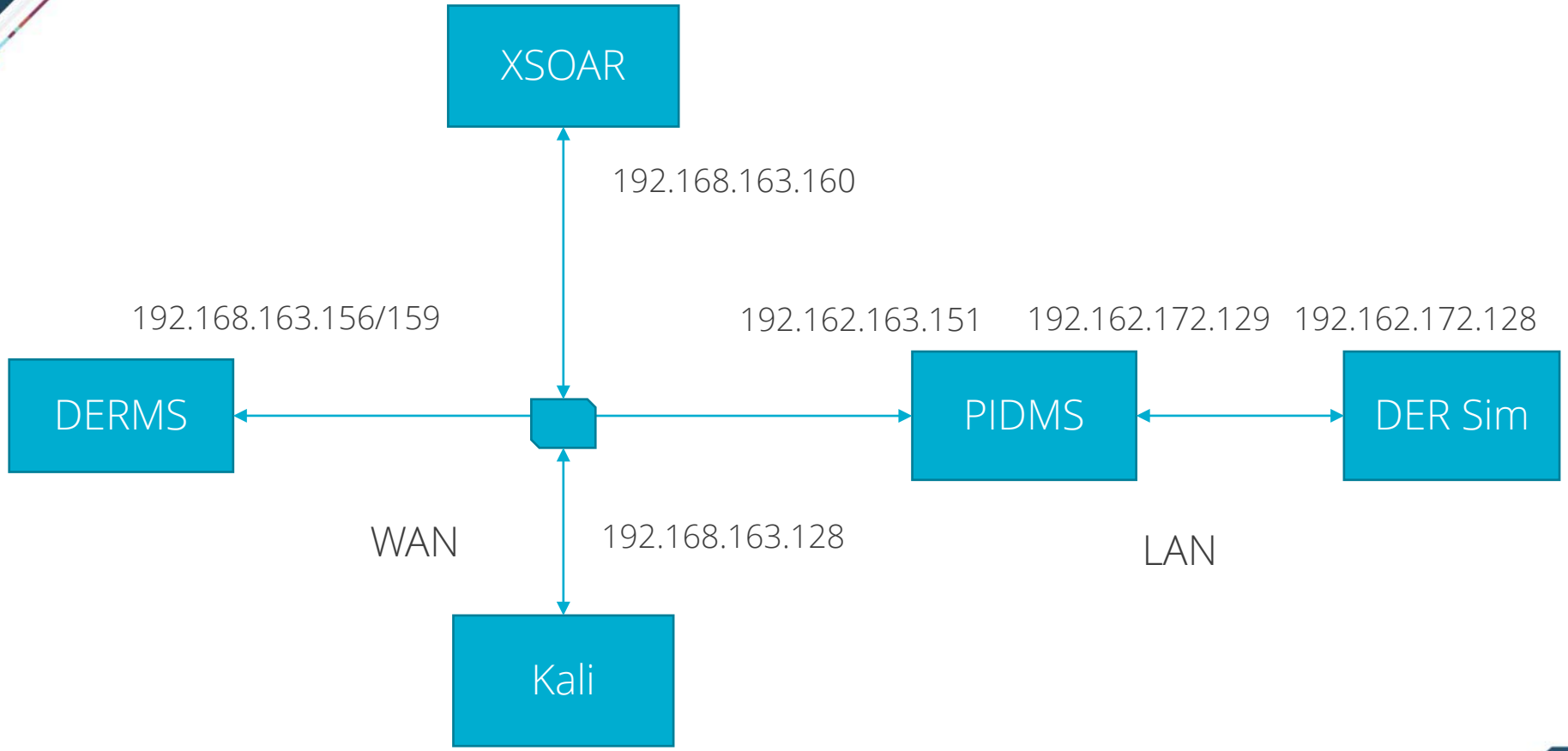
Security Orchestration for DER Equipment

- Initial SOAR work published in *Power Systems Cybersecurity* Book
- Team creating open-source DER network defense playbooks to incorporate with solar operators and aggregators
- Investigating 3 SOAR tools:
  - NSA's WALKOFF
  - Palo Alto Network Cortex XSOAR
  - Splunk SOAR
- Talking with solar operator about field experiments



J. Johnson, C. B. Jones, A. Chavez, S. Hossain-McKenzie "SOAR4DER: Security Orchestration, Automation, and Response for Distributed Energy Resources" in Haes Alhelou, H., Hatziargyriou, N., Dong, Z.Y. (eds) Power Systems Cybersecurity. Power Systems. Springer, Cham. 2023. doi: https://doi.org/10.1007/978-3-031-20360-2_16

SOAR Virtual Machine Architecture



Vulnerability Analysis of Distributed Energy Resources (DER)

Vulnerability Analysis (DER)

- Selected DER devices
- Vulnerability assessment goals
- Bottom up approach to reviewing device
- Vulnerable Hardware
- Vulnerable Software
- Static versus Live testing
- Vendor collaboration where applicable

Vulnerability Analysis (DER) (continued)

- Physical to Web based attacks
- Vulnerabilities-
  - RCE (Remote Code Execution)
  - Firmware updates in plaintext
  - Vulnerable Login webpages
  - Poor authentication schemes
  - Poor encryption applications
  - Etc.
- Vendor/CISA Involvement

Thank you

Reach out if you'd like to chat.

Keira Elliott, Jon Hurtado, & Jay Johnson
kehaski@sandia.gov, jghurta@sandia.gov, & jjohns2@sandia.gov

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 4:

DER Vulnerability Assessments and Analysis

Jennifer Guerra, NREL – DERMS Cybersecurity and Recommendations for Aggregators

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

NREL Transforming ENERGY

Cybersecurity Guidance for Distributed Energy Resource Management Systems (DERMS)

Securing Solar for the Grid Workshop

September 14, 2023

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

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

Purpose and Audience

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

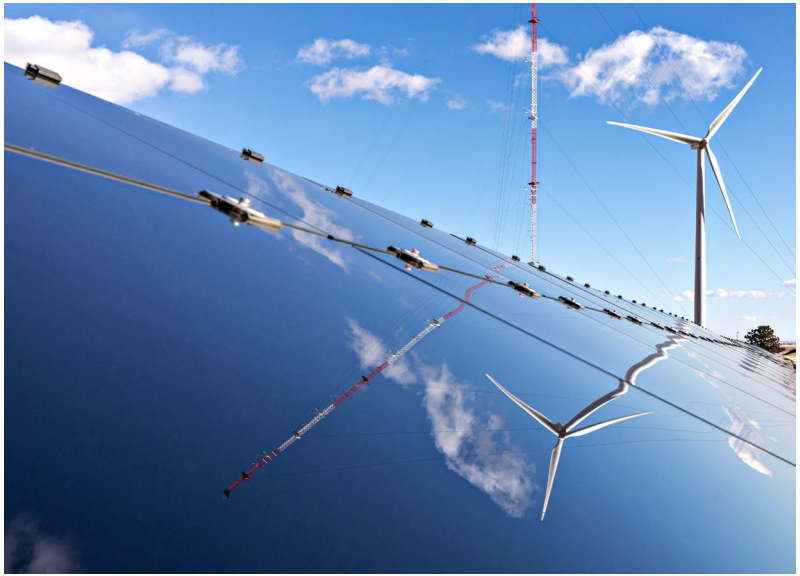


Photo by Werner Slocum, NREL 66364

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

Report Outline

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

Table of Contents

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

Example Threat Scenarios

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

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

Industry/LCC/SETO Involvement

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

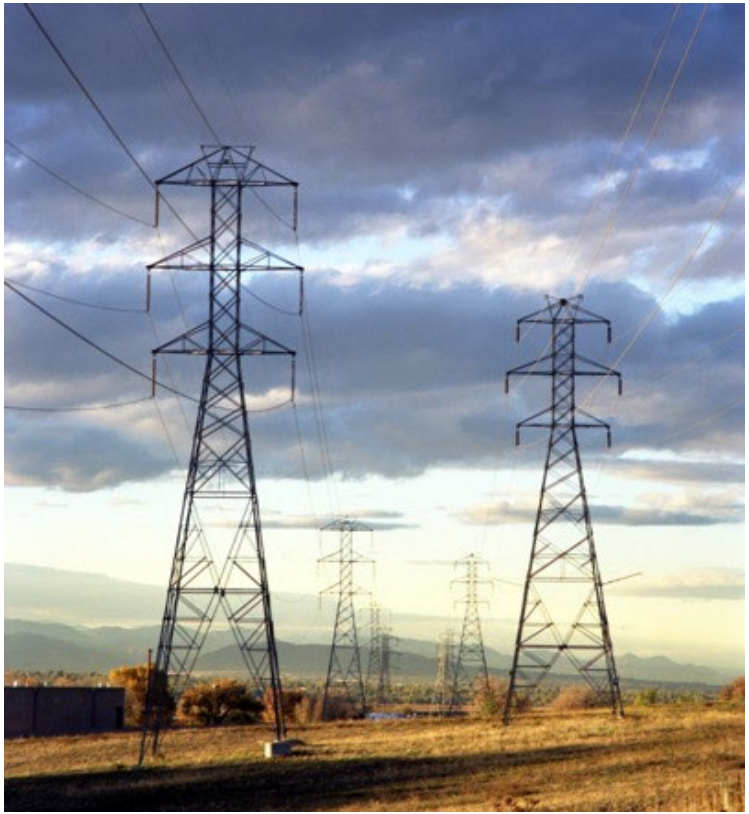


Photo by Werner Slocum, NREL 00001

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

Potential Future Work

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

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

Thank You!

