New Mexico Research Spotlight Forum

10.17.2019 Grid Resiliency

Distributed Energy Resource Grid Integration and Cybersecurity Research

Jay Johnson, jjohns2@sandia.gov

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-NA0003525. SAND2019-12358 PE

Sandia National Laboratories | Georgia Institute of Technology | ILLINOIS | PURDUE UNIVERSITY | THE UNIVERSITY OF TEXAS AT AUSTIN | THE UNIVERSITY OF NEW MEXICO | NM STATE UNIVERSITY | NEW MEXICO TECH SCIENCE • ENGINEERING • RESEARCH UNIVERSITY | U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

ABOUT ME

- Principal Member of Technical Staff at Sandia National Laboratories
- In 9 years at Sandia, Principal Investigator for over $10M in DOE-funded R&D programs in areas of renewable energy integration, control, interoperability, and cybersecurity.
- More than 100 technical publications, 7 patents, 50 invited presentations/webinars.
- Enjoy leading diverse, world-class, multi-agency research teams to solve national challenges

Research Keywords:

Power systems, renewable energy, grid integration, DER, cybersecurity

WORK IN GRID RESILIENCY

- **Electric Vehicle Charging Cybersecurity**
  - $3.0M 3-year DOE EERE VTO "Securing Vehicle Charging Infrastructure" project, 2018-2021
- **Advanced Distribution Management Systems using Interoperable DER**
  - $5.0M ($2.5M DOE, $2.5 Cost Share) 2-year DOE EERE SETO ENERGISE project, "Voltage Regulation and Protection Assurance using DER Advanced Grid Functions," 2017-2019
- **Photovoltaic Cybersecurity Roadmap, Standards Development, and R&D**
  - $2.7M 3-year DOE EERE SETO SuNLaMP "Secure, Scalable Control and Communications for Distributed PV" project, 2016-2019
  - $1.2M 3-year DOE EERE SETO "PV Cybersecurity Standards Development" project, 2018-2021.
  - $400k 2-year DOE EERE SETO "Photovoltaic Cyber Security Research" project, 2016-2018
- **Wind Energy Cybersecurity Research**
  - $1.5M 3-year DOE EERE WETO "Hardening Wind Energy Systems from Cyber Threats" project, 2018-2021.

Distribution System Impact Analysis from EV Charging Cyber Attack

Cybersecurity risk is based on probability of attack and consequence

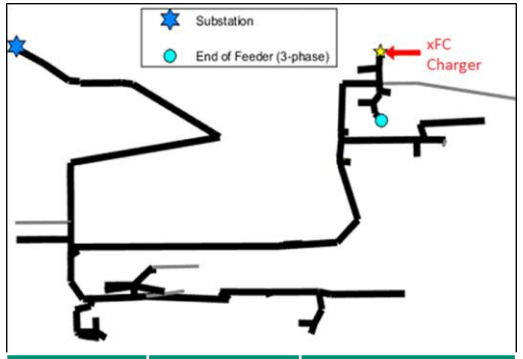
- To estimate the impact to power systems, the team studied what would happen if fleets of electric vehicle chargers were compromised.

Distribution Feeder Simulation

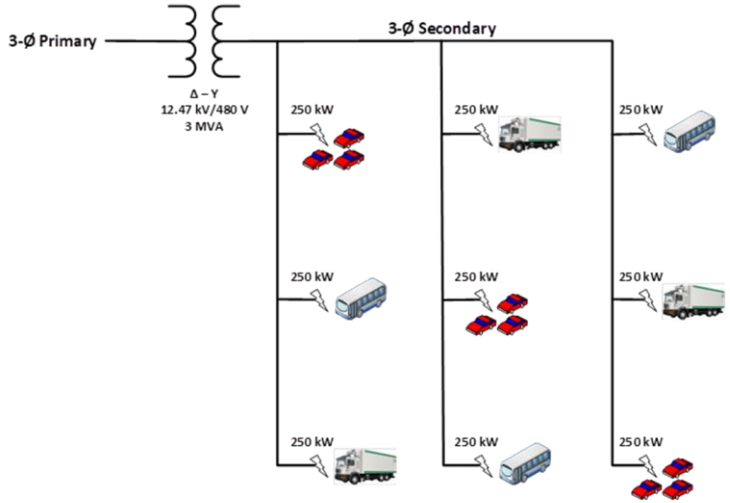
- System: Rural 12 kV distribution feeder, highly commercial load area
- Model containing 215 buses, 39 service transformers.
- 3-minute OpenDSS simulations
- Feeder voltage regulated via substation transformer load tap changer (LTC).

