SAND2019-2998C

Cyber-securing PV and DER

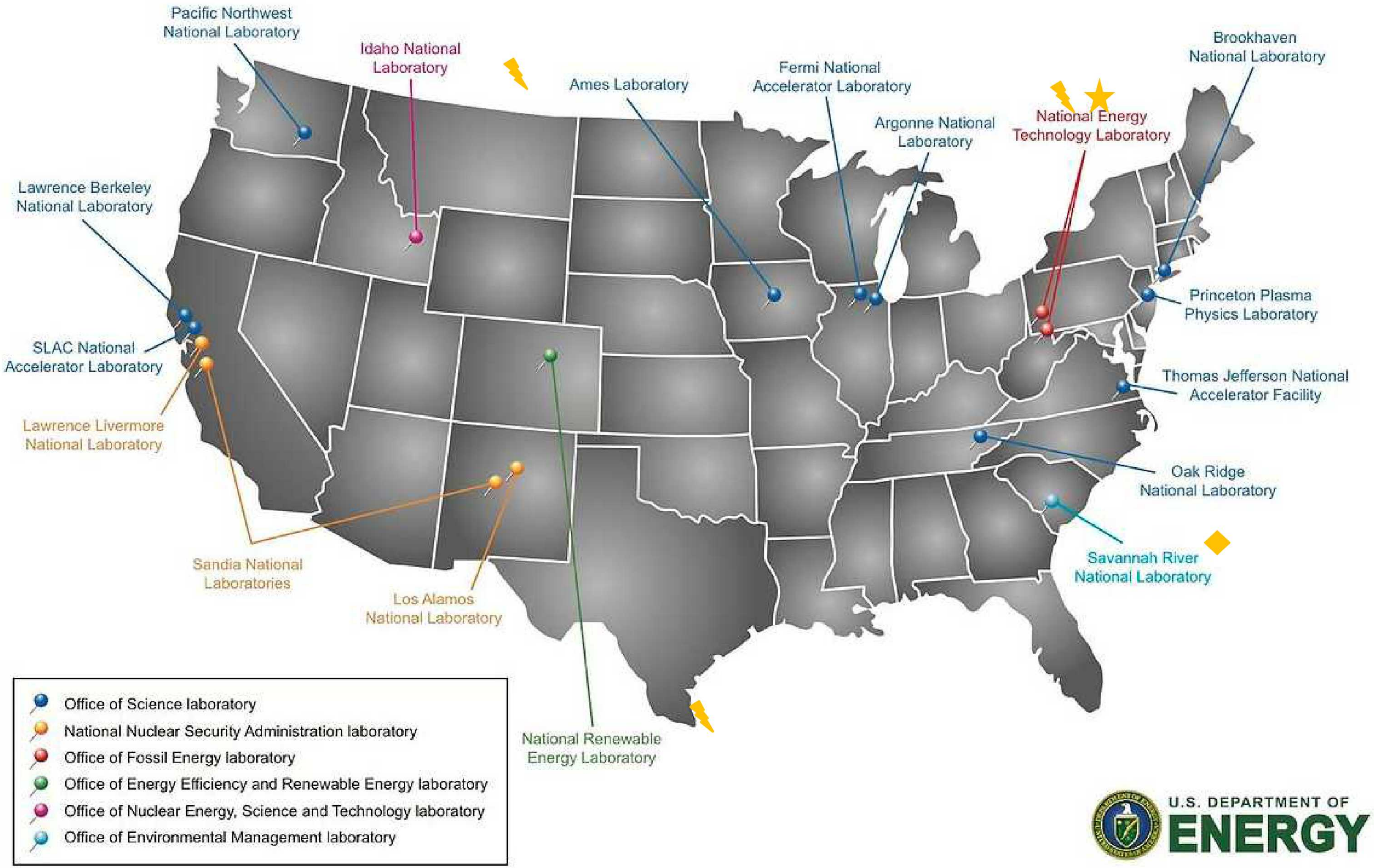
Florida International University

March 14, 2019

Dr. Abraham Ellis
Program Manager, Renewable and Distributed Systems Integration
aellis@sandia.gov

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.

DOE National Laboratories



Sandia Grid Modernization Timeline

1980s

Distributed Energy Technology Laboratory (DETL) opens

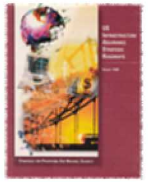
Sandia designs first battery test facility hosted by PSE&G in NJ

Lead Center for the Exploratory Battery Technology Development and Testing Project

1990/2000s

Interconnected PV systems work begins

US Infrastructure Assurance Strategic Roadmaps



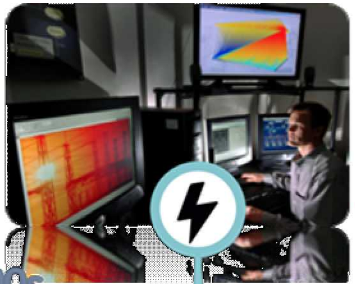
DOE designates Sandia as US Rep to IEC TC57, (standards for information exchange for power systems)

2003/04

U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability

DOE/OE Established

National SCADA Test Bed (NSTB) established



IEEE 1547: *Standard for Interconnecting Distributed Resources with Electric Power Systems*

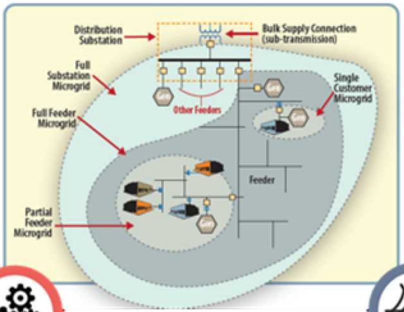
DOE/EPRI Electricity Storage Handbook Published

Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

Common Vulnerabilities in Critical Infrastructure Control Systems

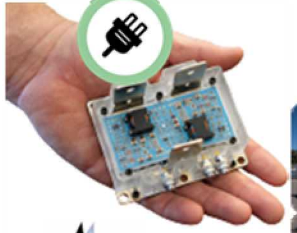
2008

Energy Surety Microgrid (ESM™) Methodology



ESM work begins-LDRD

2009

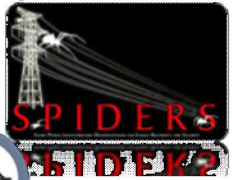


R&D 100 — SiC Power Module

ARRA-funded reconfiguration of DETL to enable high penetration experimentation on distributed generation

2010

Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) established



R&D100: Micro Power Source

Energy Storage Test Pad established as the first facility to test 1MW class storage systems at a national lab

2011

Enabling Secure, Scalable Microgrids with High Penetration Renewables Grand Challenge

SSM

R&D100 Award Winners:
-Ultra-high-voltage Silicon Carbide Thyristor
-The Demand Response Inverter

2013

Sandia develops the DOE/SNL Global Energy Storage Database

2014

Grid Modernization Continuum established & Sandia participates in 29 GMLC projects

GRID MODERNIZATION LABORATORY CONSORTIUM

2015

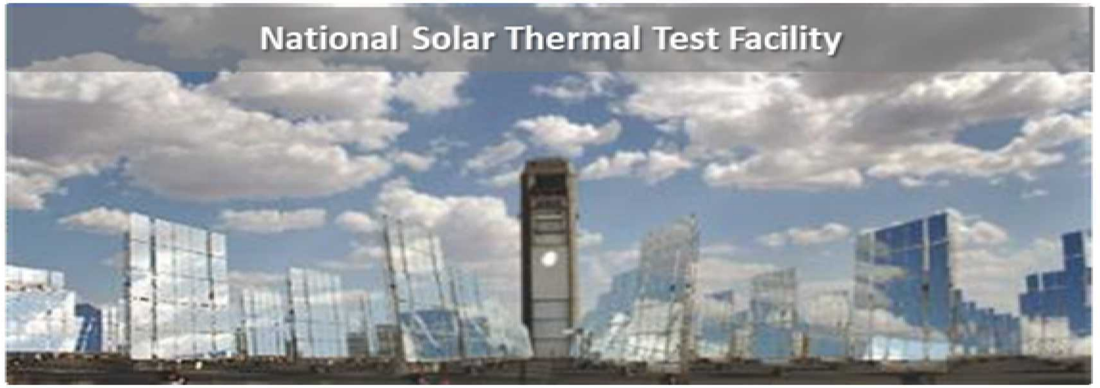
2015 R&D 100 WINNER

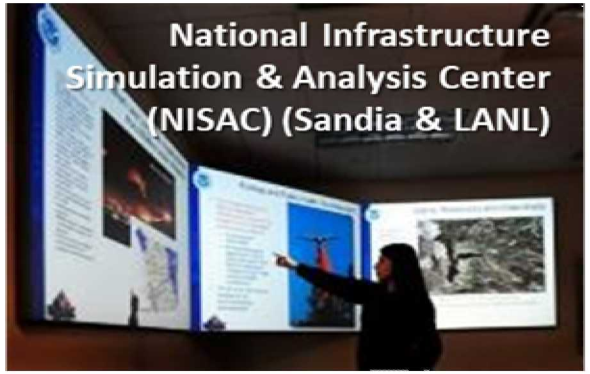
Sandia and United Silicon Carbide, Inc., create new high voltage switch

