SANDIA REPORT

SAND2017-13262
Unlimited Release
Printed December 2017

Roadmap for Photovoltaic Cyber Security

Jay Johnson

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

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

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	http://www.ntis.gov/search

SAND2017-13262
Unlimited Release
Printed December 2017

Roadmap for Photovoltaic Cyber Security

Jay Johnson
Renewable and Distributed Systems Integration
Sandia National Laboratories

Abstract

Cyber-secure, resilient energy is paramount to the prosperity of the United States. As the experience and sophistication of cyber adversaries grow, so too must the US power system's defenses, situational awareness, and response and recovery strategies. Traditionally, power systems were operated with dedicated communication channels to large generators and utility-owned assets but now there is greater reliance on photovoltaic (PV) systems to provide power generation. PV systems often communicate to utilities, aggregators, and other grid operators over the public internet so the power system attack surface has significantly expanded. At the same time, solar energy systems are equipped with a range of grid-support functions, that—if controlled or programmed improperly—present a risk of power system disturbances. This document is a five-year roadmap intended to chart a path for improving cyber security for communication-enabled PV systems with clear roles and responsibilities for government, standards development organizations, PV vendors, and grid operators.

ACKNOWLEDGMENTS

This work was funded by the Department of Energy (DOE) Energy Efficiency and Renewable Energy (EERE) Solar Energy Technologies Office (SETO).

The author would like to thank the diverse collection of reviewers who provided comments to the roadmap: Jason Stamp, Eric Vugrin, Patricia Cordeiro, Adrian Chaves, Clifford Hansen, Lon Dawson, Christine Lai, Ahmad Jrad, Cedric Carter, and the SunSpec Distributed Energy Resource (DER) Cyber Security Working Group.

The CEDS and DHS program information and budgets were compiled by Lauren Amagai.

CONTENTS

FIGURES

TABLES

NOMENCLATURE

AAA	Availability, Authorization, and Accounting
AAL	Advanced Analytics Laboratory
AC	Alternating Current
ACL	Access Control List
AES	Advanced Data Encryption Standard
AMI	Advanced Metering Infrastructure
ANSI	American National Standard Institute
API	Application Programming Interface
ARM	Advanced RISC Machine
ART	Adaptive Resonance Theory
BITW	Bump-in-the-Wire
BPS	Bulk Power System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
C-SCRM	Cyber Supply Chain Risk Management
C2M2	Cybersecurity Capability Maturity Model
CA	Certificate Authority or California
CAP	Cybersecurity Assurance Program
CBC	Cipher Block Chaining
CEA	Consumer Electronics Association
CEDS	Cybersecurity for Energy Delivery Systems
CI	Critical Infrastructure
CIA	Confidentiality, Integrity, and Availability
CIGRE	International Council on Large Electric Systems
CIP	Critical Infrastructure Protection
CMU	Carnegie Mellon University
COP	Common Operating Picture
CPS	Cyber-Physical Systems
CPU	Central Processing Unit
CPUC	California Public Utilities Commission
CRC	Cyclic Redundancy Checking
CRISP	Cybersecurity Risk Information Sharing Program
CSD	Cyber Security Division
CSET	Cyber Security Evaluation Tool
CSIP	Common Smart Inverter Profile
CTA	Consumer Technology Association
CVE	Common Vulnerabilities and Exposures
CYMSA	Cyber-Physical Modeling and Simulation for Situational Awareness
DARPA	Defense Advanced Research Projects Agency
DC	Direct Current
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DER	Distributed Energy Resource(s)

DERMS	Distributed Energy Resource Management System
DES	Data Encryption Standard
DGM	Distribution Grid Management
DHS	Department of Homeland Security
DMS	Distribution Management System
DNP	Distribution Network Protocol
DMZ	De-Militarized Zone
DNP3	Distributed Network Protocol
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DOE	Department of Energy
DoS	Denial of Service
DR	Demand Response
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
E-ISAC	Electricity Information Sharing and Analysis Center
EAP	Extensible Authentication Protocol
ECC	Error Detection and Correction
EdgeCT	Edge-Directed Cyber Technologies for Reliable Mission Communication
EEI	Edison Electric Institute
EMS	Energy Management System
EO	Executive Order
EPRI	Electric Power Research Institute
EPS	Electric Power System
ERO	Electric Reliability Organization
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
ESCC	Electricity Subsector Coordinating Council
ESIF	Energy Systems Integration Facility
ESS	Energy Storage System
ET	Electric Transportation
EV	Electric Vehicle
FAN	Field Area Network
FBI	Federal Bureau of Investigation
FDEMS	Facilities DER Energy Management System
FEMS	Facility Energy Management System
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standard
FW	Frequency-Watt
GCM	Galois/Counter Mode
GDOI	Group Domain of Interpretation
GIS	Geographic Information System
GOOSE	Generic Object Oriented Substation Event
GRR	Google Rapid Response
GWAC	GridWise Architecture Council
HAN	Home Area Network
HIL	Hardware-in-the-Loop

HMI	Human-Machine Interface
HTTPS	Hypertext Transfer Protocol Security
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System
ICS-CERT	Industrial Control System Cyber Emergency Response Team
ICT	Information and Communication Technologies
IdAM	Identity and Access Management for Electric Utilities
IDART	Information Design Assurance Red Team
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IOU	Investor-Owned Utility
IP	Internet Protocol
IPS	Intrusion Prevention System or Internet Protocol Suite
IPSec	Internet Protocol Security
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization, or Independent System Operator
IT	Information Technology
JWG	Joint Working Group
LAN	Local Area Network
LDRD	Laboratory Directed Research and Development
LICs	Logical Interface Categories
LLNL	Lawrence Livermore National Laboratory
LTC	Load Tap Changer
MESA	Modular Energy Storage Architecture
MIT	Massachusetts Institute of Technology
MMS	Manufacturing Message Specification
NAT	Network Address Translation
NASEO	National Association of State Energy Officials
NCCIC	National Cybersecurity and Communications Integration Center
NCCoE	National Cybersecurity Center of Excellence
NCIRP	National Cyber Incident Response Plan
NERC	North American Electric Reliability Corporation
NGO	Non-Governmental Organization
NGSCB	Next-Generation Secure Computing Base
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
NESCOR	National Electric Sector Cybersecurity Organization Resource
NREL	National Renewable Energy Laboratory
NSM	Network and System Management
NSTB	National SCADA Test Bed

NSTC	National Science and Technology Council
NVD	National Vulnerability Database
OE	Office of Electric Delivery and Energy Reliability
OMS	Outage Management System
OpenADR	Open Automated Demand Response
OSGP	Open Smart Grid Protocol
OSI	Open System Interconnection
OT	Operational Technology
OTRA	Operational Technology Risk Assessment
PCC	Point of Common Coupling
PCS	Power Conditioning System
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
PNNL	Pacific Northwest National Laboratory
PPD	Presidential Policy Directive
PUC	Public Utilities Commission
PV	Photovoltaic
QKD	Quantum Key Distribution
R&D	Research and Development
RADICS	Rapid Attack Detection, Isolation and Characterization Systems
RAID	Redundant Array of Independent Disks
RBAC	Role-Based Access Control
RD&D	Research, Development and Demonstration
REP	Retail Energy Providers
RFC	Request for Comments
RISC	Reduced Instruction Set Computer
RMP	Risk Management Process
Root-CA	Root Certificate Authority
RTCP	Real-time Transport Control Protocol
RTO	Regional Transmission Organization
RTU	Remote Terminal Unit
SA	Situational Awareness
SAE	Society of Automotive Engineers
SC	Study Committee
SCADA	Supervisory Control and Data Acquisition
SDO	Standards Development Organization
SEP	Smart Energy Profile
SIEM	Security Incident and Event Management
SIWG	Smart Inverter Working Group
SNL	Sandia National Laboratories
SNMP	Simple Network Management Protocol
SP	Special Publication, from NIST
SRTP	Secure Real-time Transport Protocol
SSL	Secure Socket Layer

TCG	Trusted Computer Group
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TNC	Trusted Network Connect
TPM	Trusted Platform Module
TR	Technical Report
TRL	Technology Readiness Level
TTP	Tactics-Techniques-Procedures
UDP	User Datagram Protocol
UFC	Unified Facilities Criteria
UK	United Kingdom
UL	Underwriters Laboratories
URL	Uniform Resource Locator
US	United States
VEN	Virtual End Node
VM	Virtual Machine
VPN	Virtual Private Network
VTN	Virtual Top Node
VV	Volt-Var
WAMPAC	Wide Area Monitoring, Protection, and Control
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WS	Web Services
XML	eXtensible Markup Language

EXECUTIVE SUMMARY

The US Department of Energy (DOE) Solar Energy Technologies Office (SETO) asked Sandia National Laboratories to create a roadmap for improving cyber security for distributed solar energy resources. This roadmap is intended to provide direction for the nation over the next five years. The roadmap focuses on the intersection of industry and government and recommends activities in four related areas: stakeholder engagement, cyber security research and development, standards development, and industry best practices.

To secure PV communication networks, experts from many disparate communities must coordinate their activities to update DER communications standards, create resilient DER-to-grid operator networks, and develop cyber-secure solutions for power electronics equipment, servers, cloud services, etc. The recommendations herein are specifically tailored to photovoltaic systems but do apply to other distributed energy resources (DER)—especially inverter-based DER—so this roadmap may be useful to other DER communities to direct and prioritize future work. The following high-priority recommendations are covered in this report:

- The PV industry should collaborate with established industrial control and power system cyber security communities to implement state-of-the-art cyber security best practices.
- Government and private organizations should establish stakeholder engagement programs—including workshops, educational programs, and technical working groups—to educate the community, build consensus-based security standards, and effectively and universally implement standards across the industry.
- Information sharing programs are needed to move actionable intelligence to decision makers before, during, and after a cyber attack.
- The solar industry must establish equipment standards, security requirements for data-in-transit, and certification protocols to verify implementation before products enter the market.
- Industry guidelines should be developed for access control, data-at-rest, and network architectures (i.e., end-to-end communications from grid operators to residential or commercial PV systems).
- Where possible, PV standards development organizations should leverage existing standards and guidelines to accelerate cyber security deployments for PV devices and communication networks.
- Research and development programs should investigate solutions across the technology readiness level (TRL) spectrum for identifying assets and risks, protecting infrastructure, detecting threats, and responding and recovering from cyber attacks.
- The PV and cyber security industry should commercialize or adopt innovative technologies to harden infrastructure, protect networks from penetration, detect intrusions, and effectively respond to security breaches.
- Standards alone cannot protect critical infrastructure, so industry should proactively conduct cyber security evaluations, implementing defense-in-depth practices, require good cyber security hygiene, rapidly patch systems, mitigate the insider threat, and address supply chain risks.

1 INTRODUCTION

In December 2015, a cyber security attack in Ukraine left 225,000 people without power.[1] A similar attack was carried out a year later that caused an outage of 200 MW.[2] This, in combination with the increasing presence of distributed denial of service (DDoS) attacks, malware, ransomware, data theft, and other internet-based attacks, indicate the scale of the challenges power grid operators face as attackers increase their level of sophistication. The emergence of cyber security threats to industrial control systems (ICS) over the last decade poses real risks to US energy delivery systems.[3] The best method for long-term resilience from these risks is to understand the latest emerging threats and harden the power system infrastructure, deploy intrusion detection tools, and establish and install novel response mechanisms through cyber security research and development (R&D) programs, industry outreach and engagement, and codes and standards development.

Roadmapping exercises are designed to chart a navigational path from the current state-of-the-art to a preferred future state. In this report, we recommend actionable R&D and stakeholder engagement activities to achieve cyber-secure interoperability for all photovoltaic (PV) systems through multiple secure pathways using several communication protocols by 2023. To reach that outcome, significant changes must be made by PV power electronics vendors, aggregators, and utilities through improved security practices. Some of these changes will be institutionalized through education and stakeholder outreach programs but other updates will be driven with security updates to DER codes, standards, and communication protocol definitions. Realistically, the challenges of shoring up US power system critical infrastructure from cyber-attacks is a much larger problem than can be solved individually by the DOE Solar Office, photovoltaic community, or DER working groups—it is shared. There are specific issues that face the photovoltaic and DER communities that must be addressed with cyber security R&D and standards development. It is the goal of this report to outline a path toward a future with highly secure solar communications.

Our desired end state is a world where grid operators, system owners, and aggregators communicate with interoperable photovoltaic systems using safe, secure, resilient networks with high availability, data integrity, and confidentiality. Transition to this end state requires the following key security features:

1. Resistance to adversarial penetration
2. Secure interfaces to data-sharing partners with associated access control and authentication
3. Supportive of updates, self-healing, and reconfiguration without loss of service
4. Monitoring and situational awareness for intrusion detection, analytics, active response, forensics, and diagnosis
5. Graceful degradation to safe, autonomous, recoverable state in the event of adversarial penetration

[1] SANS Industrial Control Systems and E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case," 18 Mar 2016.

[2] A. Greenberg, 'Crash Override': The Malware That Took Down a Power Grid, WIRED, 12 Jun 2017.

[3] Industrial Control Systems Cyber Emergency Response Team, ICS-CERT Year in Review, 2016.

6. Logging, nonrepudiation, and attribution to determine and prosecute bad actors

This cyber security roadmap was compiled based on reviews of cyber studies and other roadmaps, surveys of cyber security research across academia and government agencies, and input from cyber security experts. It also closely aligns with a previous ICS cyber security gap analysis[4] and earlier roadmapping exercises by the Energy Sector Control Systems Working Group[5] and NERC.[6] Our roadmap provides greater detail for photovoltaic systems and their communication networks and emphasizes roles for all stakeholders in establishing cyber secure PV networks. This report does not discuss specific PV sector cyber security issues or the consequences of unsecured PV systems. Those motivations along with broad DER interoperability and cyber security background information is provided in a separate DER Cyber Security Primer report.[7]

The process for improving cyber security for PV systems is shown in Figure 1. It is important to understand how efforts to improve PV system cyber security fit into the larger context of the vast cyber security landscape, so the figure depicts best practices from a range of nested communities being directed into two primary thrusts: stakeholder engagement and cyber security R&D. Within the stakeholder engagement thrust, public-private partnerships establish workshops, working groups, educational opportunities, and reach out to other cyber security working groups. Within the R&D thrust, cyber security and solar researchers design and evaluate new technologies for securing photovoltaic systems. Both the stakeholder engagement and R&D efforts feed into the creation of cyber security requirements for PV systems. With the adoption of these standards, industry will integrate new cyber security features into PV communication networks and commercialize concepts from the R&D thrust. This report is structured around the flow chart. Section 2 describes prior and ongoing work in the larger cyber security context. Section 3 discusses stakeholder engagement activities and standards update processes. Section 4 covers cyber security R&D activities; Section 5 discusses what changes to PV standards are necessary for improving cyber security practices; and Section 6 presents industry best practices.

[4] J.E. Stamp, J.E. Quiroz, A. Ellis, B. Bhagyavati, J.A. Cooley, K. Dahl, E.R. Limpaecher, Cyber Security Gap Analysis for Critical Energy Systems (CSGACES), Sandia National Laboratories Technical Report, SAND2017-8823, January 2017.

[5] Energy Sector Control Systems Working Group, “Roadmap to Achieve Energy Delivery Systems Cybersecurity,” DOE, Sept 2011.

[6] NERC, “Critical Infrastructure Strategic Roadmap,” Nov 2010.

[7] C. Carter, C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, I. Onunkwo, J. Johnson, "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators," Sandia Technical Report, 2017.

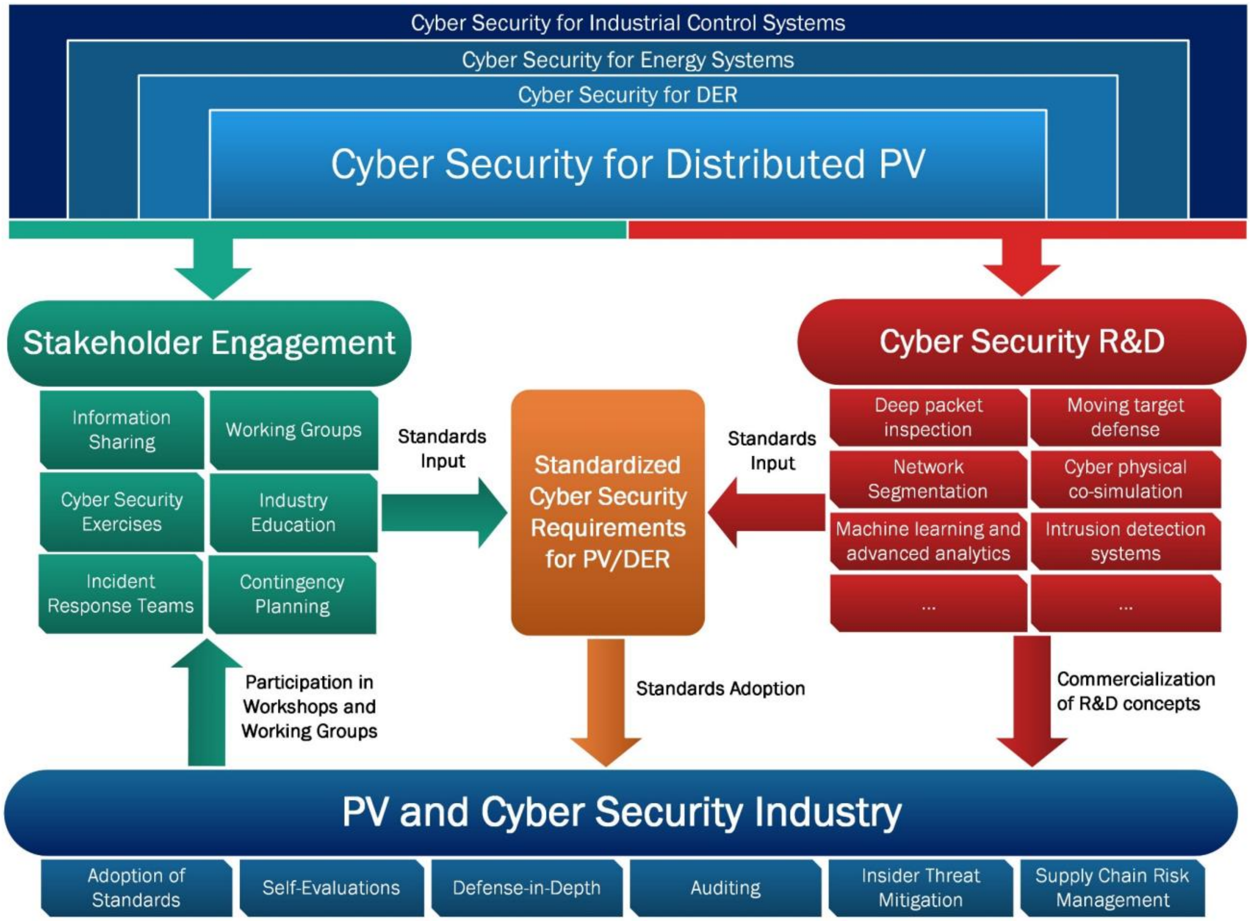

Cyber Security for Industrial Control Systems
Cyber Security for Energy Systems
Cyber Security for DER
Cyber Security for Distributed PV
Stakeholder Engagement
Information Sharing
Working Groups
Cyber Security Exercises
Industry Education
Incident Response Teams
Contingency Planning
Standards Input
Standardized Cyber Security Requirements for PV/DER
Standards Input
Cyber Security R&D
Deep packet inspection
Moving target defense
Network Segmentation
Cyber physical co-simulation
Machine learning and advanced analytics
Intrusion detection systems
...
...
Participation in Workshops and Working Groups
Standards Adoption
Commercialization of R&D concepts
PV and Cyber Security Industry
Adoption of Standards
Self-Evaluations
Defense-in-Depth
Auditing
Insider Threat Mitigation
Supply Chain Risk Management

Figure 1: Process for achieving cyber security of PV systems.

The PV cyber security roadmap is presented in Table 1. The roadmap adopts the vision, barriers, and strategies for achieving energy delivery systems cyber security developed by the Energy Sector Control Systems Working Group in the *Roadmap to Achieve Energy Delivery System Cybersecurity*. However, in this document, we build a pathway to improve PV cyber security by means of four activity categories: stakeholder engagement, research and development, standards and guideline development, and best practices for DER vendors, aggregators, and grid operators. For each activity, efforts are categorized into three strategic areas: (a) identifying and protecting systems, (b) detecting intrusions, and (c) responding and recovering from the cyber attack. Milestones for 0-2 years and 3-5 years are also provided for each of these areas along with end goals. It is essential all stakeholders participate in this process to ensure cyber security for PV control networks because relatively minor mistakes can lead to drastic consequences to the power system. Deployment of secure PV communication systems with modern R&D capabilities requires DER vendors, aggregators, and grid operators invest in these areas and work together with regulatory and government agencies. This approach gives the US power system the greatest chance of resisting cyber attacks. Measuring progress toward this goal can be difficult as there are often few quantifiable metrics for security and resilience, but the result of inaction would be an ad hoc patchwork of non-standardized DER communications systems. This roadmap provides a common set of recommendations for stakeholders to prioritize technical and organizational actions to meet the milestones and reach the goals.

