Security and Resilience Portfolio Overview

Juan Torres

National Renewable Energy Laboratory

DOE GMI Peer Review, September 4-7, 2018

Security and Resilience

GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

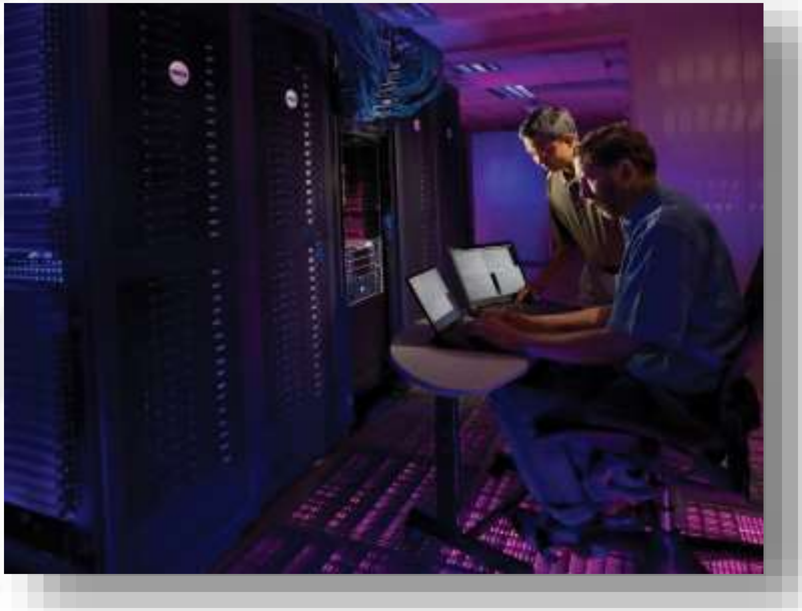
Providing a pathway to comprehensive multi-scale security and resilience for the nation’s power grid

Expected Outcomes

- Holistic grid security and resilience, from devices to micro-grids to systems
- Inherent security designed into components and systems, not security as an afterthought
- Security and resilience addressed throughout system lifecycle and covering the spectrum of legacy and emerging technologies

Federal Role

- Lead and establish security and resilience research programs to develop technology solutions and best practice guidance
- Improve adoption of security and resiliency practices, and provide technology-neutral guidance
- Inform stakeholders of emerging threats and help address threats appropriate for government response



MYPP Activities and Achievements by 2020

An All-Hazards Approach Based on NIST Cybersecurity Framework

Identify:

Develop understanding of threats, vulnerabilities, and consequences to all hazards

Outcome: Improved risk management and streamlined information sharing

Protect:

Inherent system-of-systems grid resilience

Outcome: Increase the grid’s ability to withstand malicious or natural events

Detect:

Real-time system characterization of events and system failures

Outcome: Accelerated state awareness and enhanced event detection

Respond:

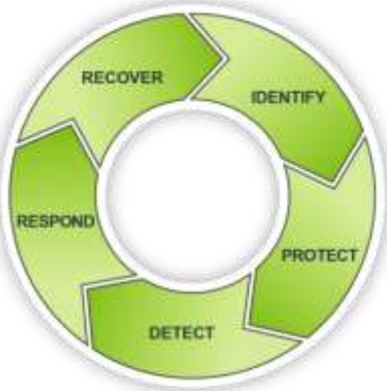
Maintain critical functionality during events and hazards

Outcome: Advanced system adaptability and graceful degradation

Recover:

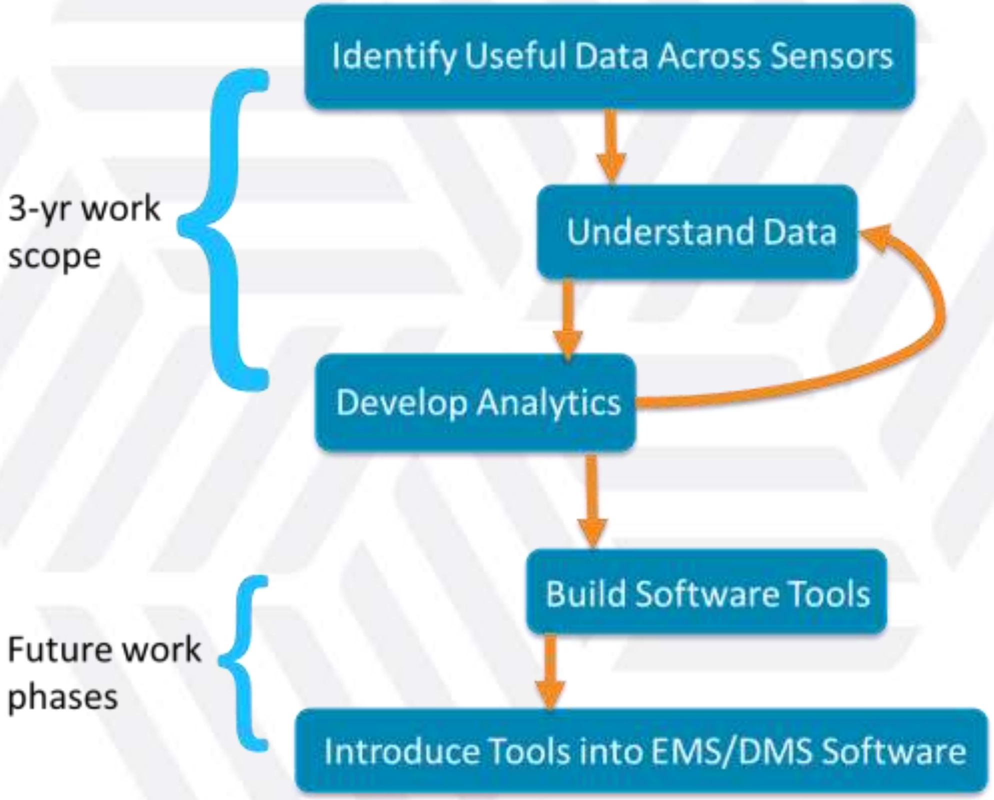
Real-time device management and transformer mobilization

Outcome: Timely post-event recovery of grid and community operations



1.4.23 - Threat Detection and Response with Data Analytics

Develop advanced analytics on operational technology (OT) cyber data in order to detect complex cyber threats. Differentiate between cyber and non-cyber-caused incidents using available cyber data.



PoP: FY16/17/18

Budget: $3M

Labs: LLNL, LBNL, INL, ORNL, PNNL, SNL

Partners:

- Electric Power Board (EPB)
- Johnson Controls
- Schweitzer Engineering Laboratories (SEL)

Connections and Collaborations

Foundational and Program Projects

MYPP Area	Foundational Projects	Program Specific Projects
Identify		GM0119 - Improved Forecasts of Electric Outages from Tropical Cyclones (ANL, PNNL) GM0217 - Web Tool for Improved Electric Outage Forecasting for Response to Tropical Cyclone Events (LANL, PNNL)
Protect	1.3.04 - Industrial Microgrid in KY 1.3.11 - Infrastructure Resilience – NOLA	GM0068 - MultiSpeak® - Secure Protocol Enterprise Access Kit (MS-SPEAK) (PNNL) GM0100 - Cybersecurity for Renewables, Distributed Energy Resources, and Smart Inverters (ANL) SI1541 - Secure, Scalable, Stable Control and Communications for Distributed PV (SNL)
Detect	1.4.23 - Threat Detection and Response with Data Analytics	GM0163 - Diagnostic Security Modules for Electric Vehicle to Building Integration (INL, ANL, NREL, PNNL)

Connections and Collaborations

Foundational and Program Projects

MYPP Area	Foundational Projects	Program Specific Projects
Respond		(GM0131) - A Closed-Loop Distribution System Restoration Tool for Natural Disaster Recovery (ANL, BNL)
Recover		(GM0180) - Recommendations for the population, location, and operation of a strategic transformer reserve (ORNL, SNL)

Accomplishments and Emerging Opportunities

Accomplishment

- 1.3.04: Kentucky Industrial Microgrid: Modeling and simulation have resulted in improvements to existing DOE microgrid analysis tools.
- 1.3.11: NOLA Resilience: First ever meeting between partners to collaboratively prioritize resilience-focused grid investments in NOLA.
- 1.4.23: Developed several data analytics algorithms to differentiate between cyber and non-cyber anomalies

Path Forward

- 1.3.04: Project completed – Advancements to open source Microgrid Design Tool Kit.
- 1.3.11: Project completed – Apply learnings to other communities, e.g. Puerto Rico.
- 1.4.23: Correlate data sets, generalize results, identify which data is useful and not useful in cyber attack response.

