SAND2018-7082PE

# DOE SETO Cybersecurity Portfolio

## Cybersecurity for DERs Workshop

July 17, 2018

**Shamina Hossain-McKenzie**[1] & Jay Johnson[2]

[1]Cyber Resilience R&D

[2]Renewable and Distributed Systems Integration

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

SAND2018-6898 PE

# Overview

- **DOE EERE offices are playing a major role in power system cybersecurity** – with more growth expected
- **Vehicle Technologies Office** is investigating electric vehicle extreme fast charging cybersecurity
- **Building Technologies Office** looking at building energy management systems and demand response cybersecurity
- **Solar Energy Technologies Office** has:
  - Funded a roadmap for solar cybersecurity
  - Advised the utility industry about the risks of DER cybersecurity
  - Supported the develop of the DER cyber security working group
  - Investigated in a range for R&D activities covering DER network protection, detection, and response
- **Other EERE offices** also entering this space
  - Coordinated effort across EERE is underway for defining the role in cybersecurity
  - Will integrate within larger government efforts with DHS, NIST, DOD, DOE CESER, etc.

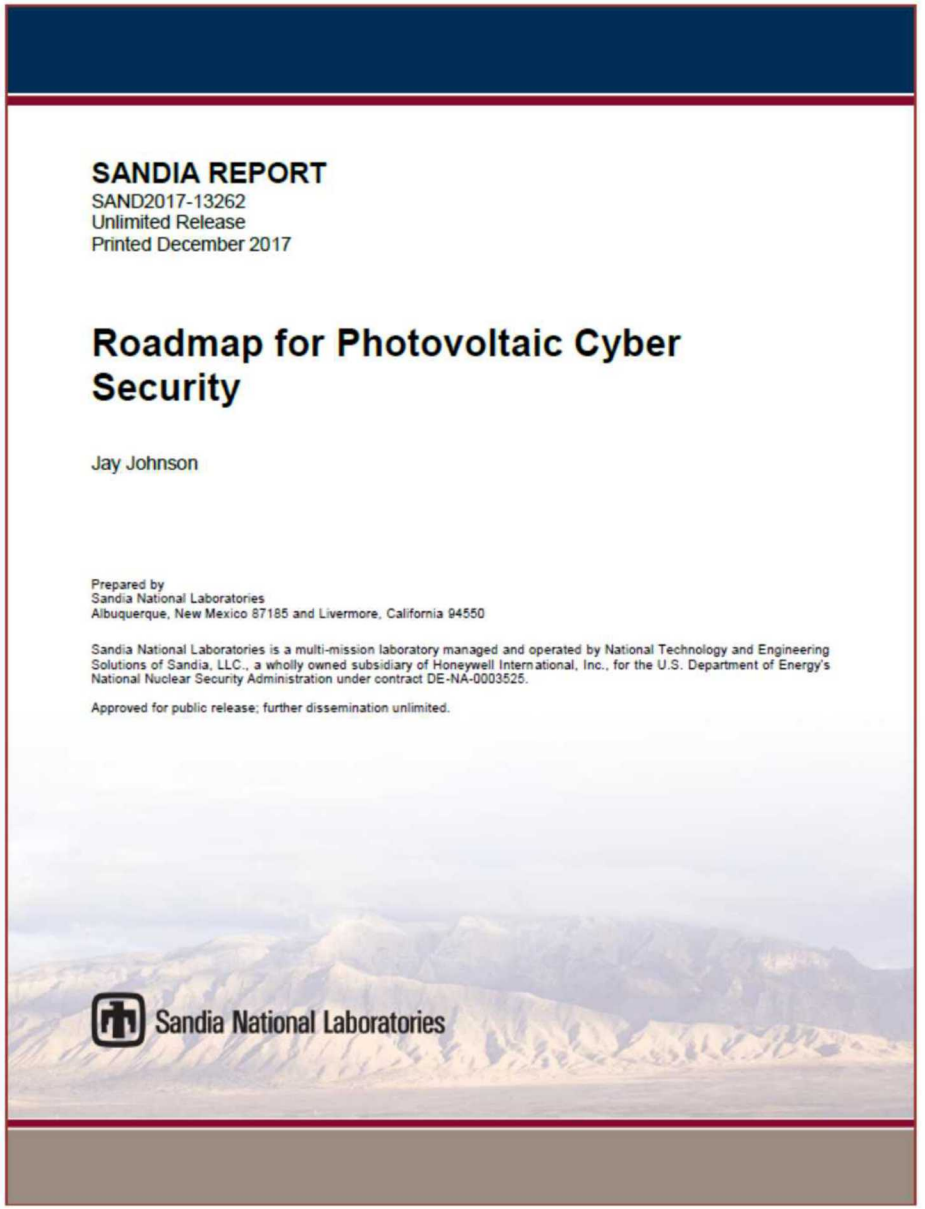
# Roadmap for PV Cyber Security

## Roadmap

- Outlines **5-year strategy** for DOE, industry, and standards development organizations in areas of Identify/Protect, Detect, and Respond/Recover
- Focused on PV, but highly **extensible to other DER**
- Closely aligned with 2011 "Roadmap to Achieve Energy Delivery Systems Cybersecurity"
- Explores existing research by DOE, other agencies, and industry