SIRFN established as Annex 5 of ISGAN

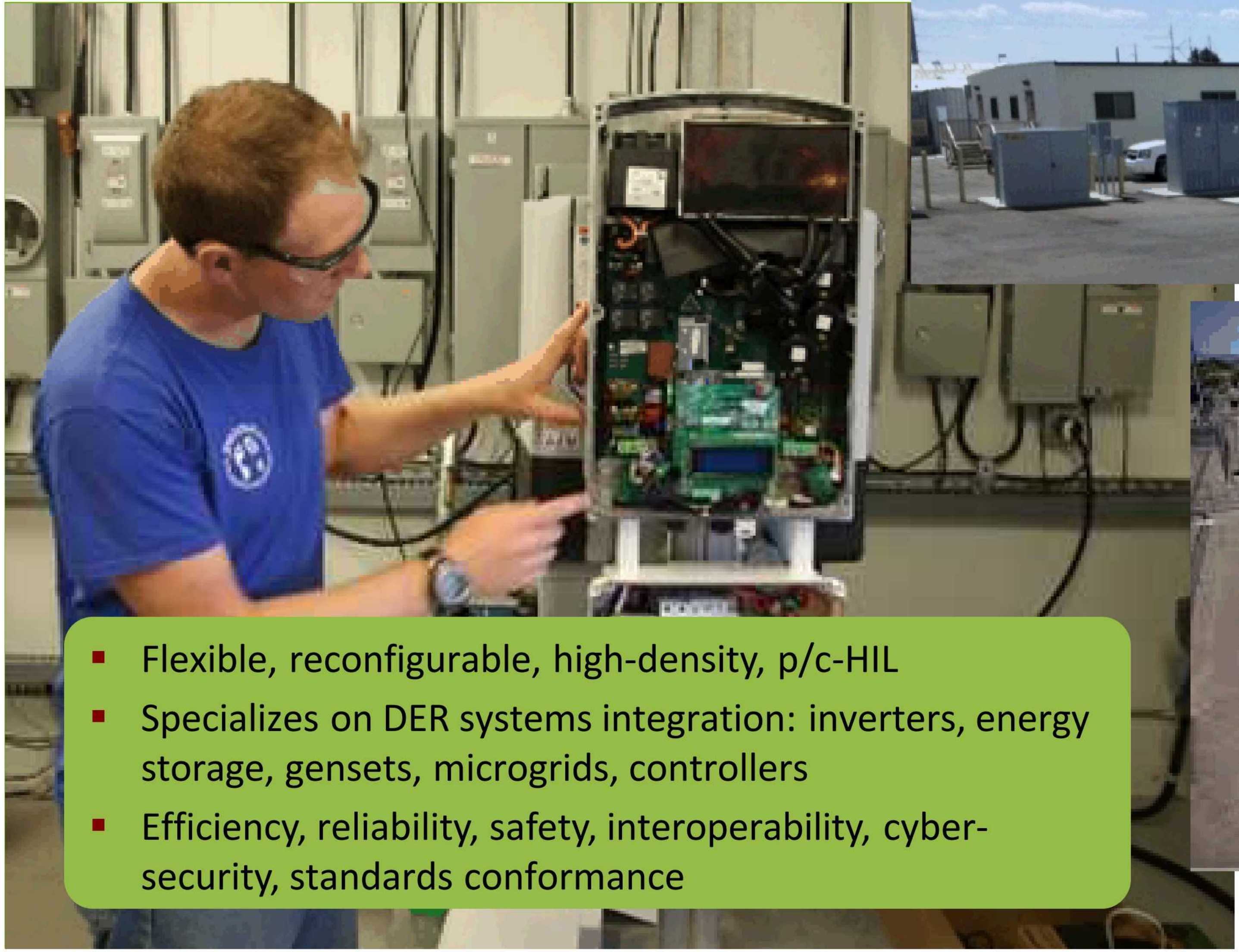
Microgrid Design Toolkit available

Energy-Related Research Platform





Distributed Energy Technologies Laboratory (DETL) Energy Storage Test Pad (ESTP)



- Flexible, reconfigurable, high-density, p/c-HIL
- Specializes on DER systems integration: inverters, energy storage, gensets, microgrids, controllers
- Efficiency, reliability, safety, interoperability, cyber-security, standards conformance

Sandia University Partnership Strategy

- Provide national leadership in science and engineering by establishing enduring partnerships with a focused set of universities.

Engage and develop talent

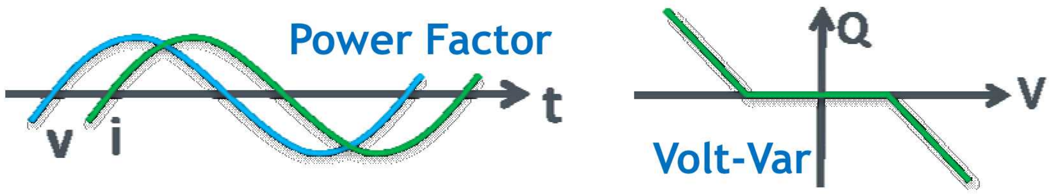
Develop joint IP and deploy new technologies

Conduct collaborative, mission-driven R&D

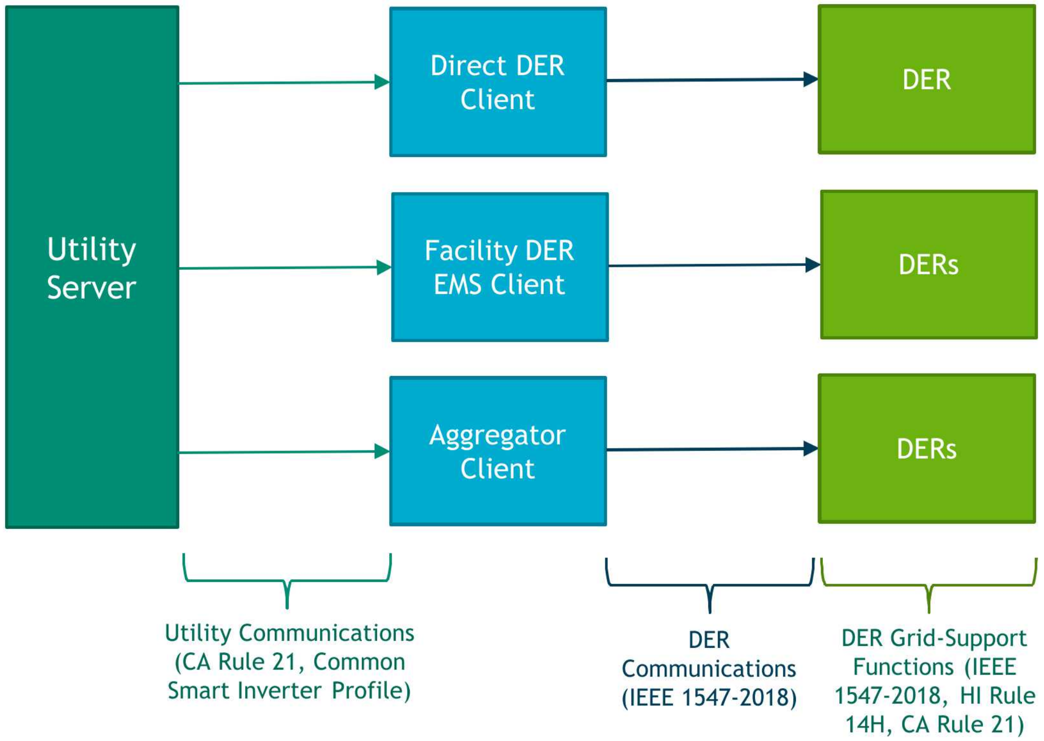
Motivation for Cyber-securing PV and DER

- Large-scale deployment of renewable energy is limited by power system constraints
  - These issues can be mitigated using inverter grid-support functions
  - Interconnection standards (e.g., HI Rule 14H) have been updated to standardize these functions
- The new national interconnection standard, IEEE Std. 1547-2018, also requires DER interoperability (communications)
  - Previously many DER devices communicated through proprietary protocols back to monitoring services ("security through obscurity"?)
  - Now common protocols (IEEE 2030.5, IEEE 1815, SunSpec Modbus) will be used by all DER devices
  - This is increasing the power system attack surface

Grid-Support Functions



DER Communications Options



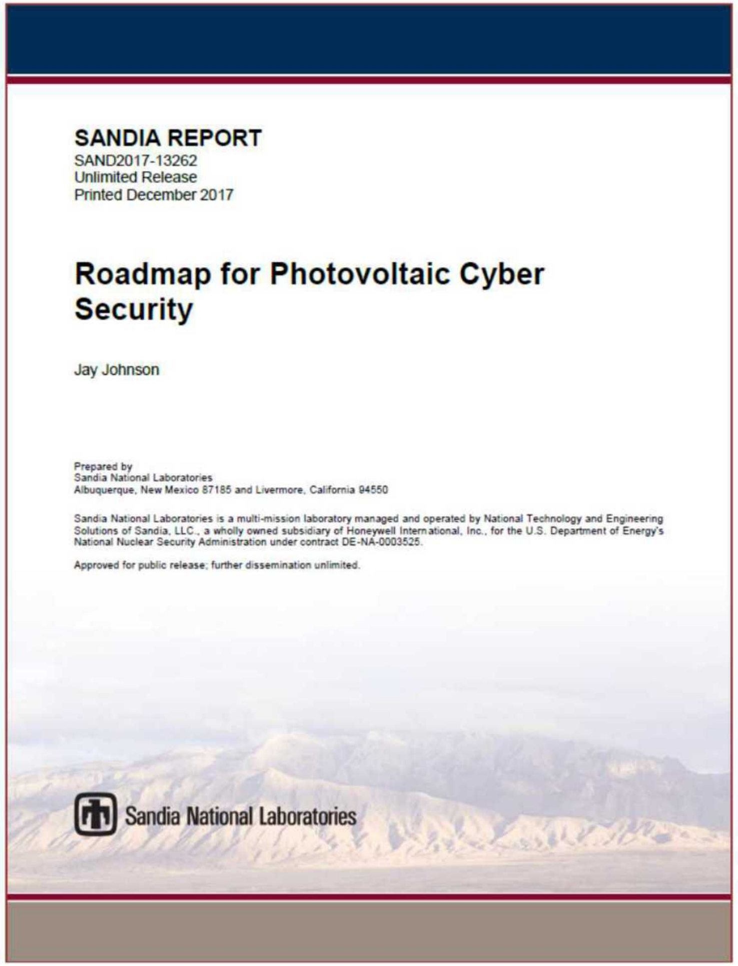
Roadmap for PV Cyber Security

❖ 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



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.