Summary

- Security and Resilience is critical to grid modernization
- Program elements leverage NIST Cybersecurity Framework
- Foundational/Demonstration Projects
  - 1.3.04: Industrial Microgrid – KY
  - 1.3.11: Infrastructure Resilience – NOLA (Complete)
  - 1.4.23: Threat Detection and Response with Data Analytics – distinguish cyber attacks from physical and other signatures
- Eight program specific projects support MYPP goals
- Outcomes of Security and Resilience Projects are making impact in today's and tomorrow's grid

GRID MODERNIZATION INITIATIVE PEER REVIEW
1.4.23 Threat Detection and Response with Data Analytics

JOVANA HELMS, PHD
ASSOCIATE PROGRAM LEADER
LAWRENCE LIVERMORE NATIONAL LABORATORY

September 4–7, 2018

Sheraton Pentagon City Hotel – Arlington, VA

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

1.4.23 Threat Detection and Response with Data Analytics
High-Level Project Summary

Project Description
Develop advanced analytics on operational technology (OT) cyber data in order to detect complex cyber threats. Differentiate between cyber and non-cyber-caused incidents using available cyber data.

Project Objectives

- ✓ Evaluate which sensor data is most valuable and could provide the biggest positive impact (in terms of grid resiliency/security) if an event is successfully detected.
- ✓ Develop analytics to identify emerging cyber incidents on the electric grid using this OT data identified in the previous objective.
- ✓ Attempt to differentiate cyber grid incidents from other grid hazard incidents, such as physical attacks, natural hazards, etc. Make determinations about the type of incident and root cause so that operators can formulate response/mitigation plans.

Value Proposition

- ✓ Understanding which data can be used to detect cyber events can inform and prioritize data collection and analysis
- ✓ Analytics being developed will assist asset owners in triaging grid incidents
- ✓ Identifying incidents in a timely manner reduces outages and associated costs.

1.4.23 Threat Detection and Response with Data Analytics
Project Team

Performers:

LLNL – AMI analytics, PI

LBNL – Inverter analytics, +1

PNNL – Buildings-to-grid system analytics

SNL – SEL Ethernet Gateway analytics

PROJECT FUNDING			
Lab	FY16 $	FY17$	FY18 $
INL	240K		
LBNL	240K	160K	170K
LLNL	210K	210K	210K
ORNL	35K		
PNNL	35K	160K	255K
SNL	240K	155K	55K