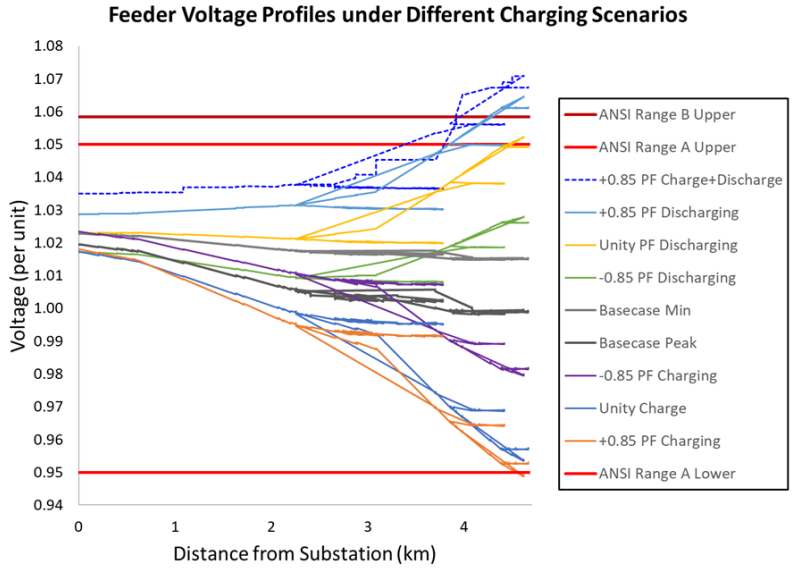
EV Interconnection Model

- 9x250 kW, 3-phase, 480 V stations simulated at the end of the feeder (2.25 MW total)
- Scenarios include charging sequences with and without V2G capabilities to generate high and low feeder voltages during peak and min load periods.
- Limited to ramp rate of 40 amp/sec, i.e. chargers get to full output in ~13 seconds.



Load Period	Date/Time	Feeder Demand (kW)
Peak	7/22 @ 13:00	3946
Minimum	3/22 @ 23:00	1483





More details: J. Johnson, "Securing Vehicle Charging Infrastructure," 2019 DOE Vehicle Technologies Office Annual Merit Review, Arlington, VA, June 10-13, 2019.

ENERGISE ProDROMOS Project

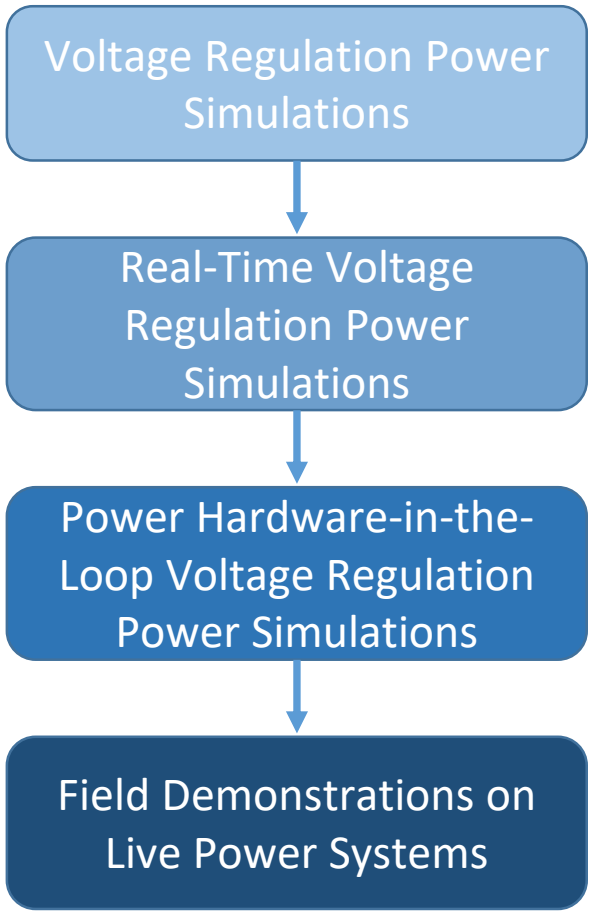
Programmable Distribution Resource Open Management Optimization System (ProDROMOS)[1]

Goal: create an **Advanced Distribution Management System (ADMS)** that captures distribution circuit telemetry, performs state estimation, and issues optimal DER setpoints based on PV production forecasts.