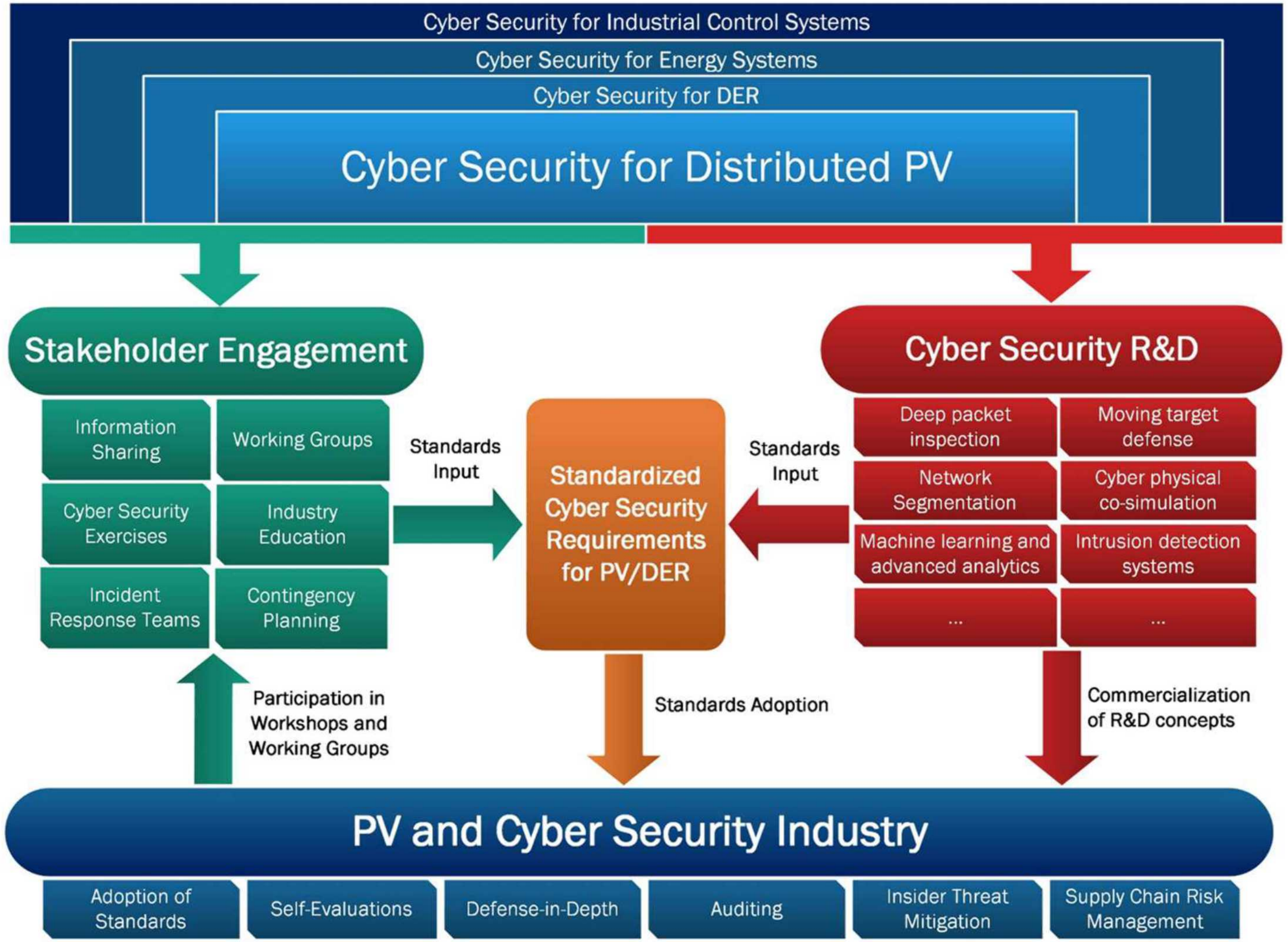
Approved for public release; further dissemination unlimited.

Sandia National Laboratories

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

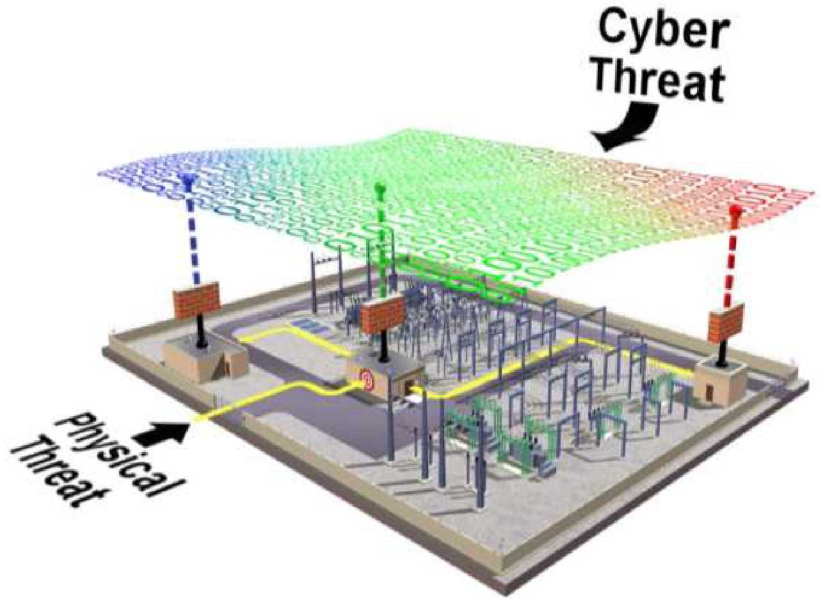
- Vision: By 2023, grid operators, system owners, and aggregators communicate with interoperable photovoltaic systems using safe, secure, resilient networks with high availability, data integrity, and confidentiality.
- **Focused on four areas**
  - Stakeholder Engagement
  - Research and Development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



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.

SunSpec/Sandia DER Cybersecurity Workgroup

- Started August 2017
- Over 300 participants from more than 50 organizations
- <u>Charter</u>: DER Cyber Security Working Group brings together DER interoperability and cyber security experts to discuss security for DER devices, gateways, aggregators, utilities and the US power system.
- <u>Primary Goal</u>: generate a collection of best practices that act as basis for (or input to) national or international DER cyber security standards.
- <u>Secondary Goal</u>: facilitate DER cyber security discussions between stakeholders to exchange perspectives and gain broad buy-in from the industry.



DER Cybersecurity Workgroup Structure

SunSpec/Sandia DER Cybersecurity Workgroup

DER Devices & Servers — Active
- **Define standardized procedure for DER and server vulnerability assessments.**
- Leads: Danish Saleem (NREL) and Cedric Carter (MITRE)
- Cases advised from known equipment vulnerabilities
- Transferring to UL STP (likely new UL Std. 2900-2-4)

Secure Network Architecture — Active
- **Create DER control network topology requirements and interface rules.**
- Lead: Candace Suh-Lee (EPRI)
- Perimeter controls
- Segmentation requirements

Data-in-Flight Requirements — Just Started
- **Define common set of encryption, authentication, and key management requirements for DER communications.**
- Leads: Nicholas Manka (GridSME) and Ifeoma Onunkwo (Sandia)
- Update protocol and interconnection std. requirements

Access Controls — Later
- **Classify data types, associated ownership, and permissions. Define set of protection mechanisms.**
- Starting Oct 2019. Lead: TBD
- Access control list taxonomy, principle of least privilege
- Password control and data privacy expectations

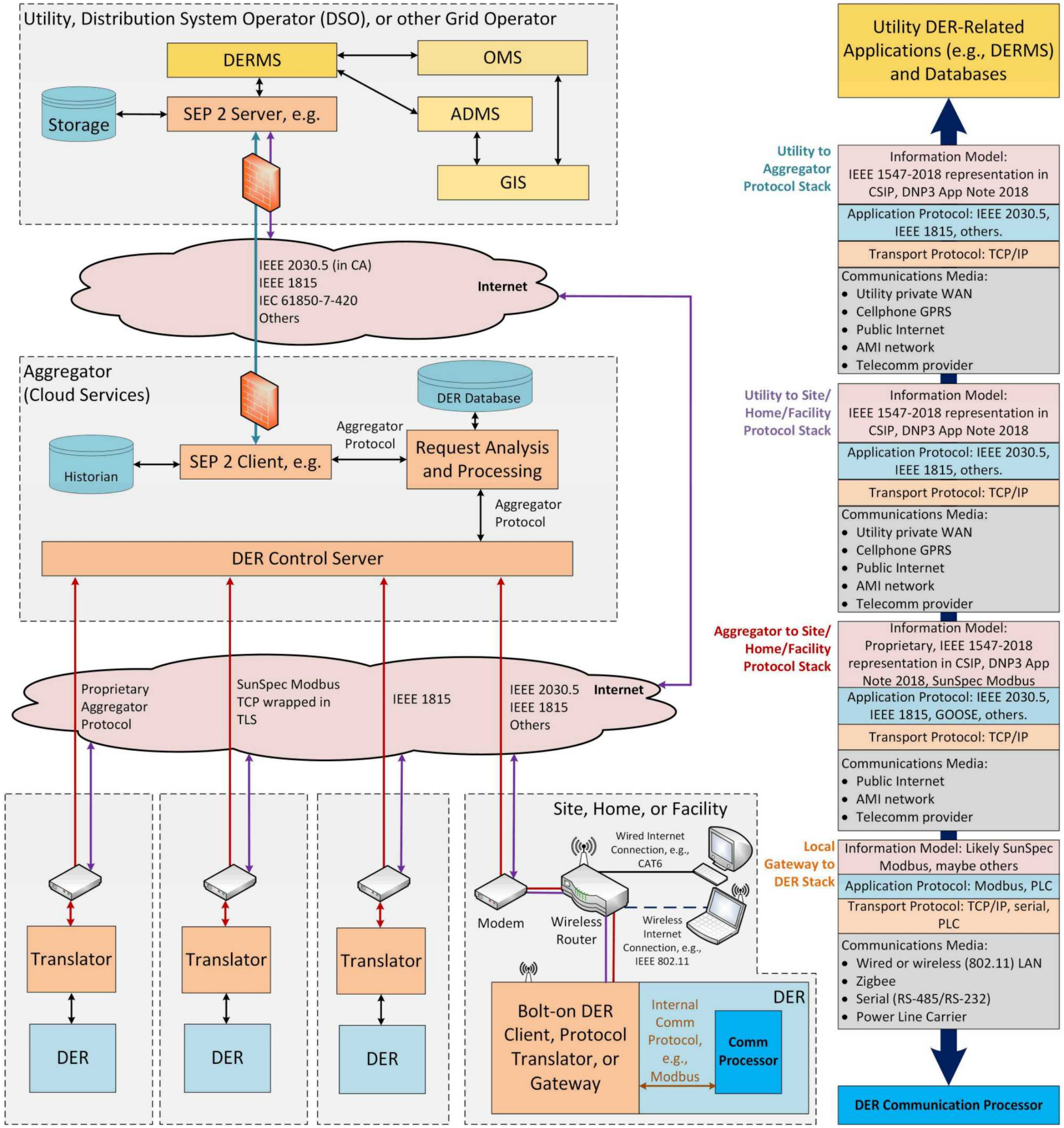
Patching Requirements — Later
- **Establish patching guidelines for DER equipment.**
- Starting Oct 2019. Lead: TBD
- Requirements for patching (e.g., update rates, expected mitigation timelines)
- Maintenance guidelines