Partners*:*

Electric Power Board (EPB) – Data, testing, and demo partner

Johnson Controls – Donating automation system hardware and software

Schweitzer Engineering Laboratories (SEL) – Data, testing, and demo partner

Pecan Street – Data, support

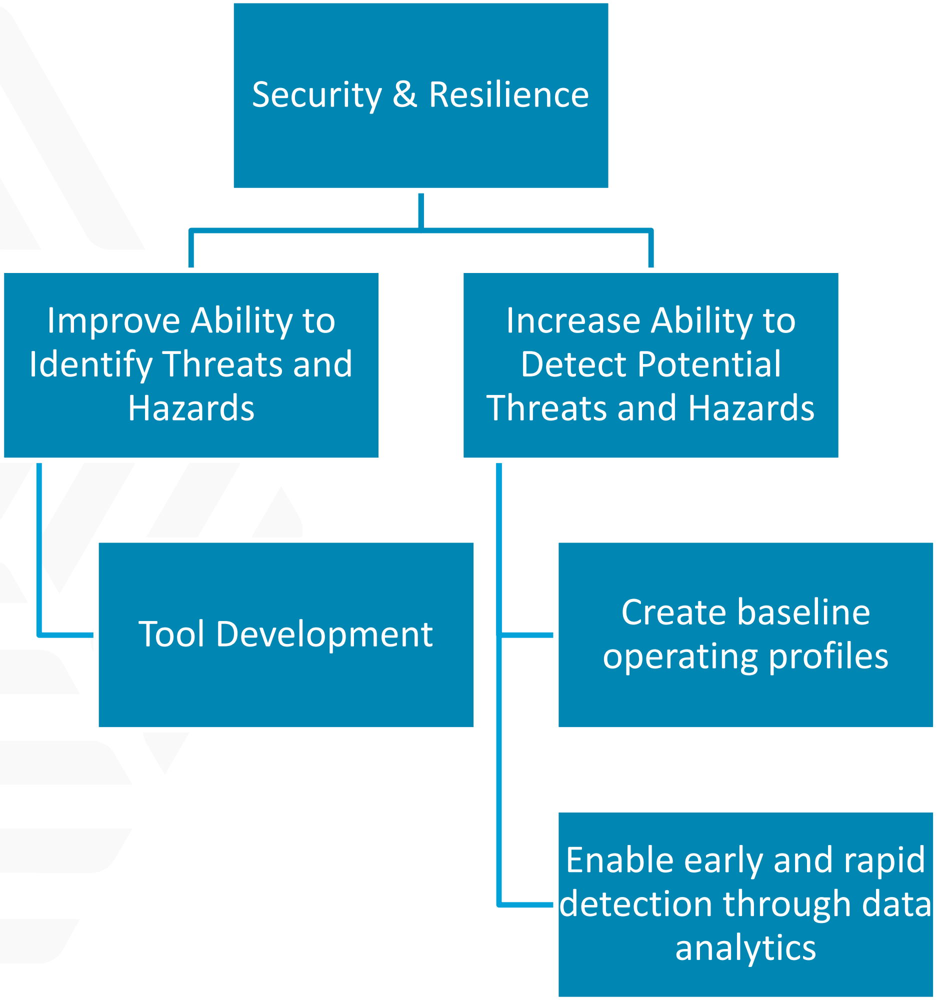
Austin Energy – potential partner for testing, donated smart meters

1.4.23 Threat Detection and Response with Data Analytics

Relationship to Grid Modernization MYPP

- This project addresses the Security & Resilience technical area by focusing on:
  - □ Improving the Ability to ***Identify*** Threats and Hazards
  - □ Increasing the Ability to ***Detect*** Potential Threats and Hazards

- We will conduct research and development on:
  - □ Data analytic tools to enhance early and rapid identification and detection of cyber threats
  - □ Baseline operating profiles as compared to off-normal profiles



