Cybersecurity for DER Devices

PV Systems Symposium

May 14-16, 2019

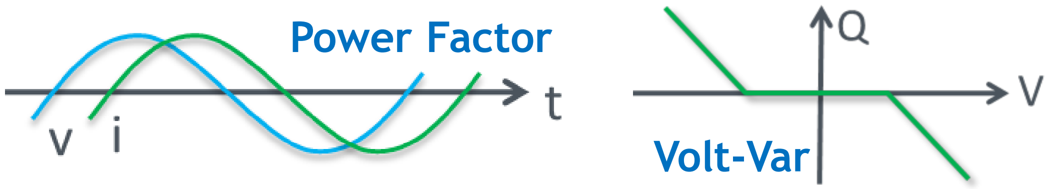
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Jay Johnson
Renewable and Distributed Systems Integration
Contact: 505-284-9586 / jjohns2@sandia.gov

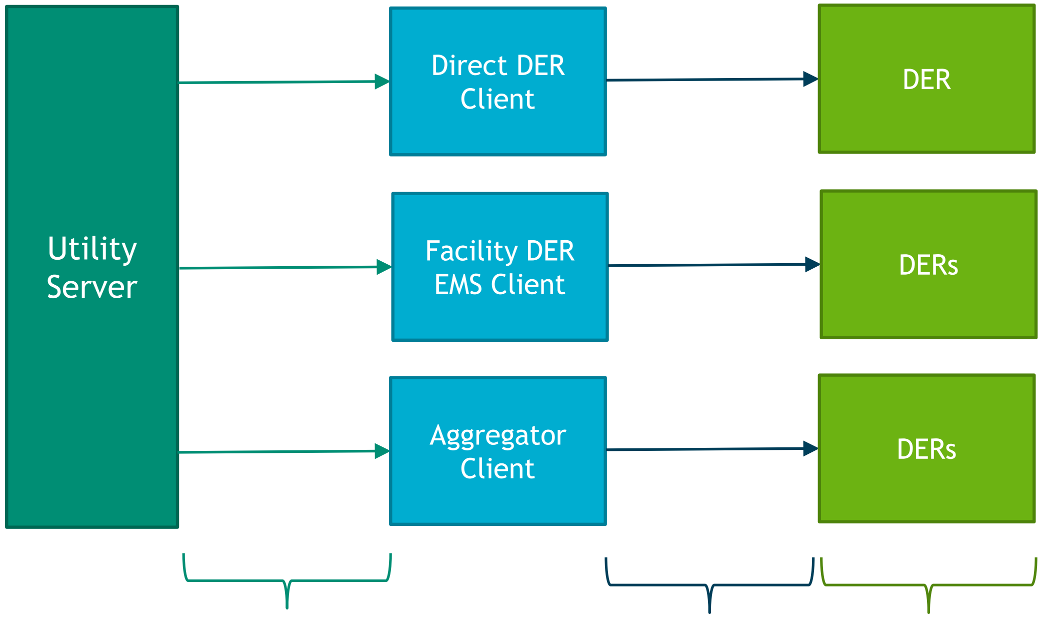
Background

- 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



Utility Communications (CA Rule 21, Common Smart Inverter Profile)

DER Communications (IEEE 1547-2018)

DER Grid-Support Functions (IEEE 1547-2018, HI Rule 14H, CA Rule 21)

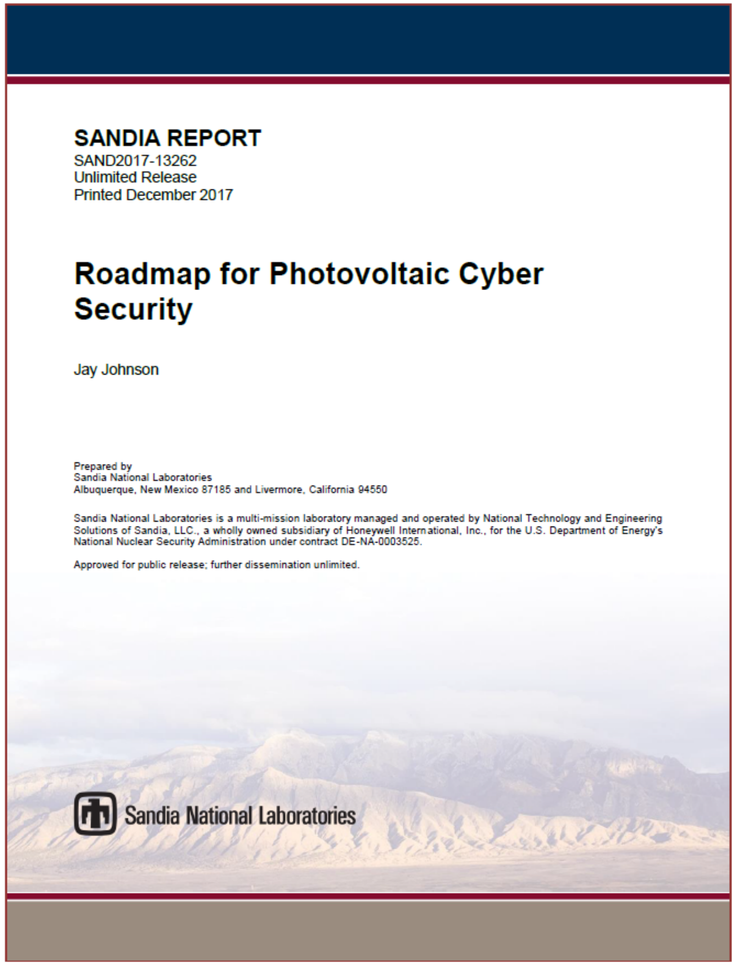
Roadmap for PV Cyber Security

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.