Utility/Aggregator Auditing Procedure — Much Later
- **Create recommended auditing practices for DER networks.**
- Planned for Oct 2020. Lead: TBD
- Step-by-step auditing procedure for internal or external compliance review. Recommend data for forensics.

Sign up at http://sunspec.org/sunspec-cybersecurity-workgroup/

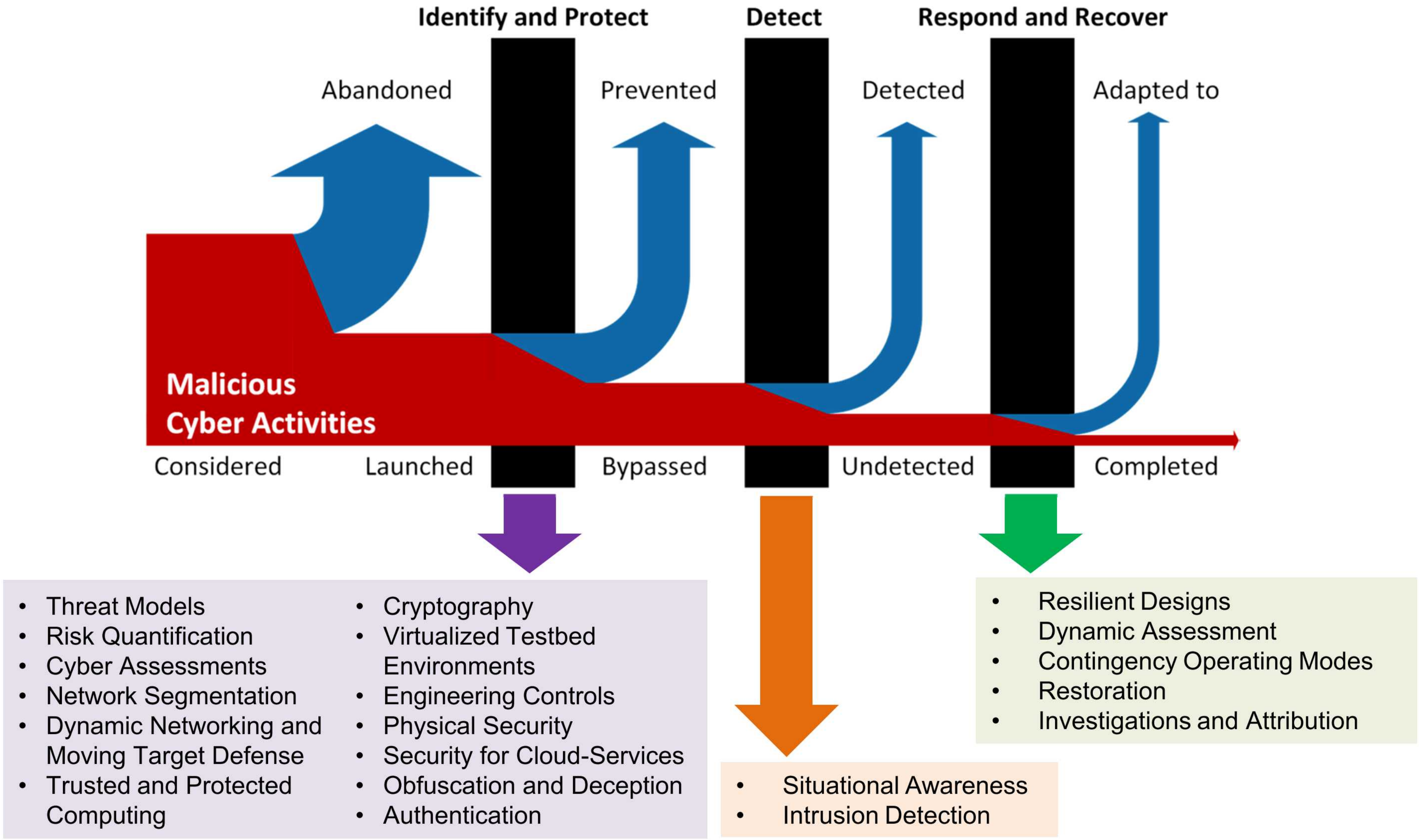
DER Communication Protocols

- **Many paths between utilities and DER**
- **Multiple DER communication protocol options**
  - Physical media could be serial, PLC, Internet, cell, AMI, etc.
  - Transport will mostly be TCP/IP between utility and DER site, home, facility
  - Application layer defined by IEEE 2030.5, IEEE 1815, Modbus
  - Information models: IEC 61850-90-7, SunSpec, CSIP, DNP3 App Note.
- **DER communication protocol basics and standards are covered in:**
  - C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, J. Johnson, "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators," Sandia Technical Report, SAND2017-13113, Dec 2017.
- **Data-in-flight encryption and trust recommendations for IEEE 2030.5 are described in:**
  - J. Obert, P. Cordeiro, J. Johnson, G. Lum, T. Tansy, M. Pala, R. Ih, “Recommendations for Trust and Encryption in DER Interoperability Standards,” Sandia Technical Report, SAND2019-1490, Feb 2019.



DER Cybersecurity R&D

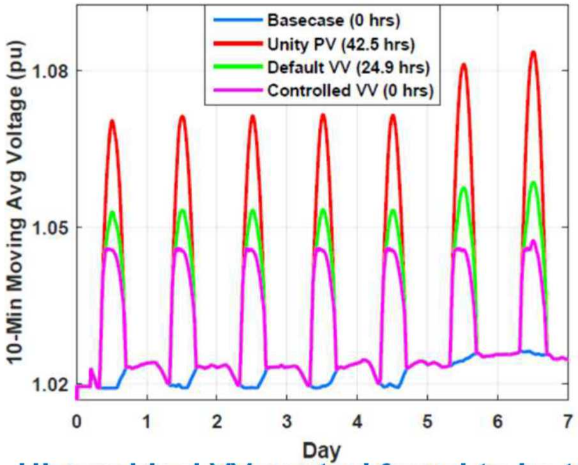
- Example: “Secure, Scalable Control and Communications for Distributed PV” project investigating cybersecurity implications of communications-enabled DER control.
    - Goal: Find optimal network architecture by quantifying tradeoffs between cybersecurity and communication latency/power system performance
    - Project also studied the impact to the power system under different cyber attack scenarios to quantify risk and quantify defensive strategies.

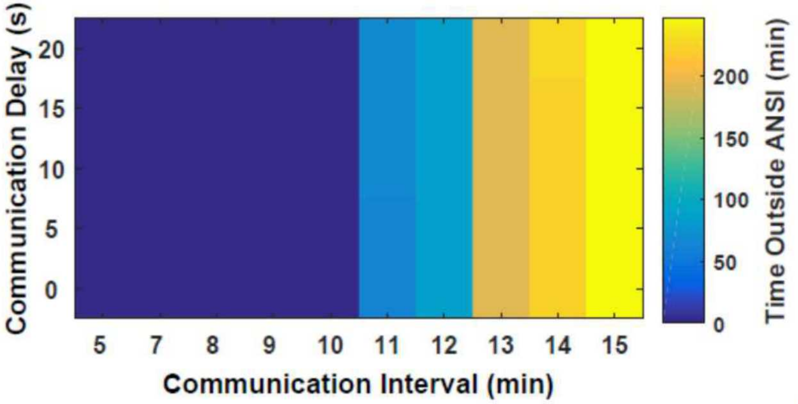


More details in “Roadmap for Photovoltaic Cyber Security” (SAND2017-13262), which outlines a 5-year strategy for DOE, industry, and standards development organizations in areas of Identify/Protect, Detect, and Respond/Recover.

