GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

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

JAMIE VAN RANDWYK, LLNL

April 18-20, 2017

Sheraton Pentagon City – Arlington, VA

1.4.23 Threat Detection and Response with Data Analytics

High Level 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.

Value Proposition

- ✓ Analytics being developed will assist asset owners in triaging grid incidents
- ✓ Identifying incidents in a timely manner reduces outages and associated costs

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.

1.4.23 Threat Detection and Response with Data Analytics

Project Team

Project Participants and Roles

LLNL – AMI analytics, PI

LBNL – Inverter analytics, Plus one

INL – Physics-centric / cyber threat fusion and analysis

ORNL – Smart-grid outage data analytics

PNNL – Building automation system analytics

SNL – SEL Ethernet Gateway analytics

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

PROJECT FUNDING

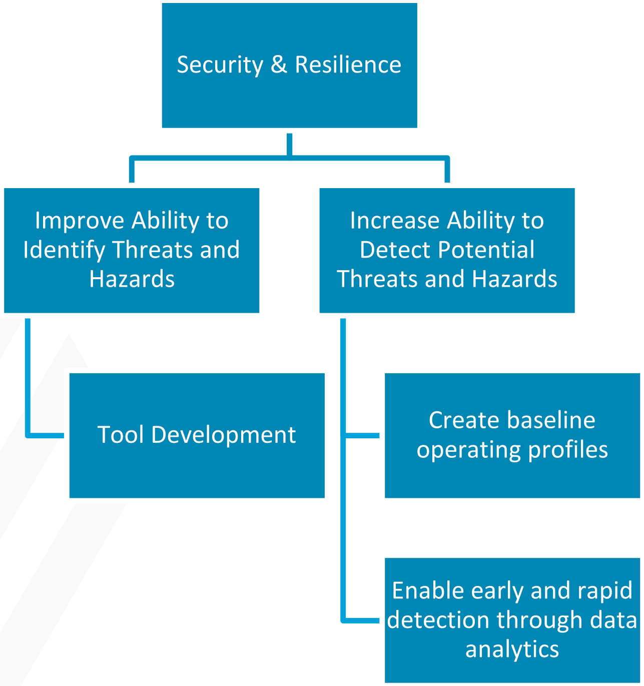
Lab	FY16 $	FY17$	FY18 $
INL	240K	155K	55K
LBNL	240K	160K	170K
LLNL	210K	210K	210K
ORNL	35K	160K	255K
PNNL	35K	160K	255K
SNL	240K	155K	55K

