GMLC 1.3.4 – Industrial Microgrid Design and Analysis for Energy Security and Resiliency

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Project Description

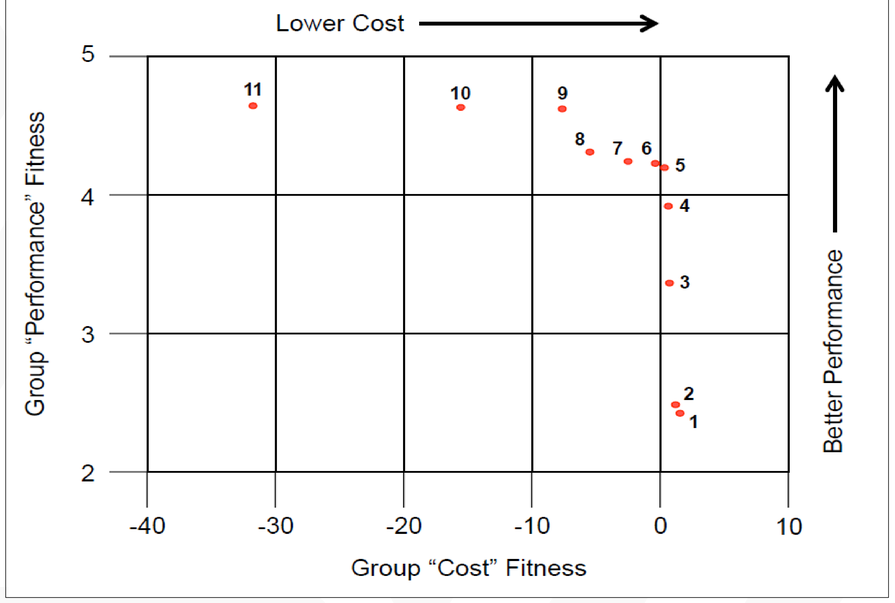
Microgrids are an effective method of providing reliable, local power to critical loads. Industrial customers on the electric grid typically consume large amounts of power and require high reliability, making them great candidates for hosting microgrids. To investigate the benefits of industrial scale microgrids, ORNL and SNL designed and performed cost/benefit analysis of an industrial-scale microgrid with the goal of sharing lessons learned and best practices with other industries and utilities.

Outcomes

- All-hazards risk analysis of facilities
- Cost/benefit analysis of industrial-scale microgrids
- Potential for grid services provision
- Roadmap to industrial microgrid deployments & lessons learned
- Results are applicable industrial consumers and utilities interested in microgrids to stimulate conversation on grid modernization.

Significant Milestones	Date
Initial Microgrid Design	10/1/2016
Risk Analysis Completed	4/1/2017
Energy Efficiency and Ancillary Service Analysis	10/1/2017
Cost/Benefit Modelling and Analysis	10/1/2017
Final Results Delivered	10/1/2017

Failure Cost Reduction		
Designs	MFC (50%)	MFC (99.99%)
Site A	14.8%	59.4%
Site B	14.4%	57.5%
Site C	14.3%	57.4%
Site D	13.9%	55.7%



Progress to Date

- Project is complete
- Comprehensive analysis of 4 microgrid sites, with multiple designs per site
- Risk analysis and mean failure cost calculated for each site
- Ancillary service economic analysis performed for blue-sky operation of microgrids
- 200+ page report delivered to DOE and UPS
- Met with utility and industry stakeholders to discuss rate programs and partnerships
- Conference paper pending review
- Journal article pending

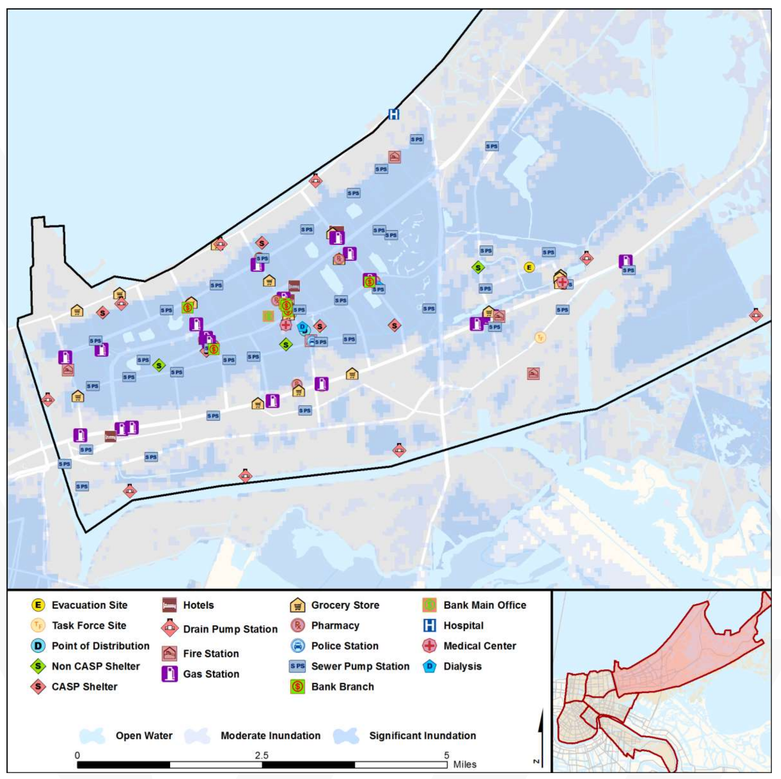
GMLC 1.3.11
Grid Analysis and Design for Energy and Infrastructure Resiliency for New Orleans

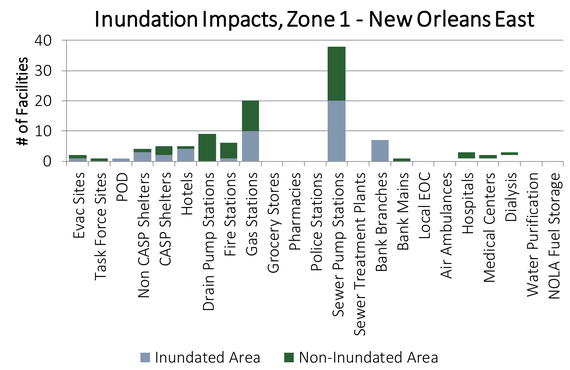
Robert Jeffers, PI (Sandia), Mary Ewers, +1 (LANL)

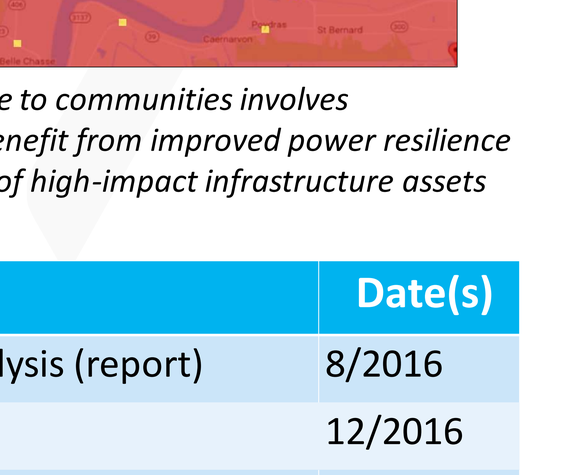
GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Project Description

- Grid resilience investments often do not fully account for impacts to **community-level resilience metrics**. This project used a community-level resilience analysis to aid the City of New Orleans in **identifying and prioritizing grid modernization options**. The focus was on understanding where collections of critical infrastructure services can be cost-effectively supported by grid investments.