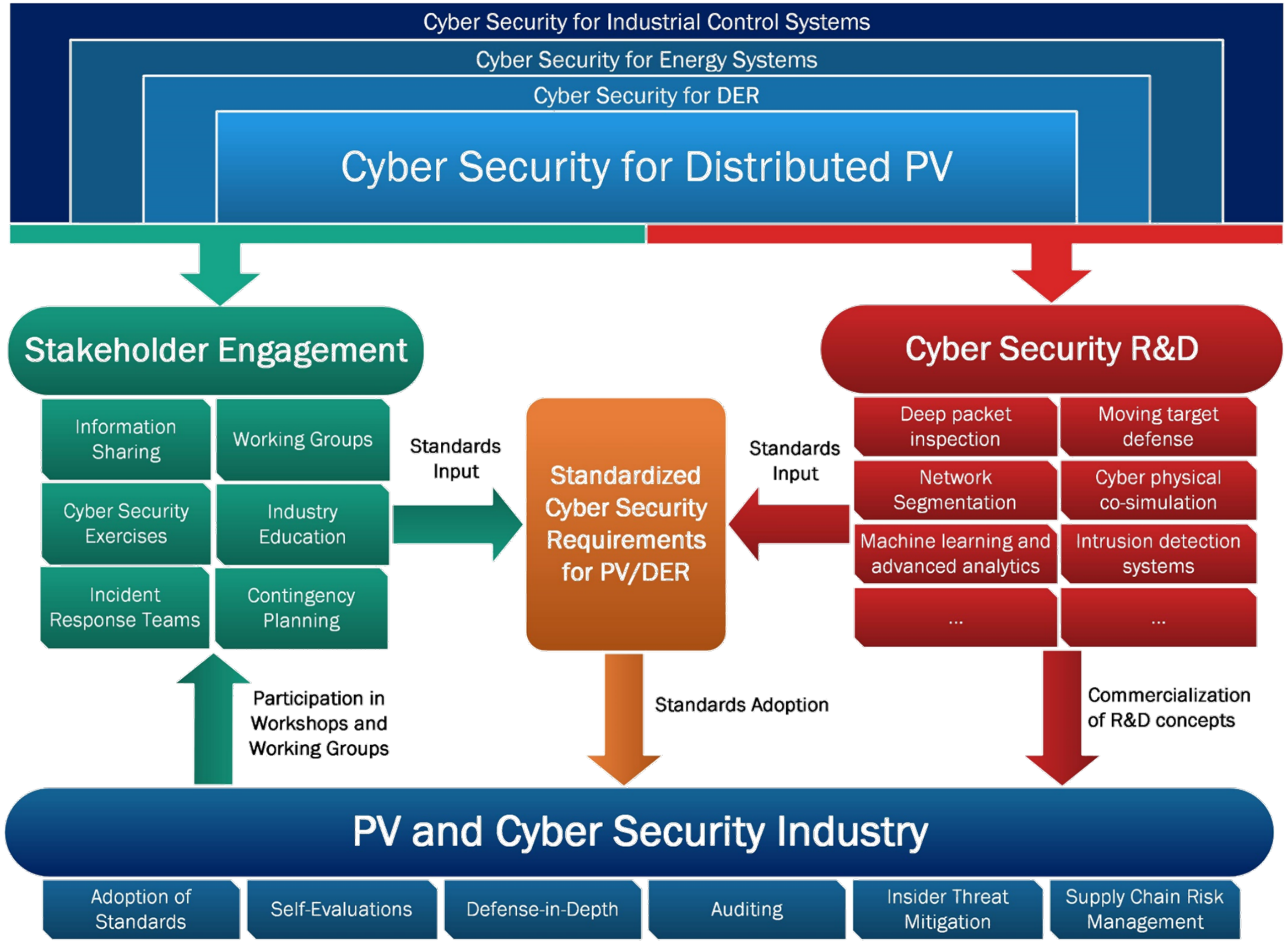
Approved for public release; further dissemination unlimited.

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



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

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

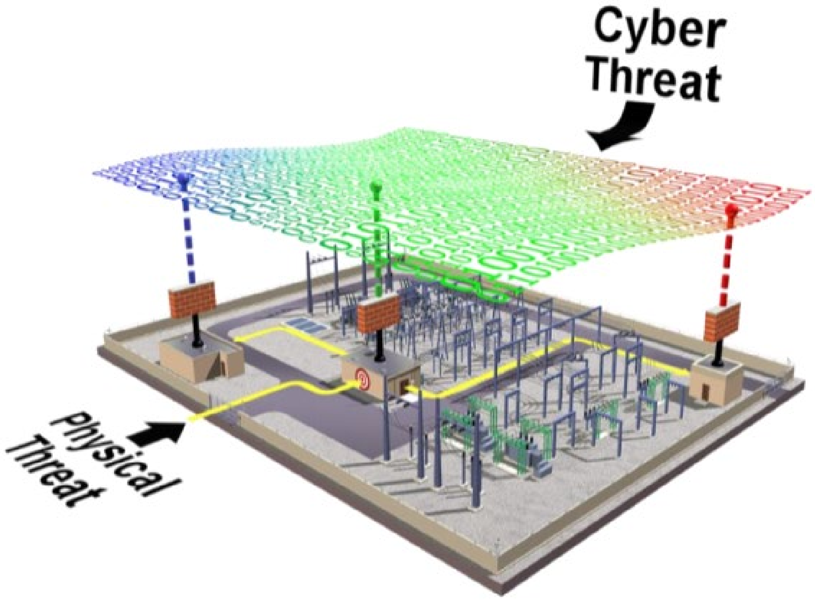
- Started August 2017

- Over 300 participants from more than 50 organizations

- Charter: 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.

- Primary Goal: generate a collection of best practices that act as basis for (or input to) national or international DER cyber security standards.

- Secondary Goal: 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: Ifeoma Onunkwo (Sandia) and Nicholas Manka (GridSME)
- 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

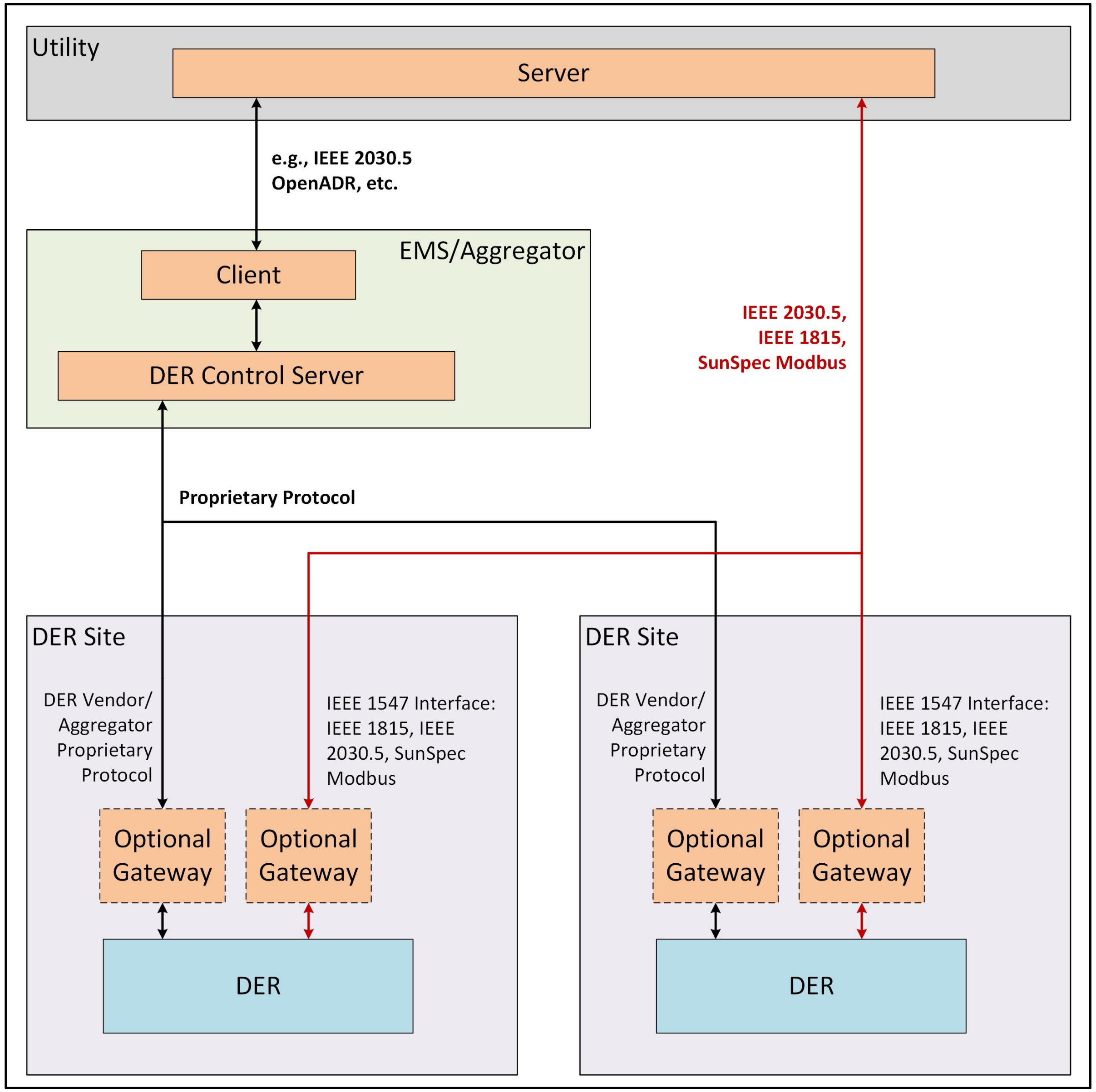
Utility/Aggregator Auditing Procedure — Much Later