Let’s work together!

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

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

NREL
Transforming ENERGY

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 4:

DER Vulnerability Assessments and Analysis

Wajid Hassan, LogicFinder – Identifying Vulnerabilities through Penetration Testing and Vulnerability Assessment

Identifying Vulnerabilities through Penetration Testing and Vulnerability Assessment

A presentation by Logic Finder

Introduction

- Penetration testing and vulnerability assessment are crucial security practices for identifying and addressing vulnerabilities in OT, IoT, and IT networks.
- Penetration testing simulates attacks to uncover vulnerabilities.
- Vulnerability assessment identifies and assesses weaknesses.
- Together, they provide a holistic view of security, enabling organizations to enhance their defenses.

Threats to OT, IoT, and IT Network Infrastructures

LogicFinder
Consulting, Development and Training

Physical threats:

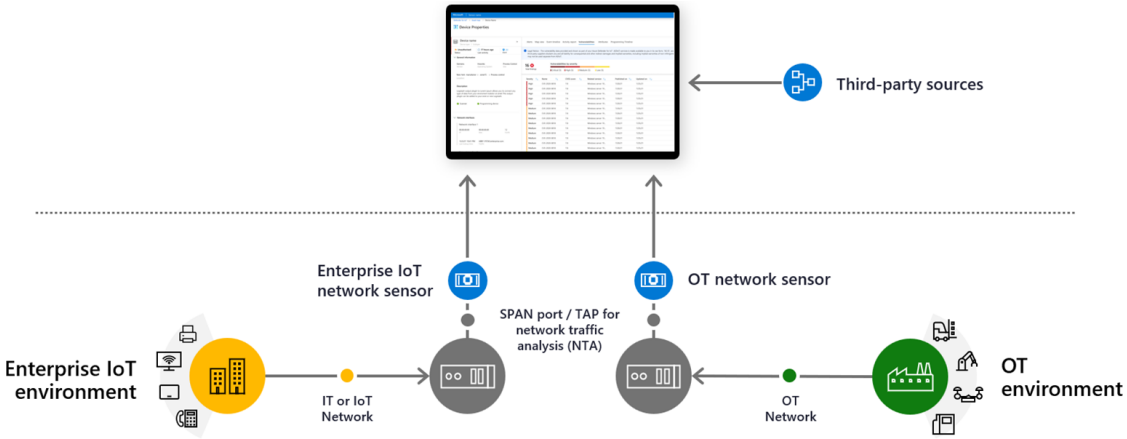
- Tampering with equipment
- Physical access to systems
- Denial-of-service attacks

Logical threats:

- Malware attacks
- Phishing attacks
- Zero-day attacks

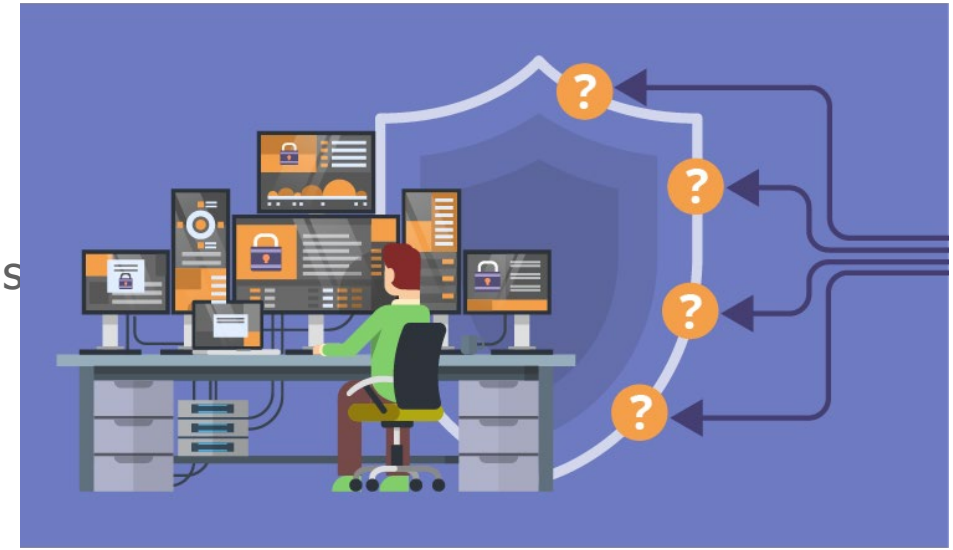
Cyber threats:

- Ransomware attacks
- Distributed denial-of-service (DDoS) attacks
- Supply chain attacks



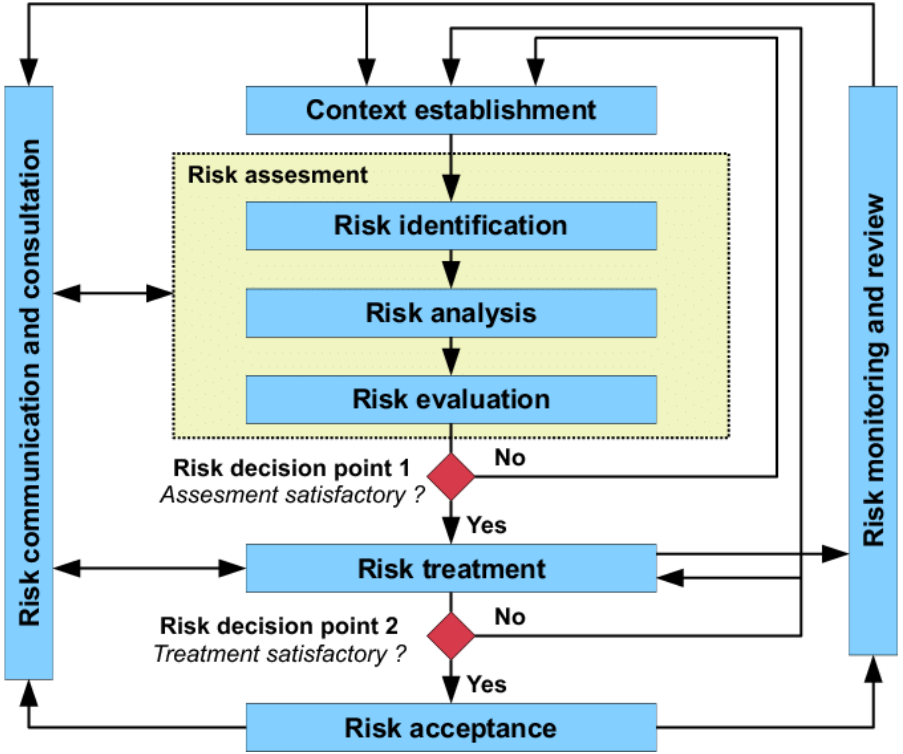
Rising OT Vulnerabilities

- OT networks are often more vulnerable to cyberattacks than IT networks.
- This is because OT networks are typically not as well-protected and are often not patched or updated as regularly as IT networks.
- OT networks also often use outdated or proprietary software that is not well-tested for security vulnerabilities.



Challenges in IT Network Security

- IT networks within the solar energy industry face unique challenges in terms of security.
- These networks often have to be accessed remotely by technicians and engineers, which can create security risks.
- IT networks are also often connected to the internet, which exposes them to potential cyberattacks.



Tools for Penetration Testing and Vulnerability Assessment

- **Vulnerability scanners:** These tools scan networks and systems for known vulnerabilities.
- **Penetration testing tools:** These tools allow security professionals to simulate attacks on networks and systems.
- **Network monitoring tools:** These tools can be used to detect and investigate suspicious activity on networks.
- **Incident response tools:** These tools can be used to respond to cyberattacks.