Table 1: Photovoltaic Cyber Security Roadmap.

Vision	**By 2023, grid operators, system owners, and aggregators communicate with interoperable photovoltaic systems using safe, secure, resilient networks with high availability, data integrity, and confidentiality.**		
Barriers	• **Cyber threats are unpredictable and evolve faster than the industry's ability to develop and deploy countermeasures** • **Security upgrades to legacy systems are constrained by inherent limitations of the equipment and architectures** • **Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations** • **Threat, vulnerability, incident, and mitigation information sharing is insufficient among government and industry** • **Weak business case for cybersecurity investment by industry** • **Regulatory uncertainty in photovoltaic cyber security**		
Strategies	**Identify and Protect**: Improve security posture and harden PV communication infrastructure to protect PV assets	**Detect**: Implement tools with protective measures which automatically recognize and warn operators of security breaches	**Respond and Recover**: Create tools and contingency plans to maintain critical operations and recuperate from cyber security attacks
Stakeholder Engagement	- Establish awareness trainings and information sharing programs for protecting critical infrastructure - Create working groups to establish industry best practices (e.g., patch management)	- Establish public-private information sharing program and industry education programs for detecting malicious network activities - Conduct cyber security exercises	- Establish incident response teams and associated incident command structure between industry and government agencies - Create contingency plans for the loss of DER due to cyber attack
Research and Development	- Create threat models based on risk quantification, red team assessments on virtualized testbeds - Design new segmentation schemes, software defined networks, engineering controls, cryptographic and obfuscation approaches for PV control networks - Assess and protect PV systems with novel physical security, supply chain, and authentication approaches	- Establish situational awareness for PV OT networks using advanced analytics and visualization - Design intrusion detection systems using out-of-band data, deep packet inspection, trust monitors, trust-weighting schemes, etc. - Create machine learning-based cyber detection tools which identify atypical network traffic or operations	- Design resilience into PV equipment so devices fail gracefully and power system operations are not impacted - Create intrusion detection systems to act after detection - Create dynamic assessment tools to manage failures, initiate cyber security remedial action schemes, and regain control given controller compromise or failure - Create forensics and investigatory tools to attribute attacks to those responsible in a timely manner
Industry Best Practices (Grid Operators and Aggregators)	- Implement risk management plan - Implement cyber security maintenance and hygiene practices - Use role-based access controls - Implement defense-in-depth approaches to cyber security	- Implement situational awareness and intrusion detection systems at the grid operator and aggregator levels - Conduct continuous security monitoring with warning and alarm systems	- Document and eradicate intrusion footholds - Design and implement response, recovery, and contingency plans - Work with government to conduct investigations - Document & share lessons learned
Industry Best Practices (PV Industry)	- Harden PV inverters through aggressive in-house and external testing - Create patching release methodology and assign personnel to rapidly respond to new vulnerabilities	- Establish anti-tamper mechanisms - Participate in information sharing programs to determine if vulnerabilities detected in other products or networks affect PV equipment	- Design PV equipment to fail in predictable, safe manner - Maintain trusted gold master firmware for re-flashing equipment after cyber attack - Respond to newfound vulnerabilities with patches
Standards and Guidelines	- Develop and standardize secure communication architectures and protocols, access rules, and certification procedures	- Create recommendations for situational awareness programs and best practices for intrusion detection system software	- Establish industry-wide guidelines for contingency operations, restoration procedures, and cyber investigations
0-2 Year Milestones	- Widespread industry engagement in working groups, trainings, and workshops	- IDS technologies field tested for aggregator and grid operator PV networks	- Industry recommendations for PV operations and recovery strategies based on simulations
3-5 Year Milestones	- Create standards or guideline recommendations for cyber-secure protocols, architectures, and certification procedures - Threat intelligence and data sharing between stakeholders	- All grid operators and aggregators have situational awareness capabilities and intrusion detection systems - Anonymize and publicize operational datasets for security analytics	- Standardize resilient design for PV/DER and associated control networks - Established cyber response teams - Field tests of automated response and recovery
Goals	- Commercialization and adoption of protection R&D solutions - Publication of cyber security standards for PV control networks	- Commercialization of intrusion detection R&D solutions - Widespread use of situational awareness and IDS technologies	- Commercialization and adoption of recovery R&D solutions - Standardize response and recovery procedures for grid operators

2 CYBER SECURITY EFFORTS

Distributed solar energy systems are a subset of distributed energy resources (DER), power systems, critical infrastructure, industrial control systems (ICS), operational technology (OT), cyber-physical systems (CPS), and internet of things (IoT)—many of which have garnered more attention from the cyber security community than solar devices. Therefore, to avoid duplication of efforts and better coordinate photovoltaic security improvement activities within these broader communities, prior roadmapping exercises, strategies, standards, guidelines, and cyber security R&D references are presented here.

2.1 National Cyber Security Strategy Ties to PV Security

Many publications have described the status of government and industry cooperation to achieve cyber security with the associated roles of DHS, DOE, NIST, NERC, ESCC, and other organizations.[8,9] These detailed relationships have been de-emphasized here and, instead, high-level comments about these organizations and specific activities applicable to PV cyber security are presented.

The Department of Homeland Security (DHS) is ultimately responsible to 'lead, integrate and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector' for the cyber security of the US critical infrastructure (CI). The US strategy to protect critical infrastructure and key resources is provided in the DHS *National Infrastructure Protection Plan (NIPP)*[10] and *Energy Sector-Specific Plan.*[11] DHS runs several programs under the National Cybersecurity and Communications Integration Center (NCCIC) to secure CI from cyber attacks including the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a private-public partnership that assesses, tracks, and reports on vulnerabilities to critical infrastructure.[12,13] ICS-CERT may be a logical place to report, track, and manage PV and other DER vulnerabilities as they are discovered.

The Department of Defense (DoD) established a cyber security strategy in 2013 for defending their information systems built on four strategic focus areas:[14]

1. Establish a Resilient Cyber Defense Posture
2. Transform Cyber Defense Operations

[8] R. J. Campbell, Cybersecurity Issues for the Bulk Power System, Congressional Research Service Report R43989, 10 Jun 2015.

[9] Bipartisan Policy Center, Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat, February 2014.

[10] https://fas.org/irp/agency/dhJundf

[11] DHS and DOE, "Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan," 2010.

[12] DHS National Cybersecurity and Communications Integration Center (NCCIC). "ICS-CERT Annual Assessment Report FY 2016," accessed 13 Sept 2017, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

[13] DHS NCCIC. "ICS-CERT Year in Review 2016," accessed 13 Sept 2017, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf.

[14] Department of Defense, "DoD Strategy for Defending Networks, Systems, and Data," November 1, 2013.

3. Enhance Cyber Situational Awareness
4. Assure Survivability against Highly-Sophisticated Cyber Attacks

As part of the process of addressing these areas to operate a secure Department of Defense Information Network (DoDIN), DoD has identified government policies, guides, and issuances associated with each goal.[15] These topic areas are also of critical importance to energy delivery systems and the application of this collection of reference materials should be considered for emerging DER communication networks. DoD is also active in the cyber security research space. Defense Advanced Research Projects Agency (DARPA) projects like the Rapid Attack Detection, Isolation and Characterization Systems (RADICS)[16] and Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT)[17] programs are investigating attack characterization and warning systems, situation awareness, network isolation, real-time analytics, anomaly detection, and dynamically reconfigurable IP stacks.

The National Institute of Standards and Technology (NIST) has developed several standards and voluntary guidelines for cyber security based on Presidential Executive Order *Improving Critical Infrastructure Cybersecurity*[18] and Policy Directive *Critical Infrastructure Security and Resilience.*[19] These documents are categorized in the following way:

- Federal Information Processing Standards (FIPS) are security standards
- NIST Special Publications (SP) are guidelines, specifications, or recommendations in the following subseries:
    - SP 800 Computer security
    - SP 1800 Cybersecurity practice guides
    - SP 500 Information technology
- NIST Internal or Interagency Reports (NISTIR) are research findings or background information

The NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Framework)[20] provides recommendations to critical infrastructure organizations for each stage of cyber incidents: identify, protect, detect, respond, and recover. The NIST Framework is the basis for many derivative security guidelines and standards, and is widely employed by organizations to assess and prioritize their cyber security efforts. NIST has also published many well-known information security standards and guidelines for information technology (IT) and operational technology (OT) applications including NIST 800-53 *Security and Privacy Controls for Information Systems and Organizations*[21] which includes well over 100 security controls and NIST 800-82 *Guide to*

[15] DoD Deputy CIO for Cybersecurity, "Build and Operate a Trusted DoDIN," accessed 15 Aug 2017, URL: http://iac.dtic.mil/csiac/download/ia_policychart.pdf

[16] W. Weiss, Rapid Attack Detection, Isolation and Characterization Systems (RADICS), accessed 10-20-17, URL: https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems

[17] J. M. Smith, Edge-Directed Cyber Technologies for Reliable Mission Communication (EdgeCT), accessed 10-2-17, URL: https://www.darpa.mil/program/edge-directed-cyber-technologies-for-reliable-mission-communication

[18] Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, 1 Feb 2013.

[19] Presidential Policy Directive (PPD) 21, "Critical Infrastructure Security and Resilience," 12 Feb 2013.

[20] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Security," Feb 2014.

[21] National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5, Rev. 5, Aug 2017.

Industrial Control Systems (ICS) Security[22] which covers defense of Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLCs). The NIST National Cybersecurity Center of Excellence (NCCoE) created guides for utilities including the NIST Cybersecurity Practice Guide 1800-2 *Identity and Access Management for Electric Utilities (IdAM)*, and the new NIST Cybersecurity Practice Guide SP 1800-7 *Situational Awareness for Electric Utilities*; and NIST is active in developing recommendations to secure AMI,[23] IoT devices,[24,25] mobile devices,[26] TLS servers,[27] and many more devices and applications. The large body of work assembled by NIST should be referenced and leveraged as security guidelines that are developed for photovoltaic system communication networks.

2.2 Energy Delivery Systems

In September 2011, the Energy Sector Control Systems Working Group released the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*.[28] This document outlined the vision that "by 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions." The five strategic areas are as follows:

- Building a culture of security
- Assessing and monitoring cybersecurity risks
- Developing and implementing new protective measures to reduce risks
- Managing incidents
- Sustaining security improvements

This roadmap is intended to align closely with the high-level goals presented in that report.

Within the NIPP, the importance of cross-sector coordination is emphasized. DOE is responsible for the energy sector and has established several guidelines for the energy sector to approach cyber security, including the *Energy Sector Cybersecurity Framework Implementation Guidance* report which provides additional information regarding the implementation of the NIST Framework. DOE has also funded the development of the Cybersecurity Capability Maturity Model (C2M2)[29] to evaluate and improve cybersecurity practices within the energy sector based on the NIST Framework.

The Edison Electric Institute (EEI) represents all the investor-owned US utility companies—who in turn provide power to 220 million Americans. EEI describes their approach to cyber security as defense-in-depth, or a multilayered risk management three-pronged approach composed of:

[22] National Institute of Standards and Technology Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, Revision 2, Rev. 2, May 2015.

[23] M. Iorga, S. Shorter, NISTIR 7823, Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework. (Draft), July 2012.

[24] T. Polk, M. Souppaya, Mitigating IoT-Based Automated Distributed Threats, NIST Project Description, Oct 2017.

[25] B. Fisher, S. Umarji, Draft Identity and Access Management for Smart Home Devices, NIST NCCoE Concept Paper, June 2016.

[26] NIST Special Publication 1800-4b, Mobile Device Security: Cloud and Hybrid Builds, Nov 2015.

[27] W. Haag, Jr., et al. TLS Server Certificate Management, NIST Project Description, Oct. 2017.

[28] Energy Sector Control Systems Working Group, "Roadmap to Achieve Energy Delivery Systems Cybersecurity," DOE, Sept 2011.

[29] U.S. Department of Energy, "Cybersecurity Capability Maturity Model," Feb 2014.

- **Standards and regulations**: mandatory, enforceable reliability and cyber security regulations, e.g., the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards that include cyber and physical security requirements.
- **Partnerships**: close coordination and information sharing between government and industry—across sectors—to prepare for and respond to a cyber incident. One example of sharing actionable intelligence is via the Electricity Information Sharing and Analysis Center (E-ISAC) Cybersecurity Risk Information Sharing Program (CRISP) partnership which enables bi-directional classified and unclassified information sharing between the Department of Energy and energy sector partners.
- **Respond and recover from cyber incidents**: maintain agreements and practical ability to share personnel and equipment to restore power after an incident, much like is already done for natural disasters.

Similarly, the Electricity Subsector Coordinating Council (ESCC), made up of CEOs from across the electricity industry who meet regularly with senior government officials, describe their approach to cyber security with four focus areas: tools and technology, information flow, incident response and recovery, and cross-sector coordination.[30]

> "The current cybersecurity landscape is characterized by rapidly evolving threats and vulnerabilities, juxtaposed against the slower-moving deployment of defense measures. Mitigation and response to cyber threats are hampered by inadequate information-sharing processes between government and industry, the lack of security-specific technological and workforce resources, and challenges associated with multi-jurisdictional threats and consequences. System planning must evolve to meet the need for rapid response to system disturbances.
>
> Information and communications technologies are increasingly utilized throughout the electric system and behind the meter. These technologies offer advantages in terms of efficient and resilient grid operations, as well as opportunities for consumers to interact with the electricity system in new ways. They also expand the grid's vulnerability to cyber attacks by offering new vectors for intrusions and attacks—making cybersecurity a system-wide concern."
>
> *Second U.S. Quadrennial Energy Review (QER), Chapter IV: Ensuring Electricity System Reliability, Security, And Resilience.*

The NERC CIP standards (currently in their 5th version) cover physical security, cyber security, and other reliability issues for the bulk power system. These standards apply to bulk equipment (>20 MW) connected at 100 kV or greater, so they do not apply to distributed energy resources. However, the structure and language of these standards could be used as a foundation for an equivalent series of standards for distribution equipment. CIP-002-5.1a identifies and categorizes cyber systems and assets; CIP-003-6 specifies security management controls; personnel training and security awareness is in CIP-004-6; electronic security perimeters for critical assets and border access point protections are in CIP-005-5, physical security is in CIP-006-6, security system management is in CIP-007-6; incident reporting and response planning is in CIP-008-5; recovery plans are in CIP-009-6, configuration change management and vulnerability assessments are in CIP-010-2; and NREC CIP also covers information protection (CIP-011-2), identification and protection for critical transmission stations (CIP-014-2), and supply chain management (forthcoming in CIP-013-1).

[30] S. I. Aaronson, "The Electricity Sector's Efforts to Respond to Cybersecurity Threats," U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Energy, February 1, 2017.

Internationally, the International Society of Automation (ISA) Special Publication (SP) 99/IEC 62443 covers cyber security for Industrial Automation and Control Systems (IACS), e.g., bulk power generation; it outlines the methodology to provide OT security with risk analysis, countermeasures, and monitoring.[31] This standard is now being refined as the IEC 62443 series of standards, *Security for Industrial Automation and Control Systems*. There are also conformance tests to assess commercial IACS products to either IEC 62443-4-2 (Embedded Device Security Assurance), IEC 62443-3-3 (System Security Assurance), or IEC 62443-4-1 (Secure Development Lifecycle Assurance).

2.3 Energy Sector Cyber Security Research

The Department of Energy funds research and development programs that address a range of cybersecurity questions. Since 2004, the DOE has been involved in addressing threats to cybersecurity and has worked to improve cyber resiliency of the nation's computer-based systems that manage operational processes in electric power and other energy industries. DOE's Office of Electricity Delivery and Energy Reliability (OE) is focused on increasing the nation's electric power grid and oil and natural gas infrastructure resiliency to cyber threats. The OE cybersecurity program supports activities in three key areas:

1. Strengthening energy sector cybersecurity preparedness which includes situational awareness and information sharing; bi-directional cyber risk information sharing; and risk analysis tools, practices and guidelines.[32]
2. Coordinating cyber incident response and recovery.[33]
3. Accelerating RD&D of game-changing and resilient energy delivery systems.[34]

2.3.1 DOE CEDS R&D

The FY18 budget request for DOE's funding to address cyber threats is approximately $335M, an increase from $312M in FY17. $42M of this funding supports the Cybersecurity for Energy Delivery Systems (CEDS) program, which is DOE's main power system cyber security research program run by the Office of Electricity Delivery and Energy Reliability (OE). CEDS has invested more than $210M in cybersecurity research since 2010, focusing on early stage R&D to mitigate cyber incidents and develop next-generation energy delivery systems through research, development and demonstration (RD&D) projects. CEDS has funded 50 projects for industry, national labs, universities, and NGOs, with research areas including secure communications, intrusion detection and response, resilient design, control systems, and configuration management among others. Of these projects, the majority are focused on cybersecurity for energy delivery

[31] International Society of Automation, "ISA99: Developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS)," accessed 11-2-2017, URL: http://isa99.isa.org/ISA99%20Wiki/Home.aspx.

[32] DOE OE, Energy Sector Cybersecurity Preparedness, accessed 11-2-2017, URL: https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0

[33] DOE OE, Energy Sector Cybersecurity Preparedness, accessed 11-2-2017, URL: https://www.energy.gov/oe/cyber-incident-response-and-recovery-0

[34] DOE OE, Cybersecurity Research, Development and Demonstration (RD&D) for Energy Delivery Systems, accessed 11-2-2017, URL: https://www.energy.gov/oe/cybersecurity-research-development-and-demonstration-rdd-energy-delivery-systems

systems through secure communications, resilient design, and intrusion detection and response, as seen in Figure 2 below.

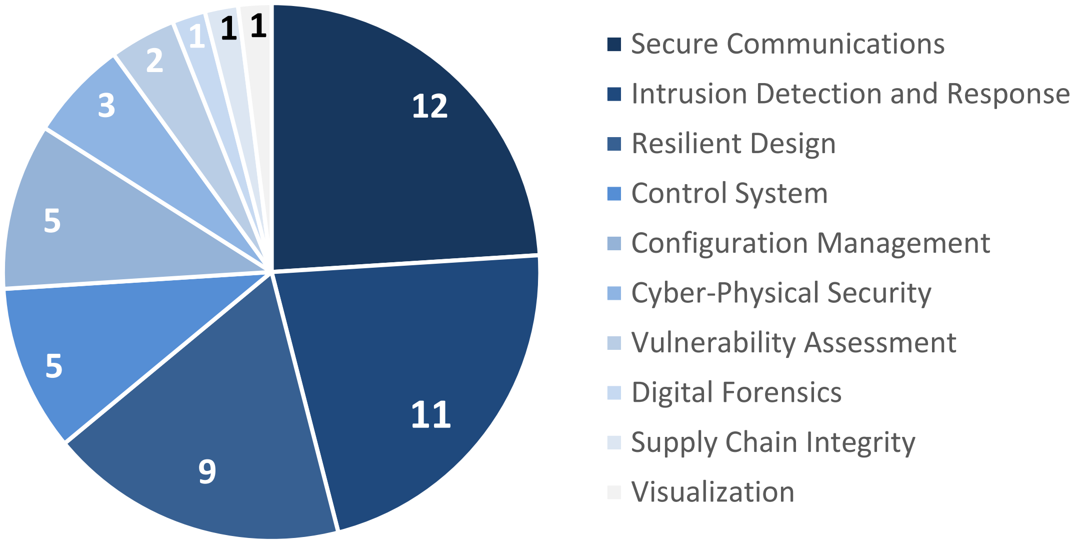


Figure 2: Currently funded DOE CEDS projects by research area.

2.3.2 DHS Cyber R&D

The FY18 budget request for DHS provides approximately $3.28 billion to address cyber threats, although this budget spans broader cybersecurity efforts in addition to those relating to energy. Energy-related activities appear to take place mainly within the Cyber Security Division (CSD), which develops next-generation cybersecurity capabilities.[35] Research spans a range of areas, including linking the oil and gas industry to improve cybersecurity and trustworthy cyber infrastructure for the power grid. DHS released a 5-year broad agency announcement in February 2017, which includes technical topic areas that may be relevant to cybersecurity for energy applications, such as cyber for critical infrastructure, cyber physical systems, and transition to practice.[36]

[35] DHS, CSD Projects, accessed 11-28-2017, URL: https://www.dhs.gov/science-and-technology/csd-projects

[36] DHS, Cyber Security Division 5-Year Broad Agency Announcement (BAA) HSHQDC-17-R-B0002, 3 Feb 2017.