Outcomes

- Supported the City of New Orleans in identifying and prioritizing areas where grid modernization options can cost-effectively improve community resilience
- Identified potential implementation paths, working in conjunction with Entergy New Orleans and community stakeholders
- Introduced the Urban Resilience Planning Process and the Resilience Node concept

Progress to Date

- Final open access report posted May, 2018 (www.sandia.gov/cities)
- Final recommendations delivered March, 2017
- Preliminary multi-infrastructure resilience assessment delivered to NOLA, Entergy, and DOE
- Preliminary report on opportunities for transactive control in NOLA

*Investing in grid modernization to minimize consequence to communities involves understanding which lifeline services receive greatest benefit from improved power resilience (**top**). Subsequently, areas are identified where clusters of high-impact infrastructure assets can be served by advanced microgrids (**bottom**).*

Significant Milestones	Date(s)
Multi-infrastructure community resilience analysis (report)	8/2016
Transactive control feasibility analysis (report)	12/2016
Draft community-level design options for resilience nodes (presentation)	1/2017
Final grid modernization report highlighting resilience benefits of resilience nodes	3/2017
Approval and release of final open access report	5/2018

Threat Detection and Response with Data Analytics (1.4.23)

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Project Description

- ❑ Develop advanced analytics on operational technology (OT) cyber data in order to detect complex cyber threats.
- ❑ Developed analytics will differentiate between cyber and non-cyber incidents
- ❑ Test developed analytics in realistic environments

Expected Outcomes

- ❑ Differentiate between cyber and non-cyber-caused incidents using available cyber data.
- ❑ Identify most valuable data sources for detecting cyber incidents
- ❑ Analytics being developed will assist asset owners in triaging grid incidents
- ❑ Identifying cyber incidents in a timely manner reduces outages and associated costs

Future Plans

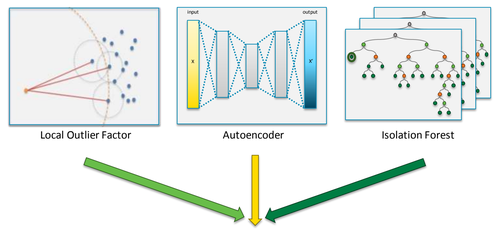
- ❑ Testbed experiments
- ❑ Scaling to larger. Realistic networks
- ❑ Integration across data sources

Significant Milestones	Date
Obtained meter data	12/2017
Developed smart meter analytics	06/2018
Developed Smart Inverter Model	11/2017
Adaptive control cyber attack mitigation	07/2018
Algorithms identifying cyber events from ethernet gateway data	07/2011
Impact analysis of cyber attacks on transactive control	08/2018
Baselining consumer behavior for anomaly detection	08/2018
ELK-based cyber-physical correlation and testbed demonstration	03/2019

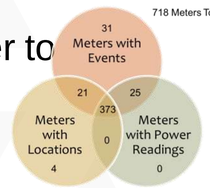
Approach & Progress to Date

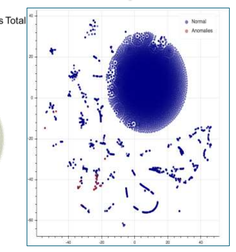
Leverage models, simulations, hardware in the loop simulations and data from different grid components and deploy ML algorithms to identify anomalies and differentiate from cyber and non-cyber events

Smart Meter Data

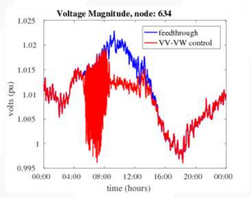


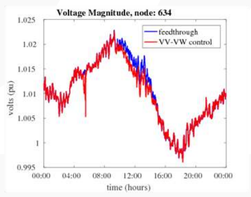
- ❑ Developed several data analytics algorithms that leverage raw smart meter data to detect anomalies
- ❑ Algorithms are ensembled together to increase performance of individual classifiers





Smart Inverter Data

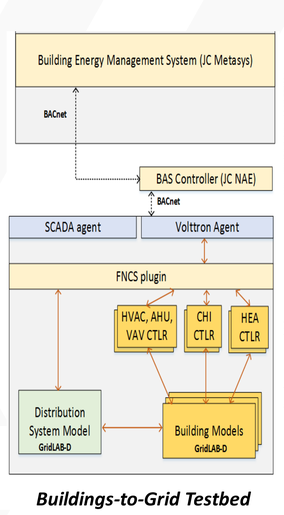




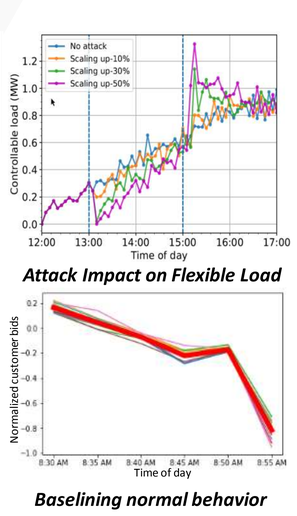
- ❑ Conducted stability analysis of interaction of DER feedback control model on distribution system voltage stability
- ❑ Developed adaptive control approach to enable model-free and no-communication strategy to mitigate effect of cyber attack

Buildings-to-Grid Data

- ❑ Analyzed operational, financial, and user comfort impacts of data integrity attacks on transactive control.
- ❑ Developed clustering techniques to group consumers for baselining.
- ❑ Developing analytics in ELK to correlate grid and cyber data to detect anomalies.