Security & Resilience

Improve Ability to Identify Threats and Hazards

Increase Ability to Detect Potential Threats and Hazards

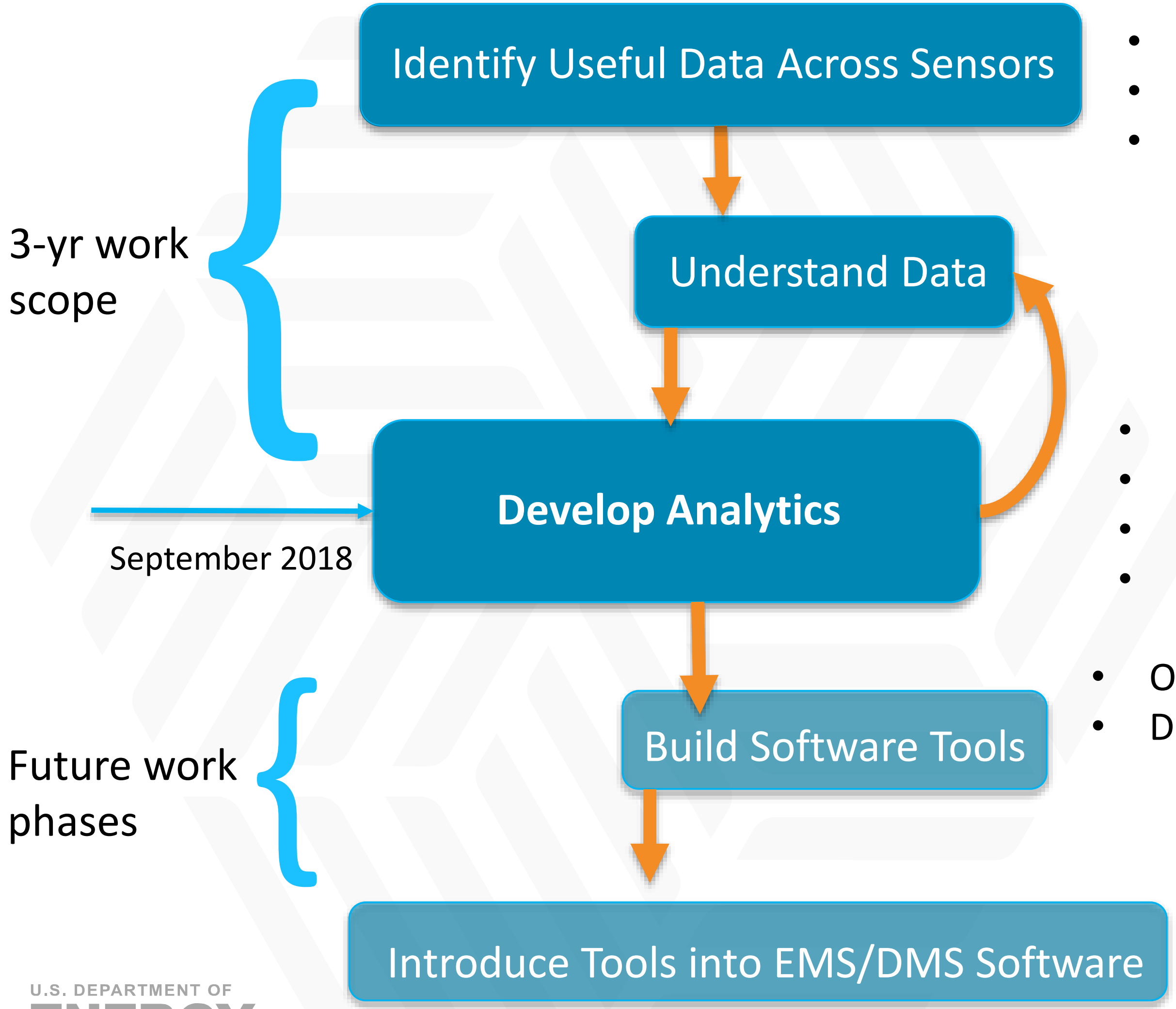
Tool Development

Create baseline operating profiles

Enable early and rapid detection through data analytics

1.4.23 Threat Detection and Response with Data Analytics

Approach



3-yr work scope

Future work phases

Identify Useful Data Across Sensors

Understand Data

Develop Analytics

September 2018

Build Software Tools

Introduce Tools into EMS/DMS Software

- Smart inverters
- Buildings-to-grid sensors
- Ethernet gateway
- AMI

- Temporal characteristics
- Locality
- Volume
- Events

- Integrate data
- Write algorithms in prototype tools
- Early demonstrations
- Iterate

- Operationalize
- Demonstrate

- Identify industry partners

1.4.23 Threat Detection and Response with Data Analytics

Approach

- ► Develop analytics for DERs, substations, AMI, and microgrids that fuse physical and cyber information
  - □ Examine physical sensors (µPMUs, AMI, SEL-3620, and more traditional sensors) useful for detecting attacks
  - □ Simulate cyber attacks on battery storage systems, power inverters, and power meters
  - □ Evaluate sensed data and compare to predicted/expected values
  - □ Use statistical analysis and machine learning to identify cyber anomalies (as opposed to existing techniques that focus on operational and customer relations issues)
- ► Develop analytics for buildings-to-grid applications
  - □ Use PNNL Buildings-to-Grid testbed to study facility-level attacks that may have grid impact

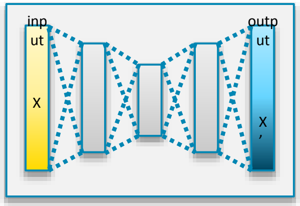
1.4.23 Threat Detection and Response with Data Analytics