2.3.3 National Laboratory Cyber Research

The U.S. national labs provide R&D solutions to national security challenges. The national labs operate cyber security research programs which encompass the full range of national critical infrastructure assets. More specifically, the labs are at the frontline of national cyber security providing:

- Crisis management solutions
- R&D to develop new cyber security tools, methodologies, and technologies
- Coordination with other government agencies and the private sector to harden the nation's cyber defenses and assist during emergency events
- Cyber-specific expertise for critical infrastructure in both the civilian and military sectors
- Targeted vulnerability and threat assessments
- Providing national awareness of cyberspace risks and guidance for the development and effective deployment of cyber-protective measures
- Laboratory and field testing and demonstrations of novel cyber security solutions

Most of the of the DOE cyber security research is led by national laboratories, including the projects under the CEDS program.

> "[A]s new distributed energy resources (DER) and behind-the-meter assets have a growing impact on grid operations, new vulnerabilities are created because these technologies are not subject to the same reliability mandates and security requirements that electric companies must meet. Electric companies do not have organization control over most DER systems, and the customers controlling DER systems do not have a thorough understanding of cyber vulnerabilities or the knowledge and capability to combat cyber threats.
>
> DER may provide an increasing number of potential entry point for access to electric companies' control systems and can affect the operation of the transmission system. DER systems are more reliant on communication and information sharing between grid components, some of which may be open to physical and internet access, making them more vulnerable.
>
> While the promise of DER can increase grid resilience, the integration of these resources at all points in the electric system must be coordinated thoughtfully. The promise of DER and its contributions to resilience require coordinated planning and investments in controls to ensure energy grid operators have visibility into these new resources."
>
> *Scott I. Aaronson, Executive Director, Security and Business Continuity, Edison Electric Institute and Secretariat Member of Electricity Subsector Coordinating Council, Statement at the U.S. House of Representatives hearing on "The Electricity Sector's Efforts to Respond to Cybersecurity Threats," Feb 1, 2017.*

2.3.4 DER Cyber Security Efforts

There has been limited DER cyber security work to date. The National Electric Sector Cybersecurity Organization Resource (NESCOR) established recommendations for DER communications[37] based on the Logical Reference Model from the National Institute of Standards and Technology Interagency Report (NISTIR) 7628[38]. A version of this logical topology is shown in Figure 3 in which DER and EVs are connected to utilities, ISO/RTOs, and markets though different communication pathways. The report details the actors in this model, a Hierarchical DER System Architecture (shown in Figure 4), and the cyber security requirements associated with each level, actor, and logical interface based on NISTIR 7628 Logical Interface Categories (LICs). It

[37] F. Cleveland, A. Lee, "Cyber Security for DER Systems," NESCOR report, Version 1.0, Jul 2013.

[38] Smart Grid Interoperability Panel (SGIP), "NISTIR 7628, "Guidelines for Smart Grid Cyber Security: Vol. 1," Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements," Aug 2010.

should be noted the hierarchy presented in Figure 4 and associated communication protocols were updated in the Smart Inverter Working Group (SIWG) Phase 2 recommendations to the CPUC.[39]

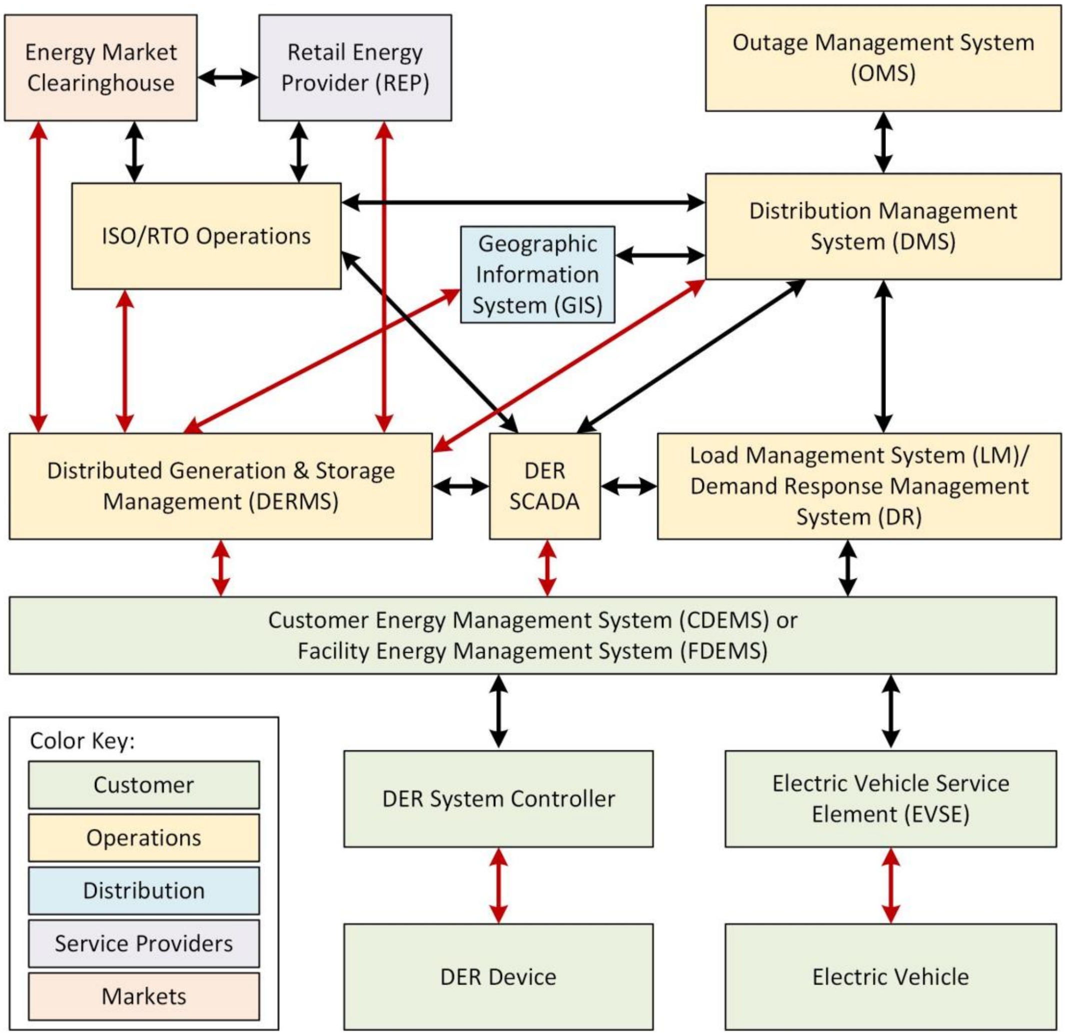

Energy Market Clearinghouse
Retail Energy Provider (REP)
Outage Management System (OMS)
ISO/RTO Operations
Distribution Management System (DMS)
Geographic Information System (GIS)
Distributed Generation & Storage Management (DERMS)
DER SCADA
Load Management System (LM)/ Demand Response Management System (DR)
Customer Energy Management System (CDEMS) or Facility Energy Management System (FDEMS)
Color Key:
Customer
Operations
Distribution
Service Providers
Markets
DER System Controller
Electric Vehicle Service Element (EVSE)
DER Device
Electric Vehicle

Figure 3: DER Logical Reference Model from NESCOR. The red connections indicate departures from NISTIR 7628.

[39] Smart Inverter Working Group, "California Energy Commission & California Public Utilities Commission Recommendations for Utility Communications with Distributed Energy Resources (DER) Systems with Smart Inverters, Smart Inverter Working Group Phase 2 Recommendations," Draft v9, 28 Feb 2015.

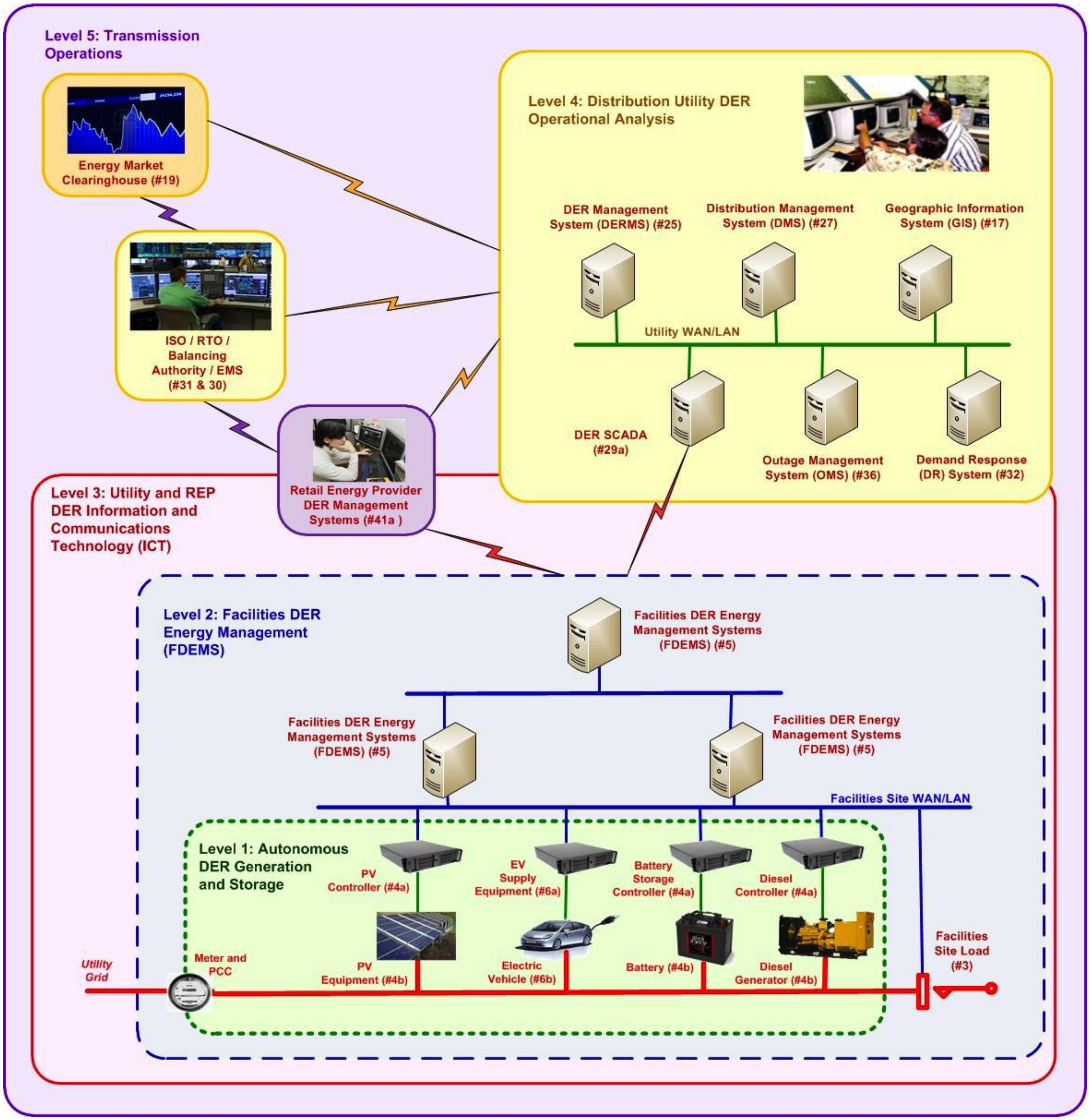

Level 5: Transmission Operations
Energy Market Clearinghouse (#19)
ISO / RTO / Balancing Authority / EMS (#31 & 30)
Level 4: Distribution Utility DER Operational Analysis
DER Management System (DERMS) (#25)
Distribution Management System (DMS) (#27)
Geographic Information System (GIS) (#17)
Utility WAN/LAN
DER SCADA (#29a)
Outage Management System (OMS) (#36)
Demand Response (DR) System (#32)
Retail Energy Provider DER Management Systems (#41a)
Level 3: Utility and REP DER Information and Communications Technology (ICT)
Level 2: Facilities DER Energy Management (FDEMS)
Facilities DER Energy Management Systems (FDEMS) (#5)
Facilities DER Energy Management Systems (FDEMS) (#5)
Facilities DER Energy Management Systems (FDEMS) (#5)
Facilities Site WAN/LAN
Level 1: Autonomous DER Generation and Storage
PV Controller (#4a)
EV Supply Equipment (#6a)
Battery Storage Controller (#4a)
Diesel Controller (#4a)
Utility Grid
Meter and PCC
PV Equipment (#4b)
Electric Vehicle (#6b)
Battery (#4b)
Diesel Generator (#4b)
Facilities Site Load (#3)

Figure 4: Hierarchical DER System Architecture.[40]

Another effort, funded by the California Solar Initiative, focused in on the cyber security requirements for IEEE 2030.5-to-Modbus and OpenADR-to-Modbus protocol translators for advanced inverters.[41,42] Cyber security recommendations for CEA-2045 (now CTA-2045) plug-in translator modules were established to enable secure communications between inverters and

[40] F. Cleveland, A. Lee, "Cyber Security for DER Systems," NESCOR report, Version 1.0, July 2013.

[41] B. Seal, et al., "Final Report for CSI RD&D Solicitation #4 Standard Communication Interface and Certification Test Program for Smart Inverters," June 2016.

[42] J. Henry, et al., Cyber Security Requirements and Recommendations for CSI RD&D Solicitation #4 Distributed Energy Resource Communications, Oct 2015.

aggregators, vendors, and grid operators. The document covers threats, vulnerabilities, cyber attacks, general recommendations for each communication module, and cyber security criticality scoring for each grid function—where each grid function impact level was scored for confidentiality, integrity, availability, authentication, authorization, and non-repudiation with respect to impact on operation, organizational assets, or individuals.

The national laboratories have been investigating DER cyber security for many years. Sandia National Laboratories has developed red team assessment methodologies[43] and the capability to co-simulate network systems with power system simulations (both transmission and distribution circuits).[44,45] These simulations will be incorporated with PV inverter virtual machines (VMs) and other emulated smart grid networking components and entities in a comprehensive environment to conduct penetration testing and red team assessments of different cyber security reference architectures.[46] NREL has developed a SCADA testbed at the Energy Systems Integration Facility (ESIF) to conduct penetration testing of distribution utility systems.[47] Under the CEDS project *Cybersecurity for Renewables, Distributed Energy Resources, and Smart Inverters*, Argonne National Laboratory is creating resilient DER architectures, threat models, and prevention, detection, and response measures for IT-OT cyber-physical networks.[48,49] The LLNL-led GMLC *Threat Detection and Response with Data Analytics* project is investigating big data analytics to identify threat signatures or cyber attacks in DER, AMI, PMU, or SCADA communication traffic or metadata to classify threats as cyber-based or physical-based so appropriate responses can be taken.[50]

Sandia and MIT Lincoln Laboratory recently completed a cyber security gap analysis for critical energy systems.[51] In the paper, the authors use the Purdue Enterprise Reference Architecture (PERA) and DOD Unified Facilities Criteria (UFC) 4-010-06[52] 5-layer Control System

[43] Sandia National Laboratories, The Information Design Assurance Red Team (IDART™), accessed 10/24/17, URL: http://www.idart.sandia.gov/

[44] J. Johnson, SCEPTRE: Power System and Networking Co-simulation Environment, SunShot National Laboratory Multiyear Partnership Workshop on Numerical Analysis Algorithms for Distribution Networks, July 2017.

[45] Sandia National Laboratories, Grid Cyber Vulnerability & Assessments, accessed 10/24/17, URL: http://energy.sandia.gov/energy/ssrei/gridmod/cyber-security-for-electric-infrastructure/grid-cyber-vulnerability-assessments/

[46] J. Johnson, "Secure, Scalable Control and Communications for Distributed PV," SunShot National Laboratory Multiyear Partnership Workshop on Numerical Analysis Algorithms for Distribution Networks, Argonne National Laboratory, Chicago, IL, 21 July, 2017.

[47] NREL, Energy Systems Integration: Cybersecurity and Resilience, NREL brochure, accessed 10/24/17, URL: https://www.nrel.gov/docs/fy16osti/65838.pdf.

[48] J. Wang, "Cybersecurity for Renewables, Distributed Energy Resources, and Smart Inverters," Cybersecurity for Energy Delivery Systems Peer Review, 7-9 Dec 2016.

[49] J. Qi, A. Hahn, X. Lu, J. Wang, C.-C. Liu, "Cybersecurity for Distributed Energy Resources and Smart Inverters," IET Cyber-Physical Systems: Theory &amp; Applications, vol. 1, no 1, p. 28-39, 2016.

[50] J. V. Randwyk, "GMLC 1.4.23 – Threat Detection and Response with Data Analytics," Grid Modernization Initiative Peer Review, Arlington, VA, 18-20 April 2017.

[51] J.E. Stamp, J. E. Quiroz, A. Ellis, B. Bhagyavati, J. A. Cooley, K. Dahl, E.R. Limpaecher, Cyber Security Gap Analysis for Critical Energy Systems (CSGACES), Sandia National Laboratories Technical Report, SAND2017-8823, Jan 2017.

[52] DOD Unified Facilities Criteria (UFC) 4-010-06, Cybersecurity of Facility-Related Control Systems, Change 1, 18 Jan 2017.

Architecture to describe the interaction between the IT and OT components of energy systems. Often, Tiers 3-5 constitute the IT system and Tiers 0-2 constitute the OT system. Traditionally, the OT system does not include authentication, authorization, or certification and devices at the OT level often have weak or no passwords; this equipment was air gapped from the public internet with heightened physical security practices, so it was assumed to be secure. Stuxnet is an example that demonstrates the implications of crossing the air gap. Furthermore, new practices of bridging IT and OT networks or connecting OT devices to the internet has exposed new attack vectors to the power system. This is particularly the case of PV and DER equipment.

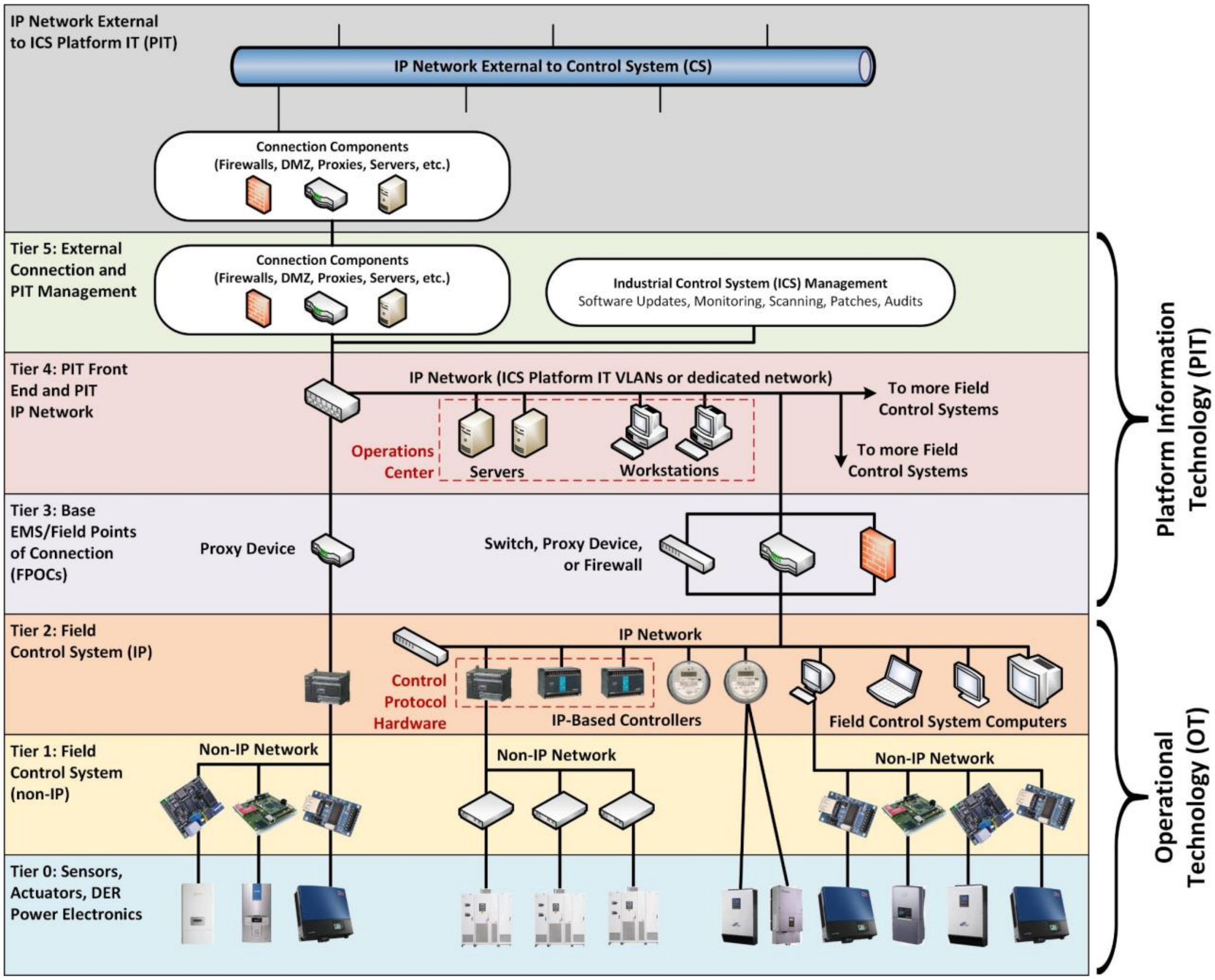

IP Network External to ICS Platform IT (PIT)
IP Network External to Control System (CS)
Connection Components (Firewalls, DMZ, Proxies, Servers, etc.)
Tier 5: External Connection and PIT Management
Connection Components (Firewalls, DMZ, Proxies, Servers, etc.)
Industrial Control System (ICS) Management
Software Updates, Monitoring, Scanning, Patches, Audits
Tier 4: PIT Front End and PIT IP Network
IP Network (ICS Platform IT VLANs or dedicated network)
To more Field Control Systems
Operations Center
Servers
Workstations
To more Field Control Systems
Tier 3: Base EMS/Field Points of Connection (FPOCs)
Proxy Device
Switch, Proxy Device, or Firewall
Tier 2: Field Control System (IP)
IP Network
Control Protocol Hardware
IP-Based Controllers
Field Control System Computers
Tier 1: Field Control System (non-IP)
Non-IP Network
Non-IP Network
Non-IP Network
Tier 0: Sensors, Actuators, DER Power Electronics
Platform Information Technology (PIT)
Operational Technology (OT)

Figure 5: Five-Level ICS Control Architecture.