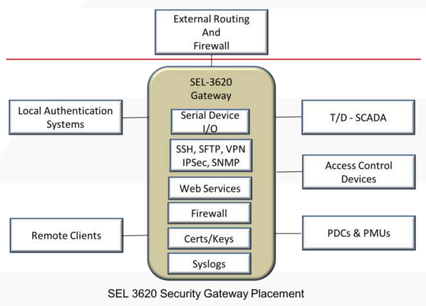
Buildings-to-Grid Testbed



Attack Impact on Flexible Load

Baselining normal behavior

Ethernet Gateway Data



SEL 3620 Security Gateway Placement

- ❑ Developed multipath machine learning algorithms to identify lowest risk communication paths
- ❑ Machine learning algorithms distinguishing cyber events from physical events based on SEL-3620/3622 syslog data

U.S. DEPARTMENT OF ENERGY

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

MultiSpeak® Secure Protocol Enterprise Access Kit (MS-SPEAK)

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

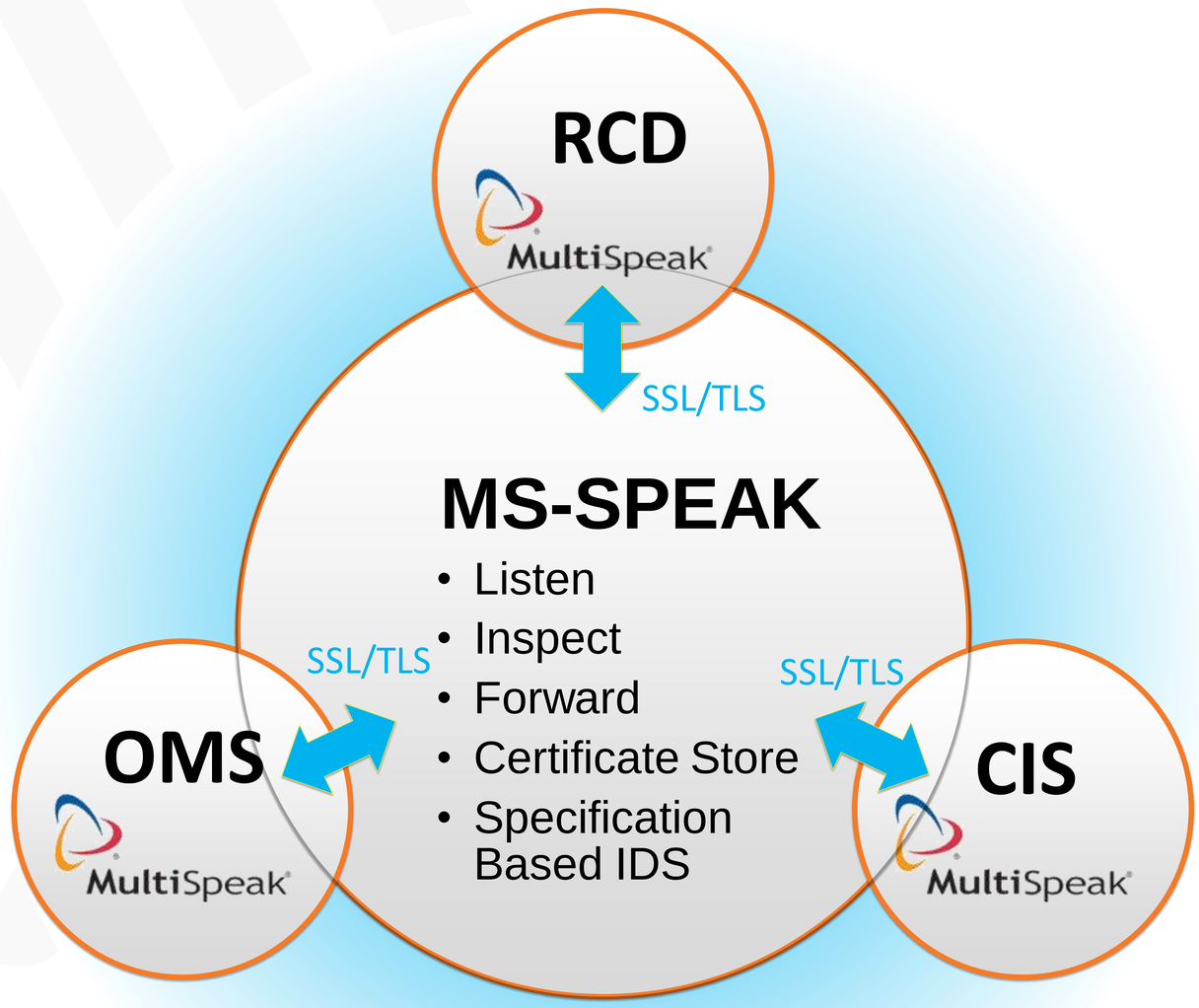
Project Description

MS-SPEAK fills a gap and makes the grid "smarter" (i.e. more intelligent and resilient) through the creation of an innovative ESB+ (enterprise service bus enhanced) for MultiSpeak. The ESB+ will support increased interoperability and security of the MultiSpeak standard and reduce costs to utilities that depend on MultiSpeak.

Expected Outcomes

- New Cyber Security Reference Architecture for MultiSpeak
- Attack Surface Analysis for Remote Meter Connect/Disconnect Functions
- Open-Source Tools for Vendors to Implement and Test Cyber Security
- Improved Cyber Security for Rural Electric Cooperatives that Serve 42M People and 56% of the U.S by area.

Significant Milestones	Date
Phase 1 Complete	*10/31/2017*
Update MultiSpeak Landscape Assessment	*3/15/2018*
Phase 2 Field Work Plan Approved	*7/6/2018*
Architecture and Attack Scenarios	10/31/2018
MS-SPEAK Tools and Test Platform	3/31/2019
Vendor Working Group Meetings	7/31/2019
Vendor Workshop	8/31/2019
Reporting and Open-Source Publication	9/30/2019



Lightweight, purpose-built intrusion detection system uses the rural electric cooperative's cyber security business rules to supplement data encryption.

Progress to Date

- Released "MS-SPEAK Phase 1 Technical Report", October 2017
- Released "MultiSpeak Landscape Assessment", March 2018
- Code Repository at: https://github.com/pnnl/ms-speak

Cybersecurity for Renewables, Distributed Energy Resources, and Smart Inverters (GM0100)

Presenter: Ravindra Singh
Project Team: Argonne National Laboratory, Washington State University, Electric Power Research Institute

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Project Description

Objective: Develop a holistic attack-resilient architecture and layered cyber-physical solution portfolio to protect the critical power grid infrastructure and the integrated distributed energy resources (DER) from malicious cyber attacks

Expected Outcomes

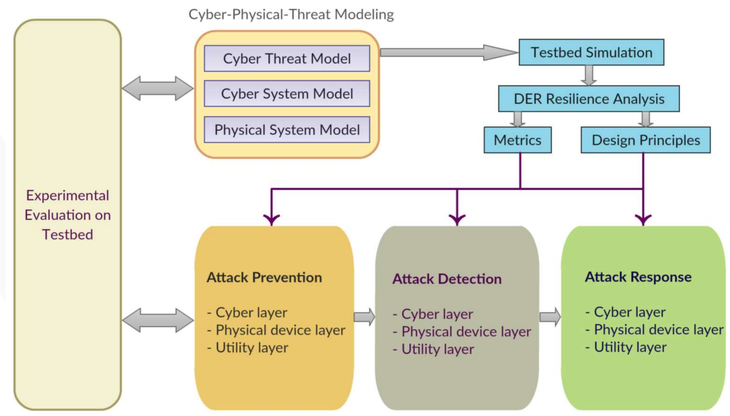
Deliverables:

- A DER cybersecurity research framework to identify technologies needed to help utilities protect, detect, and respond to attacks
- DER cyber threat modeling and resilience metrics to help utilities understand growing risks from renewable energy devices
- DER cyber attack prevention, detection, and response strategies across cyber, physical device, and utility layers of the system
- Demonstration on Washington State University's Smart City Testbed

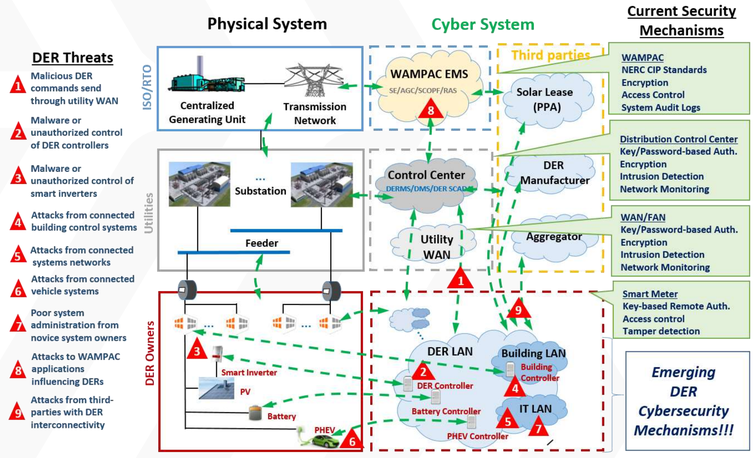
Impacts and Benefits:

- Utilities can use the resilience analysis methodology to evaluate their system and identify vulnerabilities
- Utilities and DER third parties can use the attack prevention, detection, and response strategies to harden their system, rapidly detect cyber attacks, and effectively mitigate attacks
- Smart inverter vendors can improve the cybersecurity of smart inverters using the developed cyber attack detection and mitigation measures and by the developed energy buffer
- Customers and utilities will benefit from the reduced economic cost of power outages with the enhanced security of the distribution grid against outages caused by cyber attacks on DER
- Decrease in net integration cost of DER from the enhanced resilience of the power system against cyber attacks on DER

Significant Milestones	Date
Development of DER cybersecurity framework	Oct. 1, 2016
Design of DER cyber threat modeling and resilience metrics	Apr. 1, 2017
Design of DER attack prevention and detection strategies at cyber, physical device, and utility layers	Apr. 1, 2018
Design of DER attack response strategies and completion of experimental evaluation	Apr. 1, 2019



Attack-resilient framework for DER cybersecurity



Emerging DER architecture and cyber attacks

Progress to Date

Peer-reviewed journal articles and technical reports:

1. J. Qi, A. Hahn, X. Lu, J. Wang, and C. C .Liu, "Cybersecurity for Distributed Energy Resources and Smart Inverters," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28-39, Dec. 2016.
2. Cybersecurity for Renewables, Distributed Energy Resources, and Smart Inverters Research Framework, Technical Report, Oct. 2016.
3. Cyber Attack Modeling and Impact Analysis for Large-Scale Integration of Distributed Energy Resources and Smart Inverters, Technical Report, July 2017.

Prototype Implementations, Design Software Packages and Toolboxes:

1. An advanced data driven machine learning analytics based toolbox for detecting potential cyber-attacks on DER and smart inverters.
2. A prototype implementation of the TEE-based inverter architecture on the Raspberry PI to demonstrate improved security provided by the ARM TrustZone environment.
3. HiL platform to demonstrate DER cyber-attack prevention, detection, and mitigation technologies.

Workshop and conference:

1. NREL workshop on Security & Resilience of Grid Integration with Distributed Energy Resources on 07/13/2016
2. Resilience Week conference on 08/18/2016
3. DOE-OE CEDS Program Peer Review Meeting on 12/07/2016

Improved Forecasts of Electric Outages from Tropical Cyclones

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Project Description

Modified original *HEADOUT* tool to:

- Improve forecasts of electric outages from tropical cyclones and
- Identify infrastructure at risk for tropical cyclone events affecting U.S. territory in the Caribbean, Atlantic seaboard, and Gulf of Mexico regions.

Improved tool would be used by DOE (and others) in preparation for and response to tropical cyclone events.

Major tasks included:

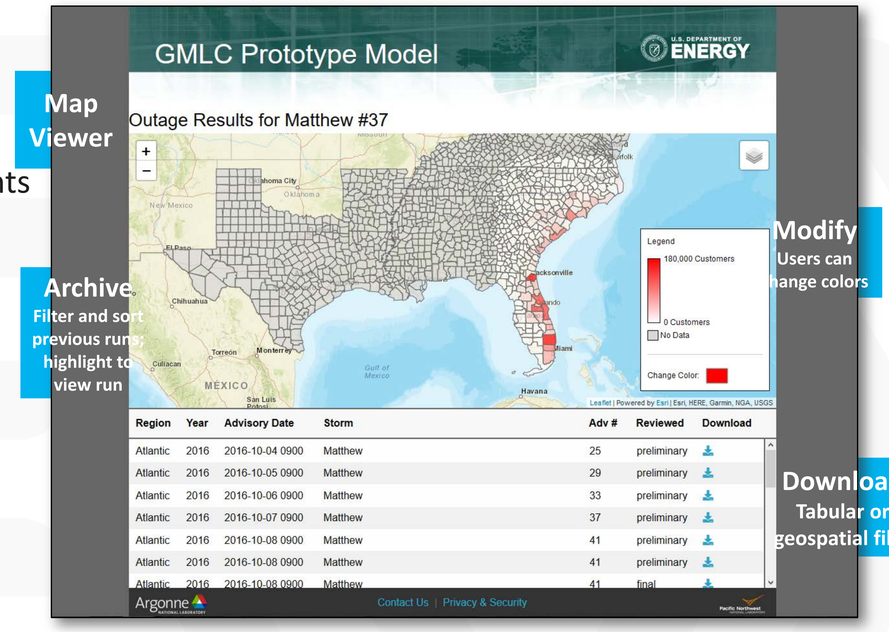
- Enhance high-resolution spatial distribution of U.S. population and households to county block level.
- Apply downscaling algorithm for hurricane-induced storm surge combined with high-resolution topography.
- Develop universal fragility curves (percent damage versus wind speed, rainfall, etc.).
- Modify algorithm with forecast data from National Oceanic and Atmospheric Administration's (NOAA) National Digital Forecast Database (NDFD).