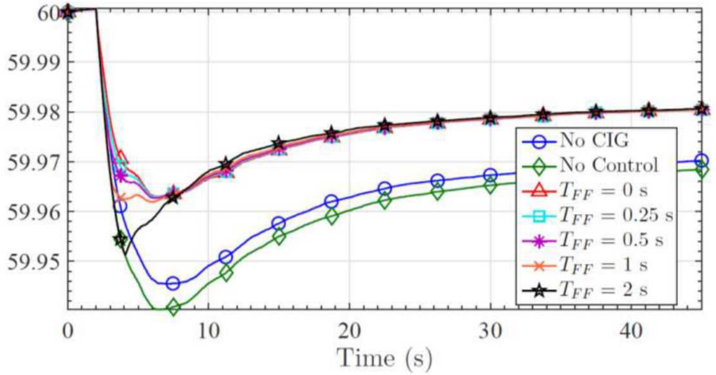
DER Network Quality of Service vs Grid Performance

- Project investigated how network topology/security features change communication speed and power system behavior
- Multiple communications-enabled DER control approaches were simulated:
  - Synthetic inertia
  - Communication enabled fast acting imbalance reserve
  - Communication enabled frequency droop
  - Hierarchical control of volt-var (VV) function
- Power system metrics determined for each control case varying DER availability and communication latency.
  - Transmission services impacted with latencies between 0.1 and 10 seconds, depending on the gains
  - Distribution services not impacted for latency below 20 seconds

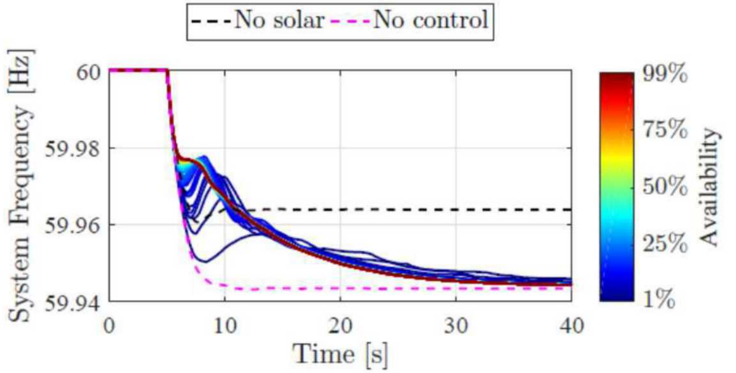




Hierarchical VV control found to be tolerant of communication delays up to 20 s [1-2].



Communications Enabled – Fast Acting Imbalance Reserve (CE–FAIR) delays caused lower frequency nadirs [3].

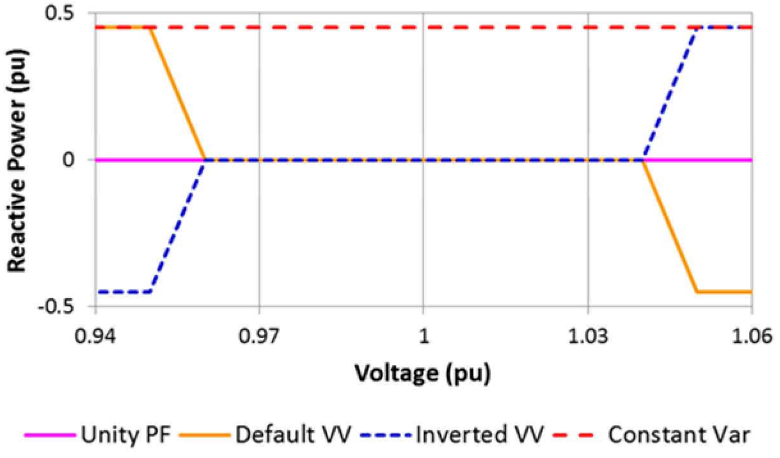


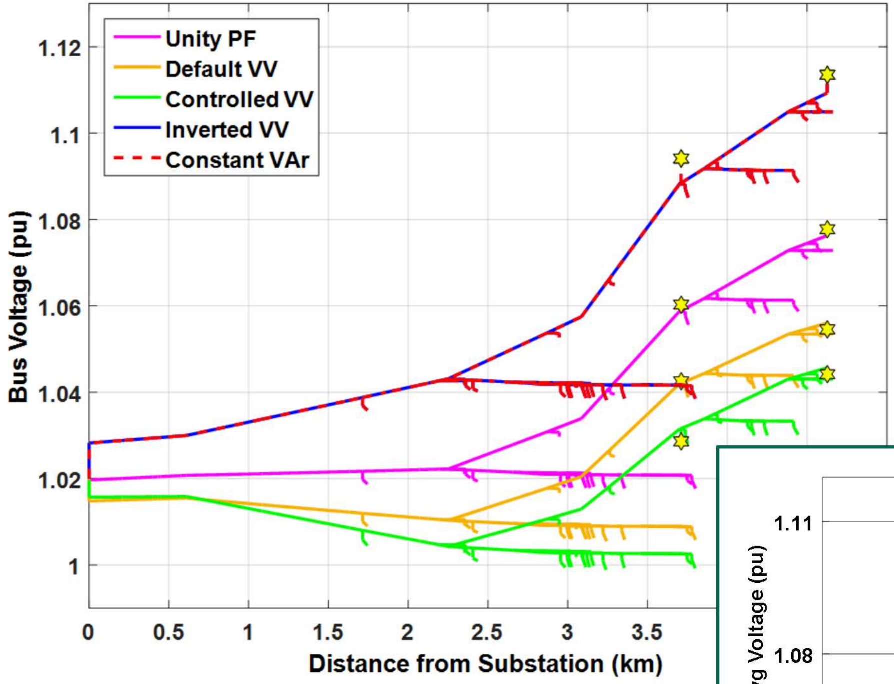
Communications Enabled Synthetic Inertia Controller transient response with different DER availabilities [4].

1. J. E. Quiroz, M. J. Reno, O. Lavrova, R. H. Byrne, "Communication requirements for hierarchical control of volt-VAr function for steady-state voltage," IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, 2017.
2. M. Reno, J. Quiroz, O. Lavrova, and R. Byrne, "Evaluation of Communication Requirements for Voltage Regulation Control with Advanced Inverters," IEEE North American Power Symposium, Denver, CO, September 2016.
3. R. Concepcion, F. Wilches-Bernal, R. Byrne, "Effects of Communication Latency and Availability on Synthetic Inertia," IEEE ISGT 2017, Arlington, VA, April 23-26, 2017.
4. F. Wilches-Bernal, R. Concepcion, J. Neely, R. Byrne, and A. Ellis, "Communication Enabled Fast Acting Imbalance Reserve (CE-FAIR)," IEEE Transactions on Power Systems.

…but what if the DER equipment were maliciously controlled?

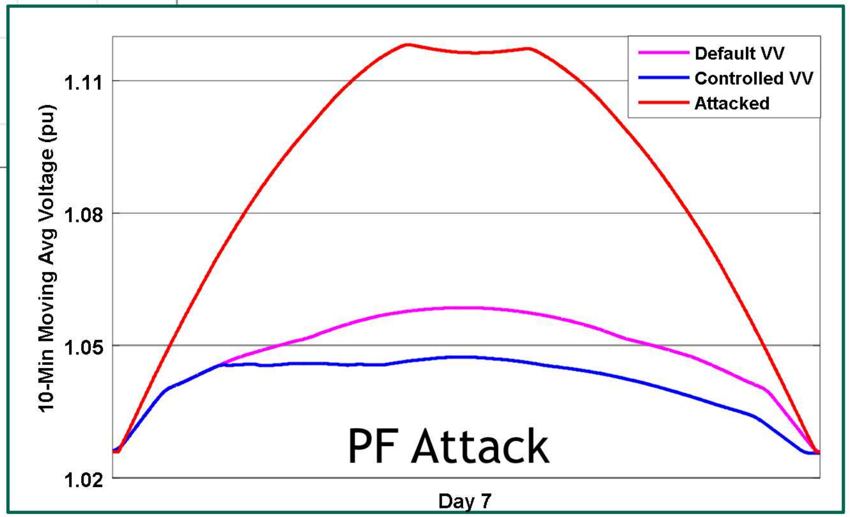
- Team investigated advanced control functions developed in this project and then extrapolated them to standard control functions defined in IEEE 1547-2018, IEC 61850-90-7, CA Rule 21, etc.
- Volt-var, power factor, and constant reactive power examples:





Result: distribution feeder experiences substantially higher voltages (above the ANSI range B limits), tripping the DER on HVRT, and possibly leading to localized outages if enough generation trips.

Attack: volt-var function is inverted to inject reactive power at high voltage and absorb reactive power at low voltage. PF and VV13 attacks lead to constant reactive power injection.

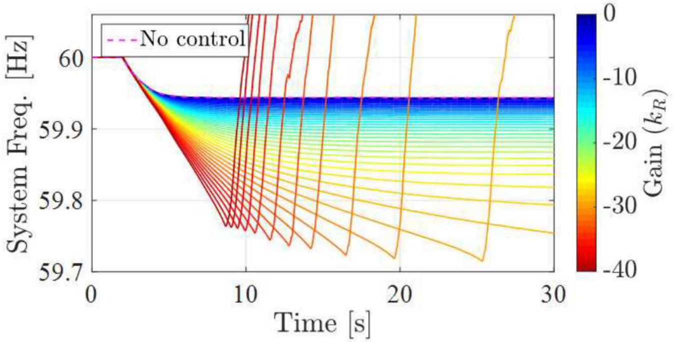


Transmission Cases

- Frequency Droop

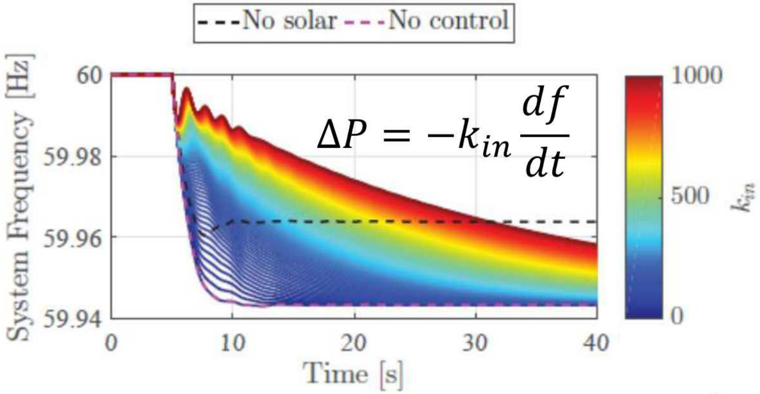
$$\Delta P_j = \frac{f_{ref} - f_{eq}}{R} = k_R(f_{ref} - f_{eq})$$