The Importance of Vulnerability Assessment

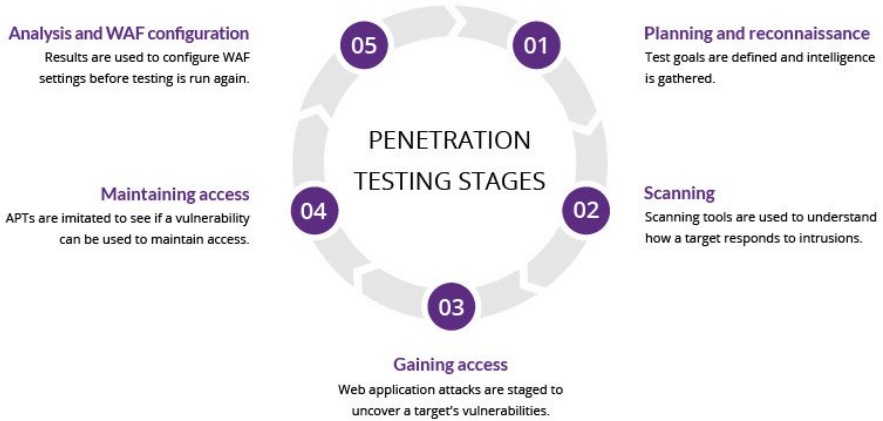
- Vulnerability assessments are essential for identifying and addressing security gaps in any infrastructure.
- These assessments should be conducted regularly to ensure that the systems are protected against the latest threats.
- Vulnerability assessments should also be conducted after any major changes to the system, such as the installation of new equipment or software.

The Value of Penetration Testing

- Penetration testing is a simulated cyberattack that can be used to identify and exploit vulnerabilities in any system.
- Penetration testing is a valuable tool for improving the security of any system.
- It can help to identify vulnerabilities that would not be detected by vulnerability assessments.

Procedures for Penetration Testing and Vulnerability Assessment

- **Planning and scoping:** This involves defining the scope of the testing, identifying the assets to be tested, and setting the objectives of the testing.
- **Information gathering:** This involves gathering information about the target systems, such as IP addresses, usernames, and passwords.
- **Vulnerability scanning:** This involves using vulnerability scanners to identify known vulnerabilities in the target systems.



Procedures for Penetration Testing and Vulnerability Assessment cont…

- **Penetration testing:** This involves manually exploiting vulnerabilities in the target systems.
- **Reporting and remediation:** This involves reporting the findings of the testing and taking steps to remediate the vulnerabilities.

Best Practices for Penetration Testing and Vulnerability Assessment

LogicFinder
Consulting, Development and Training

- Use a variety of tools and techniques to get a comprehensive view of the security posture.
- Involve stakeholders from all levels of the organization in the planning and execution of the testing.
- Follow up on the findings of the testing and take steps to remediate the vulnerabilities.
- Keep the testing process up-to-date with the latest threats and vulnerabilities.

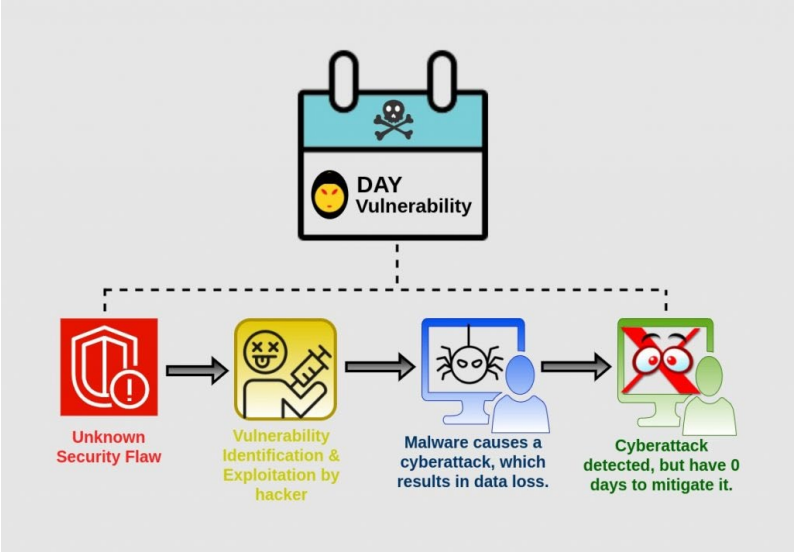
Why OT Networks Should Take Penetration Testing and Vulnerability Assessment Seriously

LogicFinder
Consulting, Development and Training

- OT networks are often more vulnerable to attack than IT networks.
- OT networks control critical infrastructure, such as power plants and solar farms.
- A successful attack on an OT network could have widespread consequences.
- Penetration testing and vulnerability assessment can help to identify and mitigate vulnerabilities in OT networks.

Logic Finder Solutions Services

- Network segmentation, zero-day attack mitigation, and zero network.
- Assessment of the organization's current network security posture.
- Design of an architecture.
- Implementation of the architecture.
- Training of the organization's staff on how to operate the architecture.



Logic Finder solutions services can help organizations

- Improve the security of their critical systems.
- Reduce their risk of attack.
- Simplify network security management.
- Improve visibility into network traffic.
- Increase network efficiency.

Helping Hands
ORGANIZATION

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Panel 4:

DER Vulnerability Assessments and Analysis

Q&A

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Training and Workforce Development

Megan Culler, INL – CyberStrike StormCloud for Solar

INL/CON-23-74522

September 14, 2023

Megan Culler
INL Power Engineer

CyberStrike STORMCLOUD

INL & Sandia

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

What is CyberStrike?

CyberStrike is a training program designed to enhance the ability of energy sector owners and operators to prepare for a cyber incident impacting operational technology .

LIGHTS OUT

- Emphasis on 2015 and 2016 Ukraine attacks
- Power system version and oil & gas version

NEMESIS

- Focus on current and emerging threats
- Additional sectors, including water

STORMCLOUD

- Renewables focus
- Grid modernization challenges, like remote access

What is CyberStrike STORMCLOUD?

The *CyberStrike STORM CLOUD training workshop was designed to enhance the ability of renewable energy and operators to prepare for a cyber incident impacting industrial control systems with specific considerations of the architectures and limitations of renewable energy.*

- Renewables focused
  - Solar
  - Wind (coming soon)
  - EVs (coming soon)
- Emphasis on emerging and unique threats for renewables
  - Remote access
  - Diverse stakeholder ecosystem
- Framework uses Lockheed Cyber Kill Chain

U.S. DEPARTMENT OF ENERGY

Energy Efficiency & Renewable Energy

U.S. DEPARTMENT OF ENERGY

Office of

Cybersecurity, Energy Security, and Emergency Response

CyberStrike STORMCLOUD

Curriculum

Unencrypted HTTP Connection

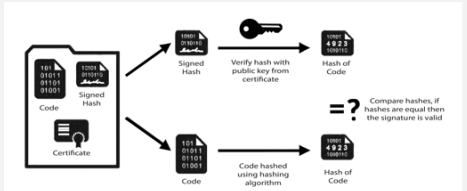
STAGE 1 — Cyber Intrusion Attempt

Brute forced password (ended up being hardcoded defaults)

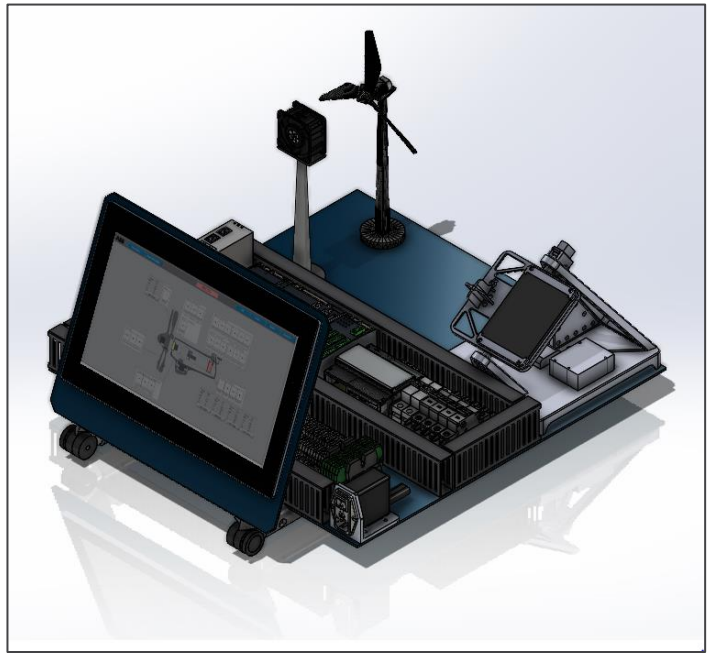
- Cracking PW for a single panel means that any panel with same default login compromised
- Allowed access to configuration changes, such as altering maximum tolerances and limits, which could cause shut down
- Found that there were matching devices on Shodan that could be hacked from public internet