Also in this work, a list of research areas for ICS systems was developed, as shown in Figure 6,[53] wherein R&D topics for the three stages of the lifecycle of the system were classified into the DoD-favored categories of protect, detect, react, and restore.[54] In general, the ICS R&D

[53] J.E. Stamp, J. E. Quiroz, A. Ellis, B. Bhagyavati, J. A. Cooley, K. Dahl, E.R. Limpaecher, Cyber Security Gap Analysis for Critical Energy Systems (CSGACES), Sandia National Laboratories Technical Report, SAND2017-8823, Jan 2017.

[54] Director, Operational Test and Evaluation (DOT&E), "Cybersecurity Test and Evaluation Guidebook," Department of Defense (DoD), policy reference, Jul 2015.

recommendations include both cyber security as well as resiliency because perfect security is unattainable and therefore monitoring, response, recovery, and restoration must be included in the suite of cyber security capabilities. By blending system protection with advanced detection and remediation, the ICS system security posture can be hardened. Since PV communication systems represent one form of an ICS control system, many of these R&D topic areas are applicable to PV systems, as discussed in further detail in Section 4.

Category	Protect	Detect	React	Restore
Secure Design • Intrinsic capabilities • Resilience and security	**Moving Target Defense (6)** • Variability in configuration • Rotating security parameters **Protected Computing (7)** • Leverage trusted execution/ Trusted Platform Module (TPM) • Minimum privilege/sandboxing		**Resilient Systems (18)** • Algorithms minimize impacts • Graceful degradation	
Reinforced Implementation • Enhance security during system & component development • Resiliency support	**Obfuscation (8)** • Misleading additional ICS traffic • High-detail honeynets • Conformal coatings **Defense-in-depth (16)** • Network enclaves/zones • Anti-tamper protection • Apply cryptographic protections **Boundaries/Authentication (17)** • Connect different trust zones • Multi-factor authentication support	**Security Analytics (4)** • Alarms for strong/weak indicators • Requires ICS network sensors • Assimilate all data (platforms, networks, threat indicators, etc.) • Apply varying trust for data • Monitor configuration by measuring response to minor perturbations **Trusted Monitors (1)** • Deep inspection for components • Support physical data resampling to detect deception	**Minimize System Impact (14)** • Separate safety engineering from networked control • Minimum-set digital supervision or voting to block dangerous actions • Analog limiter backup protection	**Trusted Gold Masters (5)** • Protected, secure change control • Regular evaluation for Trojan code
Deployment & Operation • Instantiated systems • Maintenance/ testing	**System Adaptation (11)** • Risk-informed reactions • Changes in operational posture, patches, and upgrades	**System Assessment/Audit (12)** • Verify logic systematically (components or entire system) • Automated audit • Quantitative metrics	**Temporary Capability (13)** • Maintain acceptable performance, enable forensics/evidence collection • Virtualized failover systems • Portable temporary equipment	**Secure Recovery (9)** • Golden master change control • Rapid acceptance/ reauthorization for replacement equipment

Cross-cutting Capabilities • Covers testing and assessment • Strong focus on virtualization	**Field Device Security (2)** • Virtualization for firmware analysis and simulation support • Independent verification & validation of security	**Virtualization (3)** • Evaluate changes & TTPs • Persistent training environment • Near-real-time model generation & updates	**Threat Analysis (10)** • Automated threat discovery and fusion with indicators • Actionable indicators without jeopardizing sources or methods	**Policy/Personnel (15)** • Assess conflicting and unfavorable requirements • Develop security TTPs • Data security definitions • Training

Figure 6: Categorized ICS cyber security R&D topics with suggested priority in parentheses.

3 STAKEHOLDER ENGAGEMENT

Stakeholder engagement is critical to developing cyber secure PV communication systems. Engagement activities bring together individuals across industry, academia, and government to exchange ideas and educate one another. This will predominantly be directed by government agencies, such as the Department of Energy, but other organizations (e.g., IEEE, SunSpec, etc.) may also conduct these activities. Using the DHS NIPP as a guide, stakeholder engagement should help the private sector secure DER cyberspace by:

- Managing infrastructure by maintaining awareness of critical assets, vulnerabilities, and risk.
- Participating in information sharing programs.
- Assessing the security of networks by conducting regular audits, implementing best practices, and creating continuity plans.
- Improving resiliency and minimizing risks by examining alternative cyber security solutions.
- Promoting secure out-of-the-box implementations of software and hardware systems
- Encouraging adoption of cyber-secure communication protocols and guidelines.
- Demonstration of the ease and practicality of operating cyber security features.
- Identify existing or newly created research gaps.

Stakeholder engagement should create effective forums for academia, government, national labs, industry, grid operators, and others to congregate and discuss short- and long-term direction. These forums will enable the processes for (a) reporting, analyzing, and responding to cyber attacks, (b) prioritizing R&D investment, and (c) accelerating commercialization by establishing pilot projects to demonstrate innovative technologies. Additional details of these components are provided in the following sections.

3.1 Information Sharing

As the President and CEO of the North American Reliability Corporation (NERC) said in a February 2017 House of Representatives Subcommittee on Energy hearing, the United States "cannot win a cyber war with regulation and standards alone. Industry must be agile and continuously adapt to threats and to do that we need robust sharing of information regarding threats and vulnerabilities."[55]

Often sharing actionable threat information is difficult because it tends to be sensitive or classified because of the source, collection methods, or associated proprietary information. However, mechanisms are being developed for sharing this type of information between government agencies and stakeholders. Within the energy sector, the Cybersecurity Risk Information Sharing Program (CRISP) is a DOE-OE-funded public-private partnership designed to facilitate the exchange of classified and unclassified threat information. CRISP is also developing near-real-time situational awareness tools for critical energy infrastructure to identify and protect these

[55] Subcommittee on Energy of the Committee on Energy and Commerce House of Representatives, "The Electricity Sector's Effort to Respond to Cybersecurity Threats," US. Government Publishing Office, Washington, 1 Feb 2017.

resources. Utility data is provided via Information Sharing Devices to PNNL and NERC Electricity Sector Information Sharing and Analysis Center (ES-ISAC) to conduct semi-automated threat analytics.[56] While this program has been oriented to utility systems to date,[57] an expansion of this technology could be offered to PV aggregators and others involved in DER communications—whether this is a new DER-Specific cyber security information sharing program or a subset of previously created organization must be determined. Stakeholder engagement programs must also define mechanisms for disseminating credible, actionable PV threat or vulnerability information between industry and government at the classified and unclassified levels.

The NERC *Security Guideline for the Electricity Sector: Threat and Incident Reporting* provides requirements for reporting cyber security incidents.[58] Similar requirements should be established for PV control systems so the latest attack behaviors are known by all stakeholders. This information should be provided through an established cyber security risk sharing program or a newly developed program specific to DER control networks. In the case of DER devices, customer data privacy is a concern with information sharing. Working within standards organizations and working groups, policy makers, federal agencies, and industry must determine the quantity and type of customer data necessary to generate effective threat and vulnerability assessments. Several information sharing recommendations were provided in the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative[59] that may be used a foundation for PV system recommendations.

3.2 Industry Education

Educating the PV industry about the risks, solution space, and codes and standards for cyber security are essential for efficient improvements to the DER security posture. This education can occur in a range of methods, including:

- Technical and non-technical publications from industry experts, government organization, NGOs, etc.
- Webinars such as the Sandia/SunSpec DER Cyber Security Working Group Educational Series[60] or the NREL Smart Grid Educational Series that often cover cyber security topics.[61]
- Workshops such as the NREL Cybersecurity & Resilience Workshops[62]
- Conferences such as DEF CON, Industrial Control Systems Cyber Security Conference, Black Hat conference series, IEEE Cybersecurity Development Conference, etc.

[56] M. Light, J. Mauth, "Cybersecurity Risk Information Sharing Program (CRISP)," PNNL-SA-109415, April 2015.

[57] M.E. Smith, Cybersecurity Risk Information Sharing Program (CRISP): Bi-Directional Trust, RSA Conference, San Francisco, Feb 29-Mar 4, 2016,

[58] NREC Critical Infrastructure Protection Committee, "Security Guideline for the Electricity Sector: Threat and Incident Reporting," Version 2, 1 April 2008.

[59] Bipartisan Policy Center, Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat, February 2014.

[60] SunSpec Alliance, SunSpec DER Cybersecurity Workgroup, accessed 10-30-2017, URL: https://sunspec.org/sunspec-cybersecurity-workgroup/

[61] NREL, Smart Grid Educational Series, accessed 10-30-2017, URL: https://www.nrel.gov/esif/sges-webinars.html

[62] NREL Cybersecurity & Resilience Workshop, accessed 10-31-2017, URL: https://www.nrel.gov/esif/workshop-cybersecurity-2017.html.

- Training courses offered by the SANS Cyber Security Institute, DHS Cyber Storm, and US-CERT.
- General discussions with the PV industry about the impacts of improved cyber security on reliability, cost, efficiency, etc.

3.3 Working Groups

In 2017, Sandia National Laboratories and the SunSpec Alliance launched the DER Cyber Security Workgroup to bring together DER interoperability and cyber security experts to discuss security for DER devices, gateways, and other networking equipment, owned or operated by end users, aggregators, utilities, and grid operators. The objective of establishing the group is to generate a collection of best practices that act as basis for, or input to, national or international DER cyber security standards. Initially the work was subdivided into four subgroups:[63]

- **Communication and Protocol Security** to define requirements and draft language for data-in-transit security rules.
- **Secure Network Architecture** to create DER control network topology requirements and interface rules.
- **Access Controls** to classify data types, associated ownership, and permissions, and define a set of protection mechanisms.
- **DER/Server Data and Communication Security** to define standardized procedure for DER and server vulnerability assessments.

Bringing together experts in this working group and standards development organizations (SDOs) to discuss best practices and requirements for PV equipment is necessary as interoperability requirements are implemented. It is also essential that representatives from cyber security working groups and SDOs coordinate through open, honest dialog about the focus of each effort and how the activities complement each other.

3.4 PV Cyber Security Exercises

It is recommended that utilities, PV aggregators, and PV vendors participate in simulated cyber security exercises. These exercises would be similar to, or integrated with, (a) NERC GridEx exercises, (b) U.S. Cyber Command, DHS and Federal Bureau of Investigation (FBI) Cyber Guard attack simulations,[64] or (c) the DOE/National Association of State Energy Officials (NASEO) cyber-energy preparedness exercises.[65] The exercises can expose gaps in the defense of PV networks prior to compromise by state-sponsored persistent threats or less organized actors. DER systems could play the role of another attack vector for the US power system. The benefit of conducting these exercises is that unknown vulnerabilities in PV equipment or DER communications networks will be exposed prior to exploitation.

[63] J. Johnson, D. Saleem, “Distributed Energy Resource (DER) Cyber Security Standards,” NREL Cyber Security & Resilience Workshop, Denver, CO, 9 Oct 2017.

[64] DOD, Teams Defend Against Simulated Attacks in Cyber Guard Exercise, U.S. Cyber Command News Release, 5 Jul 2017, URL: https://www.defense.gov/News/Article/Article/1237898/teams-defend-against-simulated-attacks-in-cyber-guard-exercise/.

[65] DOE, “Liberty Eclipse Energy – Energy Assurance Exercise & Event, December 8–9, 2016,” Exercise Summary Report, accessed 13 Sept 2017. https://energy.gov/sites/prod/files/2017/05/f34/LE%20FINAL%20Exercise%20 Summary%201May2017_Public%20Doc.pdf

3.5 Incident Response

When there is a cyber security incident, detection and appropriate response to the situation will help lead to quick mediation. In the case of PV control networks, which can be classified as critical infrastructure, there is a need to be especially disciplined and vigilant in applying the correct response. NIST SP 800-61 *Computer Security Incident Handling Guide* discusses some of the standardized approaches to this response covering containment, eradication, and recovery. It is likely that integration and coordination with government agencies may be necessitated. In 2016, President Obama issued PPD-41, *United States Cyber Incident Coordination*, for the coordination of the federal response.[66] The National Cyber Incident Response Plan (NCIRP) describes the US approach to cyber incident and the roles for the private sector, local and state government agencies, and the federal government.[67] While the private sector will naturally be the primary responders, DHS offers assistance through the National Cybersecurity and Communications Integration Center (NCCIC) for affected entities and coordinates with federal agencies to initiate a unified response, facilitate restoration processes, and contact law enforcement to begin legal action.[68] Understanding the roles and responsibilities of each organization during a cyber security incident and the support provided by government organizations is important as PV control systems become a major component of power system infrastructure. Lines are likely to be drawn based on an impact scale; NCCIC will not mobilize for a handful of vulnerable residential devices but will become involved if the risk crosses a yet-to-be defined threshold.

3.6 Power System Contingency Planning

The large-scale deployment of DER, principally PV, storage, and demand response, is transforming today's power grid. Increasingly, communications-enabled functionality is being incorporated into DER to enable price response and configurable grid support functionality, in coordination with markets, utility control systems, DER aggregators. Communications also enable DER owners, utility system operators, and equipment manufacturers to interact with and possibly reconfigure DER devices. As significant centralized generation capacity is displaced, DER will be required to provide critical reliability services such as frequency and voltage regulation. Because many of these interactions will occur through communication channels including the open internet, where additional cyber vulnerabilities come into play, there is a concern about cybersecurity and information protection. A key question is the extent to which vulnerabilities can compromise the ability of DER to provide critical reliability services and system response and recovery in case threat events occur. Grid operators should consider new types of N-1 failure scenarios. Instead of sizing the operating reserves based on system needs when the largest generator trips, failure scenarios should be studied in which common-mode vulnerabilities are exploited resulting in large portions of PV generation tripping off-line.

[66] Presidential Policy Directive (PPD) 41, "United States Cyber Incident Coordination," 26 Jul 2016.

[67] DHS, National Cyber Incident Response Plan, Dec 2016.

[68] DHS, DHS Role in Cyber Incident Response, accessed 11-1-2017, URL: https://www.dhs.gov/sites/default/files/publications/DHS%20Cyber%20Incident%20Response%20Fact%20Sheet%20v15%20-%20508%20Compliant.pdf

4 PHOTOVOLTAIC CYBER SECURITY R&D

Here we summarize R&D research topics that could be part of the broader solution for cyber security for PV. Unlike traditional power plants with ICS, PV systems communicate to aggregators, utilities, and other grid operators through the public TCP/IP networks; PV systems represent a growing percentage of power generation on the grid so disruptions in these devices can lead to critical infrastructure failures. Therefore, the photovoltaics industry is at the forefront of new cyber security challenges. And it is up to this industry, with support from government agencies, to develop solutions to these unique challenges. Novel methods for detecting, mitigating, and recovering from cyber-attacks must be developed to counteract rapidly evolving threats and vulnerabilities. Techniques of identifying and removing compromised/ unauthorized DERs, segmenting DERs into resource pools to minimize damage in the event of successful compromise, and safeguarding the DER from mass compromise must be developed.

In 2016, the National Science and Technology Council (NSTC) released the *Federal Cybersecurity Research and Development Strategic Plan*, which recommended continuously strengthening defensive elements to improve success in thwarting malicious cyber activities.[69] Like the NSTC plan, we compartmentalized the R&D efforts into *Identify and Protect*, *Detect*, and *Respond and Recover* research areas to thwart attacks—as shown in Figure 7.

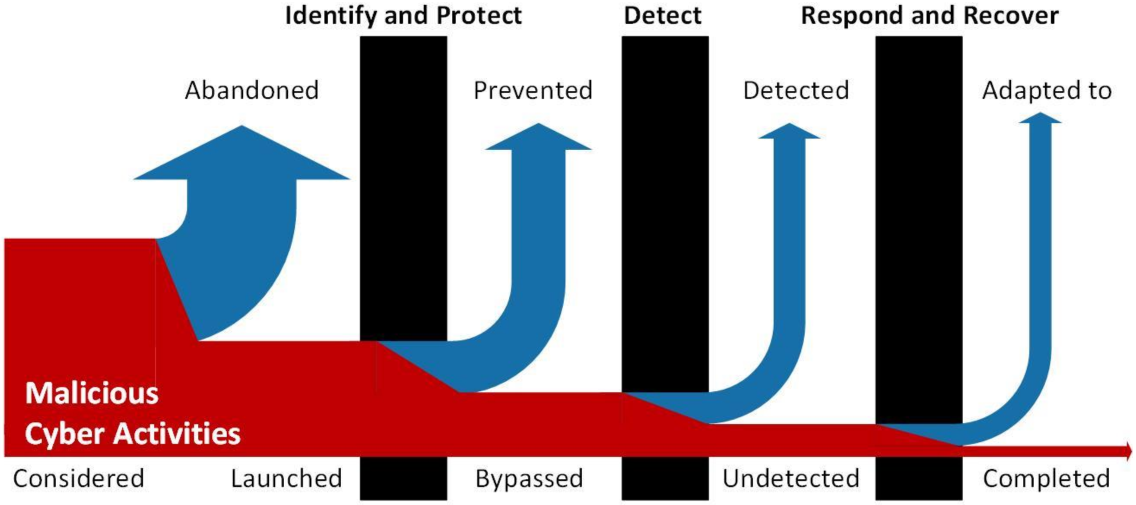


Figure 7: Thwarting malicious cyber activities by strengthening defensive elements through R&D, adapted from the NSTC strategic plan.

4.1 Identify and Protect

It is essential to identify and, where possible, reduce the attack surface for DER equipment to protect critical infrastructure. Many well-understood intrusion prevention system (IPS) techniques, e.g., firewall rules, white-listing, black-listing, etc. can be supported with novel methods for preventing unauthorized network access. According to the FY 2016 ICS-CERT assessment

[69] National Science and Technology Council, Federal Cybersecurity Research and Development Strategic Plan, Feb 2016.

summary, boundary protection was the largest vulnerability for ICS systems. During the network design and configuration stages, there are several R&D topics that hold promise to prevent network penetration, which are discussed below.

4.1.1 Threat Models

Threats exploit vulnerabilities to obtain information, damage, or otherwise manipulate assets. Understanding the threat is necessary to successfully defend against it. Threat modeling identifies high-value assets, attack vectors, and vulnerabilities to determine credible threats. Systematically identifying and enumerating the threats to DER communication systems helps direct the design of appropriate security features for utility, aggregator, and DER networking equipment.

Vulnerabilities must be discovered, classified, and enumerated as part of the threat modeling process. As an example, in 2011, INL reported anonymized energy delivery control systems vulnerabilities discovered over seven years as part of a DOE-OE-funded National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB) program.[70] They quantified the most common vulnerabilities and the risks presented by each. From this information, prioritization decisions were made to minimize risk and defend against system threats. Similar threat modeling and vulnerability assessments must be completed for PV inverters and other DER to create realistic threat models. Sandia National Labs performed a host-based cyber security assessment of two DER in 2017,[71] but more work of this kind is necessary to flesh out a credible threat model. As DER control networks are designed, cyber assessments (e.g., red teaming) and network penetration testing should be conducted to discover effective attack vectors and the difficulty/complexity in executing them.