Accomplishments to Date: Smart Meter Data

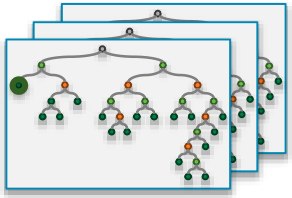
Technical Insights

- ❑ Obtained data from Pecan Street in December 2017
  - ✓ Meter Events
  - ✓ Power Consumption (5 / 15) minute intervals
  - ✓ Partnering with Austin Energy
- ❑ Developed several data analytics algorithms that leverage raw smart meter data to detect anomalies (06/08/2018)
  - ✓ System allows the inclusion of more algorithms in a generic fashion
  - ✓ Correlating meter event data load profile
- ❑ Acquired 8 smart meters and are currently in the process of installing them in the test lab (09/2018)
  - ✓ Will allow us to generate a cyber-attack-baseline that we can use to fine-tune our anomaly detectors
- ❑ DDoS and meter data spoofing attacks will be implemented in Skyfall testbed (12/2018)
- ❑ To differentiate between cyber and non-cyber anomalies we must create a baseline

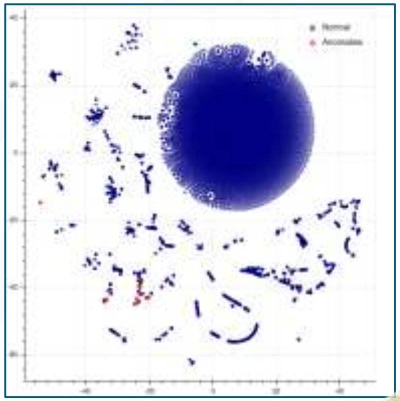
Local Outlier Factor

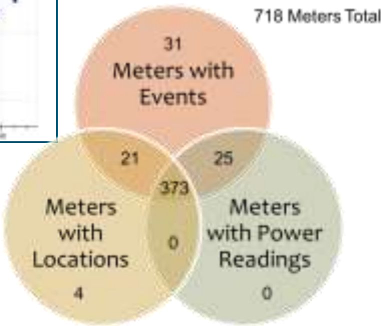


Autoencoder



Isolation Forest





Engagements: Pecan Street, Austin Energy

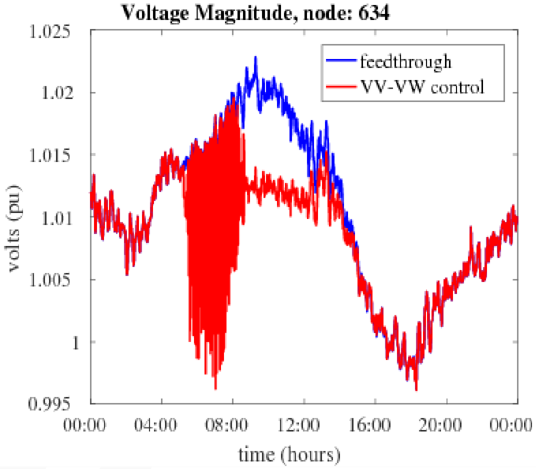
Distinctive Characteristics: Approach works directly on raw smart meter data and combines machine learning algorithms in a generic fashion that allows the addition of more algorithms while increasing performance.

1.4.23 Threat Detection and Response with Data Analytics

Accomplishments to Date: Smart Inverter Data

Technical Insights

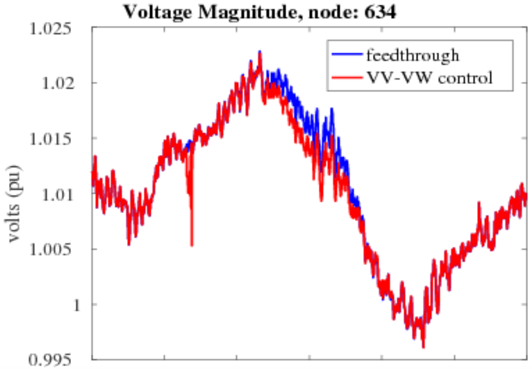
- ❑ Developed nonlinear feedback control model of DER smart inverter functions (11/2017)
- ❑ Conducted stability analysis of interaction of DER feedback control model on distribution system voltage stability (04/2018)
- ❑ Developed adaptive control approach to enable model-free and no-communication strategy to mitigate effect of cyber attack (07/2018)



Voltage profile during instability

Engagement/Preparation

- ❑ Engaging NRECA to gather feedback from NRECA member utilities (12/2018)
- ❑ Journal paper in preparation (10/2018)



Voltage profile when DER have adaptive control

Distinctive Characteristics: When compromised DER (who have had their control parameters adjusted) create an instability in the distribution grid, this approach re-dispatches settings in non-affected DER to automatically mitigate the attack.

