GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Category 1 (Foundational/Regional) Project Final Report

Report Completion Date:

Section 1: Project Information

Project Information	
Control #: Title:	**1.4.23**
Project Title:	**Threat Detection and Response with Data Analytics**
Project PI Name and Lab Affiliation: Project Co-PI (plus-one) and Lab Affiliation:	**Jovana Helms, LLNL** **Sean Peisert, LBNL**
DOE Project Manager(s):	**Carol Hawk**
Period of Performance:	
Date Closed:	**June 2019**

Section 2: Project Assessment and Checklist

Project Assessment and Checklist	Y/N	Confirmation Date	Comments
Have all quarterly reports been submitted?	**Y**		
Have all milestones have been delivered?	**Y**		
Are all products finalized (e.g. technical reports, journal articles)?	**Y**		
Have all project products been finalized and presented/submitted to DOE Project Manager(s) and/or GMI Leadership?	**Y**		
Have all potential sensitivities been identified and addressed with DOE Project Managers and/or GMI Leadership?	**Y**		
Has the project team received feedback from Project Stakeholders (e.g. advisory group)?	Y		
Are there any open or pending costs?	**N**		

Section 3: Outcomes, Deliverables, Publications

Provide the following:
**In addition to titles, provide links to any websites or other repositories where deliverables and/or other information will be available after the project has been completed*
**Publications available for public release, URLs, etc. listed here should be uploaded to GMLC Open Point*

1. **List of Outcomes:**
   This project was the first effort looking at various data sources on the distribution side that could potentially be used for identifying and detecting cyber attacks. It set foundation for understanding how the distribution systems can be impacted by cyber attacks, what data can be used to detect them and what are potential mitigation options.
2. **List of Deliverables:**

Category 1 (Foundational/Regional) Project Final Report

Report Completion Date:

- Physical models of power inverters that will support analytics to differentiate cyber from non-cyber events
- Brief report describing experimental setup, as well as early models, analytics, and results, including models
- Analytics implemented as network IDS detection algorithms using the Berkeley Streaming Data Framework (power data + Bro IDS detection algorithms, as necessary)
- Final experimental results
- Report describing final models, analytics, and results
- Brief report describing selected NESCOR scenario
- Brief report describing integration of SEL-3622 into selected NESCOR scenario
- Identify specific feature sets relevant to detecting physical and cyber threats
- Report describing experimental results and potential future enhancements
- Simulator requirements to identify attacks on building to grid
- Report on building to grid testbed model
- Report describing results from building to grid testbed
- Proof of concept for cyber-physical signature generation
- Acquisition of smart meter data and hardware
- Data agreement with Pecan Street
- Brief report describing selected set of AMI/smart grid hardware for use in the project
- Cyber scenarios using AMI data
- Report describing implementation of analytics for detection of anomalous behavior in smart meter data and experiment results,

3. List of Publications:

- James Obert, Adrian Chavez, Jay Johnson, “Distributed Renewable Energy Resource Trust Metrics and Secure Routing”, Computers & Security Journal 88 101620, Elsevier, 2019.
- James Obert, Adrian Chavez, “Graph-based Event Classification in Grid Security Gateways”, IEEE Artificial Intelligence for Industries Conference, 2019.
- James Obert, Adrian Chavez, Jay Johnson, “Behavioral Based Trust Metrics and the Smart Grid”, The 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2018.
- Daniel Arnold, Shammya Saha, Ciaran Roberts, Anna Scaglione, Nathan G. Johnson, and Sean Peisert, “Adaptive Control of Smart Inverters for Distribution Grid Cybersecurity”, submitted to IEEE Transactions on Power Systems
- Sridhar S., A. Ashok, M.E. Mylrea, S. Pal, M.J. Rice, and S.G. Gourisetti. 2017. "A Testbed Environment for Buildings-to-Grid Cyber Resilience Research and Development." In Resilience Week (RWS 2017), September 18-22, 2017, Wilmington, Deleware, 12-17. Piscataway, New Jersey:IEEE. PNNL-SA-126405. doi:10.1109/RWEEK.2017.8088641

Category 1 (Foundational/Regional) Project Final Report

Report Completion Date:

- Pal S., S. Biswas, S. Sridhar, A. Ashok, J. Hansen, and V.C. Amatya. 2018. "Understanding Impacts of Data Integrity Attacks on Transactive Control Systems." In IEEE ISGT NA 2020. PNNL-SA-138041

- Nur N., S. Sridhar, S. Pal, A. Ashok, and V.C. Amatya. 2019. "A Clustering Approach for Consumer Baselining and Anomaly Detection in Transactive Control." In International Workshop on Applied Machine Learning for Intelligent Energy Systems (AMLIES). PNNL-SA-139353.
- Chellappan, K., Rivera-Soto, R. "Framework for Unsupervised Anomaly Detection on Smart Meter Data", submitted for publication

4. **List of Awards or Recognition: N/A**
5. **List any ROIs – Software, Intellectual Property, Licensing, Patents, Etc.**
   LBNL in process of submitting a software disclosure

Section 4: Final Costing

Each Lab Financial POC Completes Final Costing of GMLC Projects for their lab. PIs, Lab Leads will need to assist but not required to report financials with this final report.

Section 5: Final Thoughts/Comments

Final Thoughts	Comments
Lessons Learned	Distribution grid has a large attack surface and is very rich in potential data sources that can be used to detect cyber attacks. This project scratched the surface on investigating this problem. While each lab looking at a separate data source was by design, in a complex system like this a more wholistic approach, looking at the system level changes would be warranted. Additionally, from the project management perspective, integrating 4 parallel workstreams has been a bit of a challenge.
Opportunities for Improvement	Ability to distinguish cyber from non-cyber events in the grid is still a challenge. Looking at the distribution system as a whole and detecting undesired behaviors is rather than focusing on individual data streams would be a potential path forward.

Category 1 (Foundational/Regional) Project Final Report

Report Completion Date:

Future Projects: Ideas for future work? Possible next steps and research direction?	Leverage deep reinforcement learning to model the communications and powerflow of the system and teach the algorithms what the "healthy" system behavior is.
Other:	