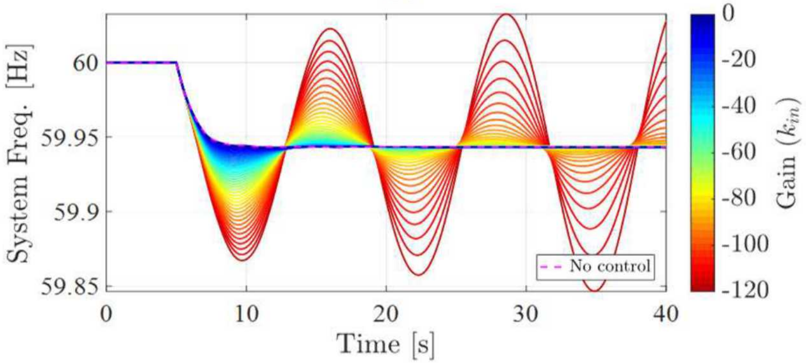
$$\Delta P_j^{attack} = -\frac{f_{ref} - f_{eq}}{R} = -k_R(f_{ref} - f_{eq})$$



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

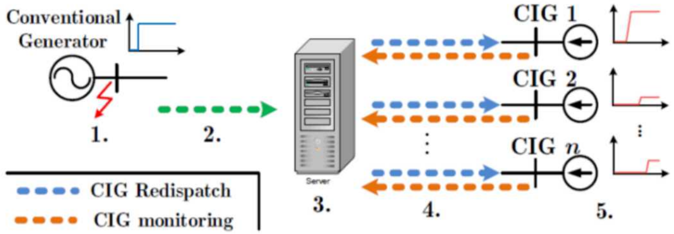
- Synthetic Inertia





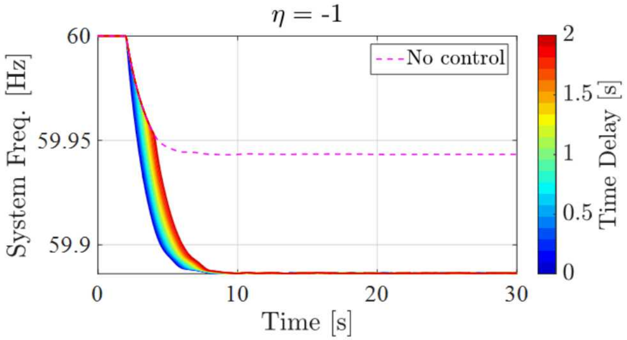
Attack: reverse sign on inertial gain to create positive feedback.
Result: Nadir is reduced and oscillatory behavior in the power system is created, leading to instability and possible blackouts.

- 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, η, is set to reduce the power by the magnitude of the imbalance. In an attack: η=-1.
Result: Imbalance is worsened, possibly leading to a blackout.

Extrapolating to additional DER grid-support functions

- Based on power system studies, estimated aggregated control risk from DER grid-support functions.
  - Low risk: limited power system impact
  - Medium risk: regional voltage effects or localized loss of load (brownouts)
  - High risk: bulks system power outages

Grid-support function	Risk	Cause
Frequency Ride-Through (FRT) Trip Settings	High	Tight FRT trip settings cause DER power loss with minor frequency deviations
Voltage Ride-Through (VRT) Trip Settings	High	Tight VRT trip settings cause DER power loss from minor voltage deviations
Normal Ramp Rate (RR)	Low	Fast RR requires faster regulation but minimal power system impact
Soft-Start Ramp Rate (SS)	Low	Fast SS requires faster down-regulation but minimal power system impact
Frequency-Watt (FW)	High	Improperly programmed FW curves cause DER power loss, possibly resulting in a blackout
Voltage-Watt (VW)	High	Improperly programmed VW curves cause DER power loss, possibly resulting in a blackout
Connect or Disconnect (INV1)	High	Aggregate DER power loss could cause blackout
Limit Max Real Power (INV2)	High	Aggregate DER power loss could cause blackout
Power Factor (INV3)	Medium	Extreme voltage conditions, DER will trip on VRT trip settings, possibly leading to outages*
Volt-Var mode (VV)	Medium	Extreme voltage conditions, DER will trip on VRT trip settings, possibly leading to outages*
Watt-Power Factor (WP)	Medium	Extreme voltage conditions, DER will trip on VRT trip settings, possibly leading to outages*
Fixed Reactive Power	Medium	Extreme voltage conditions, DER will trip on VRT trip settings, possibly leading to outages*

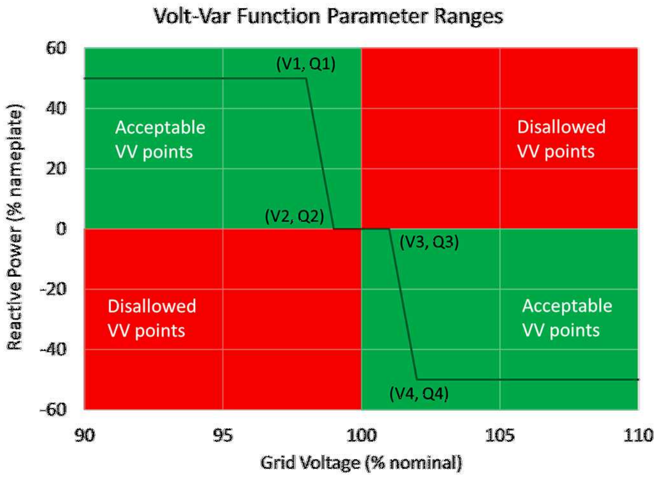
* These scenarios are difficult to predict. DER will trip on overvoltage, thereby mitigating some of the voltage issues. Current-based protection systems will not isolate portions of the feeder. However, if enough distributed generation is tripped in high penetration environments (e.g., HI), bulk system impacts could occur.

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, Jan 2019, DOI: 10.1049/iet-cps.2018.5014.

Creating solutions: a snapshot of some activities

Engineering Controls

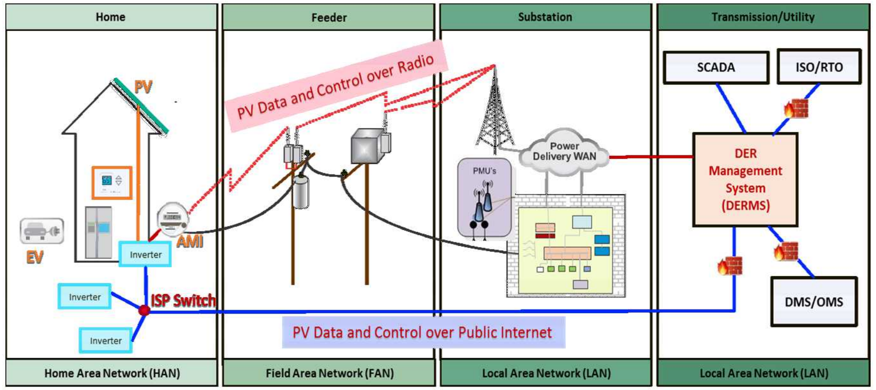
Concept: Create rules for information models/communication protocols or DER to reject grid-support parameters that are known to cause system instability or other grid problems.



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.

Data-in-flight Security

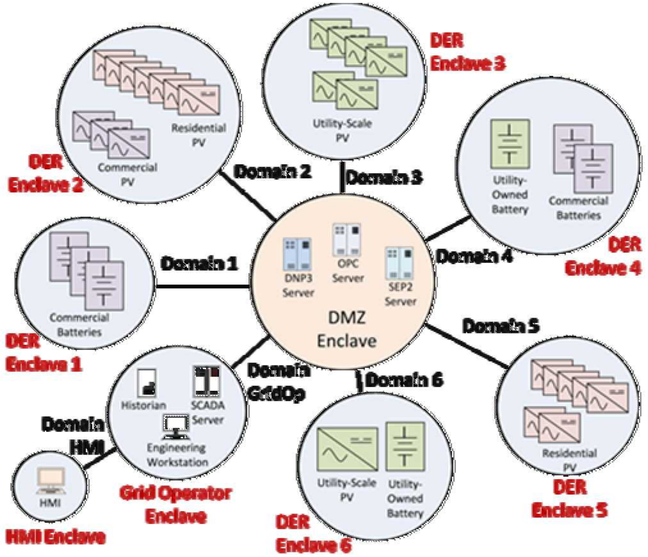
Concept: For DER traffic transmitted on the public internet, overlay TLS security on top of SunSpec Modbus or create a RESTful web services option for IEEE 1547, CA Rule 21, and other information model requirements.



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.

Enclaved DER Topologies

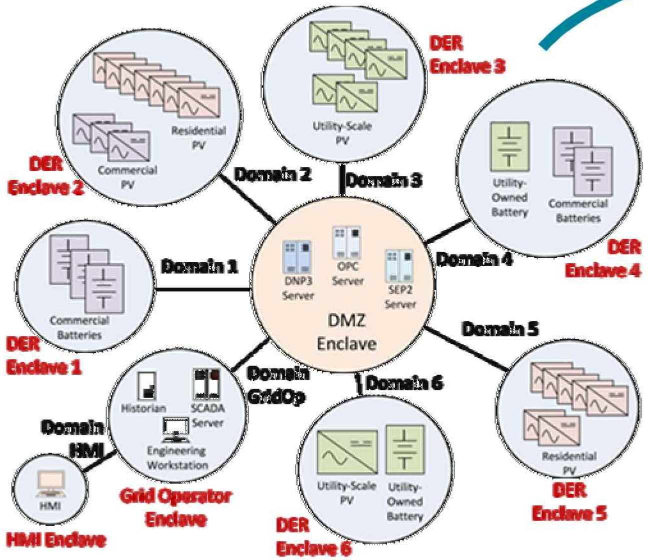
Concept: Create DER enclaves with firewall rules, VPNs, or proxies so an adversary cannot control all DER devices if an enclave is compromised.