## Major recommendations

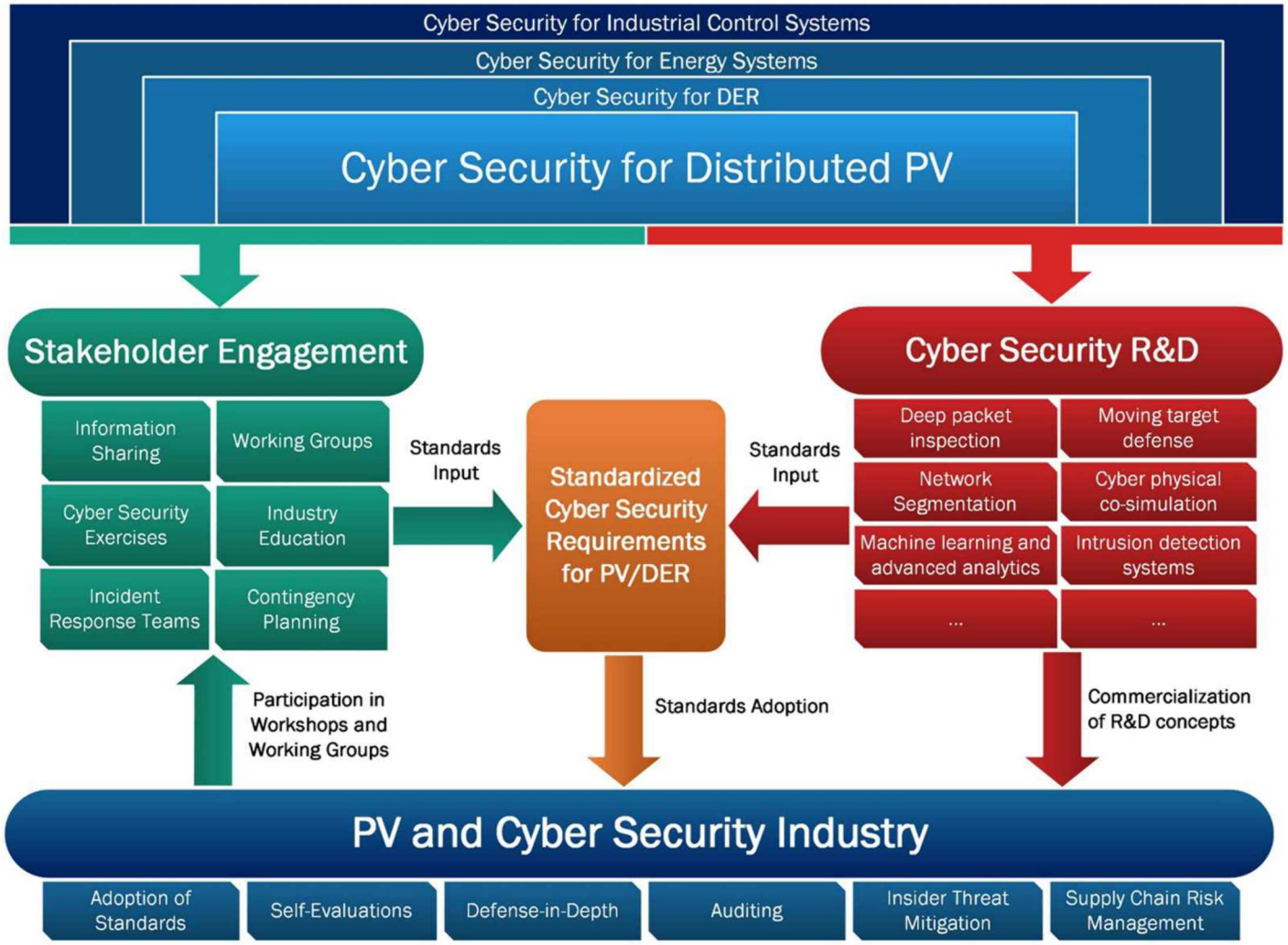
- Engage in cross-industry communication and collaborations (e.g., information sharing programs)
- Develop standards, guidelines, and best practices (leveraging existing work)
- Foster R&D programs to develop solutions for protecting infrastructure, detecting threats, and recovering from attacks
- Work to harden infrastructure, conduct self-evaluations, and practice good cyber hygiene to stay ahead of adversaries




More details in "Roadmap for Photovoltaic Cyber Security" (SAND2017-13262), which outlines a 5-year strategy for DOE, industry, and standards development organizations in areas of Identify/Protect, Detect, and Respond/Recover.