Outcomes and Deliverables

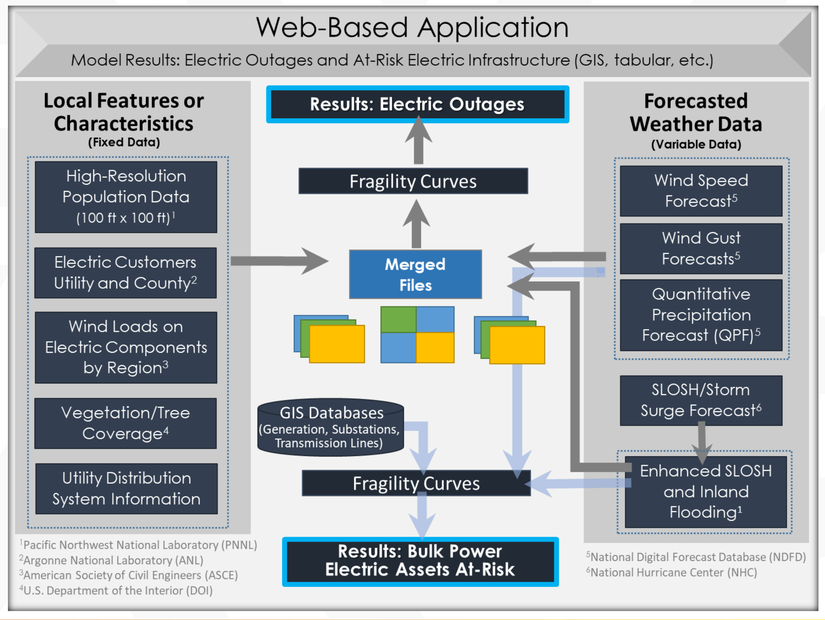
- Developed a web-based model that estimates electric outages at a 100-foot level.
- Model runs in about 10–15 minutes—it downloads NHC data, and determines customer outages and at-risk electrical infrastructure.
- Predicts which bulk power assets (transmission lines, substations, electric generators) are at risk for disruption.

Significant Milestones	Date
Develop population data at the 100-foot by 100-foot level	May 2017
Enhance precision in output from SLOSH model for coastal flooding and storm surge	June 2017
Develop universal fragility curves	June 2017
Modify existing HEADOUT Model to incorporate NOAA weather feeds	Aug. 2017
Determine impacts from tropical cyclones to electric infrastructure assets	Sept. 2017

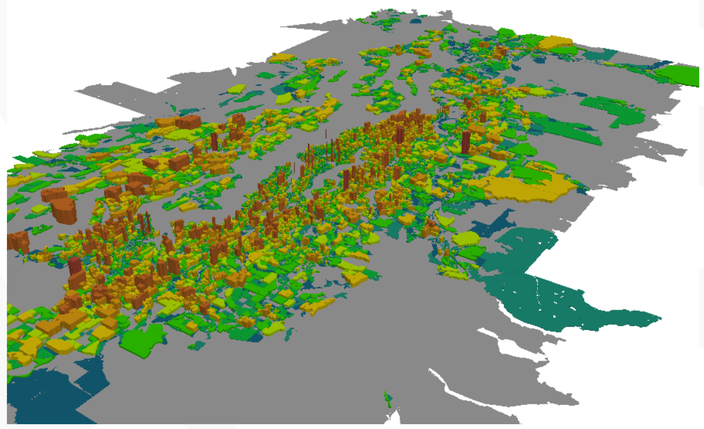
Tropical Cyclone Tool Web Interface



Tropical Cyclone Tool Architecture



Example Enhanced Population Data

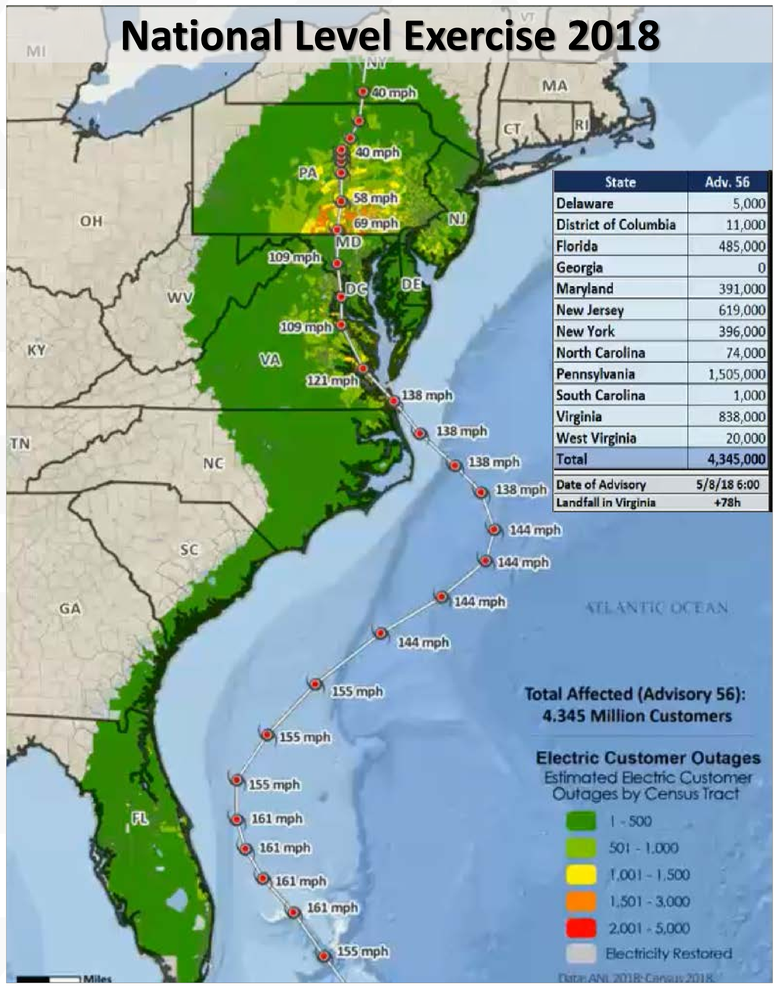


Population Density at 60-meter Resolution

Progress to Date

- Beta version of Tropical Cyclone Tool developed and tested.
- Tool validated against three recent hurricanes (Matthew, Harvey, and Nate), with predicted results for 2016 Hurricane Matthew within 30% of county actuals.
- Applied to three recent synthetic hurricane scenarios:
  - 2018 PJM Interconnection Spring Restoration Drill
  - Midcontinent Independent System Operator (MISO) 2018 Spring Drill
  - 2018 National Level Exercise (NLE)—Clear Path
- Tool results provided to and reviewed by:
  - PJM Interconnect and MISO (and multiple member utilities)
  - American Public Power Association (APPA), 74 utilities
  - Other affected utilities

National Level Exercise 2018



U.S. DEPARTMENT OF ENERGY

Stephen Folga and Leah Talaber, Argonne National Laboratory
Alan Bercheid and David Judi, Pacific Northwest National Laboratory

September 5, 2018

A Closed-Loop Distribution System Restoration Tool for Natural Disaster Recovery

PI: Chen Chen, Argonne National Laboratory
Team Members: Bo Chen, Duc Vu, Argonne National Laboratory
Meng Yue, Brookhaven National Laboratory
Zhaoyu Wang, Iowa State University

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Project Description

Objective: Develop a distribution system restoration decision support tool to assist distribution utility operators in making optimal and effective decisions for distribution system restoration under extreme weather events. This is a synergistic collaborative project among national labs, university, utilities, and vendors.