Code Signing

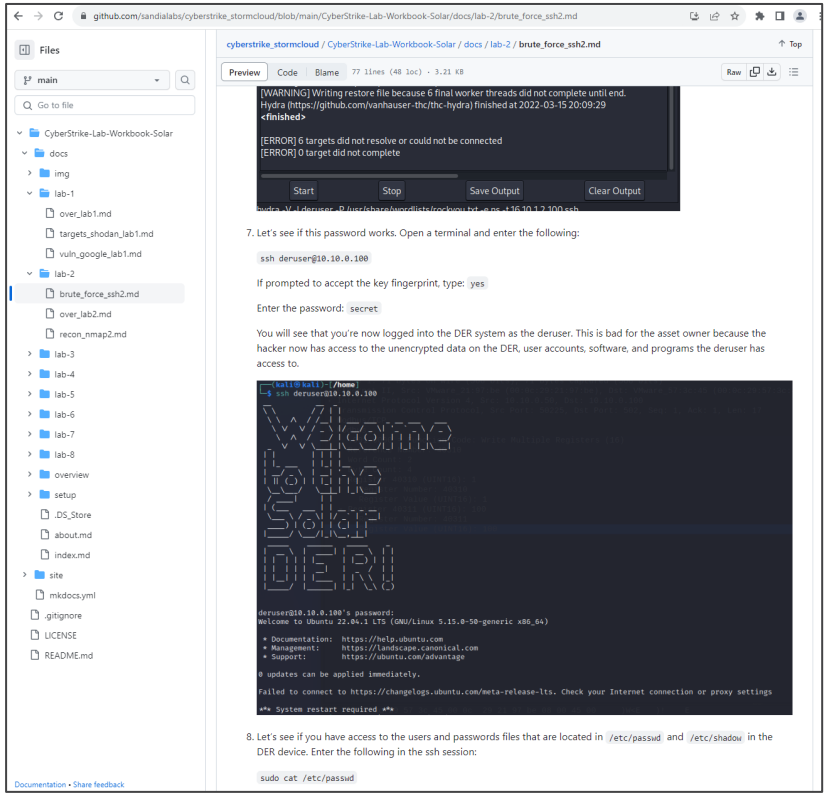
- Code signing is a method of using a certificate to place a digital signature on a final to guarantee that the file or software has not been tampered with or compromised.