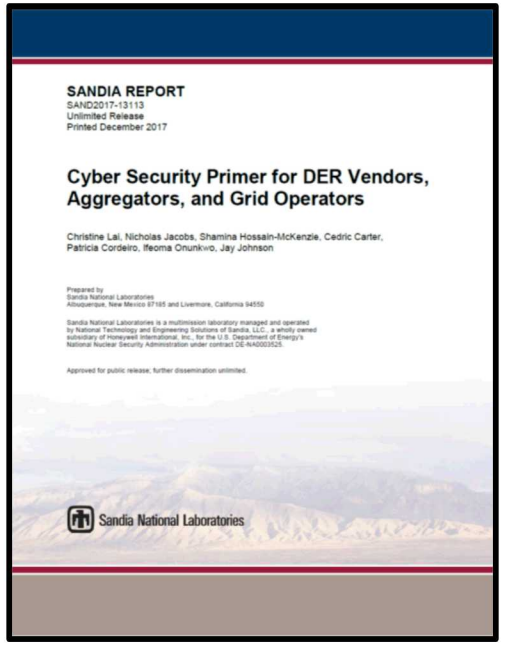
# Roadmap Work Flow

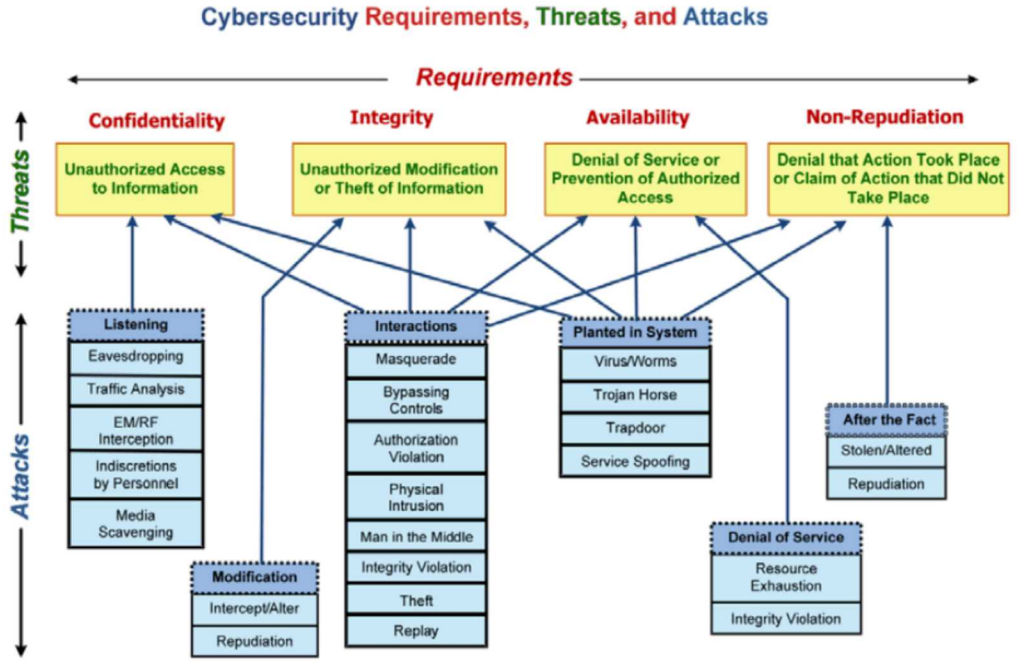
- Vision: By 2023, grid operators, system owners, and aggregators communicate with interoperable photovoltaic systems using safe, secure, resilient networks with high availability, data integrity, and confidentiality.
- **Focused on four areas"**
  - Stakeholder Engagement
  - Research and Development
  - Industry (grid operators, aggregators, and PV vendors)
  - Standards and Guidelines
- **Major goals (covered on next slides):**
  - Inform solar industry of DER cybersecurity concepts
  - Form industry working groups
  - Create cyber security standards
  - Commercialize security R&D



# Inform Industry: DER Cyber Security Primer

- Primer covers:
  - Cyber security principles
    - Confidentiality, integrity, availability, etc.
  - Types of cyber attacks and threats
  - DER communication protocols
  - Cyber security guidelines, standards, and best practices
  - Cyber recommendations for the DER community




| DER Protocol Cyber Security Features | Protocol: IEC 61850<br>Information Model: IEC 61850-90-7<br>Security Requirements: IEC 62351 Series | Protocol: IEEE 2030.5<br>Information Model: CSIP<br>Security Requirements: IEEE 2030.5 + CSIP | Protocol: IEEE 1815<br>Information Model: DNP3 Application Note<br>Security Requirements: IEEE 1815 | Protocol: Modbus<br>Information Model: SunSpec or MESA Models<br>Security Requirements: None |
|---|---|---|---|---|
| **Devices Support** | DER, Power Systems Devices | DER, Smart Grid devices | Utility, Grid Devices | Utility, Grid, ICS devices |
| **Encryption Capability** | Non-Native | Yes | BITW | BITW |
| **Encryption Required** | No | Yes | No | No |
| **Supported Transport Protocols** | N/A | TCP or UDP | Serial or TCP | Serial or TCP |
| **Supported Networks** | N/A | IPv4, IPv6 | IPv4 | IPv4, IPv6 |
| **Authentication Support** | Non-Native | Yes | Optional | Non-Native |
| **Type of Communication Protocol** | IEC 61850-90-7 contains functions for power converter-based DER systems | Communication protocol for device integration with the Smart Grid | Communication protocol for real-time monitoring and control | Communication protocol for real-time monitoring and control |
| **Type of Information Model** | IEC 61850-90-7 | CSIP | DNP3 Application Note | SunSpec and MESA are information models for Modbus |
| **Type of Security Requirements** | IEC 62351 Series | IEEE 2030.5 + CSIP | IEEE 1815 | There are no security requirements for Modbus communications |
| **Type of Data Transmitted** | DER settings, control modes, and measurements | DER measurement and control data | Data objects with defined attributes and priority levels | DER measurement and control data |
| **Aggregation Support** | Utility or aggregators can collect data | Yes | Yes | Yes |