- **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/

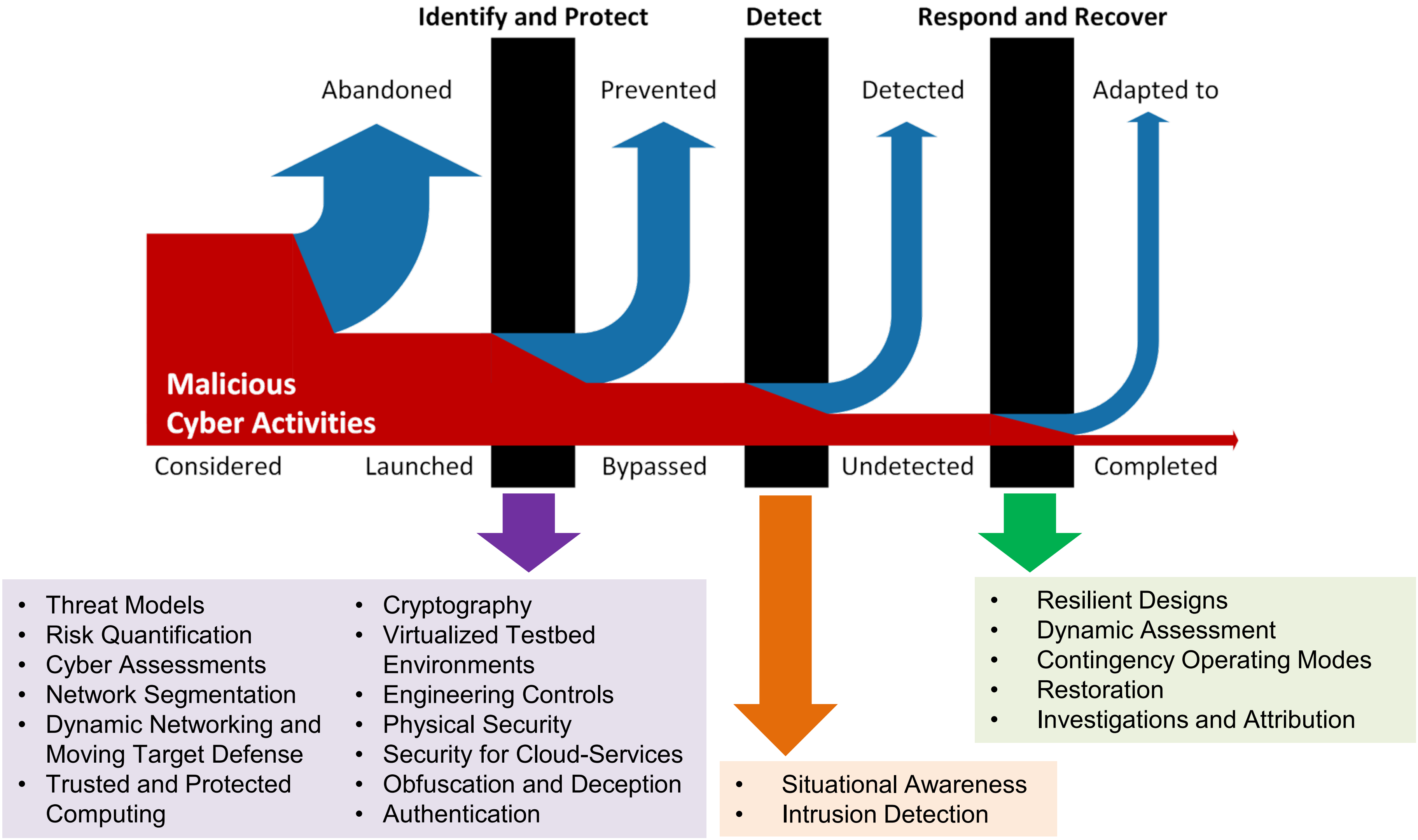
DER Communication Protocols

- **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.



- 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

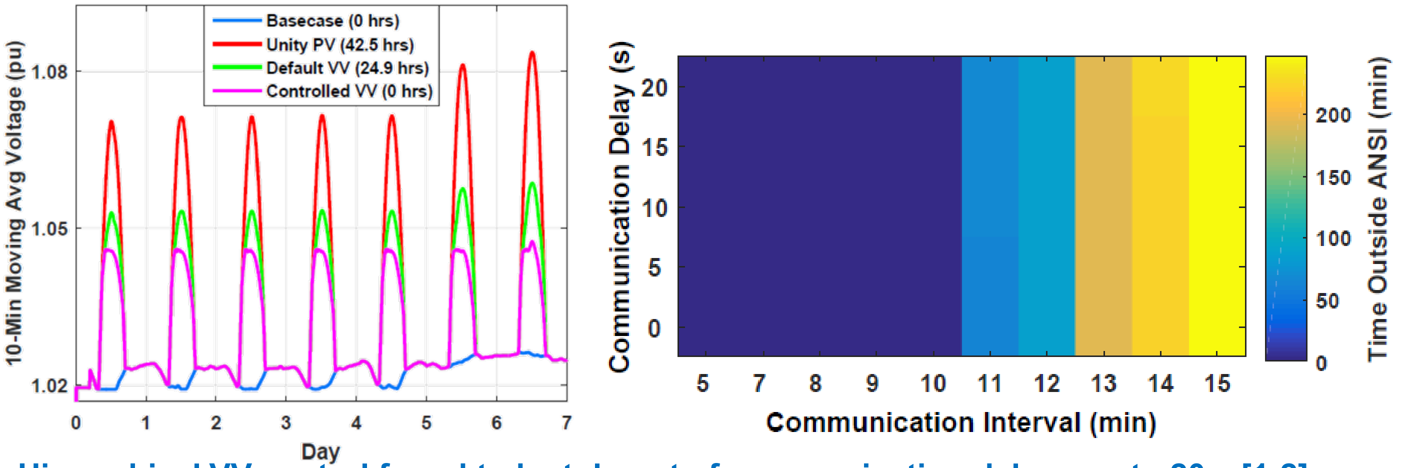
- Situational Awareness
- Intrusion Detection

