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

DarkNet

Advancing Communication Architecture for Energy Sector's Critical Infrastructure

Background

The nation's energy infrastructure has become a major target of cyber-attacks. The frequency, scale, and sophistication of cyber threats have increased, and attacks have become easier to launch. Cyber risks from unintentional acts, such as operator error, software upgrades, and equipment failures, have also grown as the nation's electricity and fuel delivery systems have become more sophisticated.

Energy owners and operators have the responsibility to protect their systems from all types of risk; the federal government shares an interest in reducing this risk. As nation-states and criminals increasingly target energy networks, the federal government must help reduce the types of cyber risk that could trigger a large-scale or prolonged energy disruption.

Objectives

DarkNet's goal is to use existing network operational requirements coupled with information, guidance and requests provided by the project's Technical Advisory Board (TAB) to define and refine the "state-of-the-implemented-art" in network design, operations, and engineering for energy delivery systems.

The DarkNet project addresses two research areas, communication network design and a demonstration system utilizing innovative sensors and systems, which are complementary with future devices, systems, practices for deployment on network(s).

Project Description

The project team will research, develop and deploy an innovative, secure, resilient and redundant critical communications infrastructure for transmission/generation level facilities to demonstrate network architecture and related technologies.

DarkNet will secure communications networks based on existing optical fibers and develop communication technologies to secure existing networks. The project will:

- Develop and demonstrate a next-generation network architecture that ensures resilient, end-to-end or point to point communication for the nation's electricity infrastructure.
- Minimize external (e.g., Internet) connectivity with the high-fidelity sensors possessing the physical multifunction sensors to collectively train their measurements onto grid system states.
- Demonstrate layered deployment and testing of developed devices and system elements within the ORNL testing facility.
- Validate the resilient network architecture and a network linking with substations within the Power Marketing Administrations (PMAs), pilot integration systems deployed in multiple sites, and utilization of the ORNL testing facility.
- Incorporate quantum key distribution (QKD) to further secure networks.

Benefits

- Ensures resilient, end-to-end or point to point communication for the nation's electricity infrastructure
- Secure communications networks based on existing optical fibers
- Communication technologies, hardware and software, to secure existing networks

Partners

- Oak Ridge National Lab (lead)
- Lawrence Livermore National Laboratory (LLNL)
- University of Tennessee-Knoxville
- Virginia Tech
- Brixon
- National Rural Electric Cooperative Association (NRECA)
- Tennessee Valley Authority (TVA)
- Nevermore Security
- Electric Power Board of Chattanooga (EPB)
- Readiness Resource Group
- Jim Fama
- Western Area Power Administration

Period of Performance

February 2019 – September 2020

Project Cost

Total: $10,000,000

Content last updated: March 2019

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

Peter Fuhr
Principal Investigator
Oak Ridge National Laboratory
865-574-2694
fuhrpl@ornl.gov

Current Contact as of Aug. 2020

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

Technical Approach

The project team will use existing network operational requirements coupled with information, guidance and requests provided by the project's Technical Advisory Board (TAB) to define and refine the "state-of-the-implemented-art" in network design, operations, and engineering. The developed infrastructure design will be provided to relevant standards organizations (most notably ISA, IEEE, IEC) for their use and dissemination.

Task 1: Network Architecture Enhancements

- Research, develop and demonstrate (RD&D) wiring components and installation practices needed for instrumentation wiring
- Develop and validate a best practice guide for grid communication infrastructure
- QKD communication systems interfaces in utilities and PMAs. Gather from ongoing CEDS-sponsored quantum research to implement this technology to secure communications.
- Optimization of the system network architecture. Provide the details of the communication architecture and the relevant tools and technologies for an optimized network architecture design for demonstration of secure connectivity and data sharing between PMAs.

Task 2: DarkNet Implementation and Laboratory Testing

- Laboratory scale implementation of the designed DarkNet communications architecture
- Demonstrations of the DarkNet communications architecture scalability by testing communications protocols applications for grid management
- DarkNet communications architecture resiliency demonstration
- Field deployment and testing

Task 3: Enhance Darknet Communications Architecture

- Development of high-fidelity software/hardware resiliency sensors
- Development of a decentralized data network architecture
- Integration of DarkNet communication architecture and technologies
- Network demonstration integration and testing

Task 4: Communications Architecture and Technology Integration

- Network demonstration integration and testing

End Results

Project results will include the following:

- Internet-free, secure communications
- Use of quantum encryption for further security by enhancing the fidelity in grid operations
- Architecture to ensure connectivity and to secure data sharing between PMAs
- "Tool Kits" for utilization by utilities of varying sizes, existing infrastructures and overall technological sophistication (including sensors, systems, communications, business operations, and hardware/software)
- Organizational structure to facilitate the concept and complexity of "getting the grid off the public internet"
- Frameworks and architectural designs for scaled DarkNet implementation from co-ops to muni's to IOUs