Focus on **distribution system voltage regulation** and **protection** with high penetrations of PV

Team used PHIL experiments to gain confidence in control algorithms, verify communication interfaces, and predict performance prior to deploying the ADMS on a live feeder in Massachusetts.

[1]Prodromos is Greek for "forerunner" and the prodromoi were a light cavalry army unit in ancient Greece used for scouting missions.

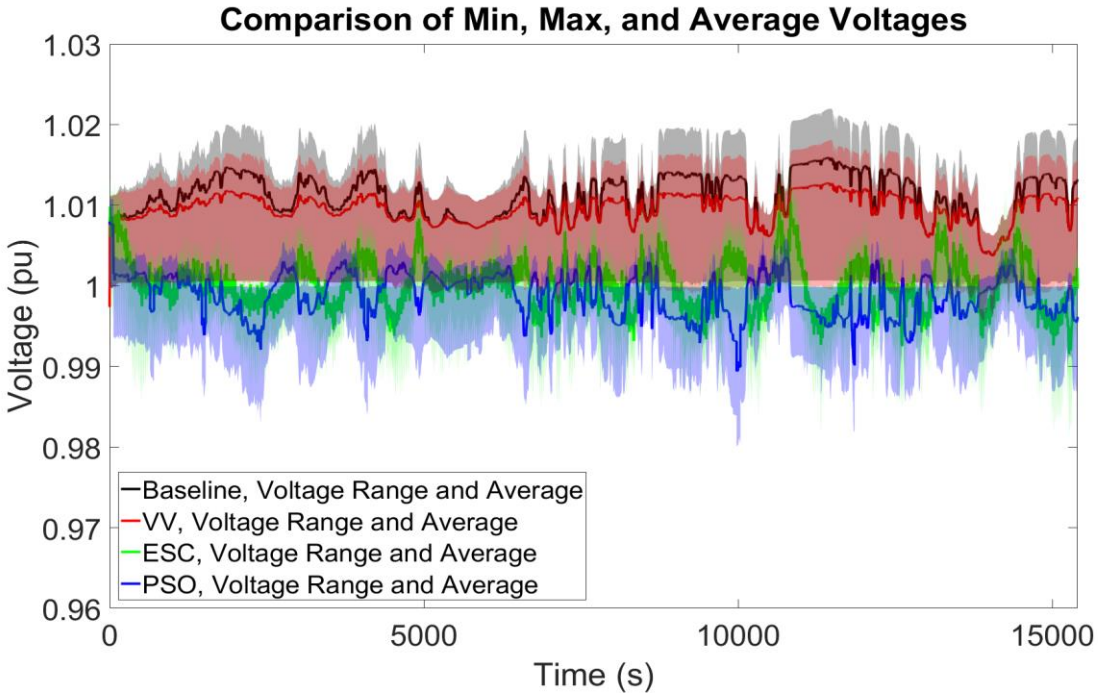


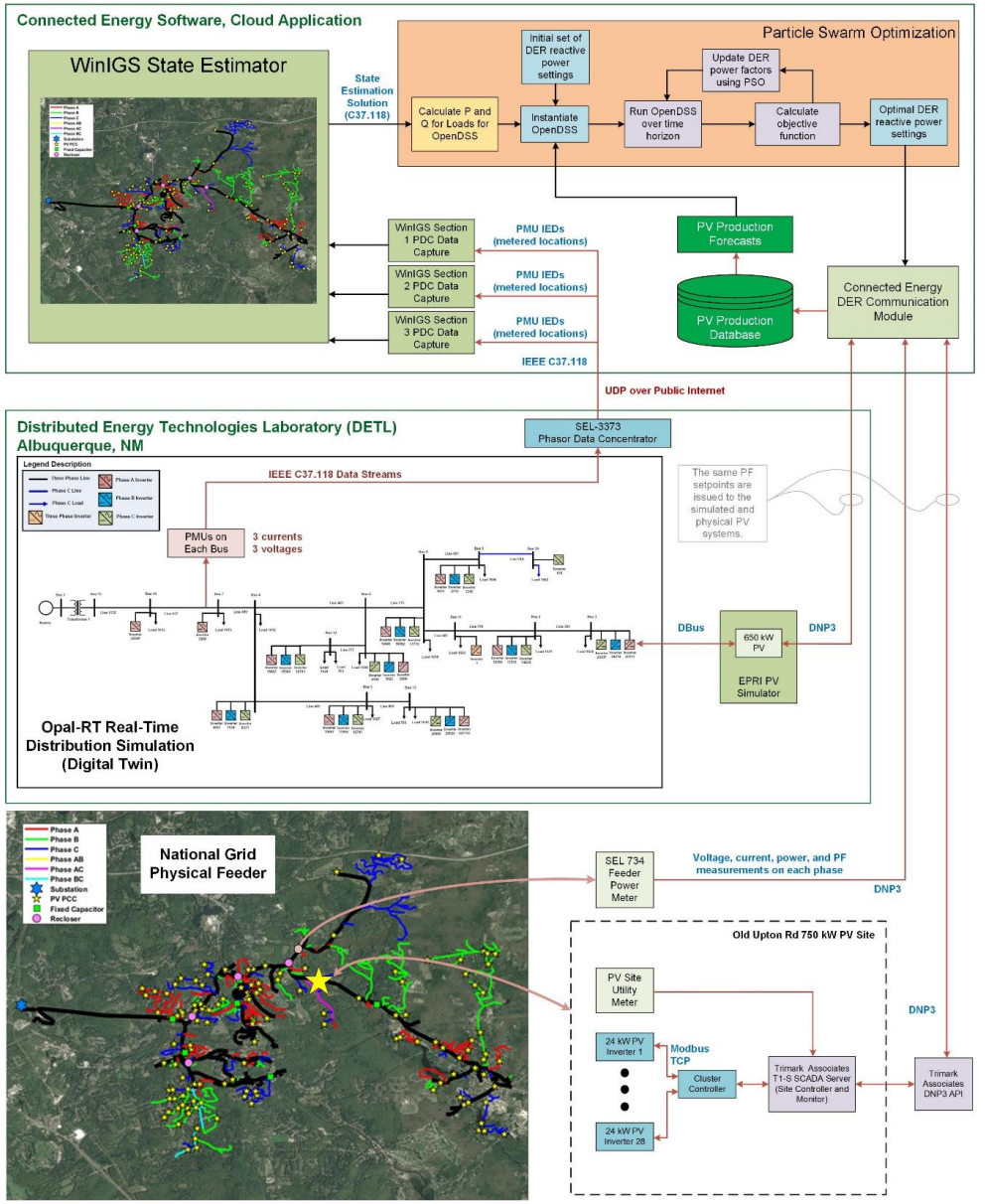
28 PV inverters controlled at 672 kVA PV Site

J. Johnson, et al., "Optimal Distribution System Voltage Regulation using State Estimation and DER Grid-Support Functions," Sandia Technical Report (forthcoming).

PHIL Simulations and Digital Twin

Extensive power hardware-in-the-loop real-time simulations were conducted to compare different voltage regulation control technologies.





Real-time digital twin of the National Grid feeder was used to estimate distribution operations and voltages for live demo.