# Create Industry Working Groups/Create Cybersecurity Standards

## SunSpec/Sandia DER Cybersecurity Workgroup

bringing together DER interoperability and cyber security experts to discuss security for DER devices, gateways, and other networking equipment that are owned or operated by end users, aggregators, utilities, or grid operators.

### DER Devices & Servers

- **Define standardized procedure for DER and server vulnerability assessments.**
- Leads: Cedric Carter (Sandia) and Danish Saleem (NREL)
- Known equipment vulnerabilities
- Establish certification and auditing procedures
- Maintaining compliance, requirements for patching
- **In process of transferring this to UL STP (likely to become a UL 2900-2-4 standard)**

### Secure Network Architecture

- **Create DER control network topology requirements and interface rules.**
- Lead: Candace Suh-Lee (EPRI)
- Perimeter controls
- Segmentation
- Physical security

### Access Controls

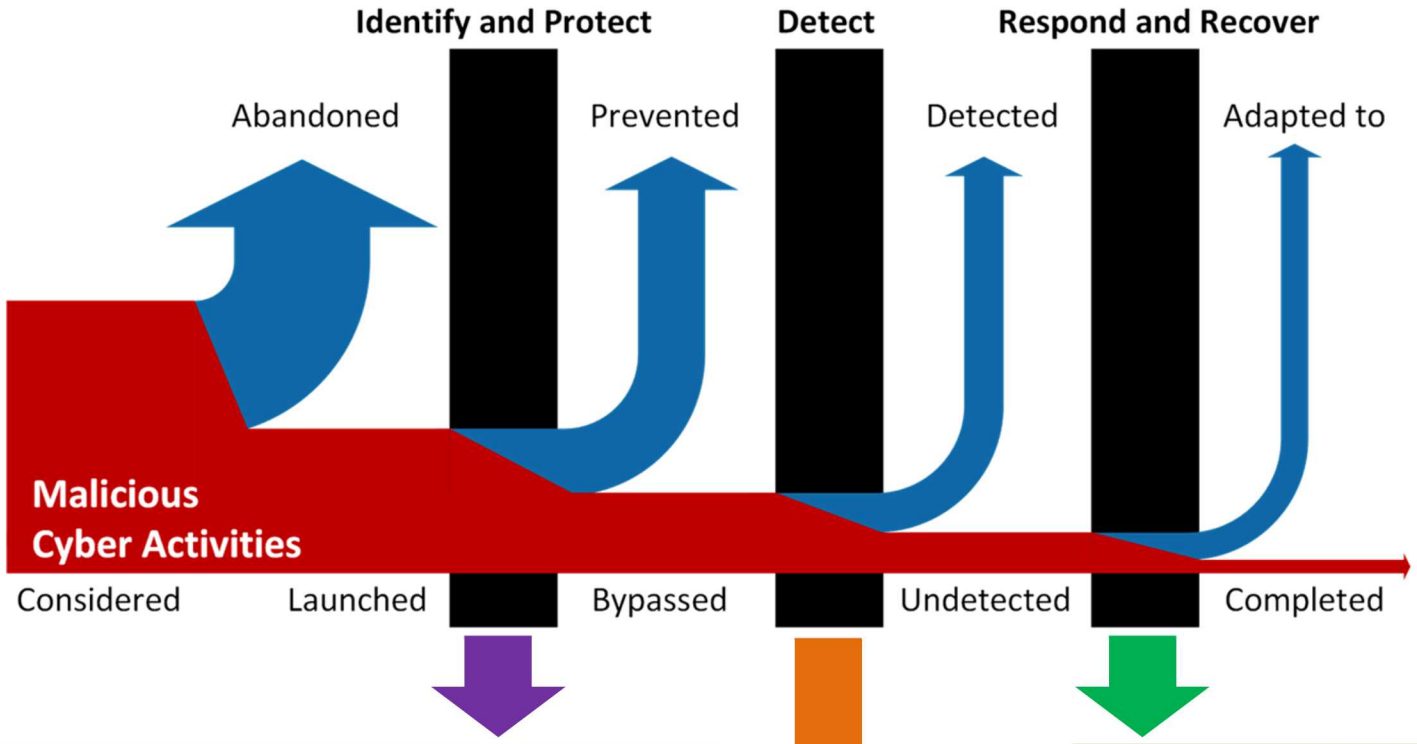
- **Classify data types, associated ownership, and permissions. Define set of protection mechanisms.**
- Not Started
- Access control lists
- Password control
- Data privacy

