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

Resilient Network Optimal Design with Secure Edges and Nodes

Los Alamos NATIONAL LABORATORY EST. 1943

Improving the resilience of cyber-physical networks using physics-aware design tools

Traditional analyses of industrial control system (ICS) networks focus on predefined physical components and on developing operational measures to improve the security or configuration of networks. Existing analytical tools use ad hoc methods to locate opportunities for security enhancements in control systems by evaluating the costs and benefits of existing and new technologies. This project models, formulates, and solves network resilience design problems for ICS by developing optimization-based, physics-aware design tools to help allocate and locate cybersecurity components in power system cyber-physical networks. These tools will account for the network's physical response to, and the consequences of, cyberattacks.

KEY TAKEAWAYS

- Optimizes security enhancements to improve the design of resilient cyber-physical networks
- Provides models of cyber and cyber-physical interactions and formulates optimal resilient design
- Describes case studies and types of resilient cyber-physical architectures

OUTCOME

This project fills a research gap by providing tools to design and evaluate candidate architectures, concepts, and protocols before devices are built. Results of the optimal allocation and location analysis will be used to determine the costs and benefits of existing, new, and combination security technologies. It helps developers and operators to implement a systems approach to building, integrating, and operating resilient energy delivery systems.

PARTICIPANTS	ROLE
Los Alamos NATIONAL LABORATORY EST.1943	Develops a power-flow simulation and optimization toolkit to assess the impact of network disruption on the power grid.
VT	Provides an extremely high-fidelity power grid model that will be used to validate network design and power flow optimization tools.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Raymond Newell
Principal Investigator
Los Alamos National Laboratory
505-695-4370
raymond@lanl.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 2017 – March 2021

Total Award Value: $550,000
DOE Share: $550,000
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: June 2021