U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Assess the Impact and Evaluate the Response to Cybersecurity Issues (AIERCI)

To ensure uninterrupted grid operations, Brookhaven National Laboratory (BNL) and team members will build the AIERCI tool to thwart cyber-attacks targeting essential short-term forecasting data – such as weather and load – that are required for economic energy dispatch.

Background

Energy delivery systems are increasingly dependent on sophisticated forecasting data for efficient operations. Weather data, load profiles and forecasting information about renewable generation are vital to scheduling functionalities for both transmission and distribution operations. A shortfall in operating reserves due to compromised critical short-term forecasting data could impact grid operations. Also at risk is the economic viability of utility operations if errant data triggers uneconomic dispatch. BNL identified a need for an integrated tool and database for cyberattack assessment and mitigation of compromised short-term forecasting data.

Objectives

The information acquired from this investigation will be used to understand the state-of-the-art in identifying cyber issues and vulnerabilities, resulting in a method to detect and mitigate cyber-attacks. The tool will be made available to both transmission and distribution utilities. The AIERCI integrated software tool solution will ensure reliable operation of the grid without failure or detrimental impact to operations – the flow of energy will not be impeded.

Project Description

The team partners led by BNL will build a user friendly tool to assess the impact and evaluate the response to cybersecurity issues on forecasting data used to operate energy delivery systems. BNL will provide weather, power systems and statistical modeling expertise to determine potential impacts and evaluate feasible cybersecurity solutions with assistance from UNC. ORU will provide system forecasting information and other data required for electrical operations. INL will lead the cybersecurity aspects to understand potential vulnerability and exposure in data flows between forecasting input and grid operations. ANL will help deploy the AIERCI tool for scheduling functions.

The tool will evaluate cyber issues based on different scheduling functionalities and will quantify risk measures posed by cyber issues, ranking the cyber issues, and design detection algorithms and mitigation solutions. After the tool is evaluated by a "Red team" and benchmarked using real operational data, the tool will be demonstrated in real-time operation. By using this tool, resilient energy delivery systems will be designed, installed, operated and maintained to survive a cyber-incident while sustaining critical functions.

Benefits

- Detection and capture of rogue forecasting data (cyber intrusions)
- Provides real-time corrective actions to allow grid operations to continue unimpeded
- Provides a path to commercialization of the AIERCI tool

Partners

- Brookhaven National Laboratory (BNL) (lead)
- Idaho National Laboratory (INL)
- Argonne National Laboratory (ANL)
- University of North Carolina at Charlotte (UNC)
- Orange and Rockland Utilities (ORU)

Period of Performance

October 2015 – September 2021

Total Project Cost

$2,283,000

Content last updated: April 2016

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Meng Yue
Principal Investigator
Brookhaven National Laboratory
631-344-7140
yuemeng@bnl.gov

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov

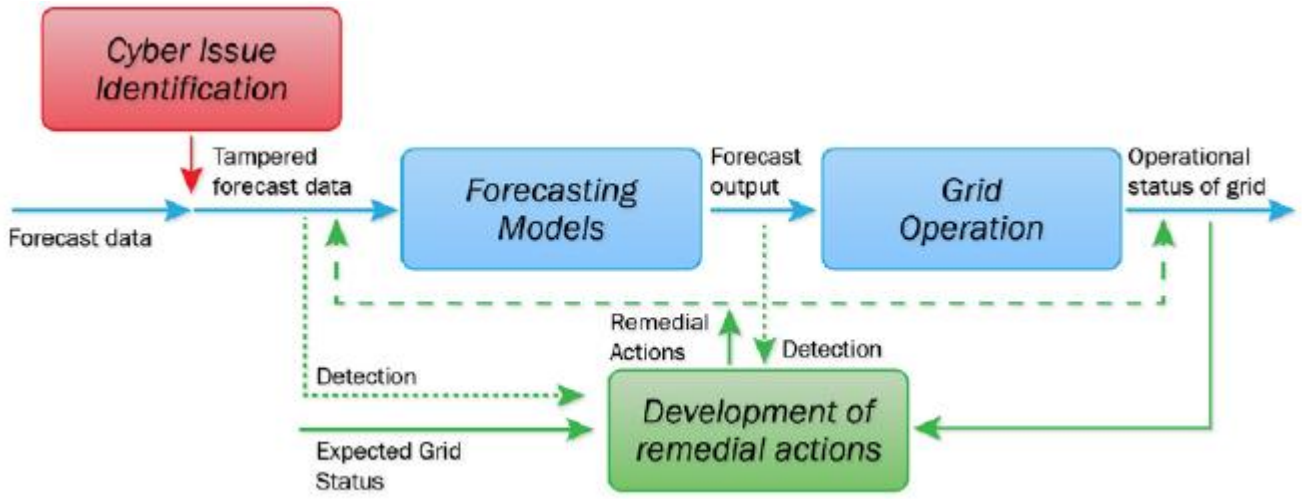

Figure 1: Technical Approach Proposed for Addressing Cyber Issues to Forecasting

Technical Approach

The tool will use mathematical models to identify cyber issues correlated with forecasting paradigms in operational planning or operation. Input to the model includes data sets, communication protocols, and other media or storage. The technical approach for addressing cyber issues includes:

- Understand and identify potential vulnerability and exposure in data flows between forecast input and grid operations
- Identify the potential means for compromising the forecast input and output data
- Determine how the cyberattack could feed tampered data to the forecasting model or grid scheduling
- Establish what impacts or consequences the cyberattack could have on grid operations
- After analysis of all anomalies, determine the mitigations or remedial actions to correct the compromised forecast and bring the grid back to normal operation

Grid Operational Forecasting Models

The AIERCI tool will be used to protect the following forecasting models from cyber intrusions:

- **Short-term load forecasting**
  Input includes meteorological forecast data, historic load data, measures of economic and demographic activity, energy efficiency, price response demand and metering data
- **Fuel pricing forecasting**
  Factors include inventory, production decisions, seasonal price fluctuations, futures market, exchange rates and natural calamities disrupting supply chain
- **Generation forecasting**
  Important elements include Distributed Energy Resources (DER), demand-response, non-dispatchable generation such as solar and wind power, and weather predictions

End Results

Project results will include the following:

- Advance the state-of-the-art and enhance the cybersecurity of energy delivery control systems by providing real-time corrective actions so that energy flow continues non-stop
- Ensure the integrity of short-term and very short-term forecasting data used in operations scheduling
- Detect, and mitigate the consequences of compromised information from distributed energy resources (DER), customers, and other data providers to protect utility grid operations