The EPRI-led National Electric Sector Cybersecurity Organization Resource (NESCOR) is public-private partnership with the Department of Energy (DOE) that has developed an extensive list of over 125 failure scenarios, covering DER, Advanced Metering Infrastructure (AMI), Wide Area Monitoring, Protection, and Control (WAMPAC), Electric Transportation (ET), Demand Response (DR), and Distribution Grid Management (DGM).[72] NESCOR has also mapped these scenarios to NISTIR 7628 vulnerability classes and associated mitigations,[73] completed detailed failure scenarios for select electric sector failure scenarios,[74] and created a utility-focused Microsoft Excel-based toolkit developed to support evaluation of the failure scenarios to indicate specific threats, vulnerabilities, and mitigations.[75] The EU-funded Smart Grid Protection Against Cyber Attacks (SPARKS) project also created a Threat and Risk Assessment Methodology with steps to determine smart grid risk.[76] These reports and the NESCOR toolkit are a good starting

[70] Idaho National Laboratory, "Vulnerability Analysis of Energy Delivery Control Systems," INL/EXT-10-18381, Sept 2011.

[71] C. Carter, I. Onunkwo, P. Cordeiro, J. Johnson, "Cyber Security Assessments of Distributed Energy Resources," IEEE PVSC, Washington, DC, 25-30 Jun 2017.

[72] NESCOR, "Electric Sector Failure Scenarios and Impact Analyses," Version 3.0, Dec 2015.

[73] NESCOR, "Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping," Version 2, December 2015.

[74] NESCOR, "Analysis of Selected Electric Sector High Risk Failure Scenarios," Version 2, December 2015.

[75] NESCOR, Failure Scenario Based Risk Assessment Toolkit for the Electricity Subsector, Version 0.3, June 2014.

[76] P. Smith, et al., Threat and Risk Assessment Methodology, SPARKS Deliverable 2.2, 31 Mar 2015.

place for assessing DER cyber risks, but more thorough PV threat assessments with vulnerability assessments of physical equipment must be conducted to establish the knowledgebase for focused cyber security countermeasures. With additional R&D it may be possible to create threat forecasting capabilities that can be used to prioritize preventative and protective mechanisms and sensor deployments. Furthermore, automated discovery of threats through network monitoring, analytics, and data correlation is an active research field. The IBM i2 Enterprise Insight Analysis[77] and Splunk for Cyber Threat Analysis[78] tools delve into mass datasets to find patterns and discover threats.

4.1.2 Risk Quantification

Certain attack scenarios may be relatively benign, whereas others could be catastrophic. Establishing methods and tools for calculating risk from different vulnerabilities, attack vectors, credible threat data, and associated targets will help prioritize security improvements. NIST SP 800-39 describes the four stages in the process as framing risk, assessing risk, responding to risk, and monitoring risk,[79] but this is tailored to IT networks. McAfee offers an Operational Technology Risk Assessment (OTRA) course tailored to look across ICS plants' people, processes, and technologies for risk, vulnerabilities, and mitigations.[80] Similarly, the UK-based BAE Systems offers consulting services to assess, design, and manage cyber solutions through awareness trainings, penetration testing, risk management, etc.[81] Sandia National Laboratories developed a modern approach for risk quantification called Risk-Informed Management of Enterprise Security (RIMES) which weighs consequence and scenario difficulty to determine the risk of given scenarios.[82,83] Each of these methods should be investigated for application to the solar industry.

4.1.3 Cyber Assessments

Good offense can sometimes lead to better defense. In a Trend Micro survey of 250 SCADA vulnerabilities, they found the majority of the issues to be in memory corruption, poor credential management, code injection bugs, and lack of authentication/authorization and insecure defaults—all of which can be corrected with improved coding practices.[84] By performing cyber security assessments, white hat or blue hat penetration testing, and ethically hacking PV inverters, communication modules, and utility and aggregator servers and networks, the discovery of many

[77] IBM Corporation, IBM i2 Enterprise Insight Analysis," accessed 10-31-2017, URL: https://www.ibm.com/us-en/marketplace/enterprise-insight-analysis.

[78] Splunk Inc., "Splunk for Cyber Threat Analysis - A Big Data Approach to Enterprise Security," accessed 10-31-2017, URL: https://www.splunk.com/web_assets/pdfs/secure/Splunk_for_Cyber_Threat.pdf.

[79] NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View, Mar 2011.

[80] McAfee and Intel Corporation, Operational Technology Risk Assessment, Data Sheet, 2016.

[81] BAE Systems, Cyber Security for Operational Technology, Brochure, 2016.

[82] G. D. Wyss, "Risk-Informed Management of Enterprise Security: Method and Example Applications," Sandia National Laboratories Presentation SAND2014-1011C, 2014.

[83] B. Cipiti, G. Wyss, F. Duran, T. Lewis, L. Mendoza, "Risk-Informed Analysis Applied to Small Modular Reactor Security," American Nuclear Society Summer Meeting, SAND2013-4528C, 2013.

[84] B. Gorenc, F. Sands, "Hacker Machine Interface: The State of SCADA HMI Vulnerabilities," Trend Micro Research Paper, 2017, accessed 13 September 2017, https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf

vulnerabilities can be made prior to implementation. There are huge cost savings for organizations that participate in these activities (e.g., fuzzing, spoofing, elevation or privilege, auditing APIs) in the design process because it locates software bugs, architectural mistakes, or other vulnerabilities early in the product lifecycle. After deployment, conducting these assessments is still valuable because there are new threats emerging all the time.[85] Assessments are likely to follow standardized methodologies provided by NIST SP 800-82, ICS-CERT Cyber Security Evaluation Tool (CSET),[86] or custom assessment techniques like the Information Design Assurance Red Team (IDART^{TM}) methodology[87] which consists of multiple attack vectors including denial-of-service (DoS), packet replay, man in the middle attacks, vulnerabilities scans, and modified firmware uploads, along with inspection of password handling and log management. When third-parties discover vulnerabilities, the information should be provided to the vendor and shared with the appropriate response organization like ICS-CERT, E-ISAC, or other ISACs. It should be noted that other DER and renewable energy industries, such as wind energy, can learn from these types of assessments as well, and vulnerabilities have been discovered in the past.[88] Sharing known vulnerabilities between communities is essential to maintaining up-to-date protection systems.

4.1.4 Network Segmentation

ICS network segmentation is a technique to minimize common-mode vulnerabilities. Network enclaves are isolated with firewall rules, VPNs, proxies, or other networking technologies so that traffic between them is only allowed by exception. Extensive research on segmentation for military microgrids has been completed previously.[89] The downside of this approach is that additional network administration and network latency is required. Additionally, there are challenges to develop a similar technology for PV communications systems because the entire network will not necessarily be owned by a single entity. It may be possible to enclave the devices if communications are passed directly to the DER through networks that are owned by the grid operator, e.g., through an AMI mesh radio network or through dedicated SCADA networks to utility-owned PV systems. However, in the majority of commercial and residential PV systems, communications will be established through wired or wireless networks via the public internet, as shown in Figure 8. In those cases, it is more difficult to enclave the networks because internet service providers (ISPs) control the network routing and firewall rules cannot be implemented easily without assistance from the ISPs. Therefore, the use of VPNs, proxies, or some other technology would be required. This is currently a gap in PV networking, but is an active area of

[85] C. Carter, I. Onunkwo, P. Cordeiro, J. Johnson, “Cyber Security Assessments of Distributed Energy Resources,” IEEE PVSC, Washington, DC, 25-30 Jun 2017.

[86] NCCIC, Cyber Security Evaluation Tool, Factsheet, accessed 10/24/17, URL: https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf

[87] Sandia National Laboratories, The Information Design Assurance Red Team (IDART™), accessed 10/24/17, URL: http://www.idart.sandia.gov/

[88] J. Staggs, Adventures in Attacking Wind Farm Control Networks, Black Hat USA, Las Vegas, NV, 22-27, July 2017.

[89] J. Stamp, C. Veitch, J. Henry, et al., “Microgrid Cyber Security Reference Architecture (V2),” Sandia National Laboratories Technical Report Sand2015-9711, Nov 2015.

research in Sandia National Laboratory's *Secure, Scalable Control and Communications for Distributed PV* project.[90]

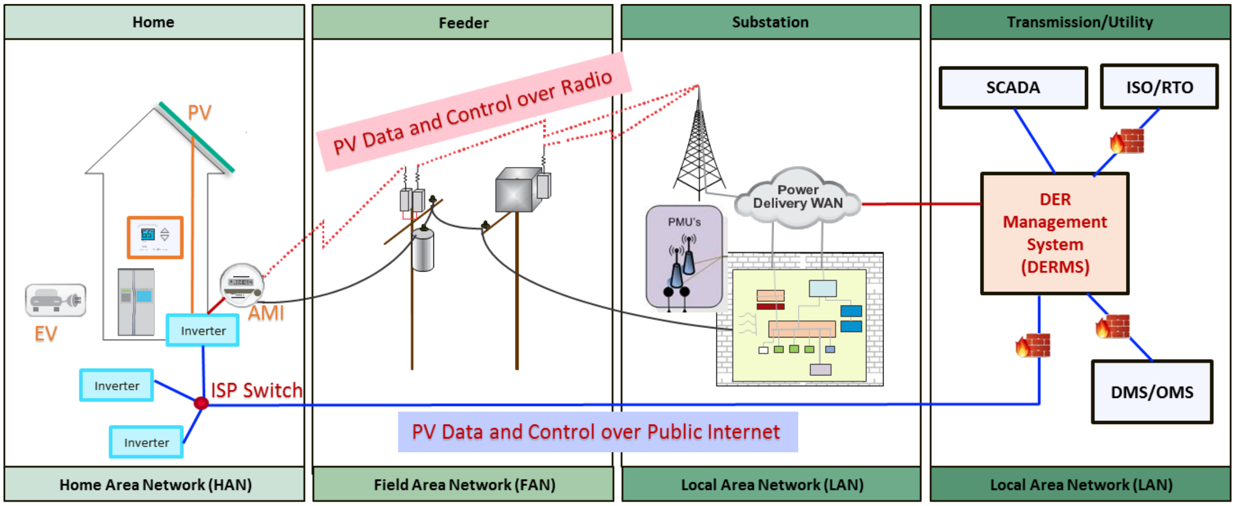


Figure 8: Wired and wireless DER communication media options.

4.1.5 Dynamic Networking and Moving Target Defense

Moving target defense secures the PV control network against cyber attack by rotating network addresses, network parameters, application libraries, or applying other cryptographic tools, without noticeably affecting system performance. This approach uses *software defined networks* to eliminate a class of adversaries that rely on known static addresses for critical infrastructure network devices. The CEDS-funded Artificial Diversity and Defense Security (ADDSec) project is currently investigating this topic; the team aims to detect threats through machine learning algorithms and then respond to those threats. [91] An example threat would be a hitlist attack where a potential response would be to automatically reconfigure network settings and dynamically randomize application communications. The response, in this scenario, could also run continuously and would convert control systems into moving targets that proactively defend themselves against attack.[92] There is additional work in this area for computer networks,[93] critical

[90] J. Johnson, "Secure, Scalable Control and Communications for Distributed PV," SunShot National Laboratory Multiyear Partnership Workshop on Numerical Analysis Algorithms for Distribution Networks, Argonne National Laboratory, Chicago, IL, 21 Jul 2017.
[91] U.S. DOE, Artificial Diversity and Defense Security (ADDSec), CEDS Information Sheet, May 2016.
[92] A.R. Chavez, Artificial Diversity and Defense Security (ADDSec), Cybersecurity for Energy Delivery Systems Peer Review, 7-9 Dec 2016.
[93] H. Okhravi, W.W. Streilein, K.S. Bauer, Moving Target Techniques: Leveraging Uncertainty for Cyber Defense, Lincoln Laboratory Journal, Volume 22, Number 1, 2016.

infrastructure,[94,95,96] and SCADA systems;[97] and there are commercial options starting to appear on the market, e.g., the Morphisec Endpoint Threat Prevention.[98] This technology could be applied to DER IP networks to increase reconnaissance difficulty and protect equipment from remote manipulation.

4.1.6 Trusted and Protected Computing

Trusted computing provides "hardware anchors in a sea of untrusted software." The Trusted Computing Group (TCG) initially formed by AMD, Hewlett-Packard, IBM, Intel, and Microsoft has created a suite of standards for endpoint compliance assessment, network access control, and security automation.[99,100] Many products such as LaGrande, TrustZone, Presidio, Next-Generation Secure Computing Base (NGSCB)/Palladium, and Longhorn include tamperproof Trusted Platform Module (TPM)[101] integrated circuits compliant to these standards. The TCG also released the Trusted Network Connect (TNC) protocol which interrogated endpoint devices to determine their integrity and compliance with security policies.[102] This allows system operators control over what software runs on the target device by authorizing network clients based on hardware configuration, BIOS, kernel version, operating system, software version, etc. The remote attestation feature allows system operators to query a cryptographic hash of a target device (PV/DER) to certify the equipment. When there is a change to the software on the system, a new hash is generated. Note, there were initially privacy concerns with some TCG standards, but improvements have been made to address these concerns, e.g., adding Direct Anonymous Attestation (DAA) cryptographic primitives to authenticated trusted computers while preserving privacy of the platform. There is active research in this area for Advanced RISC Machine (ARM) processors[103] and the technology could be deployed in processors in PV power electronics equipment.

[94] H. Okhravi, A. Comella, E. Robinson et al., "Creating a Cyber Moving Target for Critical Infrastructure Applications Using Platform Diversity," International Journal of Critical Infrastructure Protection, pp. 30–39, 2012.

[95] V. Heydari and S.-M. Yoo, "Securing Critical Infrastructure by Moving Target Defense," 11th International Conference on Cyber Warfare and Security, pp. 382–390, 2016.

[96] A. Chaves, J. Hamlet, E. Lee, M. Martin, W. Stout, Network Randomization and Dynamic Defense for Critical Infrastructure Systems, Sandia National Laboratories Technical Report, SAND2015-3324, Apr 2015.

[97] C. C. Davidson, J. Dawson, P. Carsten et al., "Investigating the Applicability of a Moving Target Defense for SCADA Systems," ICS-CSR '15 Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research, pp. 107–110, 2015.

[98] Morphisec Moving Target Defense, The Ultimate Endpoint Threat Prevention, Morphisec, Ltd. Solution Brief, 2016.

[99] Antonio Maña, Antonio Muñoz, Protected Computing vs. Trusted Computing, 2006 1st International Conference on Communication Systems Software & Middleware, New Delhi, 2006, pp. 1-7.

[100] Trusted Computing Group, Open Standards from TNC, accessed 23 Oct 2017, URL: https://trustedcomputinggroup.org/work-groups/trusted-network-communications/open-standards-tnc/

[101] ISO/IEC Standard 11889, Information technology—Trusted Platform Module, 2009.

[102] Trusted Computing Group, Trusted Network Connect Standards for Network Security, TNC Briefing 10 Dec 2013.

[103] M. Kylänpää, A. Rantala, Remote Attestation for Embedded Systems. In: A Bécue, N. Cuppens-Boulahia, F. Cuppens, S. Katsikas, C. Lambrinoudakis (eds), Security of Industrial Control Systems and Cyber Physical Systems, CyberICS 2015, Lecture Notes in Computer Science, vol. 9588, Springer, 2016.

Application of sandboxes and the principle of least privilege should also be employed in PV and DER equipment. The sandboxing technique isolates the execution of programs or code so that vulnerabilities are not able to spread.[104] Anti-tamper techniques that determine if software has been modified should also be used widely; some forms of this technology are encryption, checksumming, software watermarking, code obfuscation, anti-debugging, and anti-emulation.[105,106,107] Another method called *protected computing* requires two processors: one trusted and one untrusted.[108,109] The public is not allowed to access the protected processor but the application code is divided between the two processors in a mutually dependent way. The advantage of this method is that users have more control of their systems.

4.1.7 Cryptography

Certain PV communication protocols require Public Key Infrastructure (PKI) to encrypt transmissions and maintain data confidentiality.[110] Unfortunately, the policies for exchanging keys for protocol encryption is not well-defined as to whether all DER devices will be required to have this functionality or if "bolt-on" solutions will be allowed or commonplace in the future. The SunSpec Alliance is tasked with standing up the IEEE 2030.5 (SEP2) Certificate Authority for the California Investor-Owned Utilities (IOUs) in the coming years. That process will need to answer these questions. Experience from ISO/RTOs and SCADA cryptography[111] must be leveraged to ensure a smooth rollout of these new requirements.

While there is extensive research on quantum cryptography and quantum key distribution (QKD),[112,113] applied research exploring (a) practical encryption options for DER, (b) appropriate selection of elliptic curves, (c) industry guides for microprocessor selection, and (d) experimental determination of required key exchange times and encryption/decryption times for different grid-support services are more essential needs of the photovoltaic industry in the next five years.

4.1.8 Virtualized Testbed Environments

The construction of virtualized testbeds is useful across all the R&D areas as it can be used to analyze, evaluate, and demonstrate cyber security resilience and develop preventative and

[104] B.W. Lampson, Protection. Proc. 5th Princeton Conf. on Information Sciences and Systems, Princeton, 1971

[105] G. Hachez, A Comparative Study of Software Protection Tools Suited for E-Commerce with Contributions to Software Watermarking and Smart Cards. PhD Thesis. Universite Catholique de Louvain, 2003.

[106] J. P. Stern, G. Hachez, F. Koeune, J.J. Quisquater, Robust Object Watermarking: Application to Code. In Proceedings of Info Hiding '99, Springer-Verlag. LNCS 1768, pp. 368-378, 1999.

[107] P. Wayner, Disappearing Cryptography: Information Hiding: Steganography and Watermarking. 3rd Ed, Morgan Kauffman. Dec. 2008.

[108] I. Schaumüller-Bichl1, E. Piller, A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques. Proceedings of Eurocrypt '84. Springer-Verlag. LNCS 209, pp. 446-454. 1984.

[109] A. Maña, J. López, J. Ortega, E. Pimentel, J.M. Troya, A Framework for Secure Execution of Software. International Journal of Information Security, Vol. 3, Issue 2, Springer-Verlag, 2004.

[110] C. Carter, C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, I. Onunkwo, J. Johnson, "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators," Sandia Technical Report, 2017.

[111] C. L. Beaver, D.R. Gallup, W. D. NeuMann, M.D. Torgerson, Key Management for SCADA, Sandia National Laboratories Technical Report, SAND2001-3252, Mar 2002.

[112] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin. Journal of Cryptology, vol. 5, no. 3, 1992.

[113] V. Padamvathi, B. V. Vardhan, A. V. N. Krishna, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey," IEEE 6th International Conference on Advanced Computing (IACC), pp. 556-562, 2016.

protective measures, analytic tools, and security strategies. By virtualizing the network, devices, and power system, it is possible to quickly assess different cyber security approaches and compliance to standards (e.g., IEEE 2030.5 Common Smart Inverter Profile) or guides (e.g., NIST Cybersecurity Framework).

More specifically, research teams can replicate network topologies and generate alternative cyber security architectures by building co-simulation emulation platforms (e.g., Sandia's SCEPTRE environment) to create realistic PV/DER control network topologies with protocol exchanges between utilities, aggregators, and PV/DER. Emulation environments can be coupled to power simulations (OpenDSS, PowerWorld, pypower, etc.) to realistically populate device (SCADA and PV/DER RTU) data fields and to demonstrate impacts on the power system when adversary actions are taken in the communication domain. Additionally, verification and validation of the virtualized and emulated environments is needed. To satisfy this need, a representative testbed with physical equipment must validate modeled results.

With these research platforms, PV-specific cyber attacks can be implemented whereby teams play the role of threat agents (red team) and DER stakeholders (blue team)—as color coded in Figure 9—to determine the effectiveness of cyber security countermeasures. Hardware-in-the-loop (HIL) technologies can further represent how physical devices will behave in networked or power system attack scenarios. This will be particularly useful as new recommendations are generated based on the working groups, standards development organizations, and research programs. Realistic attacks on the emulated communication networks can determine risk under different conditions, such as when the network is constructed with various:

1. interoperability protocols and communication protocols (IEEE 2030.5, IEC 61850, SunSpec Modbus)
2. network topologies (e.g., utility-to-DER, utility-to-aggregator-to-DER, etc.)
3. encryption schemes (symmetric, asymmetric), key management, and key sizes
4. firewall rules and role-based access control lists,
5. firmware update/patch levels
6. intrusion detection systems (IDSs) and intrusion prevention systems (IPSs)
7. novel research concepts[114]

[114] J. Qi, A. Hahn, X. Lu, J. Wang, C-C. Liu, Cybersecurity for Distributed Energy Resources for Smart Inverters, EIT Cyber-Physical Systems: Theory & Applications, vol. 1., no. 1, pp. 28-39, 2016.