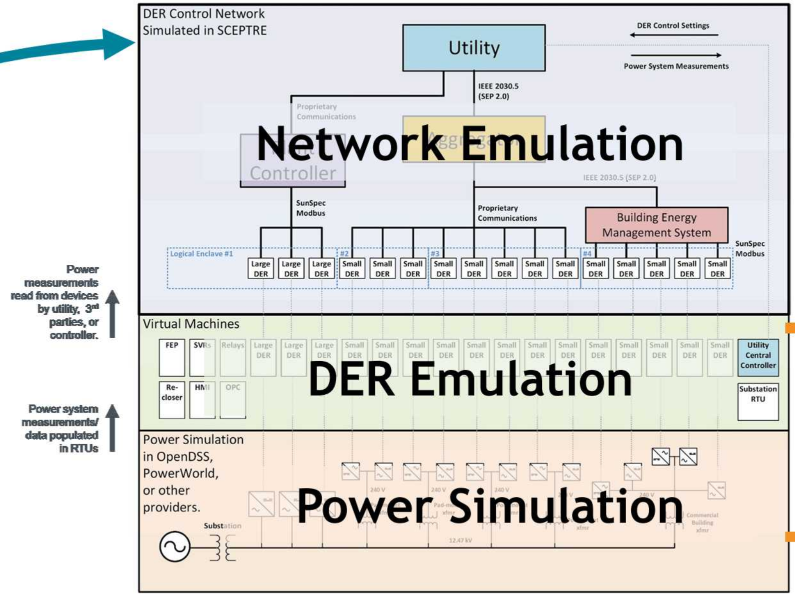


On-going work: DER Cyber Security Working group is creating recommended data architectures for utilities and DER aggregators. Also, Sandia measuring cyber metrics of different topologies with red teaming activities.

Tying cybersecurity design to grid performance

DER control network architectures are emulated in the SCEPTRE environment.





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

SCEPTRE outputs:

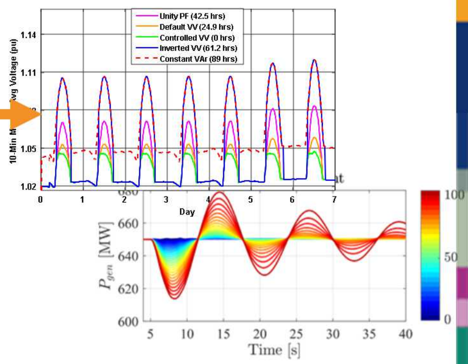
- Cybersecurity metrics
- Communication parameters
- Power system performance

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

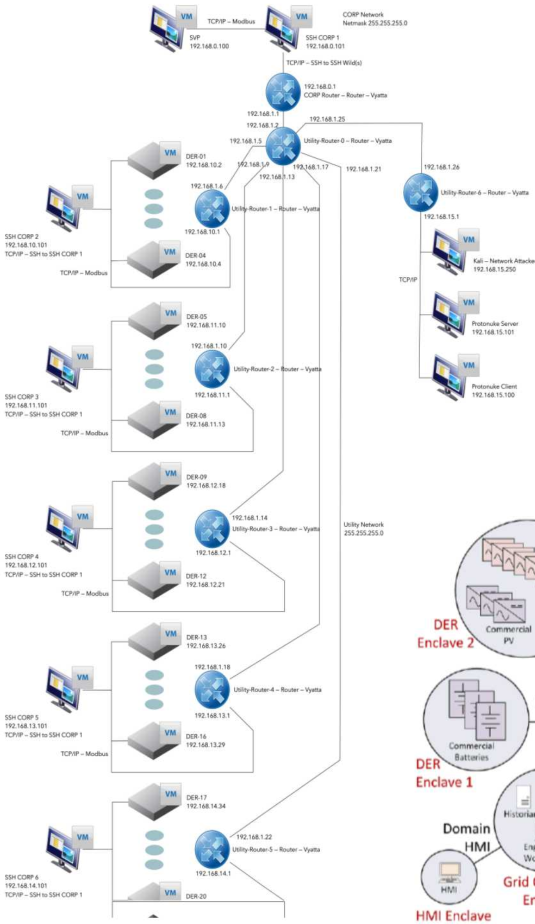


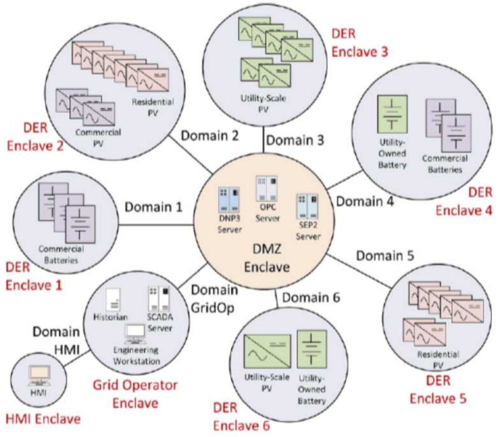
Multiple DER network architectures will be simulated to determine:

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

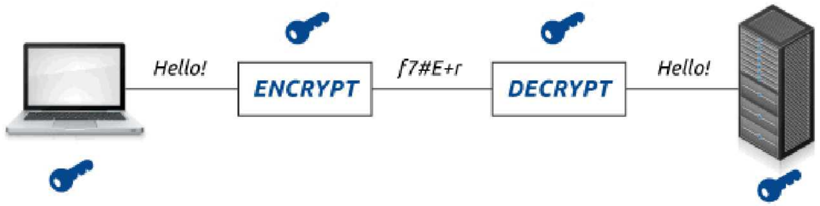
Cybersecurity Features Implemented in SCEPTRE

1. Segmentation

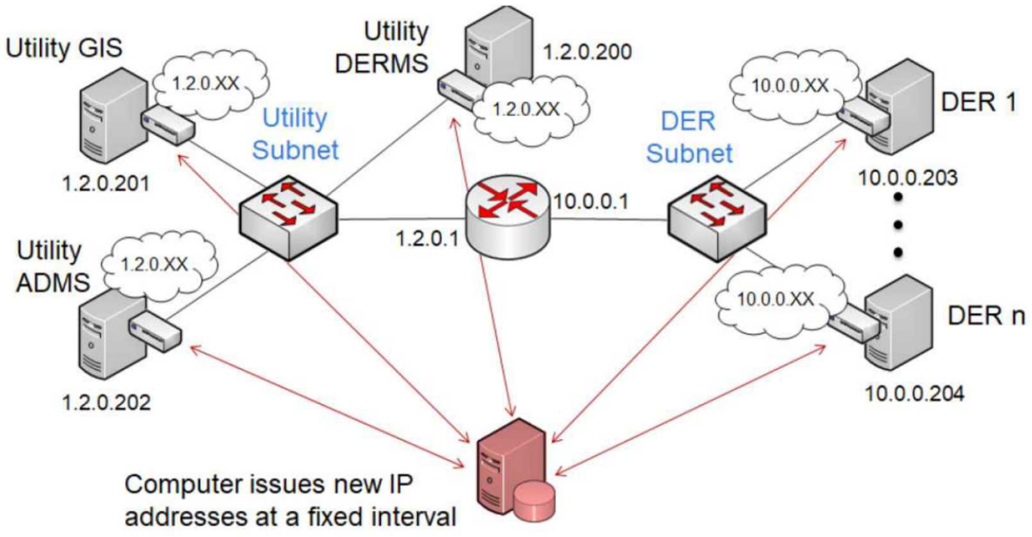




2. Encryption



3. Moving Target Defense



Red Team Assessments

- Red Team conducted the following:
  - **Reconnaissance**: inspecting the system to determine IP address, IP ports, slave ID, protocols, etc.
  - **Fabrication**: fake messages were inserted into the network and were successfully replayed.
  - **Interception**: Man-in-the-Middle (MITM) or eavesdropping of authenticated communications to read and possibly alter data communications.
  - **Interruption**: Denial of Service (DoS) was used in rendering the system unusable to authorized users, for example, by overloading the RTU processors.
- For each scenario, the DER communication network was evaluated for vulnerabilities to DoS, Replay, and MITM attacks. Risk scores were then calculated for:
  - Confidentiality based on the replay and MITM attacks
  - Integrity based on the replay and MITM attacks
  - Availability based on the DoS attack
  - A total risk score (3-15) for the given security features

This assessment leveraged prior DER device assessment experiences from 2017

DER Cyber Assessment Comparison

	Device A	Device B
Protocol	UDP/IP	TCP/IP
Analyzed Interface	Ethernet	Ethernet
Reconnaissance	✓	✓
Packet Replay	x	o
MiTM	x	x
DoS	x	x
Mod Firmware	o	o
Prevalent Logs	x	x
Password Handling	x	x

x = Exploits Exist, ✓= Successful, o = Incomplete

Details of the vulnerabilities were shared with the DER vendors to improve their cybersecurity practices.

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

Theoretical vs Actual Security Scores for Different Security Defenses

If properly implemented, the following results were expected:

Topology	Encryption	Access	Attacks			Risk Level			Total Score
			DoS	Replay	MITM	C	I	A	
Flat	None	Insider	✓	✓	✓	5	5	5	15
Flat	None	Outsider	✓	✓	✓	5	5	5	15
Flat	RFC 7539	Insider	✓			1	1	5	7
Flat	RFC 7539	Outsider	✓			1	1	5	7
Segmented	None	Insider	✓	o	o	3	3	4	10
Segmented	None	Outsider	✓			2	2	3	7
Segmented	RFC 7539	Insider	✓			1	1	4	6
Segmented	RFC 7539	Outsider	✓			1	1	3	5
Flat MTD	None	Insider	✓			1	1	5	7
Flat MTD + WL	RFC 7539	Outsider				1	1	2	4
Seg MTD + WL	RFC 7539	Outsider				1	1	2	4

- ✓ indicates the attack is possible for all DER devices
- o indicates the attack could succeed for a portion of the DER devices
- WL indicates whitelisting of the MTD network
- RFC 7539 is the IETF Protocol for the ChaCha20 stream cipher and Poly1305 authenticator

The red team was able to subvert the environments and found the following:

Topology	Encryption	Access	Attacks			Risk Level			Total Score
			DoS	Replay	MITM	C	I	A	
Flat	None	Insider	✓	✓	✓	5	5	5	15
Flat	None	Outsider	✓	✓	✓	5	5	5	15
Flat	RFC 7539	Insider	✓	✓	✓	5	5	5	15
Flat	RFC 7539	Outsider	✓	✓	✓	5	5	5	15
Segmented	None	Insider	✓	✓	✓	5	5	5	15
Segmented	None	Outsider	✓	✓		5	5	5	15
Segmented + PHIL	None	Outsider	✓	✓		5	5	5	15
Segmented	RFC 7539	Insider	✓	✓	✓	5	5	5	15
Segmented	RFC 7539	Outsider	✓	✓	o	5	5	5	15
Flat MTD + WL	None	Insider	✓			1	1	5	7

- ✓ indicates the attack is possible for all DER devices
- o indicates the attack could succeed for a portion of the DER devices
- WL indicates whitelisting of the MTD network
- RFC 7539 is the IETF Protocol for the ChaCha20 stream cipher and Poly1305 authenticator

- Results show the importance of properly deploying security features.
  - The bump-in-the-wire device creating the RFC 7539 SSH tunnel was left unsecured (no password), which enabled the red team to pivot into the rest of the network and attack all the DER devices using replay and MITM attacks.