1.4.23 Threat Detection and Response with Data Analytics

Relationship to Grid Modernization MYPP

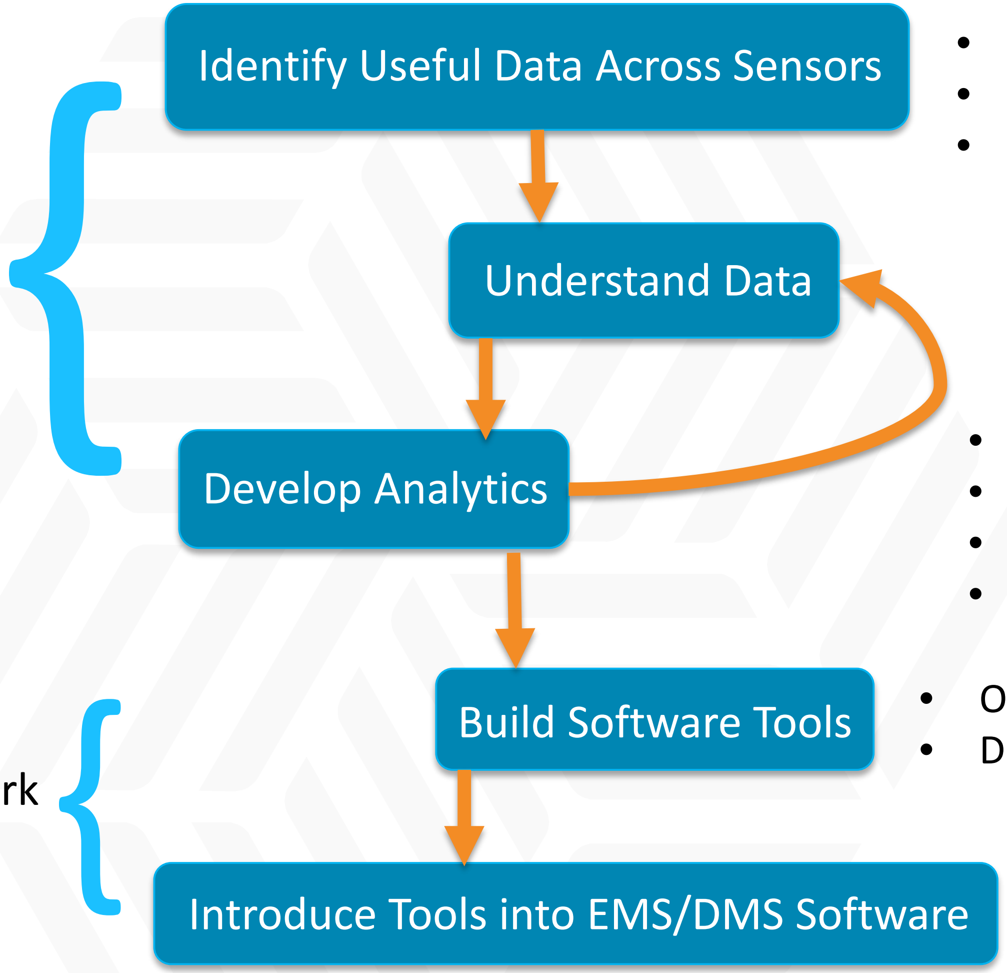
- ► This project addresses the Security & Resilience technical area by focusing on:
  - □ Improving the Ability to ***Identify*** Threats and Hazards
  - □ Increasing the Ability to ***Detect*** Potential Threats and Hazards

- ► 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

Identify Useful Data Across Sensors

- Power inverters
- Battery storage systems
- µPMUs
- AMI

Understand Data

- Temporal characteristics
- Locality
- Volume

Develop Analytics

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

Future work phases

Build Software Tools

- Operationalize
- Demonstrate

Introduce Tools into EMS/DMS Software

- 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 building automation systems (BAS)
  - □ Use PNNL Buildings-to-Grid testbed to study facility-level attacks that may have grid impact
- ► Develop analytics using outage data
  - □ Leverage normalized EAGLE-I outage data (Nov 2015 – Oct 2016) to identify outage outliers. These require further analysis and could indicate cyber attacks.

1.4.23 Threat Detection and Response with Data Analytics

Key Project Milestones

Milestone (FY16-FY18)*	Status	Due Date
Establish MOU with industry collaborator (EPB) and identify sample data sets (related to NESCOR, EPB Smart Grid operations, etc.) for analysis. (ORNL)	Complete	10/1/16
Establish use case for evaluation of case studies. (INL)	Complete	4/1/17
Select set of AMI / smart grid hardware to use for experiments. Develop data agreement with partner. (LLNL)	In progress	7/1/17
Integrate SEL-3620 into selected NESCOR scenario. Identify physical and cyber events (features) in SEL-3620 available for monitoring. (SNL)	Complete	4/1/17
Organize subset of public outage data for specific distribution outages and transmission circuits for analysis. (ORNL)	Complete	4/1/17
Identify simulator requirements to perform attack-defense-mitigation study on PNNL testbed. (PNNL)	Complete	4/1/17
Understand, document, and ensure capture of device signaling protocols (LLNL)	Not started	10/1/17
Demonstrate analytics at asset owners (ALL)	Not started	4/1/19