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

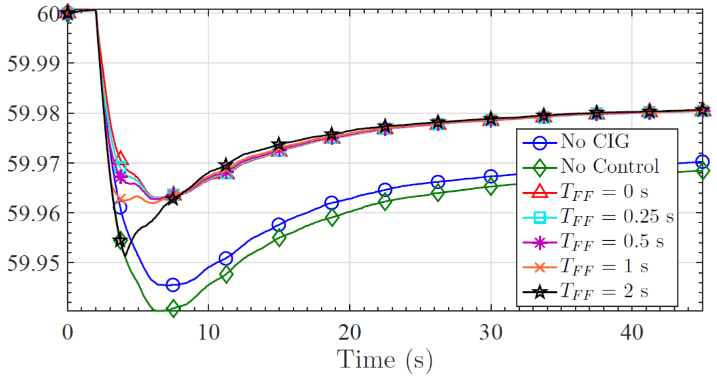
More details in “Roadmap for Photovoltaic Cyber Security” (SAND2017-13262), which outlines a 5-year strategy for DOE, industry, and standards development organizations in areas of Identify/Protect, Detect, and Respond/Recover.

DER Network Quality of Service vs Grid Performance

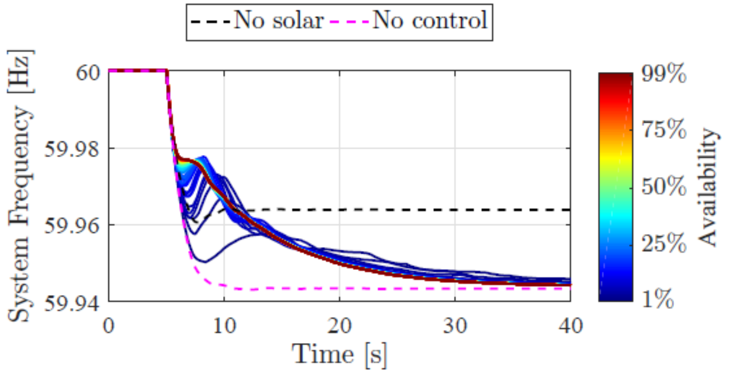
- Project investigated how network topology/security features change communication speed and power system behavior
- Multiple communications-enabled DER control approaches were simulated:
  - Synthetic inertia
  - Communication enabled fast acting imbalance reserve
  - Communication enabled frequency 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].

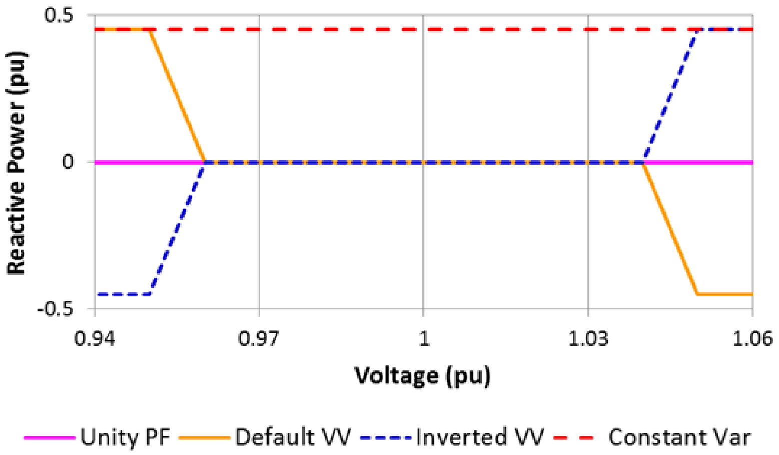


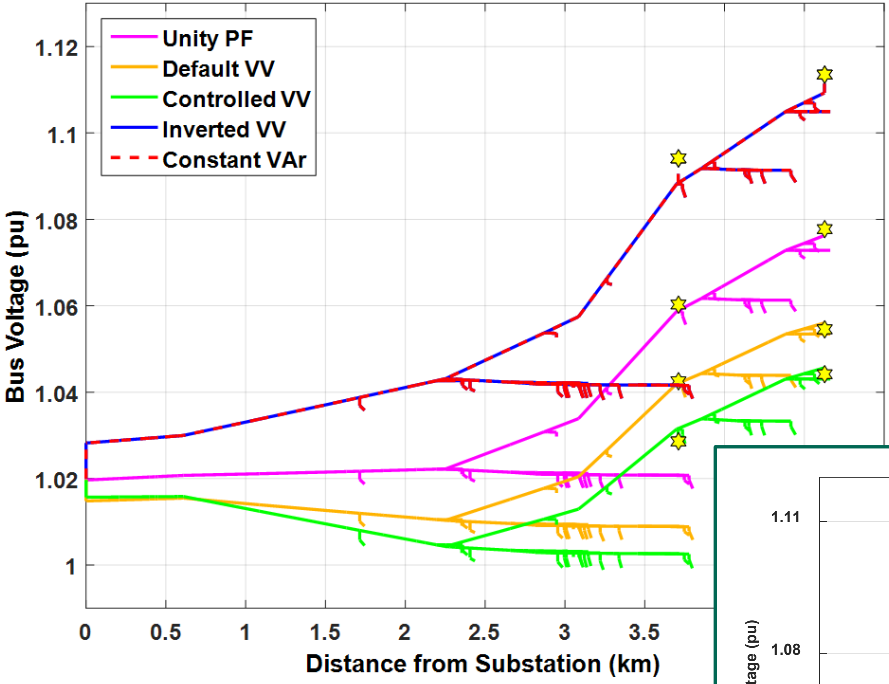
Communications Enabled Synthetic Inertia Controller transient response with different DER availabilities [4].

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.

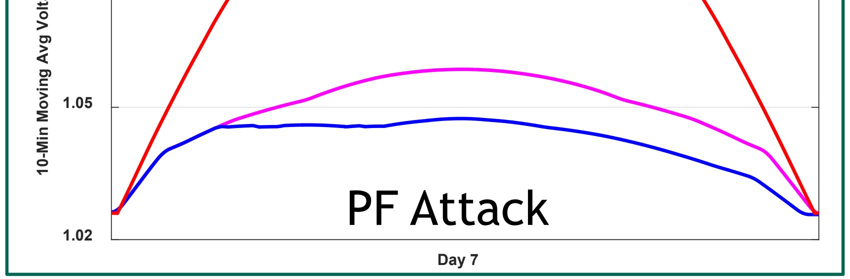
…but what if the DER equipment were maliciously controlled?

- 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.



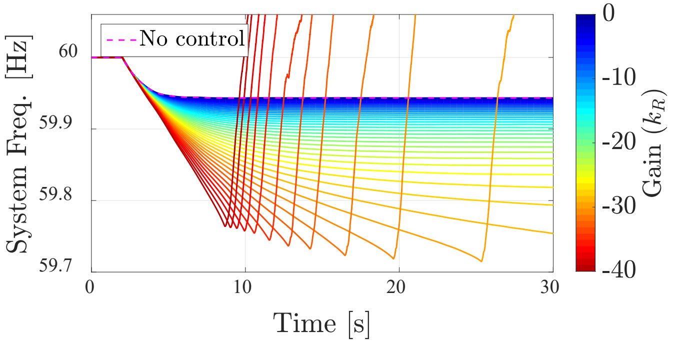
Attack: volt-var function is inverted to inject reactive power at high voltage and absorb reactive power at low voltage. PF and VV13 attacks lead to constant reactive power injection.