### Communication and Protocol Security

- **Define requirements and draft language for data-in-transit security rules.**
- Not Started
- Authentication
- Encryption requirements
- Acceptable transport protocols

**Primary Goal:** generate a collection of best practices that act as basis for (or input to) national or international DER cyber security standards. Sign up at http://sunspec.org/sunspec-cybersecurity-workgroup/

# Commercialize DER Cybersecurity R&D




- Threat Models
- Risk Quantification
- Cyber Assessments
- Network Segmentation
- Dynamic Networking and Moving Target Defense
- Trusted and Protected Computing
- Cryptography
- Virtualized Testbed Environments
- Engineering Controls
- Physical Security
- Security for Cloud-Services
- Obfuscation and Deception
- Authentication

- Situational Awareness
- Intrusion Detection

- Resilient Designs
- Dynamic Assessment
- Contingency Operating Modes
- Restoration
- Investigations and Attribution

Areas of current DOE SETO Cyber Security R&D are underlined.

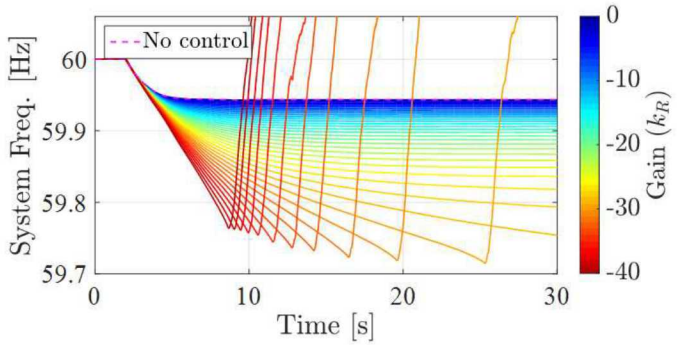
More details in “Roadmap for Photovoltaic Cyber Security” (SAND2017-13262), which outlines a 5-year strategy for DOE, industry, and standards development organizations in areas of Identify/Protect, Detect, and Respond/Recover.

# R&D Activities: Risk Quantification

## Frequency Droop

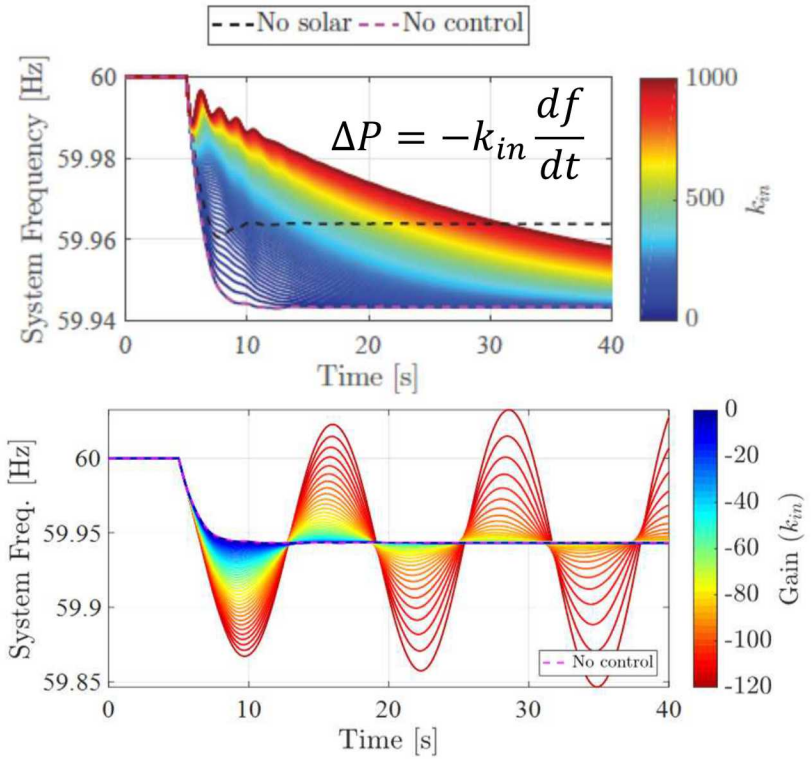
$$\Delta P_j = \frac{f_{ref} - f_{eq}}{R} = k_R(f_{ref} - f_{eq})$$

$$\Delta P_j^{attack} = -\frac{f_{ref} - f_{eq}}{R} = -k_R(f_{ref} - f_{eq})$$



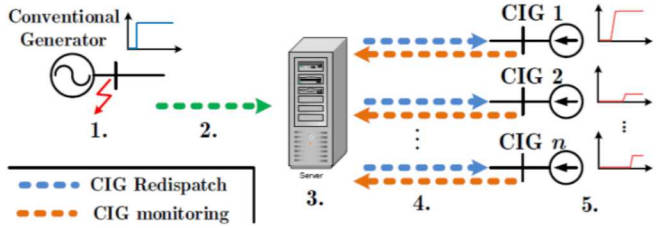

Attack: frequency-watt function is inverted to inject power at high frequency and absorb power at low frequency.
Result: Lower frequency nadirs, possibly leading to load shedding. $k_R$<-25 causes loss of synchronism

