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

Applied Resiliency for More Trustworthy Grid Operation (ARMORE)

Secure communications, inspection, and data analysis platform that enhances the security posture for legacy and modern grid devices

Background

The electric grid increasingly relies on the secure transfer of real-time data between substations to maintain control of system operations. Traditional cybersecurity practices primarily employ perimeter-level protections, such as firewalls or end-point gateways. Additionally, substation communications protocols have varying levels of security protections that interact with legacy and modern grid devices.

Security controls should provide protection at all levels of the network, incorporate both legacy and modern protocols, and consider the fast and reliable transfer of data to support advanced grid operations.

Barriers

- While some legacy protocols have been security-enhanced, support is not pervasive.
- Granular role-based control mechanisms are not widely deployed across heterogeneous systems.
- Device reconfiguration is costly and an impedance to new technology deployment.

Project Description

The ARMORE project will provide reliable, secure communications, augmented defense-in-depth security, and an analysis framework to enable faster and more secure ways to transfer substation data from both legacy and modern devices. Similar to data encapsulation methods, placing ARMORE in line with the devices to be protected allows it to transparently provide enhanced security with the ability to report violations of stated policy.

ARMORE operates using fault-tolerant communications with access control and capabilities for enhanced situational awareness and analytics. The technology integrates easily with deployed systems and enables advanced grid applications such as wide-area monitoring protection and control (WAMPAC).

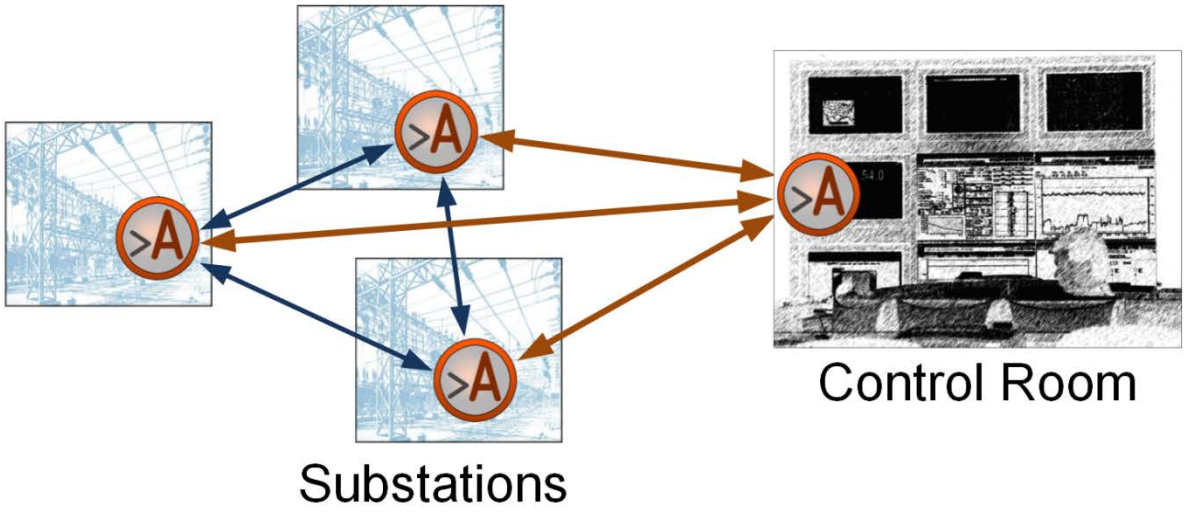
Building on past successes such as openPDC and SIEGate, ARMORE takes an open-source approach to facilitate low product cost, diversity of vendors, and commercial implementation with low technology risk.

Benefits

- Transparently enables resilient communications with security enhancements
- Easily integrates and interoperates with existing control room technology
- Provides varied support for both known (legacy and modern) and unknown protocols
- Provides modularity for easy expansion and value-add capabilities
- Provides a framework for advanced situational awareness and analysis
- Provides a high-performance, low-latency solution for securing data communications throughout an organization
- Inherently scales based on the peer-based architecture

Partners

- **Grid Protection Alliance**
- University of Illinois at Urbana-Champaign (UIUC)
- Pacific Northwest National Laboratory
- Utility Advisors



Conceptual diagram of ARMORE placed in line with substation devices and the control room to secure communications

Technical Objectives

The project consists of research, development, and demonstration activities to build a vetted, open-source solution that incorporates a secure, scalable, resilient communications framework; enhanced security for energy sector protocols; and a framework for computation to support advanced situational awareness and analysis. Commercialization efforts will occur alongside development activities.

Phase 1: Project Setup and Design

- Gather use case information
- Develop functional, security, and performance requirements
- Identify practices and processes to facilitate utility adoption
- Design a secure, flexible, and extensible platform
- Conduct a detailed design review

Phase 2: Build and Test

- Complete alpha version of the ARMORE platform, leveraging applicable knowledge and development from past efforts
- Test and evaluate ARMORE and remediate problems as necessary

Phase 3: Demonstration

- Develop performance requirements
- Deploy demonstration system

End Results

Project results will include the following:

- A more resilient and secure communications mechanism to support modern grid operation
- Improved security posture for utility infrastructure by (1) enhancing security of both known and unknown protocols and (2) extending security protection through internal perimeter protections for utility infrastructure
- Transparent operation that minimizes end-device reconfiguration, thereby reducing deployment costs and management overhead
- An extensible platform that enables future computation, data analytics, and enhanced situational awareness

Content last updated: September 2014

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

Russell Robertson
Vice President, Grid Solutions
Grid Protection Alliance
423-702-8136
rrobertson@GridProtectionAlliance.org

Current Contact as of Aug. 2020

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