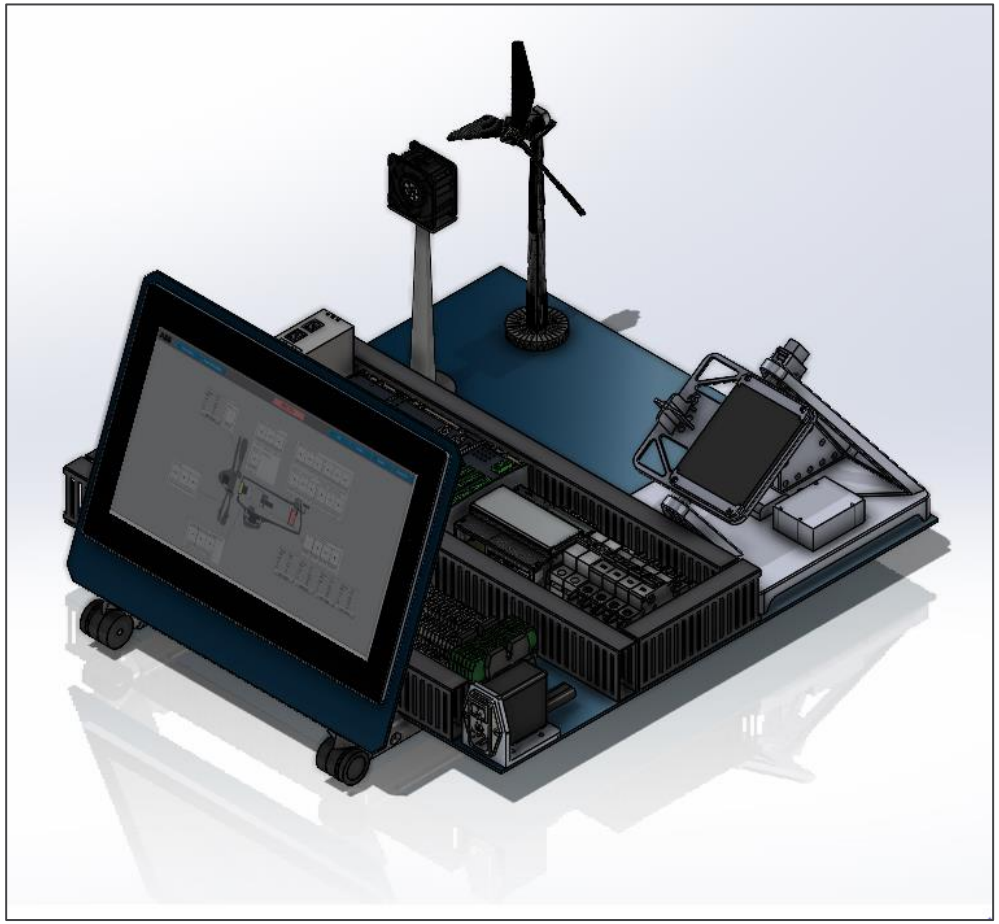
Hardware



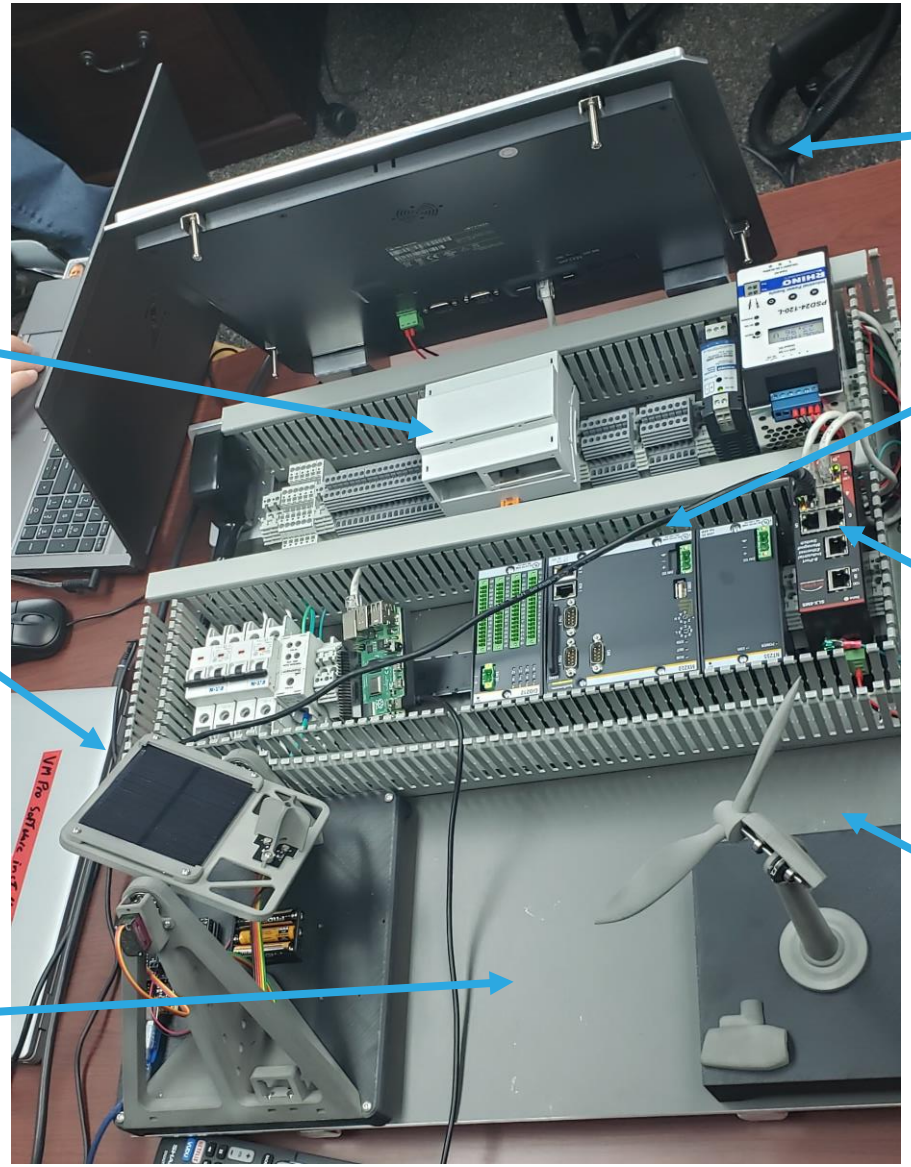
Exercises



STORMCLOUD Kit Design



CyberStrike Storm Cloud Demo Kit



HMI

Solar “inverter” – Raspberry Pi emulator

Industrial controller to be used for wind

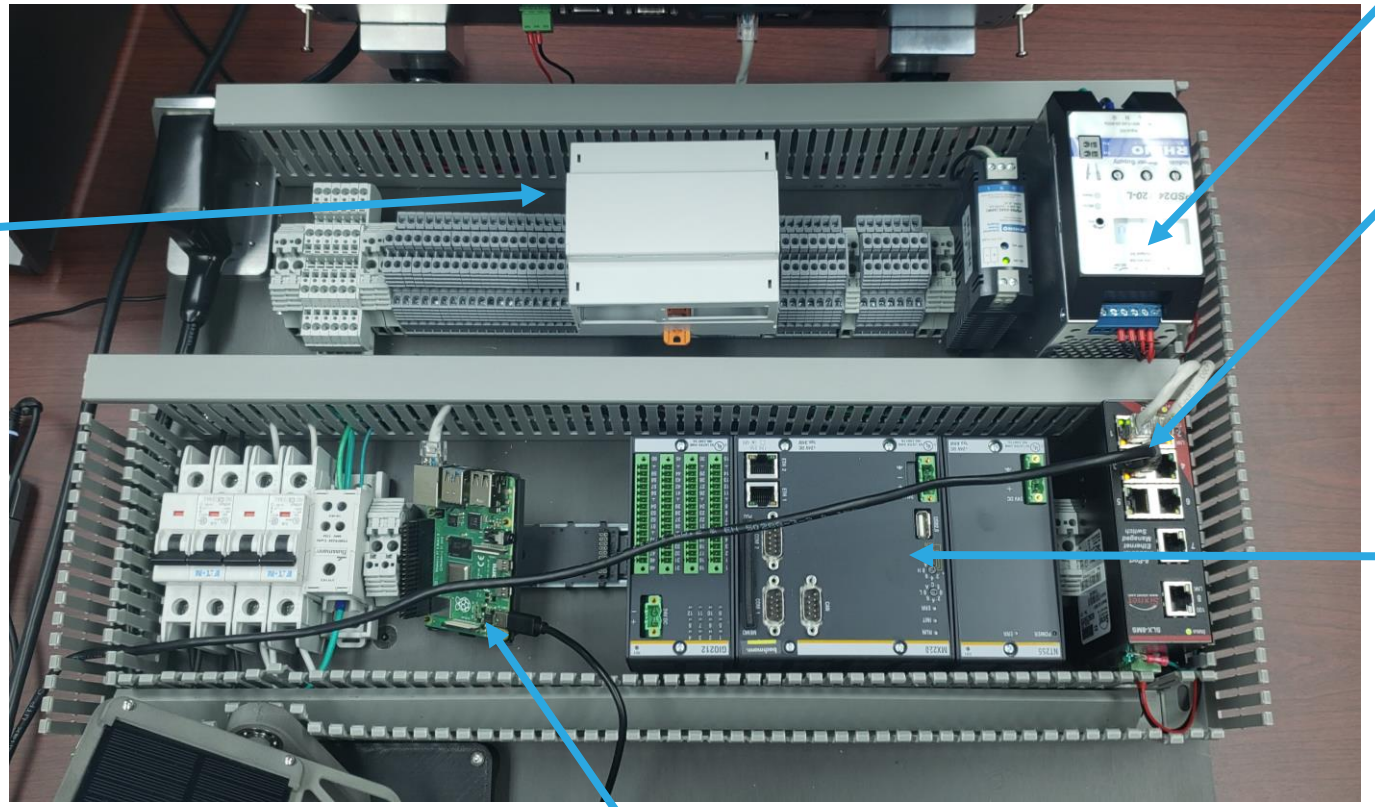
Single-axis solar

Network switch for the DER system

Space for EV model

Open platform design to allow wind turbine to blow

CyberStrike Storm Cloud Demo Kit - Networking



Raspberry Pi inverter emulation

5 V power supply

Network switch

Industrial controller for wind

Arduino board governing solar tracker

CyberStrike Storm Cloud Demo Kit – Solar module

Photoresistor measures output

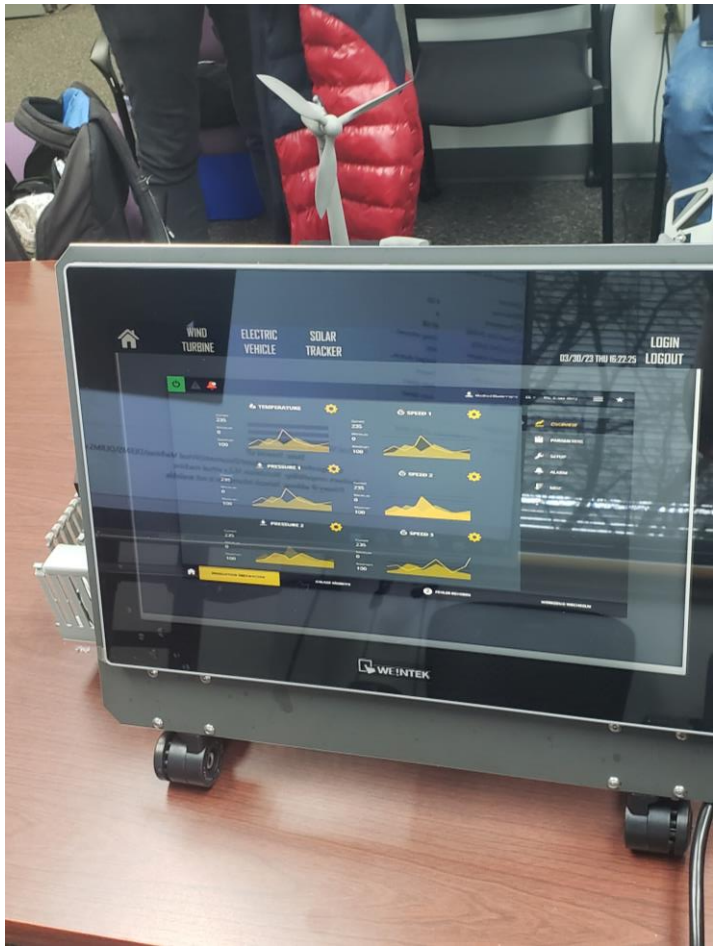
3D-printed Nylon custom frame

Arduino program uses photo-resistor output to determine an angle for the mount.

CyberStrike Storm Cloud Demo Kit – HMI

Touch screen HMI

Separate tabs for each resource



Wind mockup display

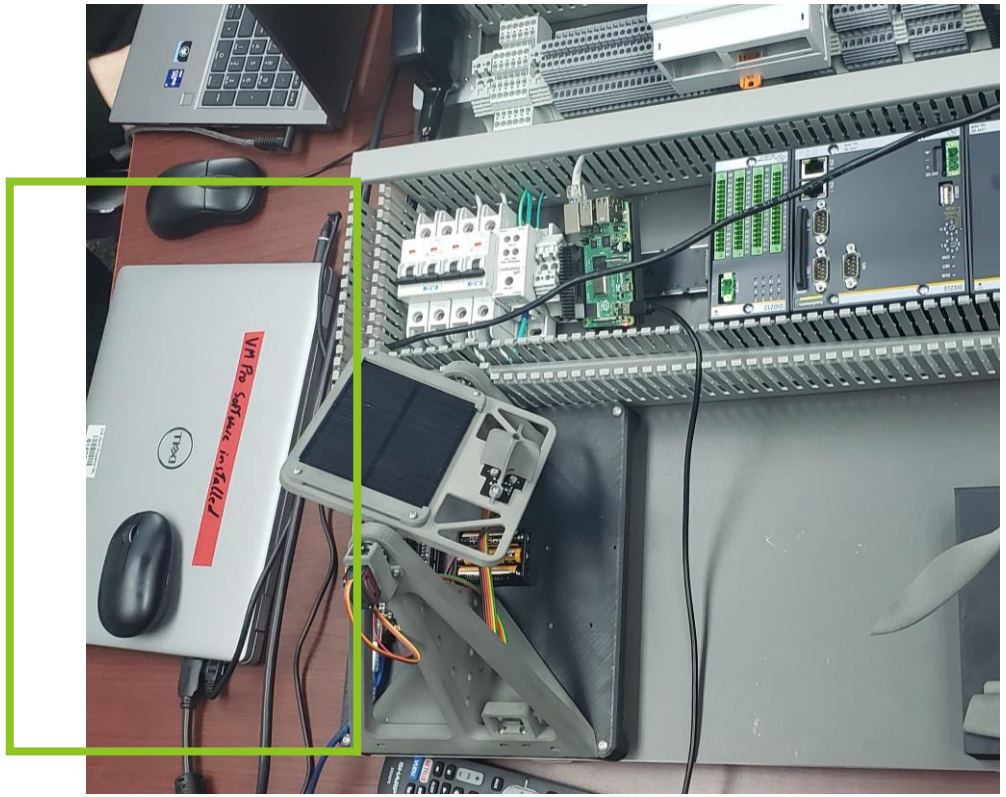
No current applications for solar (not representative of industry)