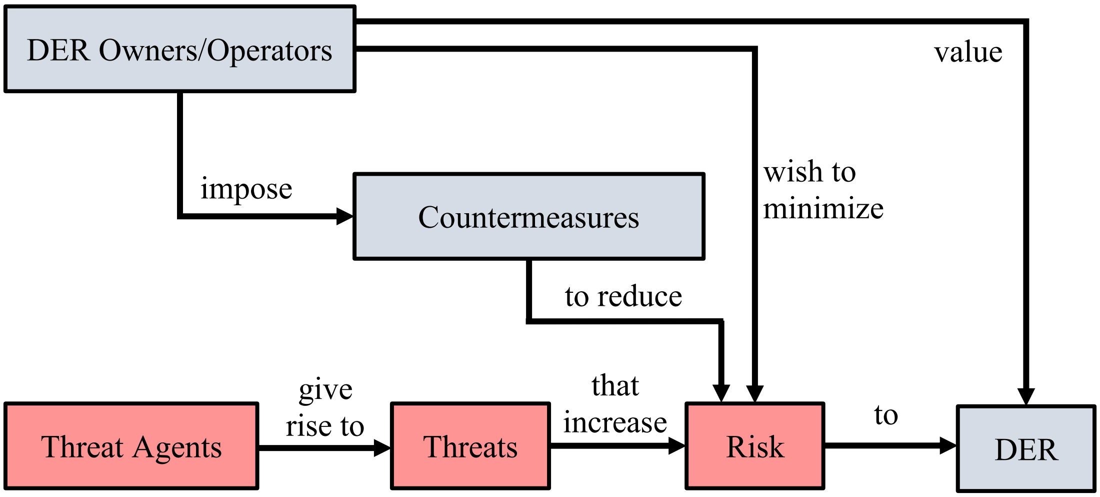


Figure 9: Relationships among threats, risk, countermeasures, and assets. Adapted from the Common Criteria for Information Technology Security[115].

4.1.9 Engineering Controls for DER

Simple engineering control rules could largely prevent PV systems from causing adverse power system effects through adversary actions or accidental misprogramming. For each of the advanced grid-support functions (e.g., volt-var, freq-watt, specified power factor, etc.)[116] the parameters that define these functions should be required to fall within specific ranges that ensure the function has the desired power system behavior. When parameters are set outside of these limits, the communication module or inverter microprocessor can verify the setting and reject the change if the parameter is outside the limits. For instance, the volt-var pointwise curves require (V, Q) points; if points are assigned to be in Q1 and Q3 in the V-Q plane, they would be rejected, as shown in Figure 10. These types of rules are currently implemented in some PV inverters, but not standardized. Defining ranges of values for each of the parameters in the information models (e.g., CSIP, DNP3 Application Note, SunSpec Modbus Models, IEC 61850)[117] or in interconnection standards would standardize the acceptable ranges for DER parameters and vendors to write code that enforced these limits. Whenever possible, whitelisting should also be enforced on communicating endpoints, protocol fields, application parameters, endpoint executables, etc.

[115] Common Criteria for Information Technology Security, Evaluation Part 1: Introduction and General Model, Version 3.1, Revision 5, Apr 2017.
[116] IEC 61850-90-7:2013, Communication Networks and Systems for Power Utility Automation - Part 90-7: Object Models for Power Converters in Distributed Energy Resources (DER) Systems, 2013.
[117] C. Carter, C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, I. Onunkwo, J. Johnson, "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators," Sandia Technical Report, 2017.

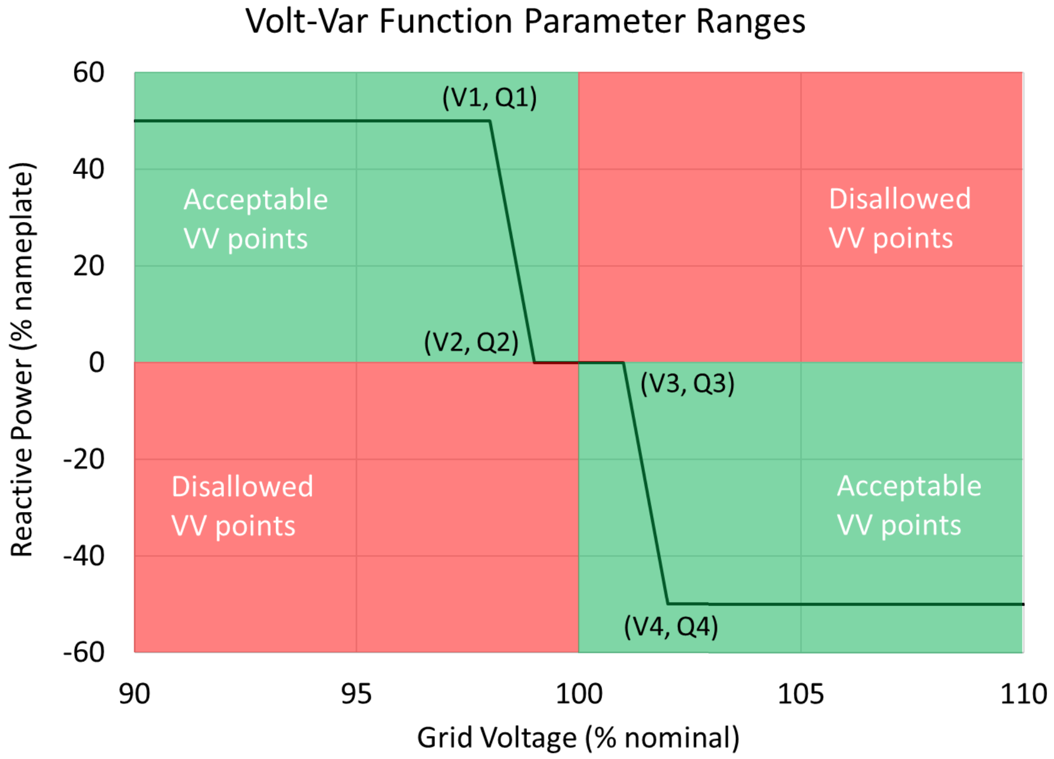


Figure 10: Example engineering control rules for VV curve parameters.

4.1.10 Physical Security

Since DER are often customer-owned devices, there are limits to DER physical security. In cases of utility-owned and commercial PV installations more extensive physical security could be applied, but in general it should be assumed that DER equipment will be accessible by an adversary. There are still physical security defense-in-depth techniques that could slow or deter an adversary. For instance, it is possible to mask the microprocessor chip type and manufacturer with an opaque conformal coating or some other obfuscation method so that the architecture (and associated vulnerabilities) are not known to the adversary. Anti-tamper protections like those used with AMI meters should be used by PV inverter manufactures and additional physical security options should be investigated and recommended to the solar industry.

4.1.11 Security for Cloud-Services

Multiple DER vendors and aggregators communicate with DER equipment via cloud computing systems. Deployment of interoperable PV systems becomes simpler because the equipment only needs to connect to the cloud through any internet connection. The redundancy, flexibility, reliability, and uptime benefits are highly attractive, but the associated security risks must be addressed appropriately.[118] One of the primary concerns is that although cloud service providers state that data on their servers is not publicly accessible, there have been many cloud breaches in the past that exposed this information.[119] If PV control data was housed on these servers, it is

[118] K. Wilhoit, “SCADA in the Cloud: A Security Conundrum?,” Trend Micro Incorporated Research Paper, 2013.
[119] J. Kirk, “Update: Citigroup breach exposes data on 210,000 customers,” InfoWorld, 9 Jun 2011.

possible an adversary could control these devices. Therefore, cloud service security for ICS, SCADA, and PV systems should be investigated in the future.

The public-private Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security, authorization, and monitoring for all US government cloud services.[120] There are currently multiple FedRAMP Ready cloud products available from companies such as Oracle, Monster, Hewlett Packard, Axon, American Institutes for Research, and others. The FedRAMP Security Assessment Framework[121] may be a good starting place for establishing baseline requirements for PV cloud services.

4.1.12 Obfuscation and Deception

Intentionally deceiving an adversary may disrupt reconnaissance and attack attempts. Obfuscation can be conducted through a range of methods, like generating false network traffic to disguise legitimate traffic or creating an overly complex program where a simpler, equivalent version would have sufficed. Similarly, honeypot and honeynets (device decoys or networks of decoys) that can be inserted into the corporate network to confuse attackers and capture their actions prior to impact to physical systems. Obfuscation techniques are not common in ICS control systems, but should be investigated in the next five years. One example of ICS obfuscation was demonstrated in the DOE CEDS-funded CodeSeal program, in which a cryptographically-secure, temper-resistant protocol was used to obfuscate software programs within the ICS.[122] In networks with limited bandwidth, the generation of pseudo-traffic may increase latencies and should be studied.

4.1.13 Authentication

Connections between different enclaves, zones, or other boundaries is necessary for maintaining a functional control network. There should be more research into authenticating access between regions using multifactor authentication mechanisms, one-time-use tokens, or other technologies that prevent password guessing attacks. These exchanges and topologies should allow for moving target defense, IDS, and other countermeasures using unidirectional gateways, data diodes, DMZs with firewalls, etc. Configurational and firmware upgrade authentication is especially important. For example, Enphase Energy remotely updated 800,000 inverters (154 MW of capacity) in two days on the Hawaiian Islands of O'ahu, Hawai'i, Moloka'i and Lana'i in 2015.[123,124] Therefore, adversaries with the correct credentials and access could manipulate hundreds of megawatts of power equipment.

[120] FedRAMP, accessed 11-27-2017, URL: https://www.fedramp.gov/

[121] FedRAMP, FedRAMP Security Assessment Framework, version 2.1, 4 Dec 2015.

[122] A.R. Chavez, Protecting PCS against Lifecycle Attacks Using Trust Anchors, CEDS Peer Review, Alexandria, VA, 20-22 Jul 2010.

[123] P. Fairley, 800,000 MicroInverters Remotely Retrofitted on Oahu—in One Day, IEEE Spectrum, 5 Feb 2015.

[124] A. Konkar, 'Something Astounding Just Happened': Enphase's Grid- Stabilizing Collaboration with Hawaiian Electric, Enphase Energy blog, 11 Mar 2015.

4.2 Detect

Continuous, automated evaluation of the risks must be completed and technical measures developed to reduce the exposure to cyber attack. Operational protective measures are designed to defend the control network so that if an adversary can gain access to PV control networks their presence is detected and malicious actions or reconnaissance hampered.

4.2.1 Situational Awareness

Advanced IT, OT, and ICS cyber security systems must include tools to capture, analyze, and visualize near-real time data from all networks. These tools enable the monitoring, detection, alerting, remediation, and accounting of benign anomalies or hazardous incidents. NIST SP 1800-7, *Situational Awareness for Electric Utilities*,[125] describes the solution as consisting of:

- Logging software or a security incident and event management (SIEM) system
- Bump-in-the-wire devices for OT encryption and logging
- Commercial or open-source software for collecting, analyzing, visualizing and storing network data e.g., historians, OMSs, DMSs, and HMIs
- Products that ensure telemetry and end-device data integrity

Situational Awareness (SA) is a predominant R&D area, with research in power system testbed designs,[126] SA frameworks,[127] wide-area SA with cloud computing and wireless sensors,[128] design implementation, visualization,[129,130] attack detection and analysis, and other CIA threat topics.[131] There is a clear need to inspect and visualize PV data traffic using SA tools with IDS analysis acting as the back-end alarm system.

4.2.2 Intrusion Detection

Detecting adversarial actions on the DER control network is necessary to implement appropriate countermeasures. Photovoltaic systems communicate a wide-range of measurement and setting information which can be used for anomaly identification and classification though inspection of

[125] J. McCarty, et al., NIST Special Publication 1800-7A, Situational Awareness for Electric Utilities, Feb 2017.

[126] U. Adhikari, T. Morris, N. Dahal, S. Pan, R. King, N. Younan, et al. Development of Power System Test Bed for Data Mining of Synchrophasors Data, Cyber-Attack and Relay Testing in RTDS. In: IEEE Power and Energy Society General Meeting, 2012.

[127] A. Mavridou, M. Papa A Situational Awareness Architecture for the Smart Grid. In: C.K. Georgiadis, H. Jahankhani, E. Pimenidis, R. Bashroush, A. Al-Nemrat (eds), Global Security, Safety and Sustainability & e-Democracy, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 99, Springer, Berlin, Heidelberg, 2012.

[128] C. Alcaraz, J. Lopez. Wide-area situational awareness for critical infrastructure protection. Computer, vol.46, no. 4, pp. 30-37, 2013.

[129] R. Tamassia B. Palazzi, C. Papamanthou, Graph Drawing for Security Visualization, in: I.G. Tollis, M. Patrignani (eds) Graph Drawing, 2008, Lecture Notes in Computer Science, vol 5417, Springer, Berlin, Heidelberg, 2009.

[130] W.J. Matuszak, L. DiPippo, Y.L. Sun, CyberSAVe: Situational Awareness Visualization for Cyber Security of Smart Grid Systems, VizSec '13 Proceedings of the Tenth Workshop on Visualization for Cyber Security, pp. 25-32, Atlanta, Georgia, 14 Oct 2013.

[131] U. Franke, J. Bryneilsson, Cyber Situational Awareness: A Systematic Review of the Literature, Computers & Security, vol. 46, pp. 18-31, 2014.

communications meta-data, or correlation/comparison with out-of-band data sources (SCADA, AMI, μPMU, etc.) or nearby DER equipment.[132] For instance, if a PV inverter is reporting a low voltage but other DER or AMI on the same feeder branch do not report the same behavior, this may indicate a spoofing, bump-in-the-wire, or other attack. This may also indicate faulty equipment, however, so efforts must be made to differentiate cyber attack-related and non-cyber-related/operational events to determine the type of incident and its root cause. Some initial research has been conducted in this area using deep packet inspection in the GMLC "Threat Detection and Response with Data Analytics" project to identify cyber-physical signatures which quickly differentiate between cyber events and non-cyber events[133]. It is also possible to use state estimation tools to validate PV inverter data, as demonstrated under the CEDS Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA)[134] and a Sandia LDRD project.[135]

Machine learning can also be used to learn typical network traffic behavior and alert when unexpected, e.g., malicious, communications are detected. For instance, Sandia developed an adaptive resonance theory (ART) artificial neural network to provide real-time monitoring of a building automation system.[136] Further IDS research should also be conducted in:

1. Protocol-aware sensors which internally conduct packet inspection
2. Probing or perturbation techniques to differentiate artificial and actual data sources
3. Creation of strong and weak indicators (based on data streams from all sensors) to warn or alert to malicious activity
4. Creation of trust-weighting schemes that value information from highly-secure telemetry over easily spoofed or accessed data sources
5. Sensor correlation—possibly with power system state estimation—to identify suspect data streams
6. Creation of "trust monitors" that monitor critical buses or equipment with out-of-band approaches, e.g., monitoring equipment power draw[137] or anomalous traffic. This technology has been developed for PLC equipment under the WeaselBoard program,[138] but would need to be updated for PV devices and control networks. Development of fast and effective sensor technologies is critical for identifying malicious traffic.
7. Visualization techniques and exfiltration detectors, such as those in the Oak Ridge Cyber Analytics[139]

[132] R. Mitchell, I.R. Chen, A Survey of Intrusion Detection Techniques for Cyber-Physical Systems, ACM Computing Surveys, vol. 46, no. 4, article 55, Mar 2014.

[133] J. Van Randwyk, S. Peisert, Threat Detection and Response with Data Analytics, GMLC Factsheet, June 2017.

[134] C. Hawk, S. Walters, Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA), CEDS Factsheet, Sept 2014.

[135] J. Johnson, et al., "Design and Evaluation of a Secure Virtual Power Plant," Sandia Technical Report, SAND2017-10177, Sept 2017.

[136] C.B. Jones, C. Carter, "Trusted Interconnections Between a Centralized Controller and Commercial Building HVAC Systems for Reliable Demand Response," IEEE Access, vol. 5, pp. 11063-11073, 2017.

[137] Power Fingerprinting Inc, "PFP Cybersecurity," http://pfpcyber:com (accessed 28 November 2016).

[138] J. Mulder, M. Schwartz, M. Berg et al., "WeaselBoard: Zero-Day Exploit Detection for Programmable Logic Controllers," SNL, Albuquerque, NM, Sandia Report SAND2013-8274, October 2013.

[139] Oak Ridge National Laboratory (ORNL), "ORCA: Advanced analytics for Cyber Security," accessed 10-30-2017, URL: http://orca.ornl.gov/Oak_Ridge_Cyber_Analytics.html.

Both IDS and machine learning should be coupled with whitelisting whenever possible. Only allowing necessary traffic by specifying protocol parameters, application parameters, allowable executables is an effective means to preventing malware from progressing. The difficulty of specifying all allowable parameters is often a challenge as the complexity of PV control networks can be significant. Research should be performed to make whitelist specifications sharable and available to a wide audience to limit the impacts of a compromised application or endpoint.

4.3 Respond and Recover

The risk to the power system is represented by the probability of an attack and the consequence of such an action. System designers must implement countermeasures to increase system resilience, extend the time and difficulty of perpetrating the attack, and minimize the impact to the system if an attack is successful. In this section, R&D topics that address response and recovery options during and after a cyber incident are described.

4.3.1 Resilient Designs

Cyber resilience is the ability of the system to maintain critical operations in the presence of adversary actions. This is typically performed using adaptive systems with components that fail gracefully so that backup, fail-over, and recovery equipment may be brought online. Cyber defenders may also isolate or quarantine certain networks or transfer operation to different processes. In the case of PV networks, switching operations to redundant backup networks or PV systems is unlikely, but grid operators may use other generators and power system equipment if the PV control network is compromised. In the near term, PV inverters should be configured with operating rules when communications are lost for extended periods of time. In the longer term, autonomic self-repair, adaptive defenses, or pushing known good firmware updates to equipment could be an option. Machine learning techniques may also be used to learn from past compromises and continue critical functions while under attack.

4.3.2 Dynamic Assessment

Like situational awareness tools, dynamic assessment technologies conduct real-time analytics on data streams. In this case the analytics are designed to understand the tactics and approach of the adversary. This information is used to assess system damage, manage future compromises, and plot a recovery course. It is also essential to understand grid operation dependencies on the PV control system so any grid services that had been provided by compromised PV systems can be transitioned to alternative equipment. For instance, if PV inverters are providing voltage regulation on a feeder, it may be necessary to transfer operations to transformer load tap changers (LTCs) or capacitor banks. Similar adjustments from PV power to traditional generation would be necessary if PV was providing a significant amount of power—and especially if the aggregations was providing ancillary or energy services—to avoid destabilization of the bulk power system.

Google has created an open-source incident response framework with distributed forensics, called the Google Rapid Response (GRR) platform.[140] This system is helpful for determining the source of leaked corporate data, conducting periodic health checks of the system state, and isolating malware attacks.[141] Similar technology for OT/ICS/CPS should be created to quickly find and isolate malware attacks on PV networks.

4.3.3 Contingency Operating Modes

Grid operators must establish methods to recover system functionality in a timely manner, while maintaining interdependent operations. Adaptive response must coordinate autonomous, semi-autonomous, and manual defense activities in a coordinated and potentially federated response. Ideally, the response will absorb the cyber attack and recover to a known operable state quickly. Additionally, fault-tolerant algorithms should be applied when possible to increase the difficulty of an adversary to compromise a cluster of systems. Technologies to enable this adaption include software defined networks and moving target defense that reconfigure the network autonomously, and mechanisms such as enclaves to isolate compromised devices. One example is an analytical technology that regains power system control after DER controller compromise using clustering and factorization techniques.[142]

The possibility to revert centrally-controlled or automated operations to manual or distributed operating modes should be investigated. This temporary contingency mode will allow time for forensics, restoration operations, or other recovery systems to take over while still maintaining critical functionality. For PV control systems, this could be the reversion to default, low risk operating modes (default VV and FW curves, etc.) This will allow grid operators to regain control of the network while PV systems are still providing nominal voltage and frequency regulation. Extensive verification and validation of these contingency operating modes must be evaluated with virtualized or physical testbeds to understand their role in the recovery.

4.3.4 Restoration

The concept of resetting the system to a known good state or “trusted gold master” is not a new concept, but it is not a standardized practice. At minimum, organizations should maintain copies of all software to enable quick reinstallation of programs used for system operations. Using virtual machines or containers (e.g., Docker applications)[143] would allow even faster redeployment to a previous, secure state stored before network penetration. Understanding when the system became compromised is essential to select the correct image to restore. Change controls should be mirrored in the gold master copies. However, allowing the gold masters to be updated opens new attack vectors; safeguarding the good state images is paramount to effective recovery. This technology is not used in ICS/OT systems currently, but could provide a means to rapidly recover from certain types of security breaches. Finding the right frequency of checkpointing software without

[140] Google, “GRR Rapid Response: Remote Live Forensics for Incident Response,” GitHub repository, accessed 10-31-2017, URL:https://github.com/google/grr.