Expected Outcomes

Deliverables:

- A probabilistic data fusion framework to improve situational awareness of distribution grids after extreme weather hazards integrating multiple sources of information, including weather, measurements from field devices, and data from customers' end.
- Repair crew dispatch and resource allocation optimization models and solutions
- Optimal grid reconfiguration and load pick-up methodologies by utilizing distributed generation and automated switches to reduce outage sizes and durations to facilitate supply continuity.
- A Python based software tool with GUI and technical report

Impacts and Benefits

- Utilities can use the tool to expedite the restoration process and facilitate supply continuity
- Customers will benefit from the reduced sizes and durations of power outages
- ISO/RTOs will be able to use the methodologies to coordinate transmission-level restoration processes with distribution-level utilities to improve the overall system restoration
- Regulatory agencies will have a quantitative method to evaluate the resilience enhancement of distribution systems.
- Vendors may be able to use the tool to specify the requirements for development of devices and outage management systems

Significant Milestones	Date
An integrated framework development for the distribution system restoration decision support tool under natural disasters	09/01/2016
An alpha version of the restoration tool with functionalities of major modules completed	06/01/2017
A beta version of the restoration tool with software development based on Python completed	06/01/2018
Validation, testing, and demonstration of the restoration tool on test cases and possible real distribution systems with utility partners	06/01/2019

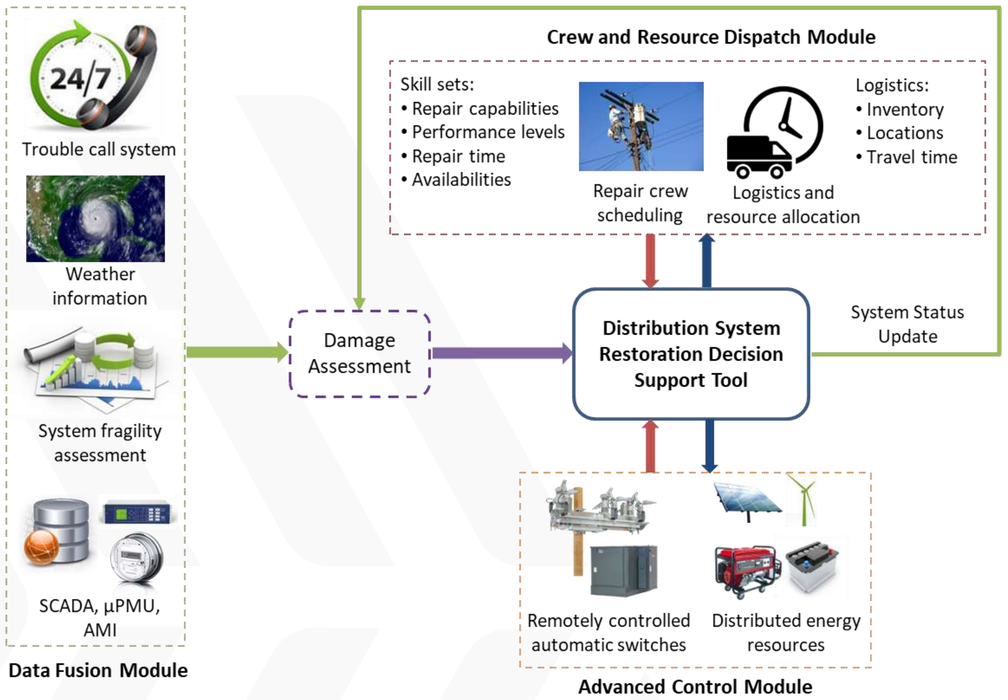


Figure 1: Framework of Distribution System Restoration Decision Support Tool

Progress to Date

Peer-reviewed journal articles:

1. C. Chen, J. Wang, D. Ton, "Modernizing Distribution System Restoration to Achieve Grid Resiliency Against Extreme Weather Events: An Integrated Solution", *Proceedings of the IEEE*, vol.105, no.7, pp.1267-1288, 2017.
2. B. Chen, C. Chen, J. Wang, K. Butler-Purry, "Sequential Service Restoration for Unbalanced Distribution Systems and Microgrids", *IEEE Trans. on Power Systems*, vol.33, no.2, pp.1507-1520, 2018.
3. B. Chen, C. Chen, J. Wang, K. Butler-Purry, "Multi-Time Step Service Restoration for Advanced Distribution Systems and Microgrids", *IEEE Trans. on Smart Grid*, in press.
4. Z. Wang, J. Wang, C. Chen, "A Three-Phase Microgrid Restoration Model Considering Unbalanced Operation of Distributed Generation", *IEEE Trans. on Smart Grid*, vol.9, no.4, pp.3594-3604, 2018.
5. A. Arif, Z. Wang, J. Wang, C. Chen, "Power Distribution System Outage Management with Co-Optimization of Repairs, Reconfiguration, and DG Dispatch", *IEEE Trans. on Smart Grid*, vol.9, no.5, pp.4109-4118, 2018.
6. M. Yue, T. Toto, M. P. Jensen, S. Giangrande, "A Bayesian Approach Based Outage Prediction in Electric Utility Systems Using Radar Measurement Data," *IEEE Trans. on Smart Grid*, in press.
7. A. Arif, S. Ma, Z. Wang, J. Wang, S. Ryan, and C. Chen, "Optimizing Service Restoration in Distribution Systems with Uncertain Repair Time and Demand," *IEEE Trans. on Power Systems*, in press.

Workshop and conference presentations:

1. DOE-OE MYPP Workshop on Resilient Electric Distribution Grid, 07/12/2016.
2. 2016 DOE Smart Grid R&D Program Peer Review Meeting, Chicago, 08/16/2016.
3. Eversource Energy Center and EPRI workshop on predictive analytics and storm situational awareness for grid resilience, 01/19/2017.
4. IEEE PES T&D Conference and Exposition Panel Session, Denver, 4/19/2018.
5. 2018 DOE Smart Grid R&D Program Peer Review Meeting, Charlotte, 6/6/2018.
6. IEEE Smart Grid Webinar, 08/02/2018.