## Synthetic Inertia



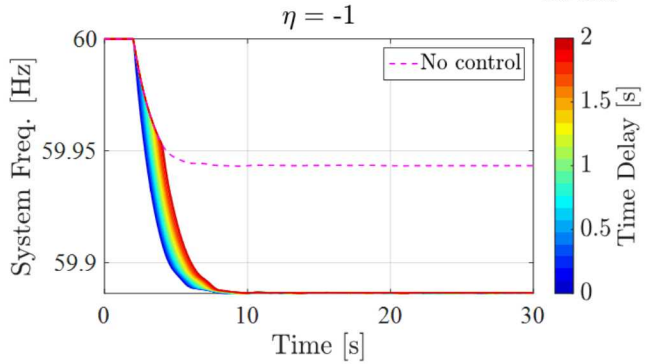

Attack: reverse sign on inertial gain to create positive feedback.
Result: Nadir is reduced and oscillatory behavior in the power system is created, leading to instability and possible blackouts.

## Fast Acting Imbalance Reserve




CIG = Converter-Interfaced Generator

$$\Delta P_i = K_{FF}^i P_{imbal} \quad K_{FF}^i = \eta \frac{P_i}{P_{avail}}$$



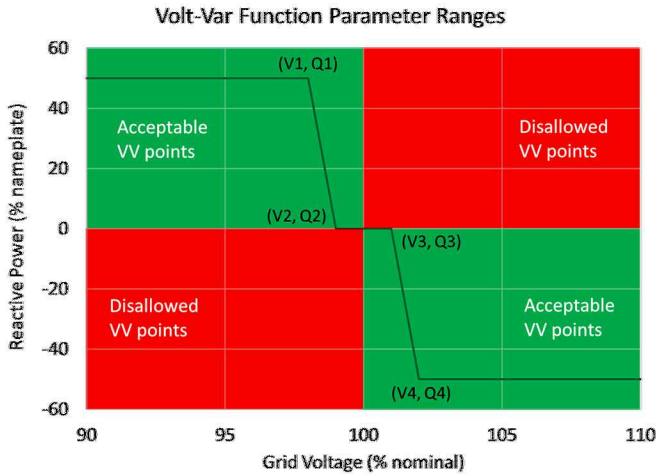

Attack: imbalance power compensation level, $\eta$, is set to reduce the power by the magnitude of the imbalance $\eta$=-1.
Result: Imbalance is worsened, possibly leading to a blackout.

J. Johnson, J. Quiroz, R. Concepcion, F. Wilches Bernal, M. Reno, "Power System Effects and Mitigation Recommendations for DER Cyber Attacks," IET Cyber-Physical Systems: Theory & Applications (in review).

# R&D Activities

## Engineering Controls

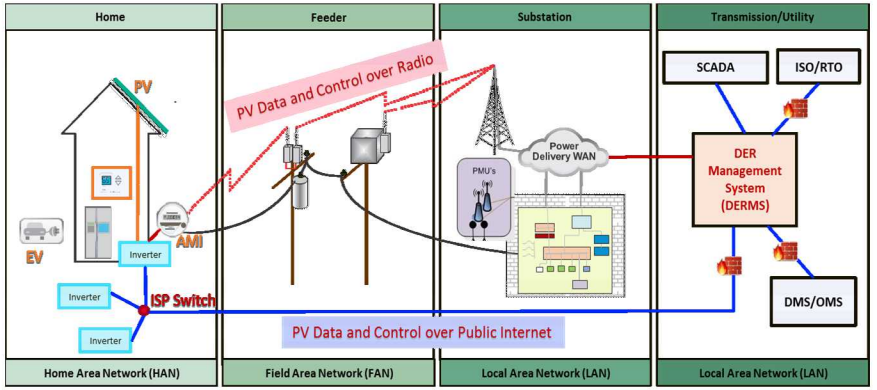
Concept: Create rules for information models/communication protocols or DER to reject grid-support parameters that are known to cause system instability or other grid problems.




On-going work: Sandia is investigating updating pysunspec (Python driver for SunSpec Modbus) to add specific rules to filter out malicious or erroneous commands that could negatively impact the power system.

