Threat Detection and Response with Data Analytics

CHALLENGE

Large amounts of data related to regional outages, cyber health, distribution sensors, and advanced metering infrastructure (AMI) are gathered from the electrical grid. However, it is difficult to identify cyber-attacks and differentiate them from non-cyber incidents. Furthermore, degradation of the grid can come in many forms, including failure of materials, equipment, and information infrastructure resulting from natural or malicious events. Consequences from any of these scenarios can affect the reliability, maintainability, and availability of data required for decision making at numerous levels.

APPROACH

This project will develop advanced analytics using operational technology (OT) cyber data to detect complex cyber threats. Analytics will be developed that can assist in differentiating between cyber and non-cyber-caused incidents using available cyber data. To this end, the project team will conduct the following activities:

- Evaluate which sensor data are most valuable and could provide the biggest positive impact (in terms of grid resiliency/security) if an event is successfully detected. Possible data sources are phasor measurement units in electrical distribution systems, renewable generation and distributed energy resources (photovoltaics/inverters), demand response data for energy dispatch on the bulk electric system or electric vehicles on the consumer side, AMI data, and building automation data.
- Develop analytics to identify emerging cyber incidents on the electric grid using 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.
- Test analytics with industry and asset owner partners.

At-A-Glance

PROJECT LEADS

- **Jamie Van Randwyk**
  Lawrence Livermore National Laboratory
  vanrandwyk1@llnl.gov
- **Sean Peisert**
  Lawrence Berkeley National Laboratory
  sppeisert@lbl.gov

PARTNERS

- Electric Power Board
- Johnson Controls
- Schweitzer Engineering Laboratories

BUDGET

$3 million

DURATION

April 2016 – March 2019

TECHNICAL AREA

Security and Resilience

Lead: Juan Torres

National Renewable Energy Laboratory

Juan.Torres@nrel.gov

Rev. 2 September 2017

EXPECTED OUTCOMES

This project will identify “cyber-physical” signatures that will allow us to quickly differentiate between cyber events and non-cyber events on the grid. By differentiating between cyber-related and non-cyber-related/operational events, determinations can be made about the type of incident and its root cause. We will partner with a U.S. utility to obtain sensor data and validate prototype analytics against the data.

Research results will lead to development of commercial tools that will improve a utility’s ability to differentiate between cyber and non-cyber incidents so that they can make the most appropriate response during an event.

LAB TEAM

BERKELEY LAB

INL Idaho National Laboratory

Lawrence Livermore National Laboratory

OAK RIDGE National Laboratory

Pacific Northwest NATIONAL LABORATORY

Sandia National Laboratories

Launched in November 2014 under the U.S. Department of Energy’s Grid Modernization Initiative, the GMLC is a strategic partnership between DOE Headquarters and the national laboratories, bringing together leading experts and resources to collaborate on national grid modernization goals. The GMLC’s work is focused in **six technical areas** viewed as essential to modernization efforts:

Devices and Testing | Sensing and Measurements | Systems Operations and Control
Design and Planning | Security and Resilience | Institutional Support