Transmission Cases

❖ Frequency Droop

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

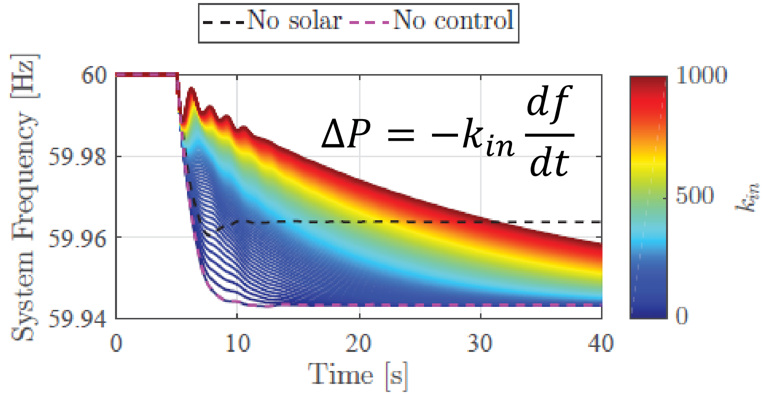
$$\Delta P_j^{attack} = -\frac{f_{ref} - f_{eq}}{R} = -k_R(f_{ref} - f_{eq})$$



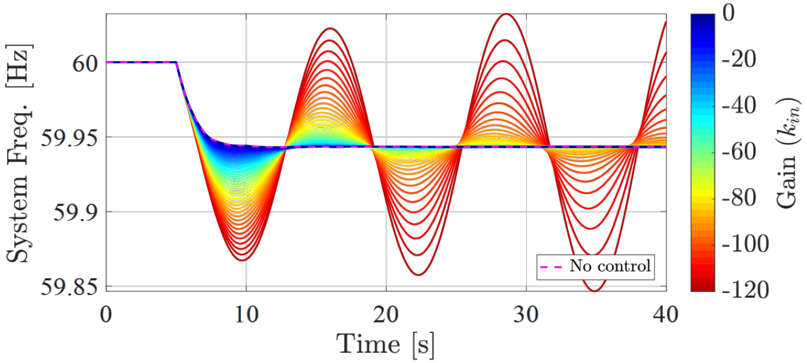
Attack: frequency-watt function is inverted to inject power at high frequency and absorb power at low frequency.

Result: Lower frequency nadirs, possibly leading to load shedding. k_R<-25 causes loss of synchronism

❖ Synthetic Inertia



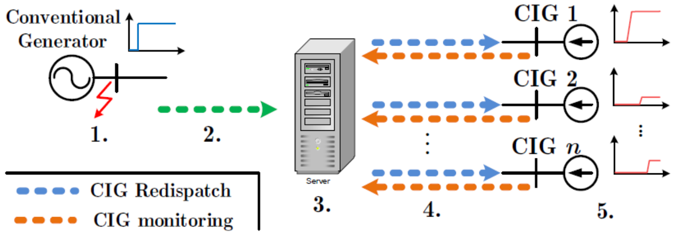
$$\Delta P = -k_{in}\frac{df}{dt}$$



Attack: reverse sign on inertial gain to create positive feedback.

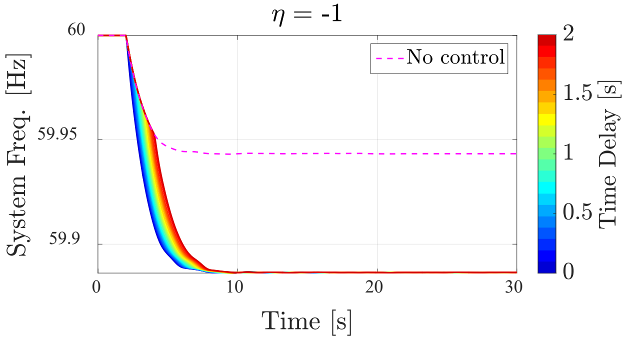
Result: Nadir is reduced and oscillatory behavior in the power system is created, leading to instability and possible blackouts.

❖ Fast Acting Imbalance Reserve



CIG = Converter-Interfaced Generator

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



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.

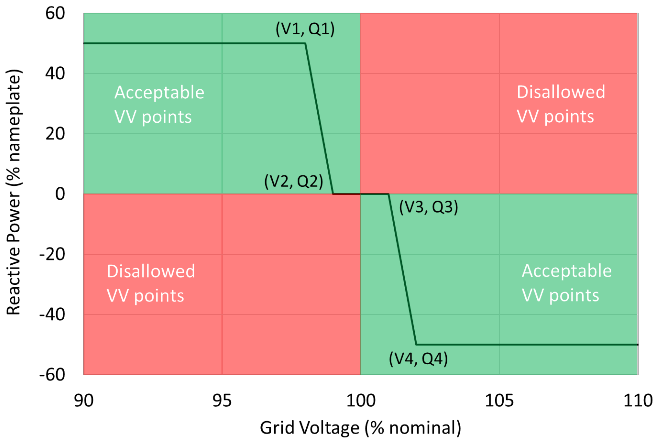
J. Johnson, J. Quiroz, R. Concepcion, F. Wilches Bernal, M. Reno, "Power System Effects and Mitigation Recommendations for DER Cyber Attacks," IET Cyber-Physical Systems: Theory & Applications, Jan 2019, DOI: 10.1049/iet-cps.2018.5014.

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.