CyberStrike Storm Cloud Demo Kit - Software

Workstation is a Kali Linux machine

Two VMs used to run the exercises

- Attacker Kali VM
- DERMS Windows VM



Lab manual on VM images for easy access

Lab exercises currently developed:

- Uses real solar firmware images
- Uses real solar protocols

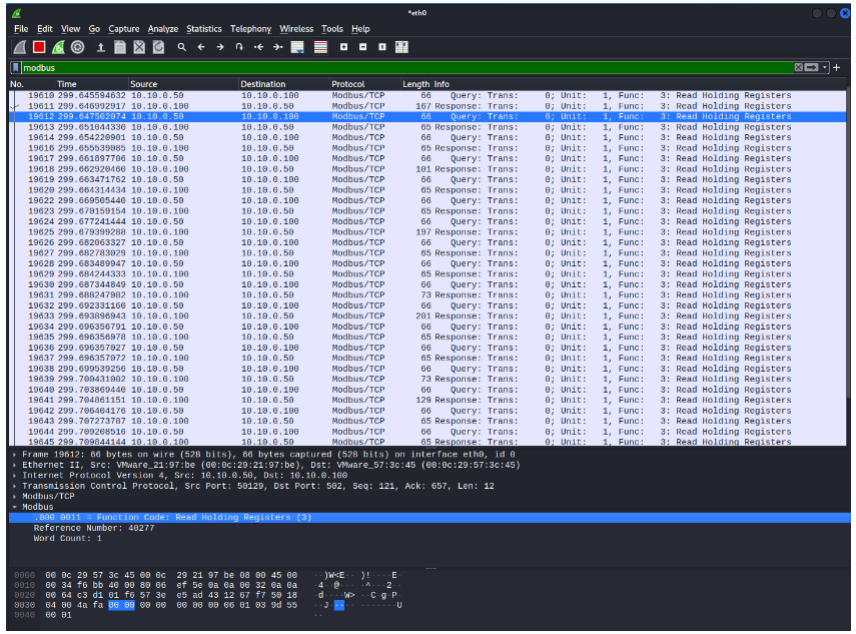
Lab Interfaces and Tools

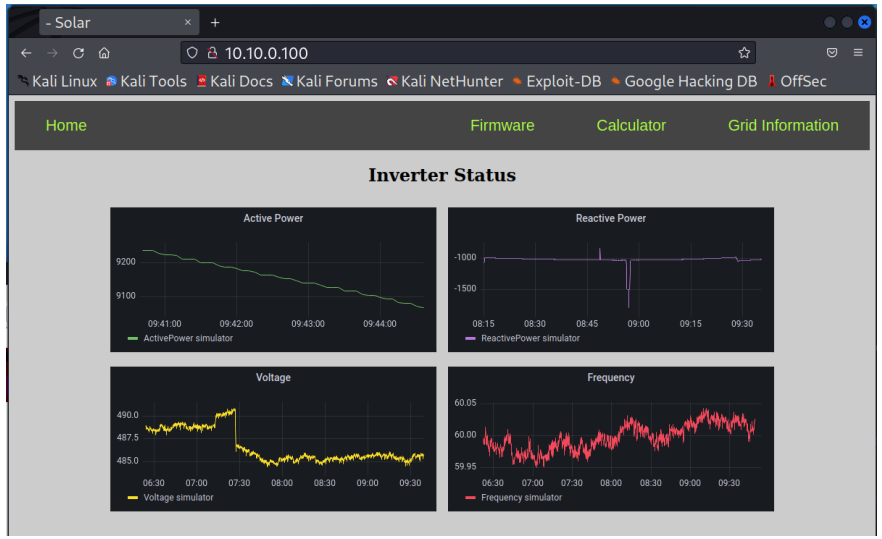
Cybersecurity Tools

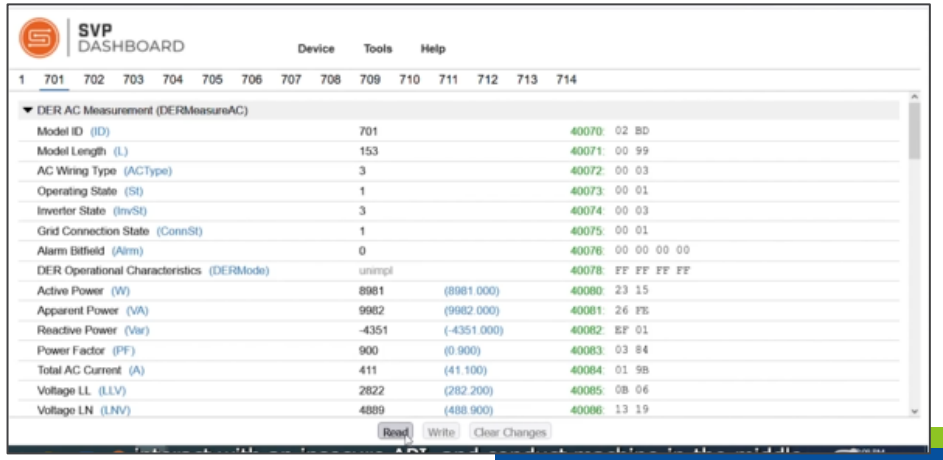
- Shodan
- Xhydra
- NMAP
- Wireshark
- Ettercap