Diagnostic Security Modules for Vehicle to Building Integration

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

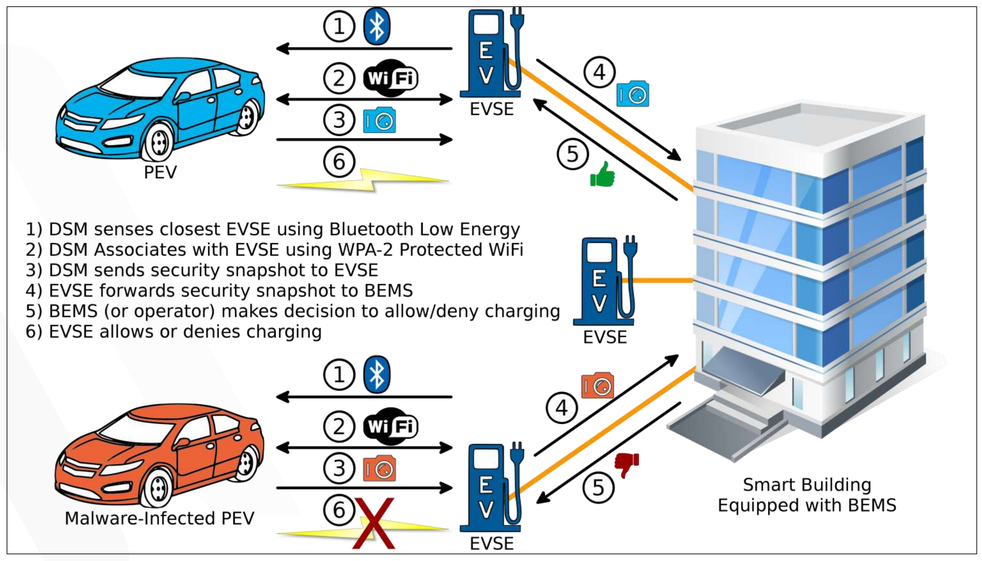
Project Description

Developing a Diagnostic Security Module (DSM) Framework to provide secure communications between electric vehicles (EVs), Electric Vehicle Supply Equipment (EVSE), and Building Energy Management Systems (BEMS)

Expected Outcomes

- Provide near real-time information regarding the security state of the monitored systems so that operators can make informed decisions and allow or deny EV charging
- Demonstrate a multi-vendor integrated environment running hardware, software, and monitoring algorithms that exchange security health information with a centralized server and operator
- Publish all findings and developed methods and algorithms to aid in the adoption of emerging security and protocol standards (SEP 2.0, SAE J2931/7, ISO 15118-1, DIN 70121, OCPP, etc.)

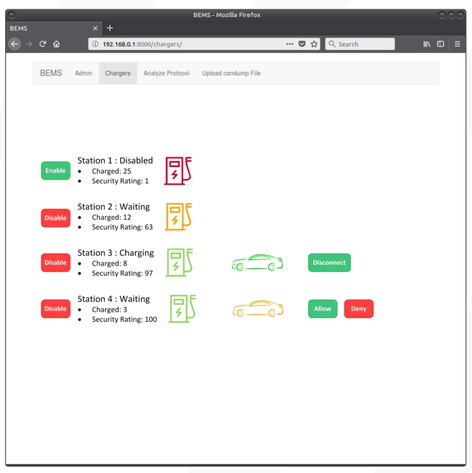
DSM Communications Overview

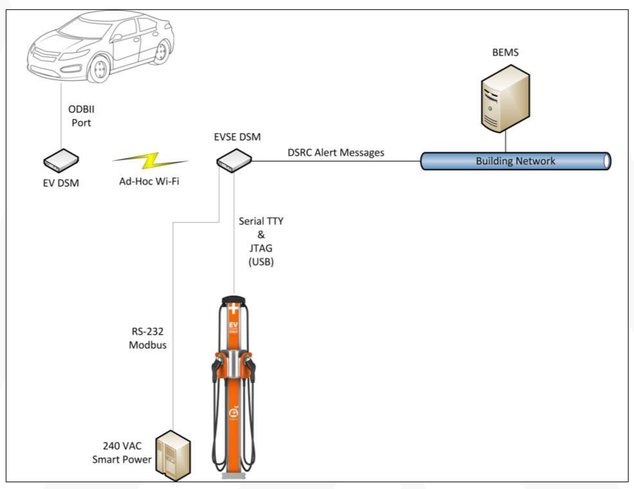


Progress to Date

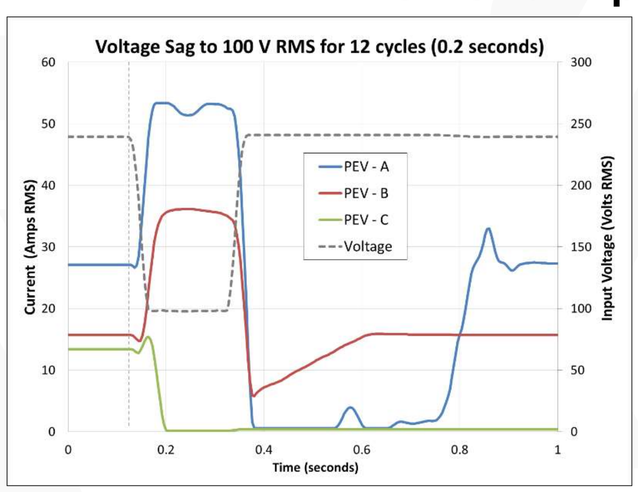
- Cyber Security assessments of two commercial Level-2 AC EVSE and one DC Fast Charger
- DSM nodes and framework undergoing beta testing
- Develop DSM hardware and algorithms for monitoring DCFC and the connected EV
- Simulation and evaluation of potential EVSE grid impacts

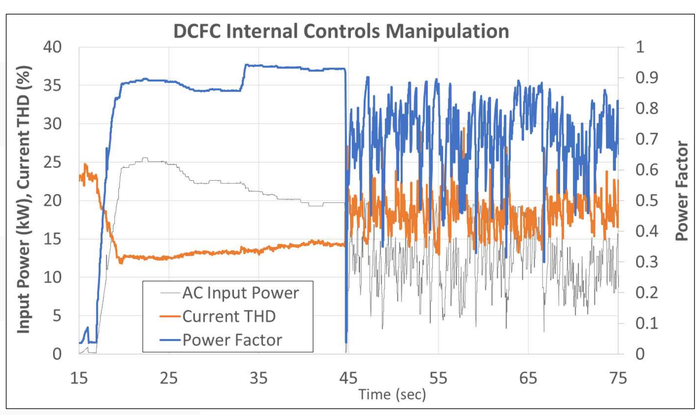
DSM Hardware and Software





EVSE Grid Impacts





Significant Milestones	Date
EVSE Cyber Assessments Complete and Reports Sent to Vendors	June 2017
Initial DSM (BEMS-to-EVSE-to-EV) Framework Implemented	May 2018
Demonstration of DSM System at CyberAUTO 2019	July 2019