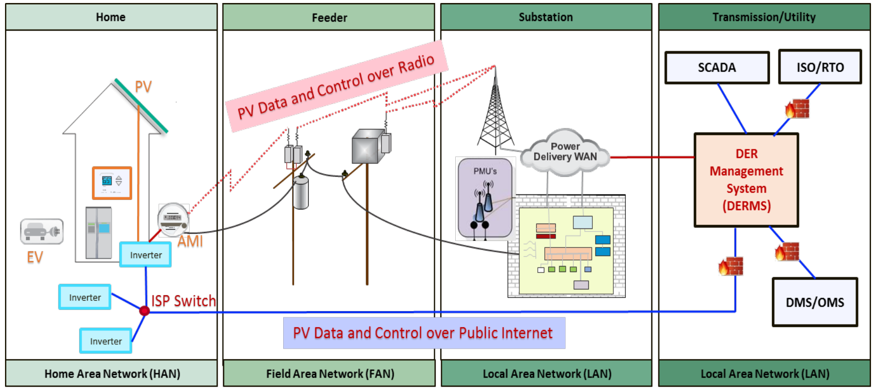
Volt-Var Function Parameter Ranges



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

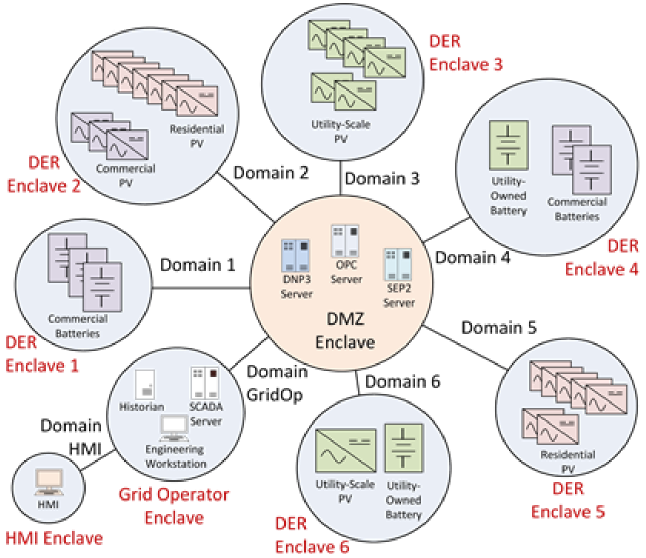
Concept: For DER traffic transmitted on the public internet, overlay TLS security on top of SunSpec Modbus or create a RESTful web services option for IEEE 1547, CA Rule 21, and other information model requirements.



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

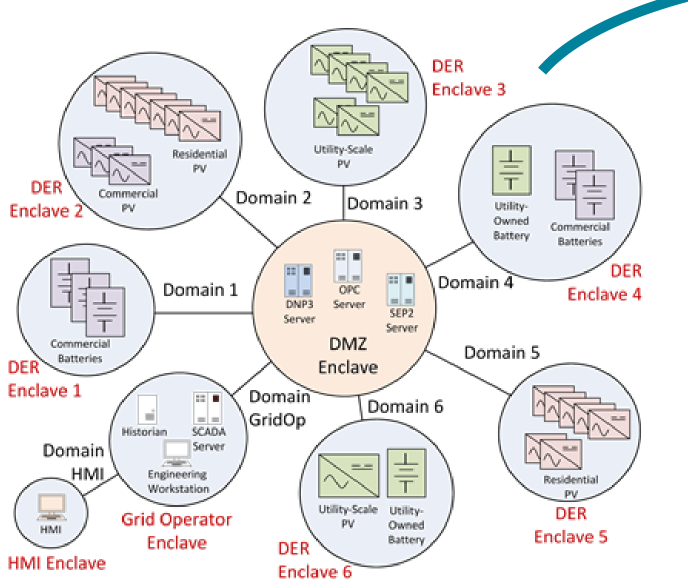
Concept: Create DER enclaves with firewall rules, VPNs, or proxies so an adversary cannot control all DER devices if an enclave is compromised.

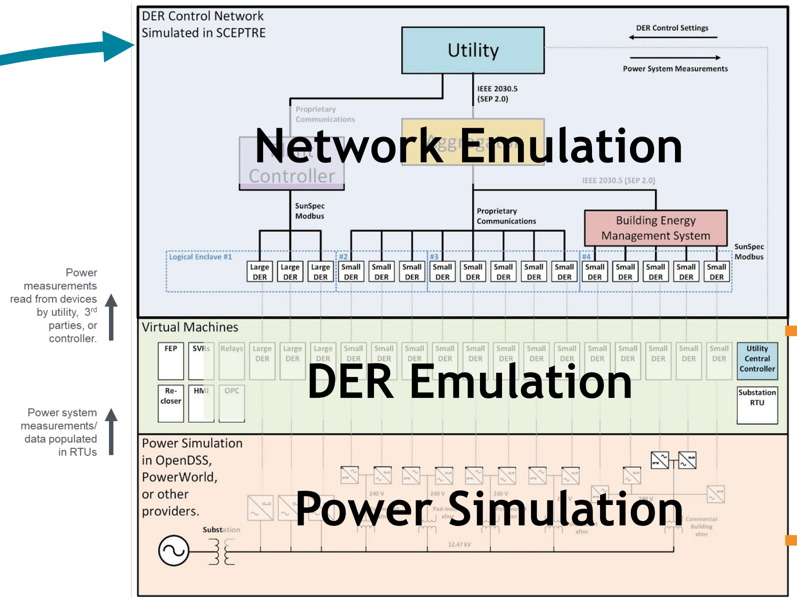


On-going work: DER Cyber Security Working group is creating recommended data architectures for utilities and DER aggregators. Also, Sandia measuring cyber metrics of different topologies with red teaming activities.

Tying cybersecurity design to grid performance

DER control network architectures are emulated in the SCEPTRE environment.





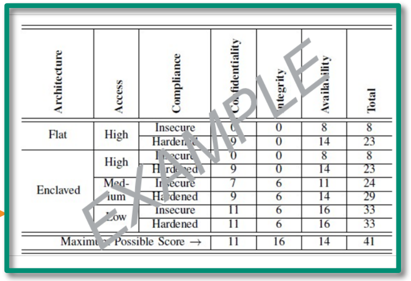
DER Control Network Simulated in SCEPTRE
Utility
DER Control Settings
Power System Measurements
IEEE 2030.5 (SEP 2.0)
Proprietary Communications
Network Emulation
Controller
IEEE 2030.5 (SEP 2.0)
SunSpec Modbus
Proprietary Communications
Building Energy Management System
SunSpec Modbus
Logical Enclave #1
#2
#3
#4
Large DER
Small DER
Power measurements read from devices by utility, 3rd parties, or controller.
Virtual Machines
FEP
SVRs
Relays
Re-closer
HMI
OPC
Utility Central Controller
Substation RTU
DER Emulation
Power system measurements/ data populated in RTUs
Power Simulation in OpenDSS, PowerWorld, or other providers.
Power Simulation
Substation

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

SCEPTRE outputs:

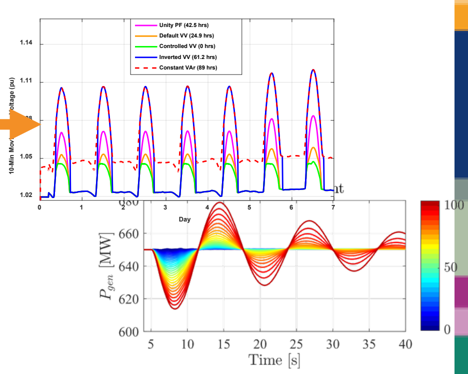
- Cybersecurity metrics
- Communication parameters
- Power system performance