DER Interfaces

- Custom web interface
- VNC Viewer
- SSH
- SunSpec MODBUS
- IEEE 2030.5

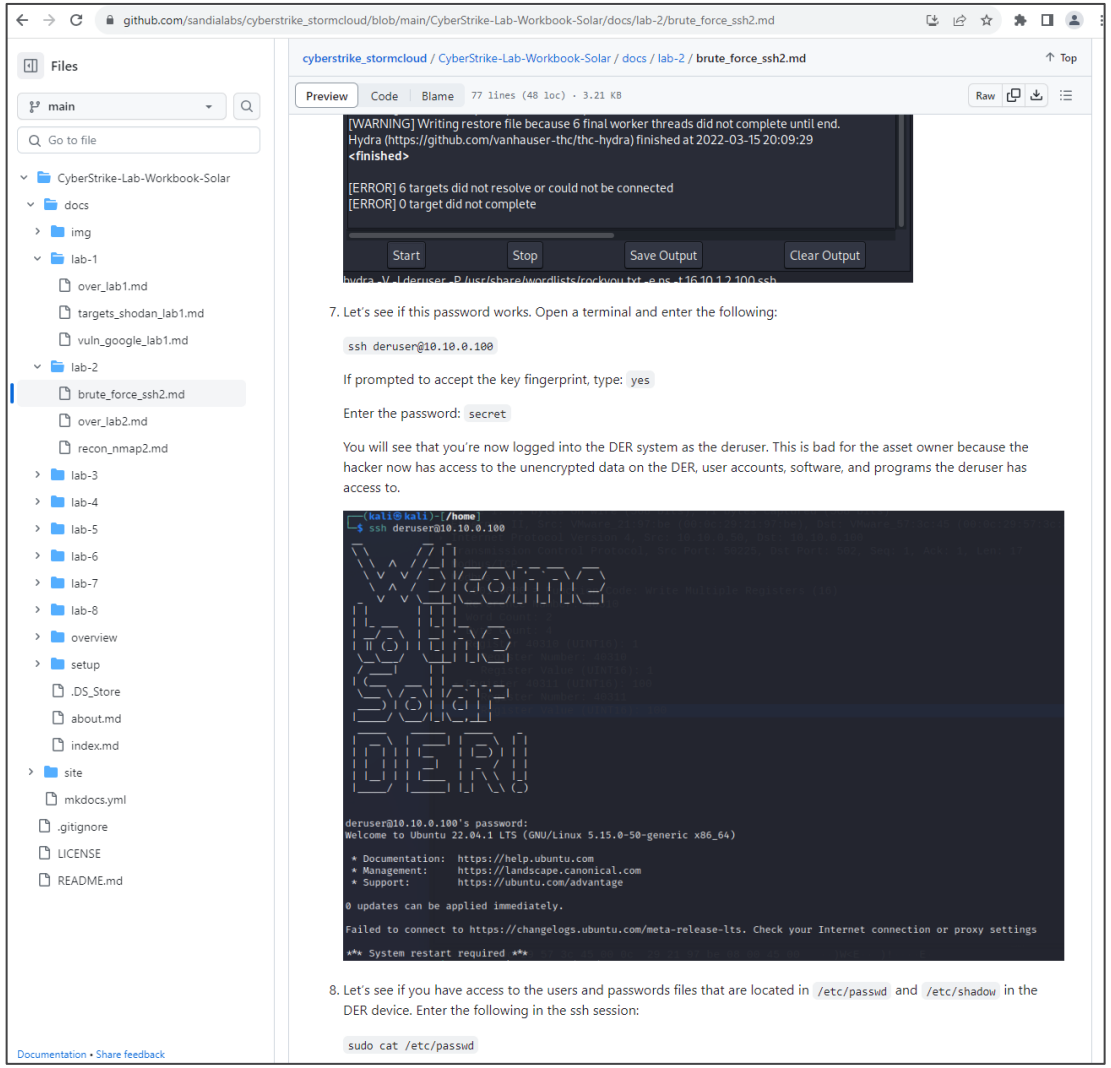






Lab Exercises

- Reconnaissance
  - OSINT demo
  - NMAP port scanning
- Brute-forced passwords
  - Password cracking tools
- Denial-of-service
  - Network flooding
- Malicious firmware updates
  - Code signing and certificates
- Web exploitation
  - SQL injection
  - Code injection
- App inspection
  - Credential harvesting
- Replay and Man-in-the-middle
  - ARP spoofing and packet modification
- Defense
  - Host-based firewall rules



https://github.com/sandialabs/cyberstrike_stormcloud/

FY24 Plans

- Virtualization
  - Virtual platform allows students to take the training on their own time.
  - Interaction with hardware occurs through virtual machines and IP cameras watching the hardware.
- Updated curriculum with 2023 events and vulnerabilities
  - Keep content relevant
  - Update based on feedback from industry events
- Industry engagement
  - Target workshops at relevant industry events to continue rollout and solicit feedback

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Networking Break

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Future Areas of Research & Industry Feedback

Marissa Morales-Rodriguez, SETO
Guohui Yuan, SETO

Danish Saleem, NREL
Scott Mix, PNNL

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

&

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

Increasing Renewable Generation and System Reliability through Coupling PV and Hydropower

EAGLE CREEK RENEWABLE ENERGY

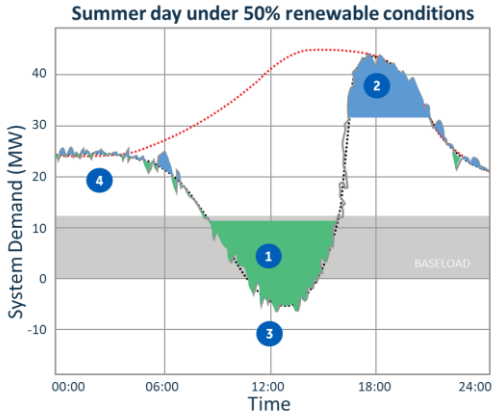
Q CELLS

Presenter: Arvind Tiwari

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office Award Number DE-0009342.
The views expressed herein do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

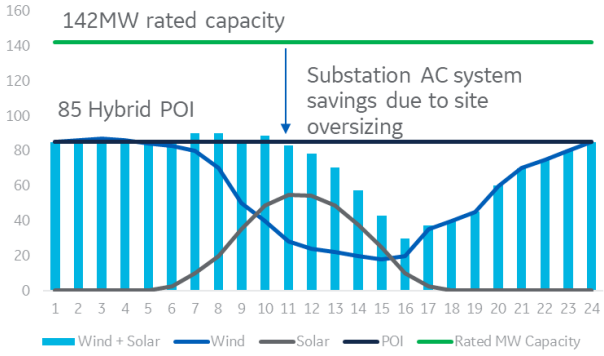
Increased renewables require improved dispatchability, grid stability & affordability that Hybrid Systems can provide

Integrating Storage



1. **Renewables curtailed** - ES charged with free or negative priced energy
2. **Peak Load** - ES discharged during peak demand
3. **Spinning Reserve** – ES discharged during dynamic events
4. **Frequency Regulation** – ES continuously charged and discharged to maintain grid stability

Integrating multi energy resources



Leveraging complementarity of energy resources to:

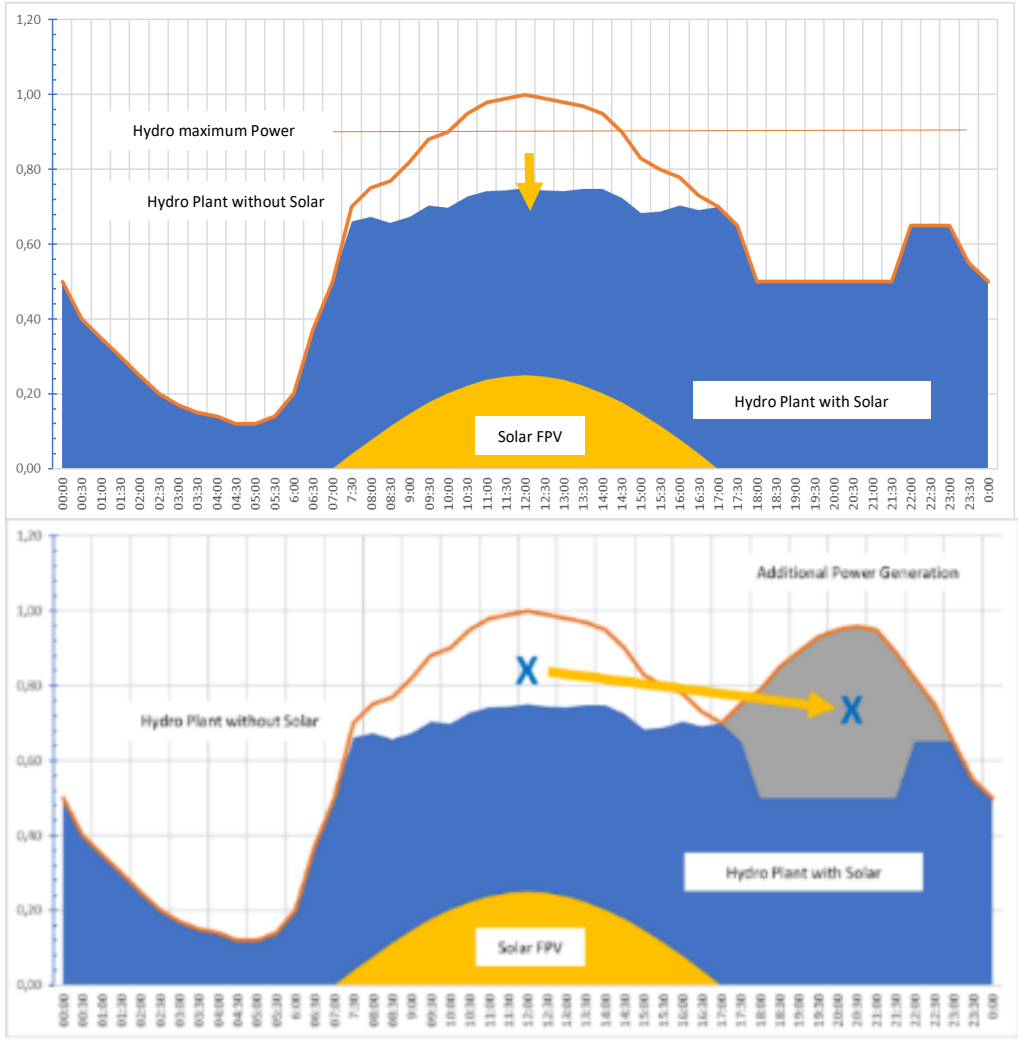
- Increase Capacity Factor
- Optimize EBOP and interconnection
- Optimize use of land
- Improve combined LCOE

©2021 General Electric.