Secure, Scalable Control and Communications for Distributed PV

PI: Jay Johnson, jjohns2@sandia.gov
Project Team: Raymond Byrne, Bryan Richardson, Keith Schwalm, Nick Jacobs, Christine Lai, Patricia Cordeiro, Ifeoma Onunkwo, Jimmy Quiroz, Felipe Wilches Bernal, Brian Wright, Ricky Concepcion, Trevor Hutchins, Matt Reno, Shamina Hossain-McKenzie, Adrian Chavez, Ross Guttromson

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Project Description

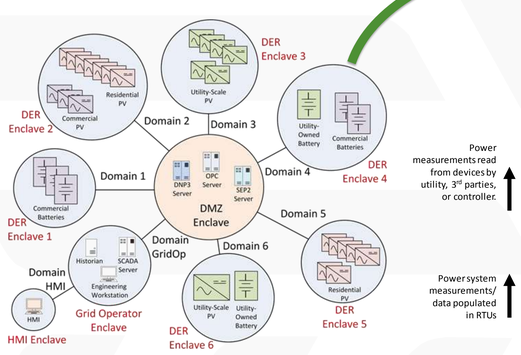
This project seeks to determine communication requirements and cybersecurity recommendations for a range of grid services when using a distributed energy resource (DER) control network. To effectively provide specific grid services (e.g., voltage regulation, frequency reserves, protection, etc.) with DER devices, specific latency, networking dropout tolerance, and communication availability requirements exist. Using these performance requirements as a guide, appropriate cybersecurity architectures have been designed to provide grid services while maximizing control network security. These architectures are simulated and evaluated using an adversary-based assessment methodology to quantify their effectiveness.

Expected Outcomes

- Networking requirements and optimal cyber-secure control architectures will be determined for multiple grid services, including:
  - Distribution circuit voltage protection
  - Synthetic inertia to support the bulk power system
- Cybersecurity network penetration tests will be conducted on a communication and power co-simulation to indicate methods to improve the U.S. power system cybersecurity posture.
- This work will inform utilities, grid operators, DER vendors, and DER aggregators of recommended cyber-secure reference architectures to provide secure grid-support services.

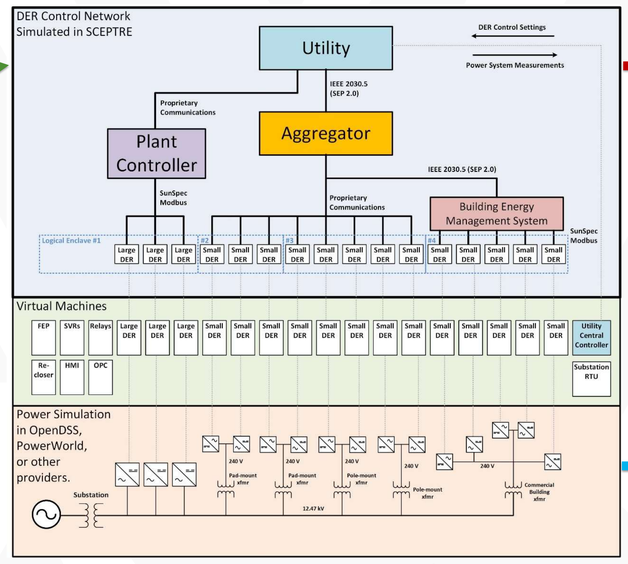
This project uses SCEPTRE—a live, virtualized power system and control network co-simulation platform developed at Sandia—to investigate the tradeoff between power system performance and cyber resilience. Network architectures and power simulations are input into SCEPTRE to produce power system performance and cybersecurity metrics, which can then be used to advise the industry on best cybersecurity practices for DER networks.

Different control architectures are virtualized in the SCEPTRE environment.



Segmentation strategy where no more than 20% of generation is placed in one enclave. Enclaves are constructed using firewall rules, hardware proxies, or virtual private networks (encrypted tunnels between the grid operator and the DER) to minimize common-mode vulnerabilities. If an adversary gains access to one of the enclaves, they cannot control the utility/aggregator power devices in the other enclaves—reducing the risk of widespread grid failures.

SCEPTRE

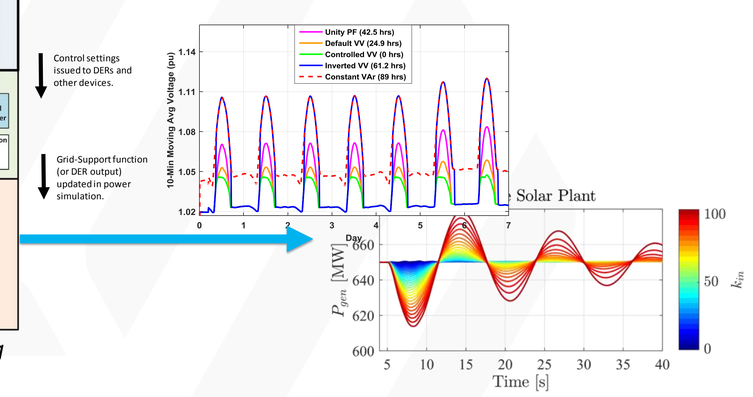


SCEPTRE provides a comprehensive ICS/SCADA modeling and simulation hardware-in-the-loop capability that captures the cyber-physical impacts of controls systems and targeted cyber events. Changes in the network are reflected in the power simulation, and changes in the power simulation are reflected in the communication system, thereby, allowing researchers to analyze the complex interactions in an cyber-physical environment.

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
	Med-ium	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

Red team assessments of the simulated DER control network are conducted to generate performance scores for each network architecture scenario.



SCEPTRE interfaces with and runs different power simulation programs (pypower, PowerWorld, OpenDSS) depending on the use case. These simulations coupled to the simulated control network demonstrate the performance of DER grid-support control functions under different cybersecurity architectures, protocols, and additional security features.

Significant Milestones	Date
Determine grid service performance when varying the SunShot communication metrics of availability and latency.	11/30/16
Development of cybersecurity reference architecture.	11/30/17
Quantify increased latency from various cybersecurity schemes	11/30/18
Comparison of control/communications complexity for different approaches	11/30/18

Progress to Date

- Determined communication requirements for multiple distribution and transmission grid services.
- Completed installation of communication network and power co-simulation capability at Distributed Energy Technologies Laboratory (DETL) at Sandia National Labs.
- Deployed multiple communication network topologies with diverse security features (enclaving, encryption, moving target defense) in SCEPTRE to evaluate communication latency and cyber resilience.
- Red-team assessment methodology created for the adversary-based evaluations of the virtualized DER networks.

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. SAND2018-9159 D