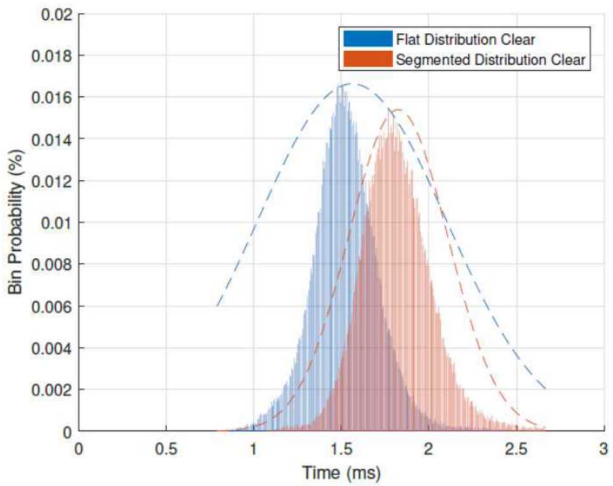
I. Onunkwo, B. Wright, P. Cordeiro, N. Jacobs, C. Lai, J. Johnson, T. Hutchins, W. Stout, A. Chavez, B. T. Richardson, K. Schwalm, "Cybersecurity Assessments on Emulated DER Communication Networks," SAND2019-2406, March 2019.

Conclusions from the Red Team Assessments

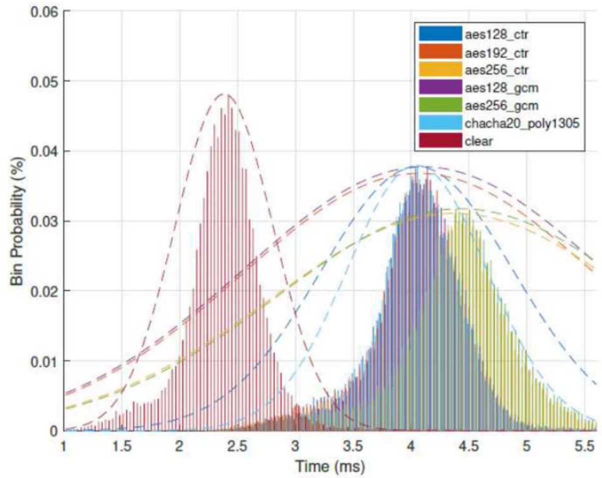
- Denial of service is very difficult to prevent. Aggregators/utilities should implement firewall whitelists to prevent these types of attacks.
- Segmentation makes it difficult for the adversary to move between subnets. Only through flaws in the networking implementation could the red team manipulate all DER devices.
- Encryption between the DERMS and DER drastically reduces the risk of Replay and MITM attacks.
- MTD has the potential to drastically improve security for DER networks, but this is still an area of research.
- It is important that developers add layers of defense by reviewing and pushing secure code to applications.

Latency from Network Security Features vs Device/Network Delays

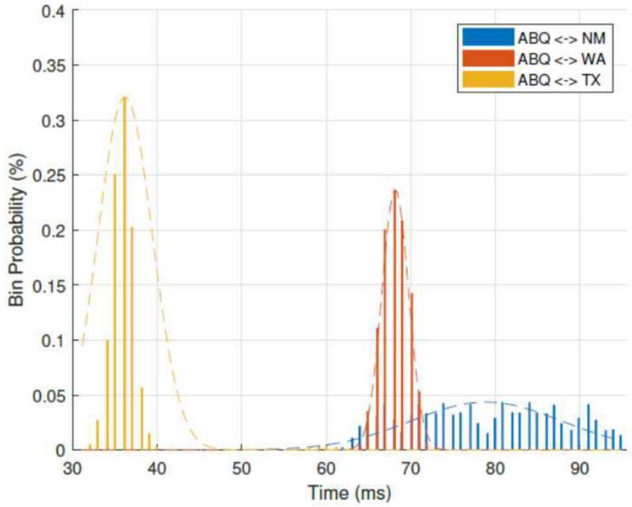
- Increased latency when adding segmentation, encryption, and moving target defense is minimal
  - In prior work, it was found that MTD increased the average latency **<1 ms** but caused slightly higher dropout rates (approx. 1 dropout per 33.3 seconds with IP randomization every 3 seconds) [1]
- Architecture (switch and router hops) and communication medium (copper vs. fiber) is more important to data-in-fight times than geographic separation
  - Connection to TX is over a dedicated fiber line and has minimal network hops.
  - NM PMU has numerous routers and switches in the communication path which slow down the packets.
- DER Modbus Read/Write times vary significantly. Sometimes taking over 1 second!



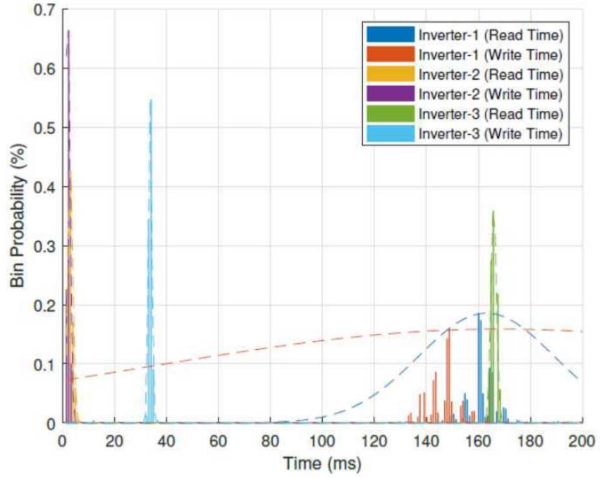
Segmenting the network leads to ~**1 ms** of additional latency



Encryption adds ~**3-5 ms** of additional latency



Latency from GPS timestamps from 1-way PMU data exchange



1000 Modbus read and write times for two commercially available residential-scale DER devices and one CHIL device

[1] A. R. Chavez, J. R. Hamlet, and W. Stout, “Artificial diversity and defense security (ADDSec) Final Report," Tech. Rep. SAND2018-4545, Sandia National Laboratories, April 2018.

Will adding security features to DER networks compromise performance?

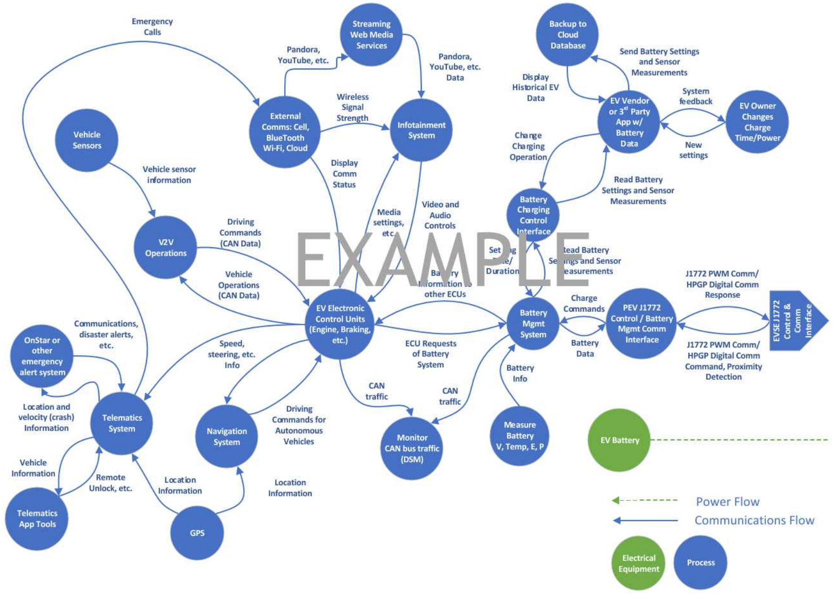
- **Device and network latency is large**
  - Network topology, media, and geographic distances have the possibility of adding 50-100 ms of latency for utility-to-DER communications
  - DER read and write times vary widely. They can be 1+ seconds in some situations.
- **Additional latency from security features is relatively small**
  - Network segmentation adds less than 1 ms
  - Encryption adds on the order of 3-5 ms of additional latency
  - MTD adds 1 ms of latency
- **Finding**: For the proposed cybersecurity features, it is not believed they will impact the grid-support service performance since they add only contribute a minor percentage of the total latency between the utility and DER.

Recommendations for Future Research

- Understand the Risk
  - Create generalized threat model (e.g., using STRIDE modelling) for PV systems that includes utilities, aggregators, and DER vendors
  - Continue to red team equipment and investigate firmware-level vulnerabilities in DER devices
  - Expand power system simulations of "nightmare" attacks
- Harden Networks
  - Create Intrusion Detection System (IDS) technologies for aggregators and grid operators
  - Develop power system fallback operating modes under cyber attacks or low communication scenarios
  - Use virtualized networks with DER emulation to study new defense technologies, e.g., Moving Target Defense
- Harden DER equipment
  - Deploy Trusted Platform Modules (TPMs) or Secure Elements to securely store DER cryptographic keys
  - Use Physical Unclonable Functions (PUFs) to provide authentication for network nodes
  - Investigate software obfuscation to disguise DER functionality from reverse engineers
  - Prevent unauthorized tampering of executable code over the network with TrustZone or Mobile Trusted Modules (MTMs)

Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

STRIDE Threat Model for PEV Charging (Vehicle Side)



aellis@sandia.gov, 505-844-7717