[141] M. Cohen, D. Bilby, G. Caronni, Distributed Forensics and Incident Response in the Enterprise, Journal of Digital Investigation, vol. 8, pp. S101-S110, 2011.

[142] S. Hossain-McKenzie, M. Kazerooni, K. Davis, S. Etigowni, and S. Zonouz. “Distributed Controller Role and Interaction Discovery,” International Conference on Intelligent Systems Applications to Power, Sept. 2017.

[143] Docker, “What is a Container,” accessed 11-1-2017, URL: https://www.docker.com/what-container

degrading the OT network performance is a challenge that would need to be addressed to restore software to more current states.

4.3.5 Cyber Security Investigations and Attribution

Following a cyber attack, it is necessary to dissect the sequence of events that led to the breach to patch those holes in the security posture. It is also necessary to identify those responsible to begin criminal proceedings or other law enforcement arrangements. Log file inspection tools for attribution and other forensics technologies like those at the ICS-CERT Advanced Analytics Laboratory (AAL)[144] are necessary to begin the judicial processes. Reverse engineering malware can determine the creator, the target equipment, and accessed data. One longer-term objective of the National Science and Technology Council's approach to cyber security is to develop technologies to accurately and automatically identify malicious actors in real-time with sufficient precision to impose rapid prosecution, sanctions, or other responses.[145]

[144] DHS ICS-CERT, "ICS-CERT Monitor: March/April 2016," accessed 10-30-2017, URL: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Mar-Apr2016_S508C.pdf

[145] National Science and Technology Council, Federal Cybersecurity Research and Development Strategic Plan, Feb 2016.

5 STANDARDS DEVELOPMENT

Standards development organizations (SDOs) rely on subject matter experts from government, non-governmental organizations, and industry to create and update standards. In the majority of cases, photovoltaic system requirements are defined in DER standards such as IEEE 1547, so it is necessary to create or update these requirements to secure PV devices and networks. The process of refining DER interconnection and interoperability standards is a lengthy (multiyear), consensus-based procedure. It is anticipated that development of PV cyber security requirements will take similar durations, though these requirements are likely to be spread between communication protocol standards, interconnection and interoperability standards, and grid operator/aggregator architecture requirements. Oftentimes, standards—while comprehensive—are difficult to digest for those without deep expertise in the subject area. For this reason, industry education through workshops and how-to guides are necessary to implement the requirements as intended. It is also necessary to have both normative (prescriptive) requirements in standards as well as descriptive instructions to provide guidance that more aligns with practice so that industry can follow a real-world path to compliance. This minimizes the risk of misinterpreting potentially ambiguous requirements and accelerates standards adoption.

To minimize duplication of efforts, standards development must not happen in a vacuum and liaising with other working groups is critical. Any PV cyber security standard development process must connect with external SDOs, such as those responsible for:

- IEC 62351 series
- ISO/IEC 15408 Common Criteria
- ISO/IEC TR 19791 Security assessment of operational systems
- ISO/IEC 27001 and 27002 information security management system standards
- International Society for Automation (ISA)/IEC 62443 (formerly Industrial Automation and Control System Security standards)[146]
- UL 2900 Software Cybersecurity for Network-Connectable Products Standards Technical Panel
- NIST working groups including NIST Federal Information Processing Standards (FIPS)
- IEEE 1547 and IEEE 1547.1 DER Interconnection and Interoperability working groups
- ISO/IEC 19790 Security requirements for cryptographic modules
- IEEE 1711 Cryptographic protocol for cyber security of substation serial links
- Internet Engineering Task Force (IETF)
- CIGRE (International Council on Large Electric Systems) SC B5 Protection and Automation working group, e.g., JWG B5/D2.46[147]

[146] J. Gilsinn, ISA-99 – Industrial Automation & Control Systems Security, Grid-Interop, Phoenix, AZ, Dec 5-8, 2011.

[147] D. Holstein, T. W. Cease and M. G. Seewald, "Application and Management of Cybersecurity Measures for Protection and Control," International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Xi'an, China, 17-19 Sept. 2015, pp. 76-83.

- European Commission Smart Grids Task Force Expert Group 2 Regulatory recommendations for privacy, data protection and cyber-security in the smart grid environment
- And others[148,149]

It has been said *standards protect against yesterday's risks, not future threats*. Standardization is a critical mechanism to establish equipment interoperability, consistent interconnection standards, and certification procedures, but it only establishes a baseline security level for the industry—standards do not guarantee cyber security. In fact, with specific cyber security standards, industry often targets the minimum (cost competitive) set of features to achieve compliance, without a focus on achieving comprehensive and effective cyber security. However, with well-designed cyber security standards, the baseline security posture of the PV industry will be elevated. Appropriate cyber security standards prevent minority bad actors from compromising the security of the entire system.

There are three types of PV cyber security standards needed:

1. *Equipment standards* that define the design and operation rules of the PV equipment
2. *Communication standards* that define the protocol stack, information models, and associated security requirements
3. *Certification standards* that confirm compliance to equipment and communication standards

These could either be stand-alone standards, updates to in-use PV standards, or new references to existing standards. Additionally, best practice documentation and guides should be created for each of these areas as well as recommended network architectures, access controls and roles, etc.

5.1 Equipment Standards

In the same way interconnection standards (e.g., IEEE 1547) define the minimum electrical functionality of DER, a new equipment standard (or section in IEEE 1547) is needed to establish the minimum cyber security requirements for PV inverter systems. This standard will define data exchange requirements for PV systems including allowable services, protocols, and minimum confidentiality (encryption), integrity, and availability levels. There are limited DER cyber security requirements in the IEEE Std. 1547 series or IEEE Std. 2030 series.[150] This must change once the interoperability requirements in IEEE 1547 full revision are imposed.

One example of this type of equipment security standard is IEEE 1686 which establishes standard cyber security requirements for access, operation, configuration, firmware revision, and data retrieval for Intelligent Electronic Devices (IEDs).[151] This standard includes safeguards, audit mechanisms, and alarm indication functions and features for critical infrastructure protection

[148] F. Cleveland, "List of Cybersecurity for Smart Grid Standards and Guidelines," May 2013.

[149] F. Cleveland, "Matrix of Standards with Cybersecurity," accessed 5 October 2017, URL: http://xanthus-consulting.com/Publications/documents/Matrix_of_Standards_with_Cybersecurity.pdf

[150] C. Carter, C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, I. Onunkwo, J. Johnson, "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators," Sandia Technical Report, 2017.

[151] IEEE Std 1686, Standard for Intelligent Electronic Devices Cyber Security Capabilities, 2013.

programs. Similarly, IEEE C37.231 is a guideline for producers, distributors, and users of microprocessor-based protection equipment with specific recommendations on firmware updates with respect to the technical and operational ramifications on the power system.[152] In the next 1-2 years a massive, fast-tracked effort to create nation-wide cyber security requirements for PV inverters and other DER equipment is needed.

5.2 Communication Standards

In the latest IEEE 1547 full revision, DER are required to communicate using Modbus, IEEE 2030.5, or IEEE 1815.[153] The cyber security requirements for the data-in-transit are not defined. There is a near-term need to establish a nation-level set of requirements for DER/PV communications. Fortunately, the conversation about PV inverter cyber security requirements has started. In February 2015, the Smart Inverter Working Group (SIWG) recommended (a) communications requirements to all DER equipment and (b) the CA IOUs develop cyber security requirements in each Utility's "Generation Interconnection Handbook" for Electric Rule 21 Phase 2. The cyber security requirements for the handbooks are:

- Cyber security requirements for communications, including authentication, authorization, accountability, and data integrity shall be included at a minimum.
- Other cyber security requirements, such as confidentiality shall be supported but may be enabled only when needed. References to relevant cyber security standards shall be included.
- Cyber security management requirements outside the protocol cyber security, including key management, certificate authorities, and cyber security management procedures shall be included.
- Cyber security-related passwords and cryptographic keys shall be secured from unauthorized access.
- Performance requirements, including periodicity of data exchanges, latency of data requests-responses, sizes of data files, error management, and cyber security impacts on data latency shall be included.
- Privacy policies shall clearly define what types of data shall be not available publicly, including individual data elements, utility aggregations of customer data, and third-party aggregations of data.

At this time, the Generation Interconnection Handbooks have not been developed, but the IOUs have recommended modifications to CA Electric Rule 21 to require communications to all DER equipment and that IEEE 2030.5 be used as the default application-level protocol using the California IEEE 2030.5 Implementation Guide, i.e., Common Smart Inverter Profile (CSIP)

[152] IEEE Std C37.231, IEEE Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control, 2006.

[153] IEEE P1547™ Draft Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, 2017.

requirements.[154,155,156] CSIP defines a strong set of cyber security features including encryption,[157] so in a roundabout way, the utilities are mandating cyber security in the communication networks. However, the requirement to communicate IEEE 2030.5 only applies to the connections to/from the utility. In many cases, the CA IOUs will communicate to aggregators or facility energy management systems that will relay commands to the DER via proprietary or other standardized protocols.

There are multiple DER communication protocols which exchange nearly-identical DER data and control information based on the IEC 61850-90-7 information models.[158] Since IEEE 1547 allows multiple communication protocols, defining a common set of security features for DER communications is particularly important. The approach of pushing the cyber security requirements to individual protocols implementations is not a universal solution; especially since IEEE 1547 will allow DER equipment to communicate Modbus, which includes no cyber security features natively. Generating piecemeal requirements for each utility jurisdiction is a poor solution. Instead, a national standard should be created that defines communication requirements for all DER equipment. This standard must outline clear requirements for confidentiality, authentication, availability, authorization, accountability, and integrity for all interoperable DER equipment. Certain protocols may have these features already; others may not. For those that do not, additional security features will need to be included to provide a mandatory minimum set of cybersecurity features. This standard can then be referenced by IEEE 1547 to ensure mass adoption.

It would also be wise for US SDOs to review the cyber security requirements for IEC 61850 defined in the IEC 62351. As shown in Figure 11, IEC 62351 standards apply at each layer in the GridWise Architecture Council (GWAC) stack. Similar requirements are needed at each layer in PV protocol stacks. IEEE 1815 also has a more secure extension called DNP3 Secure Authentication based on the IEC 62351-5,[159] but it is not required. SDOs should carefully consider the requirements at each layer in the protocol stack for PV/DER communications.

Some within the PV industry believe IEEE 1547.3[160]—especially the *protocols and network security considerations* section—should be updated and expanded to include these requirements. IEEE 1547.3 is currently a guide without any legal teeth, so, if taking this route, this document will need to be converted to a standard and referenced by IEEE 1547.

[154] California Smart Inverter Implementation Working Group, "IEEE 2030.5 Common California IOU Rule 21 Implementation Guide for Smart Inverters," Common Smart Inverter Profile V1.0, Aug. 31, 2016.

[155] R.G. Worden, Modifications to Electric Tariff Rule 21 to Incorporate Communication Requirements for Smart Inverters (Phase 2), Advice Letter 3532-E, SCE Memorandum, 10 April 2017.

[156] SunSpec Alliance, IEEE 2030.5/CA Rule 21 Foundational Workshop, 12 Jun 2017.

[157] C. Carter, C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, I. Onunkwo, J. Johnson, "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators," Sandia Technical Report, 2017.

[158] UL 2900-1, Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, 1st Ed., 5 Jul 2017.

[159] DNP3.org, "Why IEEE 1815 (DNP3) Secure Authentication?," accessed 10-31-2017, URL: https://www.dnp.org/DNP3Downloads/DNP3%20Secure%20Authentication%20Talking%20Points.pdf.

[160] IEEE Std. 1547, Guide for Monitoring Information Exchange and Control of Distributed Resources with Electric Power Systems, 2007.

5.3 Certification Standards

There is a clear gap in the certification procedures around PV cyber security. In the same way UL 1741[161] is used to certify the electrical and safety features of DER equipment, there must be a certification mechanism for the cyber security features of DER. The first step in this process is developing certification test sequences to verify the cyber security features and compliance to the communication and information standards.

The new IEEE 1547.1 testing standard will verify the exchange of information required in IEEE 1547. These test protocols will be a subset of the full interoperability/communication certification procedures for IEEE 2030.5/CSIP, IEEE 1815/AN-2013-001, and SunSpec Modbus; there is no plan to add general cyber security requirements to IEEE 1547.1 for the specified communication protocols. The SunSpec Alliance plans to release the IEEE 2030.5 certification program for Rule 21 in late 2017. Since IEEE 2030.5 includes detailed security functionality, this certification will include some cyber security certification procedures. However, there are no cyber security certification standards for equipment communicating IEEE 1815 or SunSpec Modbus. This is currently a gap in the standards landscape.

In the ICS realm, there are many system-level standards (ISO/IEC 27001,[162] ISO/IEC 27002,[163] IEC 62443-3-1,[164] IEC 62443-3-3[165]) and, at the device-level, most certification bodies use either the ANSI/UL 2900 series of standards[166,167] or IEC 62443-4 series as the certification procedure. (The IEC 62443-4-1[168] and IEC 62443-4-2[169] drafts, which include component requirements for control systems, are expected to be published in 2017.[170]) Underwriters Laboratories Cybersecurity Assurance Program (UL CAP) for ICS relies on UL 2700 or IEC 62443; other organizations, such as ISASecure, have similar certification programs.[171]

[161] Underwriters Laboratories 1741 Ed. 2, "Inverters, Converters, Controllers and Interconnection System Equipment for use with Distributed Energy Resources," 2016.

[162] ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems – Requirements, 2013.

[163] ISO/IEC 27002, Information technology -- Security techniques -- Code of practice for information security controls, 2013.

[164] IEC TR 62443-3-1, Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems, 2009.

[165] IEC 62443-3-3, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, 2013.

[166] IEC 61850-90-7, Communication networks and systems for power utility automation - Part 90-7: Object models for power converters in distributed energy resources (DER) systems, 2013.

[167] UL 2900-2-2, Standard for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems, 2017.

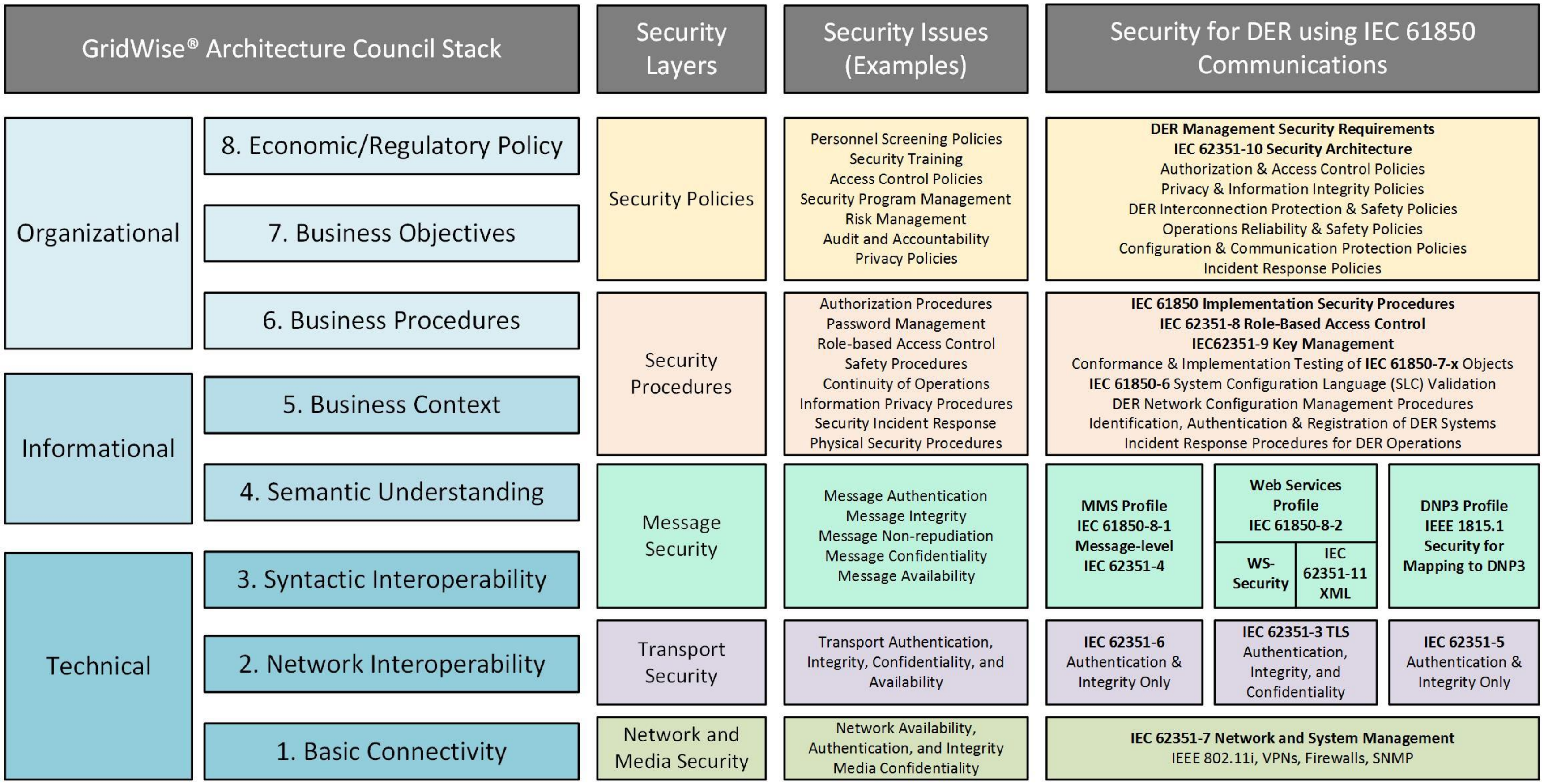
[168] IEC 62443-4-1, Security for industrial automation and control systems, Part 4 - 1: Secure product development life-cycle requirements, Draft 3, Edit 11, Mar 2016.

[169] IEC 62443-4-2, Security for industrial automation and control systems Technical security requirements for IACS components, Draft 2, Edit 4, 2 Jul 2015.

[170] ISA, "The 62443 Series of Standards, Industrial Automation and Control Systems Security," Dec 2016.

[171] ISASecure, IEC 62443 - EDSA Certification, Embedded Device Security Assurance (EDSA) - version 2.0.0 effective 01 July 2016, accessed 10/27/2017, URL: http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification

There is no requirement that PV power electronics equipment is certified to any of these standards. To prevent mass deployment of unsecured equipment on the US electric grid, the PV industry must select one of these standards, or develop a new one, to certify the cyber security posture of PV inverters entering the market. There is also a need for a second certification standard to verify PV system communications are compliant to the data-in-transit communication protocol security requirements.



GridWise® Architecture Council Stack		Security Layers	Security Issues (Examples)	Security for DER using IEC 61850 Communications		
Organizational	8. Economic/Regulatory Policy	Security Policies	Personnel Screening Policies Security Training Access Control Policies Security Program Management Risk Management Audit and Accountability Privacy Policies	**DER Management Security Requirements** **IEC 62351-10 Security Architecture** Authorization & Access Control Policies Privacy & Information Integrity Policies DER Interconnection Protection & Safety Policies Operations Reliability & Safety Policies Configuration & Communication Protection Policies Incident Response Policies		
	7. Business Objectives					
	6. Business Procedures	Security Procedures	Authorization Procedures Password Management Role-based Access Control Safety Procedures Continuity of Operations Information Privacy Procedures Security Incident Response Physical Security Procedures	**IEC 61850 Implementation Security Procedures** **IEC 62351-8 Role-Based Access Control** **IEC62351-9 Key Management** Conformance & Implementation Testing of **IEC 61850-7-x** Objects **IEC 61850-6** System Configuration Language (SLC) Validation DER Network Configuration Management Procedures Identification, Authentication & Registration of DER Systems Incident Response Procedures for DER Operations		
Informational	5. Business Context					
	4. Semantic Understanding	Message Security	Message Authentication Message Integrity Message Non-repudiation Message Confidentiality Message Availability	**MMS Profile** **IEC 61850-8-1** **Message-level** **IEC 62351-4**	**Web Services Profile** **IEC 61850-8-2** **WS-Security** **IEC 62351-11 XML**	**DNP3 Profile** **IEEE 1815.1** **Security for Mapping to DNP3**
Technical	3. Syntactic Interoperability					
	2. Network Interoperability	Transport Security	Transport Authentication, Integrity, Confidentiality, and Availability	**IEC 62351-6** Authentication & Integrity Only	**IEC 62351-3 TLS** Authentication, Integrity, and Confidentiality	**IEC 62351-5** Authentication & Integrity Only
	1. Basic Connectivity	Network and Media Security	Network Availability, Authentication, and Integrity Media Confidentiality	**IEC 62351-7 Network and System Management** IEEE 802.11i, VPNs, Firewalls, SNMP		

Figure 11. Security for Distributed Energy Resources (DER) using IEC 61850 communications and IEC 62351. Adapted from IEC TC57.[172]

[172] F. Cleveland, "IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure, June, 2012, accessed 19 Sept 2017, http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf

6 INDUSTRY BEST PRACTICES

Cyber security starts with good practices from industry to create secure products and networks. The following are several recommendations for industry organizations to improve their cyber security posture in categories of industry standards, cyber security self-evaluations, auditing, cyber security hygiene, patching, defense-in-depth, supply chain risks, and insider threats.

