U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

AIERCI: Assess the Impact and Evaluate the Response to Cybersecurity Issues

BROOKHAVEN NATIONAL LABORATORY

Defends against cyberattacks targeting essential short-term forecasting data in energy delivery systems

Assess the Impact and Evaluate the Response to Cybersecurity Issues (AIERCI) is a user-friendly tool that assesses the impact and evaluates the response to cybersecurity issues in forecasting data used to operate energy delivery systems (EDS). It delivers an integrated model and data analytics-based method for anomaly detection and mitigation in load and weather input data using an ensemble approach for a cybersecure load forecasting scheme. The tool identifies cyber issues, quantifies and ranks relative risk measures, and designs detection algorithms and mitigation solutions. It autonomously assesses EDS unit commitment, economic dispatch, and load frequency control to measure the impacts of cyberattacks on both forecasting data and distributed energy resources (DERs) and performance of detection and mitigation strategies on grid operation.

KEY TAKEAWAYS

- Provides real-time corrective actions to allow grid operations to continue unimpeded
- Detects cyber intrusions and captures rogue forecasting data
- Evaluates the impact of cyberattacks targeting forecasting data on grid scheduling functions and operation

OUTCOME

AIERCI enhances the cybersecurity of energy delivery control systems by providing real-time corrective actions to ensure uninterrupted power flow. It ensures the integrity of short-term, and very short-term, forecasting data used in operations scheduling. AIERCI detects and mitigates the consequences of compromised information from DERs, customers, and other data providers to protect utility grid operations.

PARTICIPANTS	ROLE
BROOKHAVEN NATIONAL LABORATORY	Leads the development of data analytics-based anomaly detection and mitigation methods for historical load and weather information and DER generation to ensure the integrity of essential forecasting data, cybersecure forecasting algorithms, and integrated AIERCI tool
INL Idaho National Laboratory	Leads the cybersecurity aspects to understand potential vulnerability and exposure in data flows between forecasting input and grid operations and scenario development for cyberattacks of DERs
Argonne NATIONAL LABORATORY	Deploys the AIERCI tool for scheduling functions including dynamic security assessment and mitigation strategy for cyberattacks of DERs
UNC CHARLOTTE	Provides expertise in statistical model-based anomaly detection and mitigation method for load forecasting
Orange & Rockland	Supplies system forecasting information and other data required for electrical operations

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

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

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: October 2015 – September 2021

Total Award Value: $2,588,987
DOE Share: $2,588,987
Cost Share: $0

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: September 2021