*Selected milestones shown after year 1

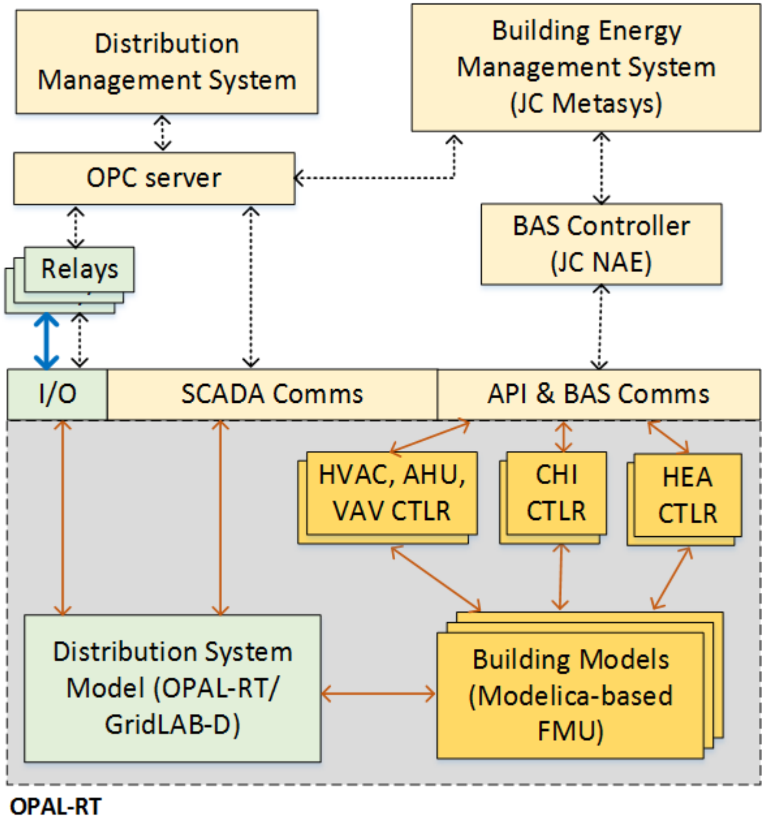
1.4.23 Threat Detection and Response with Data Analytics

Accomplishments to Date

Milestone - Identify simulator requirements to perform attack-defense-mitigation study on PNNL testbed.

Status – Complete ✓

- **PNNL Buildings-to-Grid Testbed Components**
  - ❑ Buildings-to-Grid Simulator
    - ● Opal-RT for grid simulation
    - ● Modelica-based building thermal + electrical models integrated with grid model for composite B2G model
  - ❑ Building Automation
    - ● Johnson Controls (JC) Network Automation Engine for supervisory field control
    - ● JC Metasys for building energy management system
- **Current Status**
  - ❑ Proof-of-concept study – Attack on peak load shaving implemented through direct load control (NESCOR DR.3)
  - ❑ Targeting conference publication – Resilience Week 2017



Distribution Management System
Building Energy Management System (JC Metasys)
OPC server
BAS Controller (JC NAE)
Relays
I/O
SCADA Comms
API & BAS Comms
HVAC, AHU, VAV CTLR
CHI CTLR
HEA CTLR
Distribution System Model (OPAL-RT/ GridLAB-D)
Building Models (Modelica-based FMU)
OPAL-RT

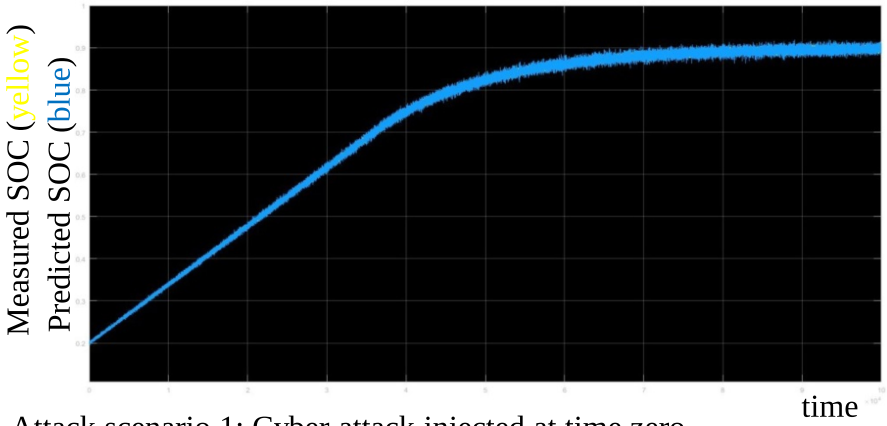
PNNL Buildings-to-Grid Testbed Architecture