## Cryptography: Data-in-flight Security

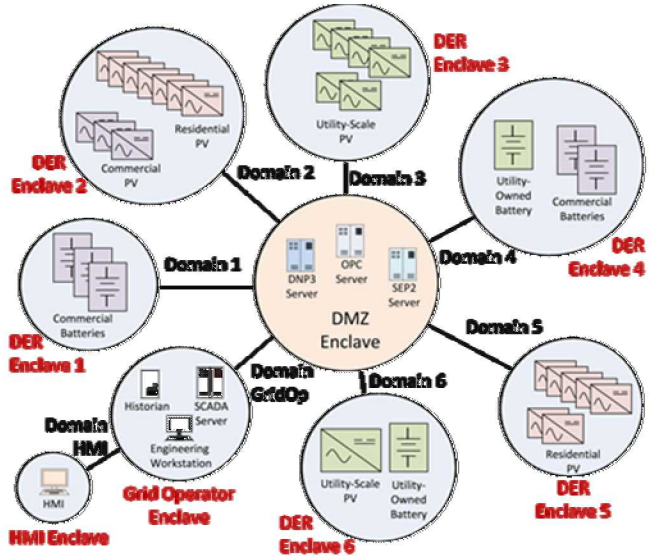
Concept: For DER traffic transmitted on the public internet, overlay TLS security on top of SunSpec Modbus or create a RESTful web services option for IEEE 1547, CA Rule 21, and other information model requirements.




On-going work: Sandia, EPRI and SunSpec are building communication stacks and investigating security features in IEEE 2030.5, IEEE 1815, SunSpec Modbus + TLS, and SunSpec-Compliant Web Services with TLS.

## Network Segmentation

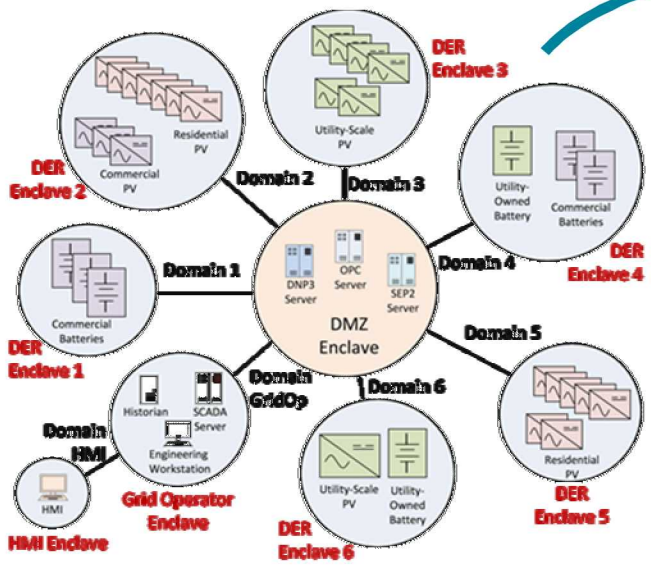
Concept: Create DER enclaves with firewall rules, VPNs, or proxies so an advisory cannot control all DER devices if an enclave is compromised.

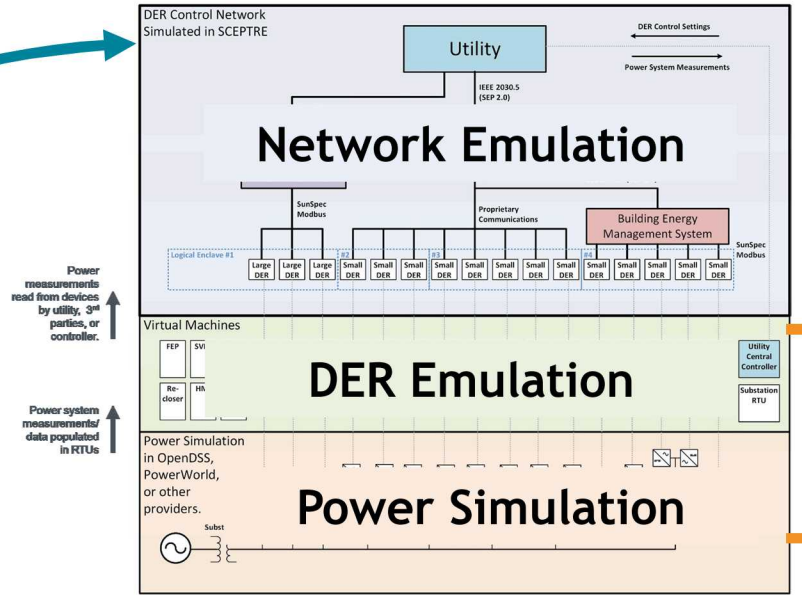



On-going work: DER Cyber Security Working group is creating recommended data architectures for utilities and DER aggregators. Also, Sandia measuring cyber metrics of different topologies with red teaming activities.

# R&D Activities: Virtualized Testbed Environments

DER control network architectures are emulated in the SCEPTRE environment.