Hybrid Dispatcher Features

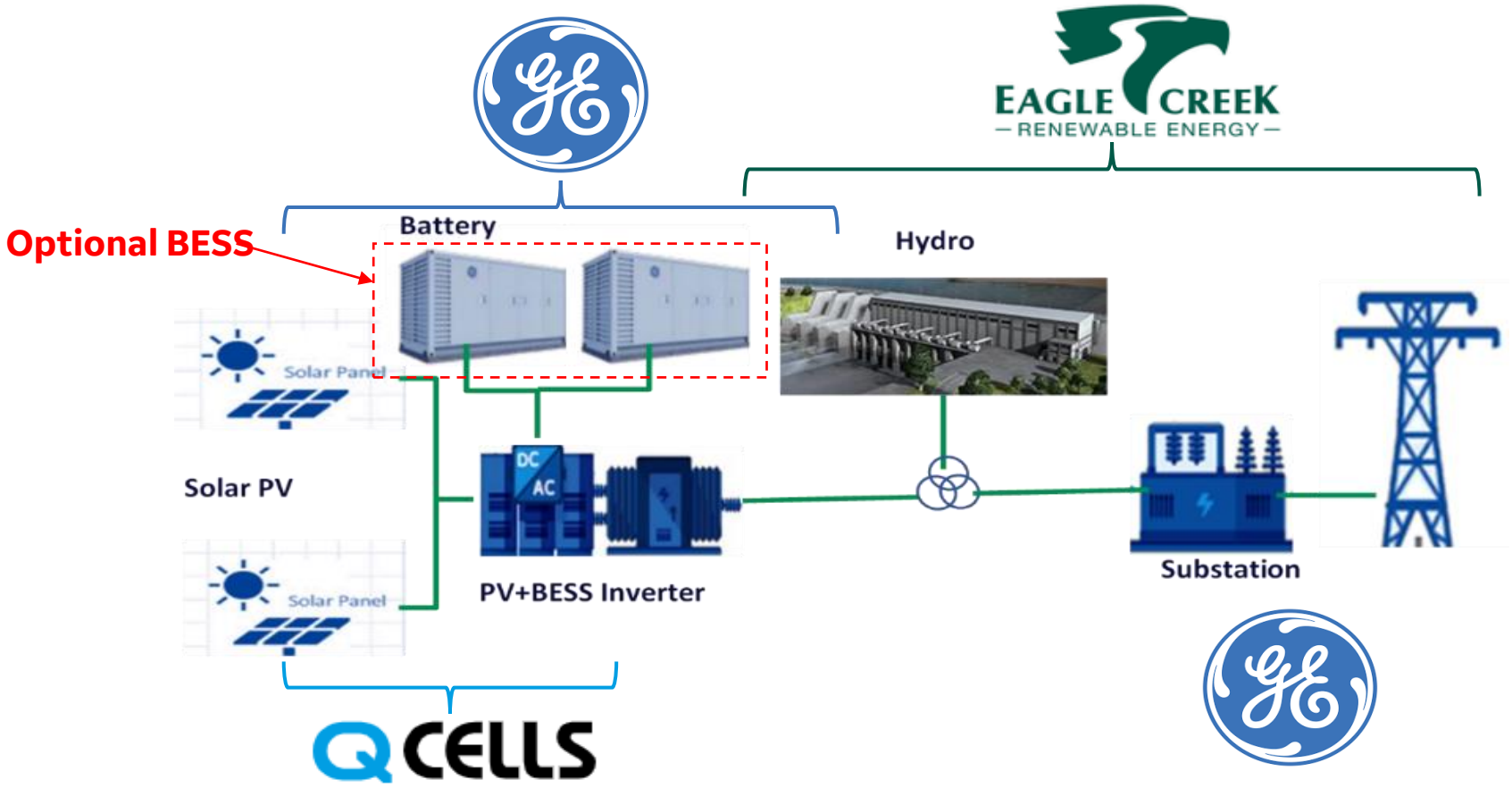
Optimal Dispatch and Scheduling

- ❑ Economics, maximize renewables, energy shifting, and maximize battery life
- ❑ Ability to incorporate real-time asset status and operating values
- ❑ Event driven optimization
- ❑ Reduced operations & maintenance



©2021 General Electric.

Hybrid Plant Architecture



Multi-disciplinary team is architecting building blocks to evaluate and demonstrate at scale a robust, reliable and cost-effective PV/Hydro Hybrid System (PHHS).

©2021 General Electric.

Down Selected Hybrid Controller Overview

Hybrid Controller Platform

Optimization Functions

- Market Participation
- Operations Planning
- Forecasting
- Scheduling
- PV Smoothing
- Mode and Event MGMT
- Portfolio Optimization
- Optimal Dispatch
- SOC Management

Real Time Functions

- Planned Islanding
- Re -synch
- Black start
- **Voltage Management**
- **Frequency Control**
- Unplanned Islanding
- **Reserve Capacity Calc**
- **Power Exchange**
- **Power Factor Management**
- Load Sharing

Hybrid Controller

- Data Communications & Gateway
- Adaptive Protection
- Feeder Sequencing and Control

Switch — Switch

IED — **Substation Bus Bar** — IED

- Load Management
- Fast Load Shedding
- Integrated HMI/SCADA

ADMS/EMS

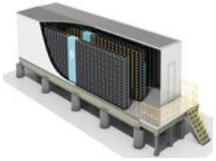
Substation Switch Yard

Hydro

Solar PV

Ground Mount PV

Simulated Storage



MW Scale Battery Energy Storage

Critical / non-critical loads

HVAC, Process, Lighting, EV, etc.

Utility Electric Grid

The selected controller provides fundamental communication and control capabilities to avoid reinventing the wheel. Additionally, it offers high flexibility and scalability to customize the plant control for PHHS.

Conclusion & Takeaways

- **Encourage hybrid technologies**
  - Allows to solve issues closer to the source and more cost-effective solutions
- **Integrated expansion and operations planning**
  - One deals with more granular events, defining which assets to use, and the other defines the new assets needed by the grid
- **Stacking of services**
  - Allows for more cost-effective solutions
- **Hybridized solution cannot be achieved without a hybridized team**
  - Collaboration amongst a diverse team leads to innovative solutions

©2021 General Electric.

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Workshop Closing

Marissa Morales-Rodriguez, SETO

Funded by:

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

SETO S2G IAB Workshop

Backup Slides

Marissa Morales-Rodriguez, SETO

S2G Industry Advisory Board

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Purpose

- To support the development of equipment and communication **cybersecurity standards** for distributed energy resources (**DERs**) and inverter-based resources (**IBR**), and to help establish a national cybersecurity **certification standard** that could become the reference for the industry.
- This project will enable national labs to verify and validate the functionalities through laboratory **testing before they get standardized**, and will help them to accelerate the development, adoption, and implementation of the cybersecurity standards.
- To **establish an industry advisory board** (IAB) to solicit feedback and reviews from key industry stakeholders and to provide updates about the project's activities.

S2G IAB

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Membership

- **Voluntary and by invitation only**.
- The subject matter experts (SME) can respond to the invitation to both **represent their organization and to provide useful feedback** on the S2G project. The selected members of IAB will serve in a purely advisory role.
- DOE reserves the right to review the proposed IAB members and decline individuals who, in their judgment, do not have the background to provide review and guidance.
- The IAB is expected to have **between 15 and 20 members** with a mix of electric utilities, equipment manufacturers and vendors, and other interested parties.

S2G IAB

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Rights

- The IAB members have the right to **publicize** the fact of their **participation** in the IAB. They have the right to disseminate work products from the projects, provided that the work products have been cleared for release by the laboratory coordination committee and DOE's SETO office.

Responsibilities

- The IAB members are responsible to **attend** bi-annually virtual **meetings** (once every six months) to **provide feedback** as requested of them and to **review the work products** (if any). IAB members are also responsible to *not disclose their own company's proprietary or other sensitive information* during IAB meetings or in their written feedback.

S2G IAB

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Meetings

- The project team will host **bi-annually virtual IAB meetings** to solicit the feedback. The IAB members are **also encouraged to join the annual in-person** continuation review meeting.

Commitment

- The project team estimates that IAB members are not expected to spend more than **2 hours on IAB work every month**. The actual time may vary from month to month.

Term of Membership

- The IAB will exist for the **duration** of the project, which is scheduled to end **September 2024**. The minimum expected term of IAB membership is one (1) year