1.4.23 Threat Detection and Response with Data Analytics

Accomplishments to Date

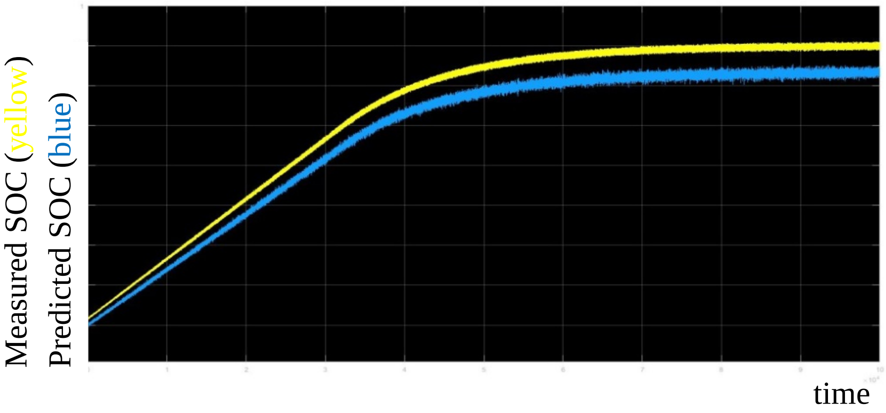
<u>Attack scenario 1</u>: No cyber attack

- Measured and predicted battery SOC statistically agree
- Statistical quality index stays below specified threshold, no statistical change declared, no physics-based anomaly alert issued



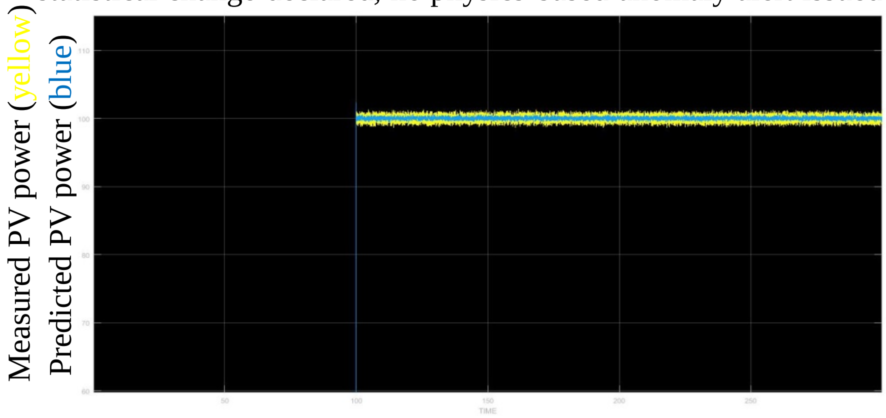
<u>Attack scenario 1</u>: Cyber attack injected at time zero

- Measured and predicted battery SOC statistically disagree
- Statistical quality index exceeds specified threshold, statistical changes are declared, and physics-based anomaly alerts are issued



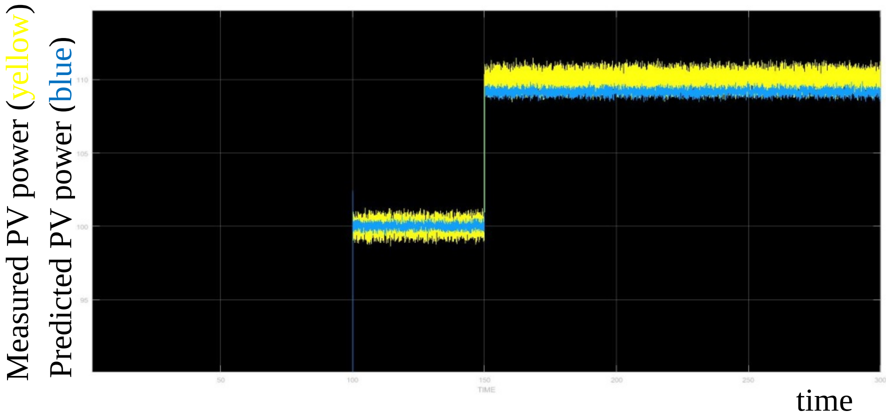
<u>Attack scenario 2</u>: No cyber attack