SCEPTRE: a live, virtualized power system and control network co-simulation platform

SCEPTRE outputs:

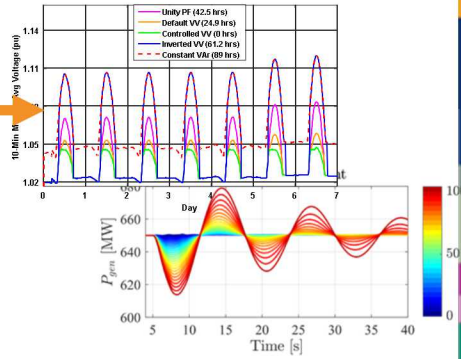
- Cybersecurity metrics
- Communication parameters
- Power system performance

IDART
Information Design Assurance Red Team

| Architecture | Access | Compliance | Confidentiality | Integrity | Availability | Total |
|---|---|---|---|---|---|---|
| Flat | High | Insecure | 0 | 0 | 8 | 8 |
| | | Hardened | 9 | 0 | 14 | 23 |
| Enclaved | High | Insecure | 0 | 0 | 8 | 8 |
| | | Hardened | 9 | 0 | 14 | 23 |
| | Medium | Insecure | 7 | 6 | 11 | 24 |
| | | Hardened | 9 | 6 | 14 | 29 |
| | Low | Insecure | 11 | 6 | 16 | 33 |
| | | Hardened | 11 | 6 | 16 | 33 |
| Maximum Possible Score → | | | 11 | 16 | 14 | 41 |

EXAMPLE

Power system studies




Multiple DER network architectures will be simulated to determine:

1. Cybersecurity resilience
2. Communication latency, dropout, and availability
3. Power system performance metrics (voltage, nadir, etc.)

# R&D Activities: Intrusion Detection Systems

**Research Question**
Can a distributed monitoring system patrol a wide range of cyber attack vectors, detect various attack methods, predict adversary movements, and implement controls that mitigate damage to DER devices?

## Create State-of-the-Art Simulation Platform

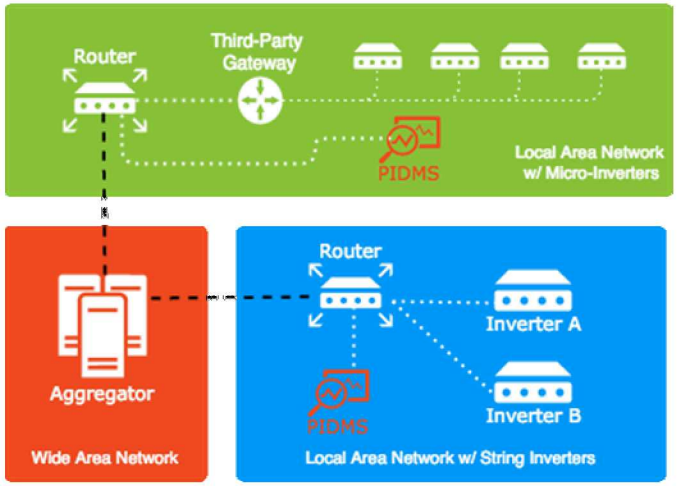
- Combination of SCEPTRE, OPAL-RT power hardware-in-the-loop simulations, and EPRI Solar PV Simulator
- Add 10,000 bus version of ePhasorSim
- Create ePhasorSim distribution models
- Enable communication drivers to support DNP3, Modbus, and etc.

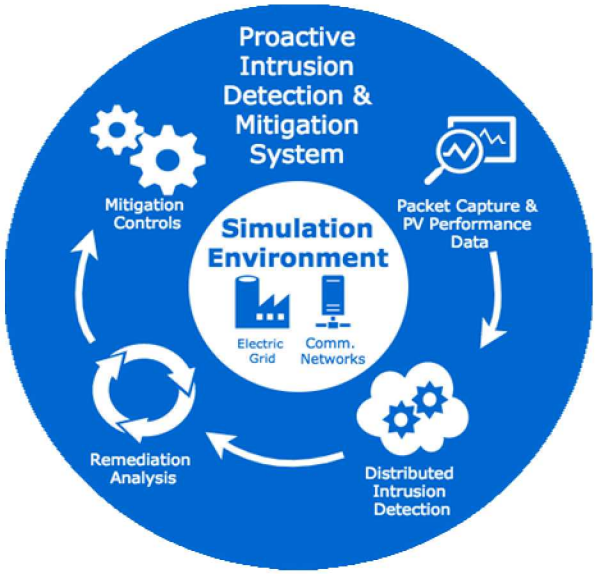
## Build Bump-In-The-Wire (BITW) Data Collection Sensor

- Create multi-lingual code package to capture and collect network packets and PV data
- Build lightweight and reliable data collection sensor with dropout rate < 0.5%
- Development stages:
  - Stage 1:
    - Enable Data Collection on Multiple Network Planes
  - Stage 2:
    - Evaluate Data Capture Error
  - Stage 3:
    - Evaluate Impact on Network
  - Stage 4:
    - Evaluate Impact on Remote Control Signals

## Develop Proactive Intrusion Detection and Mitigation System (PIDMS) Analysis and Control Methodology

- Create flexible, distributed analytics that include:
  - 1. Classification and prediction ML algorithms
  - 2. Machine-to-machine comm. protocols
  - 3. Onboard data storage
  - 4. Read/write comm. with >3 inverter manufacturer devices
  - 5. Runs data collection sensor
- Evaluate methodology:
  - Simulate various systems and attack scenarios
  - Test various IDS classification methods



Thank You!