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

Power system studies

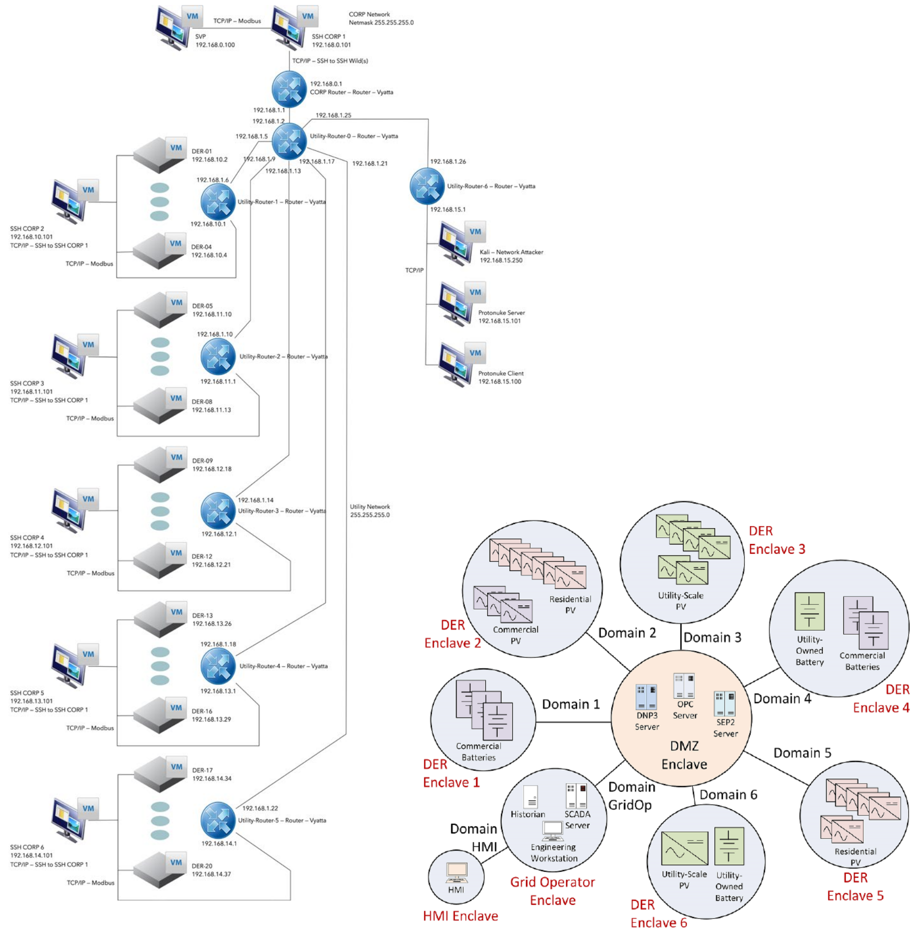


Multiple DER network architectures will be simulated to determine:

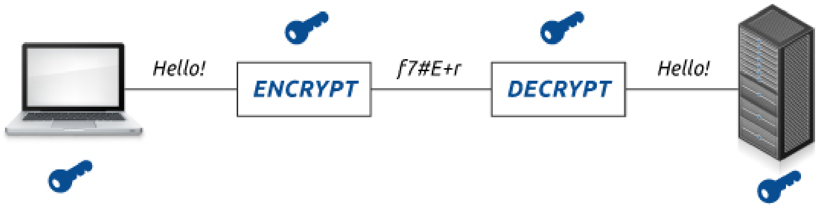
1. Cybersecurity resilience
2. Communication latency, dropout, and availability
3. Power system performance metrics (voltage, nadir, etc.)

Cybersecurity Features Implemented in SCEPTRE

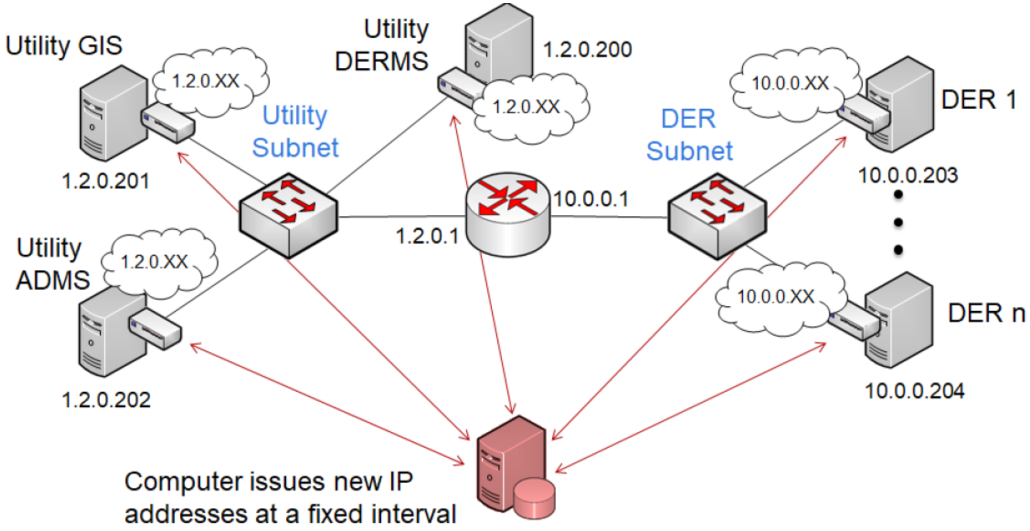
1. Segmentation



2. Encryption



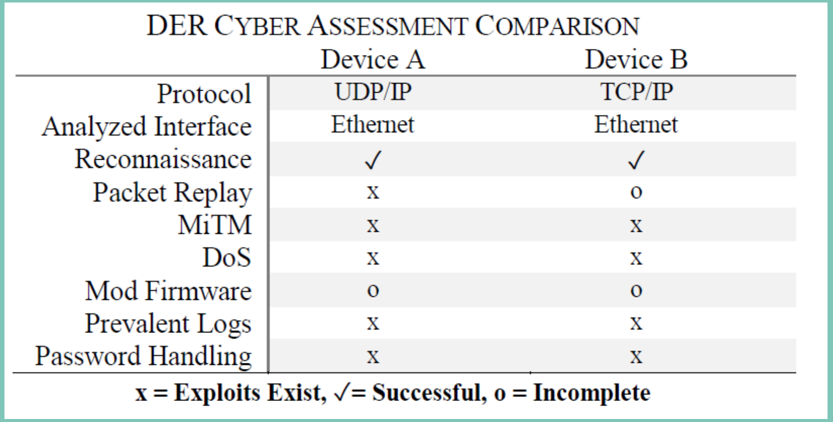
3. Moving Target Defense



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

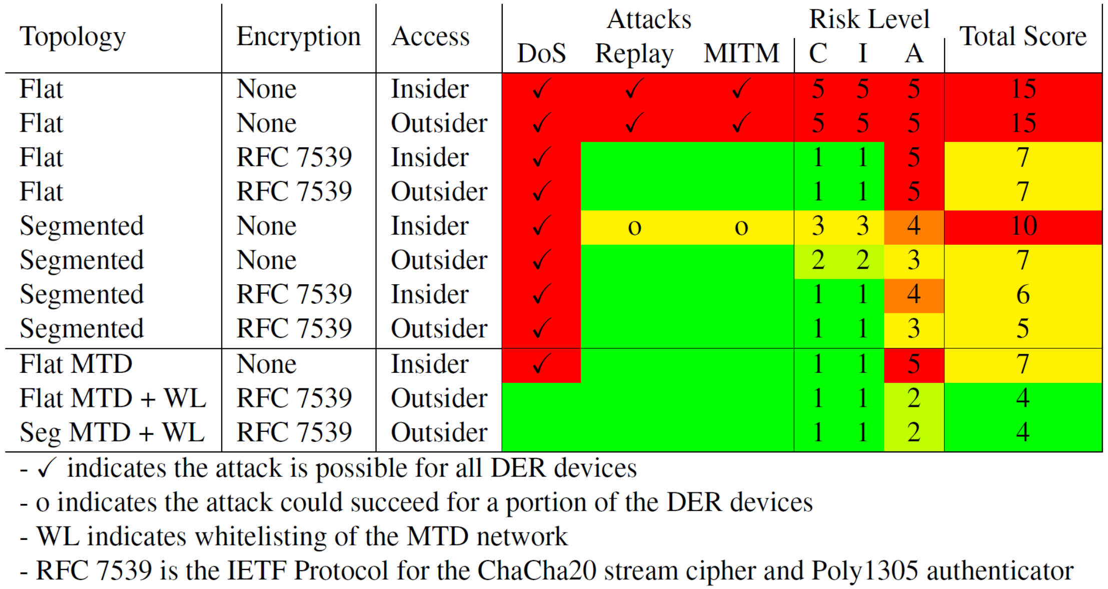
x = Exploits Exist, ✓= Successful, o = Incomplete