The same PV PF setpoints were sent to the physical and virtual PV system

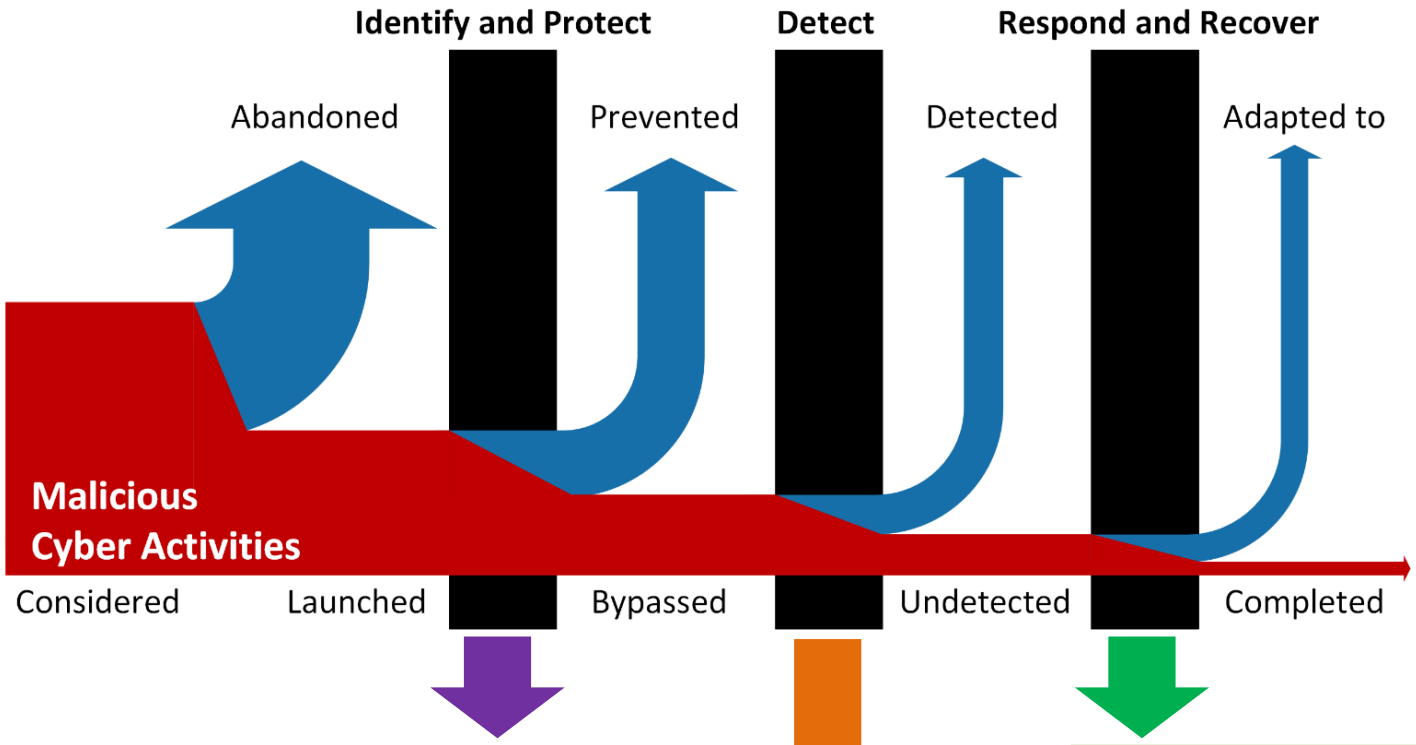
DER Cybersecurity R&D

Created Cybersecurity Roadmap for PV Systems which focused on four areas

- Stakeholder Engagement
- Research and Development
- Industry Support
- Standards and Guidelines

One R&D activity: Sandia project investigated cybersecurity implications of communications-enabled DER control.

- Goal: Find optimal network architecture by quantifying tradeoffs between cybersecurity and communication latency/power system performance



- 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

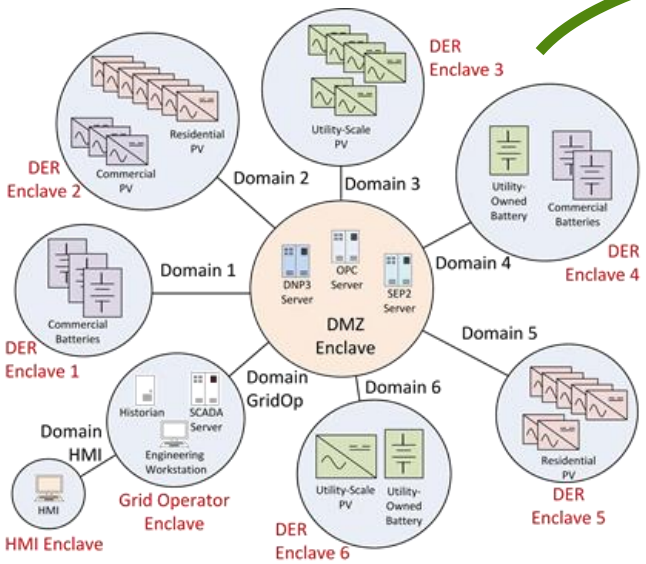
- Situational Awareness
- Intrusion Detection