6.1 Adoption of Industry Standards

Effective implementation of cyber security practices within organizations requires coordination between corporate tiers. As shown in Figure 12, executives determine and communicate mission priorities, budget, risk appetite, and available resources to the business/process level, who use these parameters as inputs to generate a “Framework Profile” (a tool to establish a roadmap for reducing cyber security risk). The Framework Profile is implemented at the operations level to secure critical infrastructure. Progress towards the target Profile and any updates on threats, assets, or vulnerabilities are communicated to the business level to update the risk landscape and communicate that with executive leadership.

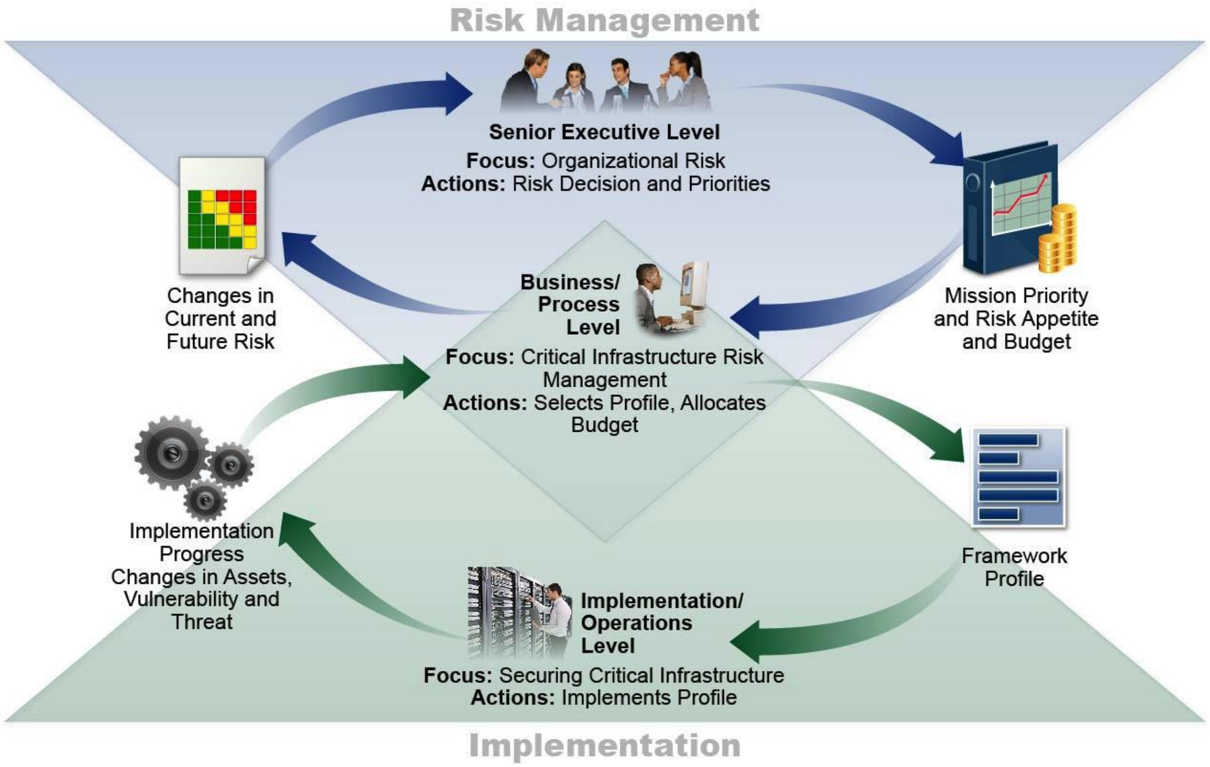

Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profile
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Figure 12: Information and Decision flows within an Organization.[173]

[173] NIST, Improving Critical Infrastructure Cybersecurity Executive Order 13636, Preliminary Cybersecurity Framework, URL: https://www.nist.gov/sites/default/files/documents/itl/preliminary-cybersecurity-framework.pdf

Grid operators, aggregators, and PV power electronics vendors should employ recommendations from NIST 800-82 Guide to ICS Security to architect the ICS control networks with best practices such as:

- Controlled logical access with unidirectional gateways, DMZs, unique OT authentication mechanisms, defense-in-depth methodologies with multiple security layers.
- Restricting physical access
- Minimization of DER exploits by regular patches, disabling unused ports and services, adopting the principle of least privilege, monitoring audit trails, using anti-virus programs, applying encryption or cryptographic hashes for data storage and communications, etc.
- Minimization of data-in-transit manipulation, falsification, or spoofing.
- Employing intrusion detection and prevention systems
- Maintaining functionality under duress: redundant critical components, restorations plans, fault tolerant systems, and graceful degradation without cascading failures—whereby the equipment can transition to emergency operations.

Additional information can be gained from the equipment selection guides[174] and other military and civilian guides.[175,176]

6.2 Cyber Security Self-Evaluations

Organizations responsible for the control or data exchange of DER equipment should regularly conduct self-evaluations of their cyber security posture. There are multiple options for these assessments including the DHS US-CERT Cyber Security Evaluation Tool (CSET)[177] which systematically evaluates the network security, identifies and ranks gaps based on ICS-CERT threat information, and reports on the assessment to recommend high-priority improvements. Another self-evaluation tool is the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)[178] which tailors the C2M2 to the power industry. This model provides a method of ranking an organization using maturity indicator levels in 10 different domains, shown in Table 2. Both the CSET and ES-C2M2 have interactive tools for entering data and generating reports.

[174] Committee on National Security Systems (CNSS) Instruction No. 1253, Security Categorization and Control Selection for National Security Systems, 27 Mar 2014.

[175] Committee on National Security Systems Instruction No. 1253, Security Control Overlays for Industry Control Systems, version 1, Jan 2013.

[176] Department of Defense, Instruction Number 8500.01, 14 Mar 2014.

[177] US-CERT, CSET Download, accessed 11-27-2017, URL: https://www.us-cert.gov/forms/csetiso

[178] DOE/DHS ES-C2M2, accessed 10-10-2017, URL: https://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf

Table 2. Energy Sector Cybersecurity Capability Maturity Model (C2M2).

DOMAIN	DESCRIPTION
1. Risk Management (RISK)	Manage the organization's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.
2. Asset, Change, and Configuration Management (ASSET)	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.
3. Identity and Access Management (ACCESS)	Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.
4. Threat and Vulnerability Management (THREAT)	Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP).
5. Situational Awareness (SITUATION)	Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.
6. Information Sharing and Communications (SHARING)	Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.
7. Event and Incident Response, Continuity of Operations (RESPONSE)	Manage the organization's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.
8. Supply Chain and External Dependencies Management (DEPENDENCIES)	Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.
9. Workforce Management (WORKFORCE)	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.
10. Cybersecurity Program Management (CYBER)	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.

Once specific areas of improvement have been identified, more detailed, targeted improvements should be performed based on guidelines or best practices. For example, NIST and DOE provide details on how to develop and apply risk management frameworks and processes;[179,180] the Software Engineering Institute at Carnegie Mellon University offers guides to mitigating insider

[179] NIST Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Feb 2010.

[180] U.S. Department of Energy, Electricity Subsector Cybersecurity Risk Management Process, Report DOE/OE-0003, May 2012.

threats,[181] conducting coordinated vulnerability disclosures,[182] and form and operate computer security incident response teams.[183]

6.3 Auditing

Much like NERC CIP audits are conducted of utility operations, PV control networks could be audited to ensure the system is appropriately architected, patched, and monitored. While there is no basis for conducting audits for PV systems now, as the percentage of generation coming from DER equipment continues to increase, these aggregations become a larger component of the country's critical infrastructure. Auditing would support equipment certification standards by conducting follow-on assessments of the devices and assessing the operating environment where the equipment had been deployed.

One good example of this auditing approach applied to energy systems is the Digital Bond Bandolier Audit Files which scan for vulnerabilities in SCADA systems like those by Siemens, Telvent, ABB, Matrikon, Emerson, AREVA, OSIsoft, Invensys, and SNC systems.[184] Another Digital Bond situational awareness system called Portaledge uses an OSIsoft PI server to analyze control systems events and alert operators of possible attacks. [185] These types of tools should be employed in aggregator and grid operator networks to regularly scan for known vulnerabilities and suspicious traffic.

6.4 Cyber Security Hygiene and Patching

Poorly managed or undocumented inventories, system topologies, controls, or security practices create vulnerabilities that can comprise security. Unfortunately, there is little financial incentive to administer best security practices for ICS. This culture results in known vulnerabilities and presents a significant barrier to DER cyber security. There are currently thousands of known vulnerabilities that exist in hundreds of common programs and operating systems. As an example of the scale of the problem, see the CVE Details website which scrapes the NIST National Vulnerability Database (NVD) XML feeds and catalogs Common Vulnerabilities and Exposures (CVE) for various products.[186] As of this writing, there are hundreds of vulnerabilities in dozens of products. It is estimated that there are on average 0.76 software mistakes per one thousand lines

[181] M.L. Collins, M.C. Theis, R.F. Trzeciak, J.R. Strozer, J.W. Clark, D.L. Costa, T. Cassidy, M.J. Albrethsen, A.P. Moore "Common Sense Guide to Mitigating Insider Threats, Fifth Edition," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2016-TR-015, 2016.

[182] A.D. Householder, G. Wassermann, A. Manion, C. King, "The CERT Guide to Coordinated Vulnerability Disclosure," Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2017-SR-022 August 2017.

[183] M.W. Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, M. Zajicek, "Handbook for Computer Security Incident Response Teams (CSIRTs)," Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2003-HB-002, April 2003.

[184] D. Peterson, Bandolier Auditing Control System Security with Vulnerability Scanners, SANS Process Control & SCADA Security Summit, Feb 2009.

[185] Digital Bond, Cyber Security Audit and Attack Detection Toolkit, Factsheet, 2008.

[186] CVE Details, Top 50 Products by Total Number of "Distinct" Vulnerabilities, accessed 10-30-2017, URL: https://www.cvedetails.com/top-50-products.php.

of commercial software source code[187] and some of these mistakes will lead to vulnerabilities, e.g., the Heartbleed Bug for OpenSSL (CVE-2014-0160).[188]

Inverters and other devices pose a significant risk to the power system if they are not appropriately patched. In the past, inverter manufacturers have remotely updated their equipment to provide grid stability in Hawaii.[189,190] Similar mechanisms for patching have been discussed in the SIWG Phase 2 meetings but the precise means of remotely issuing firmware upgrades has not been defined. DHS has provided recommendations for patch management for control systems;[191] similar guidance should be established for networked PV systems. The procedures, access controls, and technical operations for performing updates are essential to protecting the power systems in high PV penetration environments. Additionally, inverter vendors and other network component manufacturers should incorporate the ability to conduct non-bootable patching (hot patching) to minimize any downtime of the system. Contractual requirements defining patching responsibilities for vendors, installers, aggregators, and grid operators should be established.

Furthermore, rules for vulnerability disclosures should also be established and formally documented. The *Roadmap to Achieve Energy Delivery Systems Cybersecurity* recommends adopting a "Bill of Rights" for vulnerability disclosures which communicates impact and defines the responsibilities of all parties. This document should be accepted by the industry to make it clear the process and components that must be included in the disclosure, i.e., who discovered the vulnerability, the affected interfaces, and the degree of risk.

6.5 Defense-in-Depth

Solar power electronics vendors, aggregators, and grid operators must employ standardized and innovative defense-in-depth strategies to protect the U.S. power system. Defense-in-depth is the concept of layering multiple security features within the network such that the system is no longer attractive to would be attackers. As described above, PV control networks must be isolated through firewalls, proxies, VPNs, or other enclaves from other utility operations. Network operators must deploy intrusion detection systems, intrusion prevention systems, and DMZs, on control networks and use protection mechanisms such as moving target defense, protected (enclaved) computing, obfuscation, and other defense-in-depth techniques (e.g. cryptography, privilege zones, etc.). They should also use security analytics to determine the existence of adversary action through deep packet analysis and analytic tools and quantitative metrics. NCCIC and ICS-CERT define several defense-in-depth strategies in Table 3.[192]

[187] Synopsys, Inc., "Coverty Scan: Open Source Report 2014," 2015.

[188] The Heartbleed Bug, accessed 10-30-2017, URL: http://heartbleed.com/

[189] P. Fairley, 800,000 MicroInverters Remotely Retrofitted on Oahu—in One Day, IEEE Spectrum, 5 Feb 2015.

[190] A. Konkar, 'Something Astounding Just Happened': Enphase's Grid- Stabilizing Collaboration with Hawaiian Electric, Enphase Energy blog, 11 Mar 2015.

[191] DHS, Recommended Practice for Patch Management of Control Systems, Dec. 2008.

[192] DHS NCCIC and ICS-CERT, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Sept. 2016.

Table 3: DHS NCCIC and ICS-CERT Defense in Depth Strategy Elements.

Defense-in-Depth Strategy Elements	
Risk Management Program	Identify Threats Characterize Risk Maintain Asset Inventory
Cybersecurity Architecture	Standards/Recommendations Policy Procedures
Physical Security	Field Electronics Locked Down Control Center Access Controls Remote Site Video, Access Controls, Barriers
Network Architecture	Common Architectural Zones Demilitarized Zones (DMZ) Virtual LANs
PV Network Perimeter Security	Firewalls/One-Way Diodes Remote Access & Authentication Jump Servers/Hosts
Host Security	Patch and Vulnerability Management Field Devices Virtual Machines
Security Monitoring	Intrusion Detection Systems Security Audit Logging Security Incident and Event Monitoring
Vendor Management	Supply Chain Management Managed Services/Outsourcing Leveraging Cloud Services
Human Element	Policies Procedures Training and Awareness

Based on the DHS defense-in-depth recommended practice, the five key countermeasures for PV networks are:

1. Identify, minimize, and secure all network connections to PV.
2. Harden the PV network and supporting systems by disabling unnecessary services, ports, and protocols; enable available security features; and implement robust configuration management practices.
3. Continually monitor and assess the security of PV systems, networks, and interconnections.
4. Implement a risk-based defense-in-depth approach to secure PV systems and networks.
5. Manage the human element—clearly identify requirements for PV networks; establish expectations for performance; hold individuals accountable for their performance; establish policies; and provide PV network security training for all operators and administrators.

These countermeasures should be incorporated at the device and network levels to secure the communications system.

6.6 Supply Chain Risk Management

DER vendors and grid operators should establish Cyber Supply Chain Risk Management (C-SCRM) programs. In many cases, PV equipment is designed and built outside of the US, or uses commercial off-the-shelf components manufactured internationally. This exposes the power system to new risks, as the control behavior of this equipment could be changed remotely. Currently, remote access to DER equipment from foreign companies is permitted; while this could provide critical patches to software systems, it also expands the power system attack surface.

In 2015, NIST hosted a conference on cyber supply chain best practices. At this conference, they provided a brief that included the following supply chain risks:[193]

- Third party service providers or vendors with physical or virtual access to information systems or software
- Poor information security by lower-tier suppliers
- Compromised software or hardware purchased from suppliers
- Software vulnerabilities in supplier systems or supply chain management
- Third party data storage or data aggregators

They also provided recommendations for protecting the supply chain along with interviews from many leading experts at, e.g., Northrop Grumman,[194] Cisco,[195] Boeing and Exostar,[196] and NIST[197] to defend against these risks. The SANS institute has provided recommendations for combatting supply chain cyber risks by establishing recommendations for people, process, and technology elements.[198] There are also several supply chain risk management standards and best practices that apply to aerospace (SAE ARP9134[199]), electrical equipment/medical imaging (NEMA CPSP 1-2015[200]), and automotive industries (SAE AS5553A,[201] SAE AS5553B[202]). PV inverter and other DER equipment supply chain standards should reference these standards or adopt similar best practices to reduce the supply chain cyber risk.

6.7 Insider Threat Mitigation

The risk of insider actions against the control system cannot be ignored and must be managed. In the Carnegie Mellon University *Common Sense Guide to Mitigating Insider Threats*, the authors recommend many practices, such as:[203]

- Performing risk assessments; inventorying and documenting assets with associated functionality and prioritization/criticality
- Developing a formal insider threat program, and adding training for all employees

[193] NIST, “Cyber Supply Chain Best Practices,” Best Practices in Cyber Supply Chain Risk Management Conference Materials, 2015. URL: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

[194] NIST, “Northrop Grumman Corporation Trusted, Innovative, World-Class Supply Chain,” Best Practices in Cyber Supply Chain Risk Management, U.S. Resilience Project Report, 2015.

[195] NIST, “Cisco Managing Supply Chain Risks End-to-End,” Best Practices in Cyber Supply Chain Risk Management, U.S. Resilience Project Report, 2015.

[196] NIST, “Boeing and Exostar Cyber Security Supply Chain Risk Management,” Best Practices in Cyber Supply Chain Risk Management, U.S. Resilience Project Report, 2015.

[197] NIST, “Utility Sector Best Practices for Cyber Security Supply Chain Risk Management,” Best Practices in Cyber Supply Chain Risk Management, U.S. Resilience Project Report, 2015.

[198] D. Shackleford, Combatting Cyber Risks in the Supply Chain, SANS Institute Report, Sept 2015.

[199] SAE International, Standard ARP9134A, “Supply Chain Risk Management Guideline,” 6 Feb 2014.

[200] NEMA, CPSP 1-2015, Supply Chain Best Practices, Document ID: 100742, 25 Jun 2015.

[201] SAE International, Standard AS5553A, “Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria,” 26 Aug 2014.

[202] SAE International, Standard AS5553B, “Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition,” 12 Sept 2016.

[203] M.L. Collins, M.C. Theis, R.F. Trzeciak, J.R. Strozer, J.W. Clark, D.L. Costa, T. Cassidy, M.J. Albrethsen, A.P. Moore "Common Sense Guide to Mitigating Insider Threats, Fifth Edition," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2016-TR-015, 2016.

- Documenting policies and controls
- Monitor and respond to suspicious or disruptive behavior
- Consider insider and business partners threats in enterprise-wide risk assessments
- Be careful with social media disclosures
- Implement strict password and account management practices
- Use stringent access controls and monitor privileged users
- Monitor employee actions with correlated data from multiple sources
- Monitor and control remote access from all points, e.g., mobile
- Establish baseline behavior for networks and employees
- Enforce separation of duties and least privilege
- Create explicit security agreements for cloud services
- Institute change controls
- Implement secure backups and recovery processes
- Prevent data exfiltration from wired and wireless networks, portable media, etc.

CMU also created best practice checklists for specific stakeholders and mapped the practices to several national and international standards for more detailed implementation recommendations in the *Common Sense Guide to Mitigating Insider Threats*.

7 CONCLUSIONS

A five-year roadmap for photovoltaic cyber security is presented with recommendations for stakeholder engagement, research and development, standards development, and industry best practices. This roadmap guides national and local policy, standards, and public and private investment to improve the resilience of the US power system by hardening PV control networks, developing and implementing detection technologies, and preparing to rapidly respond to cyber attacks. Through collective implementation of these technologies the security of photovoltaic control systems can be strengthened without compromising the performance of the network.

The path ahead is challenging. Sustained cyber security leadership and stakeholder commitment are necessary to continuously improve PV equipment and networks, build effective standards, maintain public-private information exchanges, and support government and commercial R&D efforts. Maintaining positive momentum is the responsibility of all stakeholders. As a next step, the recommendations provided in this document should be prioritized to direct stakeholder investment toward high-impact activities.

8 DISTRIBUTION

1 Guohui Yuan
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

1 Kemal Celik
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

1 Dan Ton
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

1	MS0671	Jennifer Depoy	05628
1	MS0671	William Waugaman	05628
1	MS0671	Jason Stamp	05623
1	MS1033	Abraham Ellis	08812
1	MS1033	Jimmy Quiroz	08812
1	MS1033	Jay Johnson	08812
1	MS0161	Legal Technology Transfer Center	11500
1	MS0899	Technical Library (electronic copy)	

Sandia National Laboratories