1.4.23 Threat Detection and Response with Data Analytics

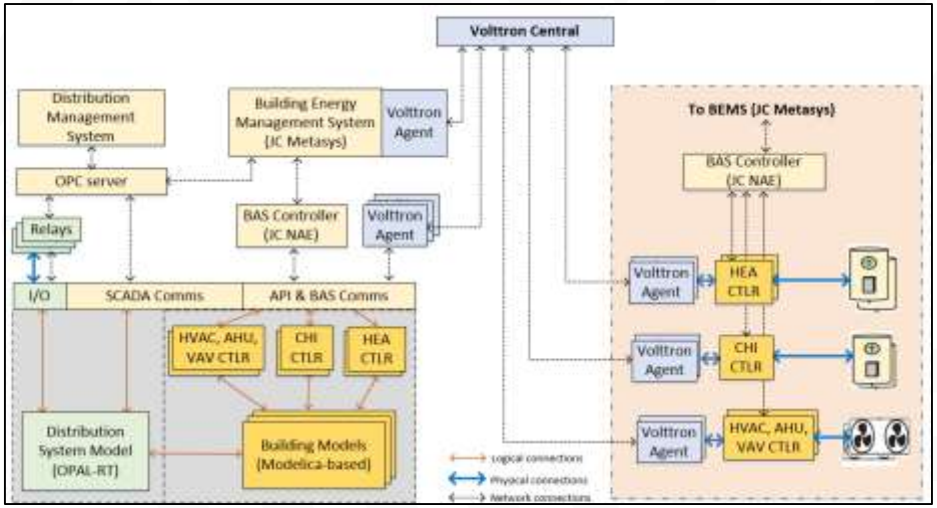
Accomplishments to Date: Building-to-Grid Data

Technical Insights

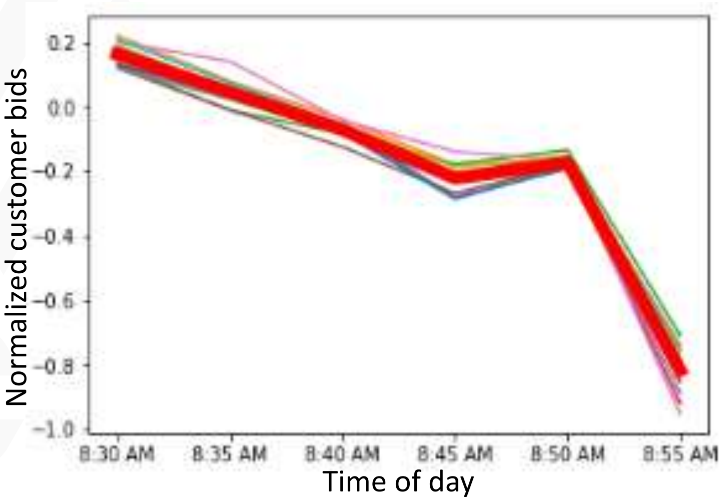
- ❑ Data integrity attacks on transactive control impact operations, economics, and comfort. [08/18]
- ❑ Consumers can be grouped into clusters with similar characteristics, which can be used for attack detection. [08/18]
- ❑ Correlations between grid physics and cyber data can be baselined to characterize normal operation. [03/19]

Engagement/Publications

- ❑ 3 conference publications (1 accepted, 2 to be submitted Aug 31).
- ❑ Cyber-physical correlation using ELK and validation using realistic datasets. [03/19]
- ❑ Testbed implementation using JC Metasys. [03/19]
- ❑ Exploring collaboration and demonstration opportunities with industry partners.