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

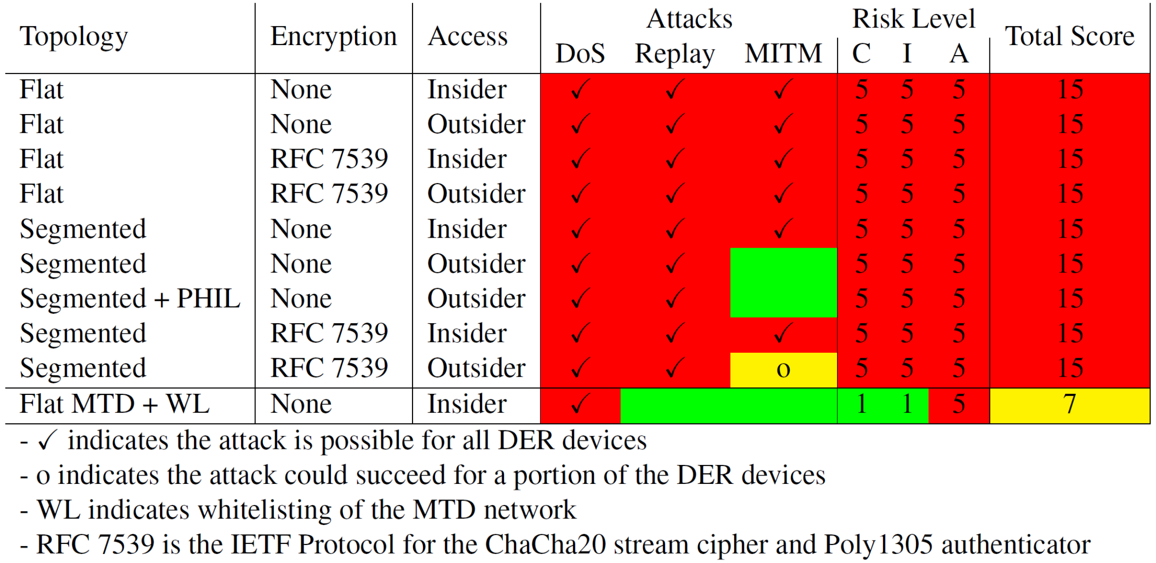
If properly implemented, the following results were expected:



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

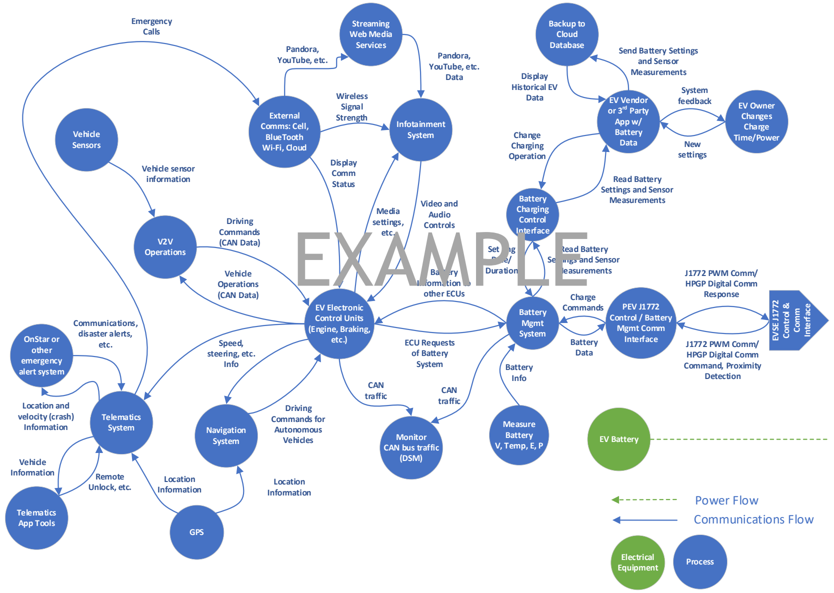
- Denial of service is very difficult to prevent. Aggregators/utilities should implement firewall whitelists to prevent these types of attacks.
- Segmentation makes it difficult for the adversary to move between subnets. Only through flaws in the networking implementation could the red team manipulate 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.

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)



Emergency Calls
Streaming Web Media Services
Pandora, YouTube, etc.
Pandora, YouTube, etc. Data
Backup to Cloud Database
Send Battery Settings and Sensor Measurements
Display Historical EV Data
System feedback
EV Vendor or 3rd Party App w/ Battery Data
EV Owner Changes Charge Time/Power
New settings
Wireless Signal Strength
External Comms: Cell, BlueTooth Wi-Fi, Cloud
Infotainment System
Vehicle Sensors
Vehicle sensor information
Display Comm Status
Change Charging Operation
Read Battery Settings and Sensor Measurements
Battery Charging Control Interface
Media settings, etc.
Video and Audio Controls
V2V Operations
Driving Commands (CAN Data)
EXAMPLE
Setting Rate/ Duration
Read Battery Settings and Sensor Measurements
Battery Information to other ECUs
J1772 PWM Comm/ HPGP Digital Comm Response
Vehicle Operations (CAN Data)
EV Electronic Control Units (Engine, Braking, etc.)
Charge Commands
Battery Mgmt System
PEV J1772 Control / Battery Mgmt Comm Interface
EVSE J1772 Control & Comm Interface
Communications, disaster alerts, etc.
OnStar or other emergency alert system
Speed, steering, etc. Info
ECU Requests of Battery System
Battery Data
J1772 PWM Comm/ HPGP Digital Comm Command, Proximity Detection
Battery Info
Location and velocity (crash) Information
Telematics System
CAN traffic
CAN traffic
Navigation System
Driving Commands for Autonomous Vehicles
Monitor CAN bus traffic (DSM)
Measure Battery V, Temp, E, P
EV Battery
Vehicle Information
Remote Unlock, etc.
Location Information
Location Information
Telematics App Tools
GPS
Power Flow
Communications Flow
Electrical Equipment
Process

Thank You!

Jay Johnson

Renewable and Distributed Systems Integration

Sandia National Laboratories

P.O. Box 5800 MS1033

Albuquerque, NM 87185-1033

Phone: 505-284-9586

jjohns2@sandia.gov