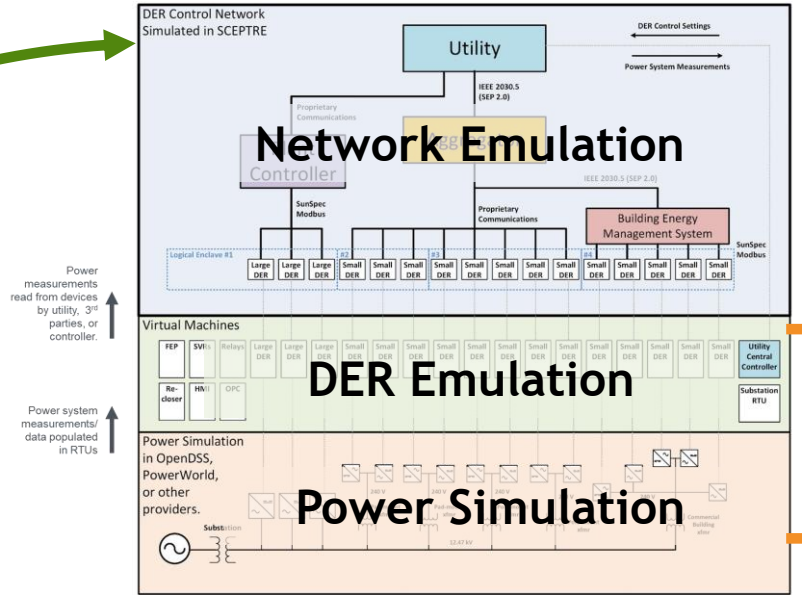
- Resilient Designs
- Dynamic Assessment
- Contingency Operating Modes
- Restoration
- Investigations and Attribution

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.

Cybersecurity Design vs Grid Performance Evaluations with Co-Simulation Platform

DER control network architectures are emulated in the SCEPTRE environment.



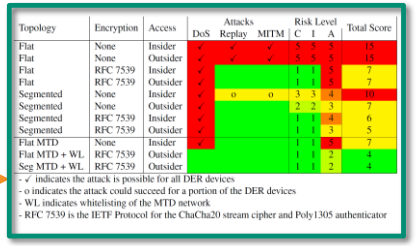


SCEPTRE: a live, virtualized power system and control network co-simulation platform

SCEPTRE outputs:

- Cybersecurity metrics
- Communication parameters
- Power system performance

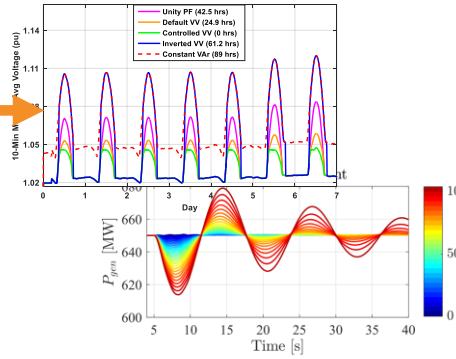
IDART
Information Design Assurance Red Team



Topology	Encryption	Access	Attacks DoS	Attacks Replay	Attacks MITM	Risk Level C	Risk Level I	Risk Level A	Total Score
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

Power system studies



Multiple DER network architectures were simulated to determine:

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

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.

RESEARCH NEEDS

- Collaboration Needs
  - Access to talent stream: we need power systems and cybersecurity interns, post-docs, and research staff.
  - Support with DOE EERE/CESER/OE competitive solicitations.
  - Promising low-TRL research for DER equipment, power systems control/operations, and cybersecurity technologies.