Testbed for attack defense experimentation and demonstration



Clustered by bidding strategy (normalized bids vs. time)

Distinctive Characteristics: Clustering and neural networks-based baselining of consumer behavior, load variation and communication patterns, and validation using transactive control datasets.

1.4.23 Threat Detection and Response with Data Analytics

Accomplishments to Date: Ethernet Gateway Data

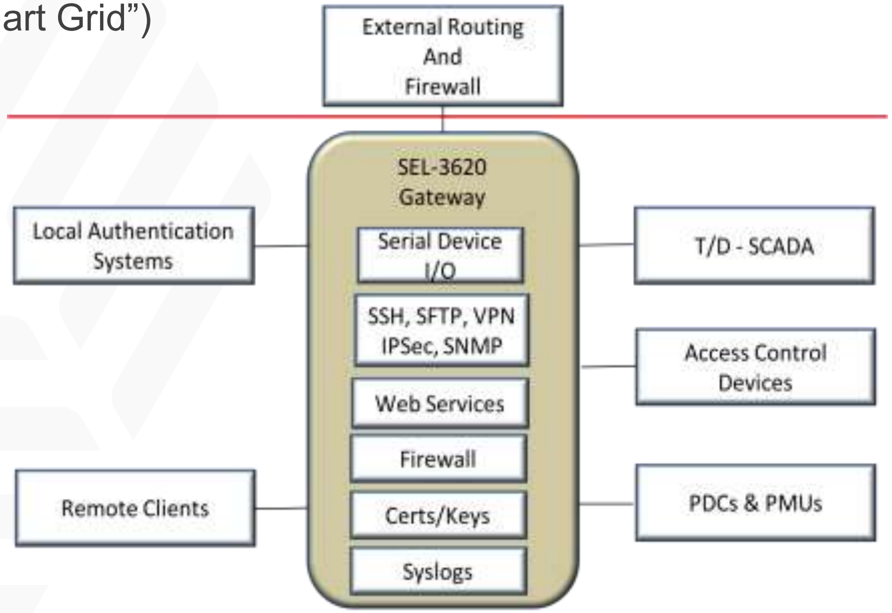
Technical insights

- ❑ Developed multipath machine learning algorithms to identify lowest risk communication paths (7/2017)
- ❑ Machine learning algorithms distinguishing cyber events from physical events based on SEL-3620/3622 syslog data (3/2017)

Engagement/Publications

- ❑ Working with Idaho Power, Fort Belvoir, Sandia's Distributed Energy Technology Laboratory (DETL) testbed, and SEL to obtain datasets and apply/evaluate ML algorithms (2/2017)
- ❑ Paper ("Behavioral Based Trust Metrics and the Smart Grid") accepted and presented at the IEEE TrustCom-18 conference (5/2018)
- ❑ Proof-of-concept developed and applied to several environments (Fort Belvoir, Idaho Power, and DETL) (4/2018)

Distinctive Characteristics: Approach has access to the entire packet payload, rather than being limited to the header.



SEL 3620 Security Gateway Placement

1.4.23 Threat Detection and Response with Data Analytics

Next Steps and Future Plans

- ❑ **Next Steps:**
  - ✓ Create baseline of what cyber attacks look like in smart meter data using smart meter hardware in the loop simulations (12/2018)
  - ✓ Conduct simulation experiments on larger and unbalanced networks
  - ✓ Testbed-based attack-defense experimentation (integration with ICS hardware/software) and demonstration of tech (03/2019)
- ❑ **Possible Integration:**
  - ✓ Sharing data sets
  - ✓ Correlating data sets – quantify whether performance improves with data fusion
- ❑ **Impact:**
  - ✓ The smarter the grid gets the more it is vulnerable to cyber attacks
  - ✓ This project informs which data sources are useful in detecting cyber attacks enabling timely and effective response
  - ✓ Which data is NOT useful is equally informative
  - ✓ Leveraging the “smartness” of devices to increase the resilience against cyber attacks
  - ✓ This research will enable asset owners and industry partners to collect the most relevant data for cyber attack detection, generate baseline of normal behavior and detect anomalies that can indicate the system is under cyber attack