- Measured and predicted PV solar power statistically agree
- Statistical quality index remains under specified threshold, no statistical change declared, no physics-based anomaly alert issued



<u>Attack scenario 2</u>: Cyber attack injected at time 150

- Measured and predicted PV solar power statistically disagree
- Statistical quality index exceeds specified threshold, statistical changes are declared, physics-based anomaly alerts are issued



1.4.23 Threat Detection and Response with Data Analytics

Response to December 2016 Program Review

Recommendation	Response
Please clarify on how the six individual lab projects will be "fused" together at the annual peer review.	We're following a multi-year research path to identify data sources, understand usefulness of that data, develop analytics, build software tools, and integrate those tools into industry grid monitoring software.
Please clarify how the results of this project will link to the work done in other projects across the Grid Modernization Lab Call.	Addressed in following slide

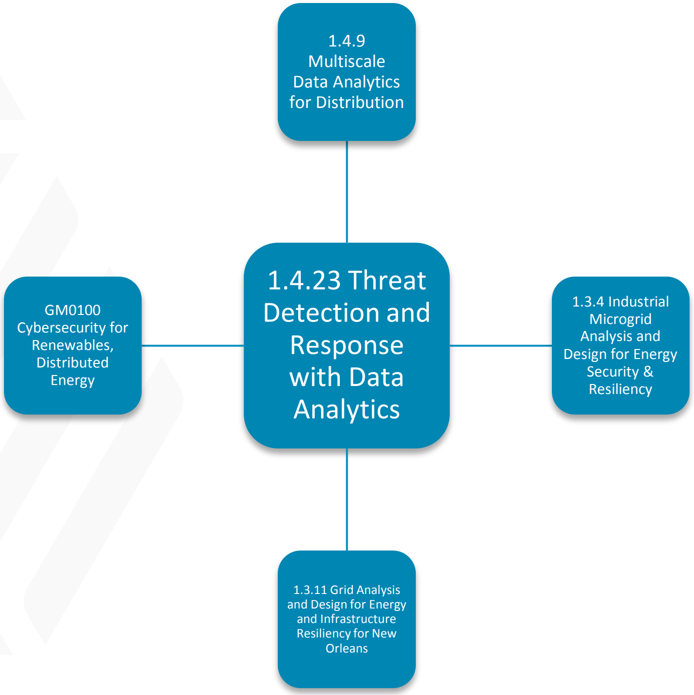
1.4.23 Threat Detection and Response with Data Analytics

Project Integration and Collaboration

- 1.4.9 – Discussing partnering to share data and explore analytic relationships between µPMU and AMI sensor data
- 1.3.4 – Lesson learned: Process control SCADA could be as significant to grid resilience as grid operations SCADA
- 1.3.11 – Lesson learned: Cyber threat resilience has generally focused on transmission but distribution has significant resilience impact as well
- GM0100 – Future collaboration

Communications:

- Preparing submittal to Resilience Week 2017
- Presented project to DARPA, EPSA, DHS, WAPA and CAISO
- Seeking further industry partners for data sharing, demonstration, and commercialization



1.4.9 Multiscale Data Analytics for Distribution

GM0100 Cybersecurity for Renewables, Distributed Energy

1.4.23 Threat Detection and Response with Data Analytics

1.3.4 Industrial Microgrid Analysis and Design for Energy Security & Resiliency

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

1.4.23 Threat Detection and Response with Data Analytics

Next Steps and Future Plans

- ▶ Two more years! Much more to come.
- ▶ Future phases
  - □ ”Robustify” tools to fit into commercial software packages
  - □ Integrate analytic tools more tightly into a uniform suite that plugs into EMS/DMS

Lawrence Livermore National Laboratory

BERKELEY LAB

INL Idaho National Laboratory

OAK RIDGE National Laboratory

Sandia National Laboratories

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

1.4.23 Threat Detection and Response with Data Analytics

Technical Details

- Include technical backup here – no more than 5 slides