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

Tools and Methods for Hardening Communication Security of Energy Delivery Systems

Development of mitigations that harden energy system communications protocols against cyber attacks

Background

Energy delivery systems rely on communication protocols to standardize data and control message exchanges between communicating entities in order to ensure reliability. Many of these protocols were not initially designed with a consideration of cybersecurity and are therefore vulnerable to cyber attacks. The use of shared or publicly accessible network resources further increases the vulnerabilities of communication protocols.

Barriers

- Incomplete and /or missing specification of exceptional message exchange scenarios results in vulnerabilities susceptible to cyber attacks
- Enforcement of proper communication behaviors is subject to vendor implementations and may not be readily available

Project Description

This project seeks to enhance the security of control and data communication in energy delivery systems. The project team will build on results from the Smart Grid Interoperability Panel Cyber Security Working Group to analyze key communication protocols for vulnerabilities, then work with standards bodies to eliminate those vulnerabilities.

The team will also design, develop and demonstrate an Agent-based, Distributed, Extensible Cybersecurity for the Grid (ADEC-G) solution that can be configured and extended to mitigate or prevent identified cyber attacks, intercepting messages and eliminating those demonstrating unexpected behavior. The solution will incorporate a Communication Policing Agent (CPA) component that can be configured with the use of an expressive communication protocol policy language to actively inspect and filter suspicious control and data transmissions in and out of an energy delivery systems domain.

These steps will result in a security management infrastructure (SMI) that limits an adversary's ability to exploit key protocols in energy delivery systems.

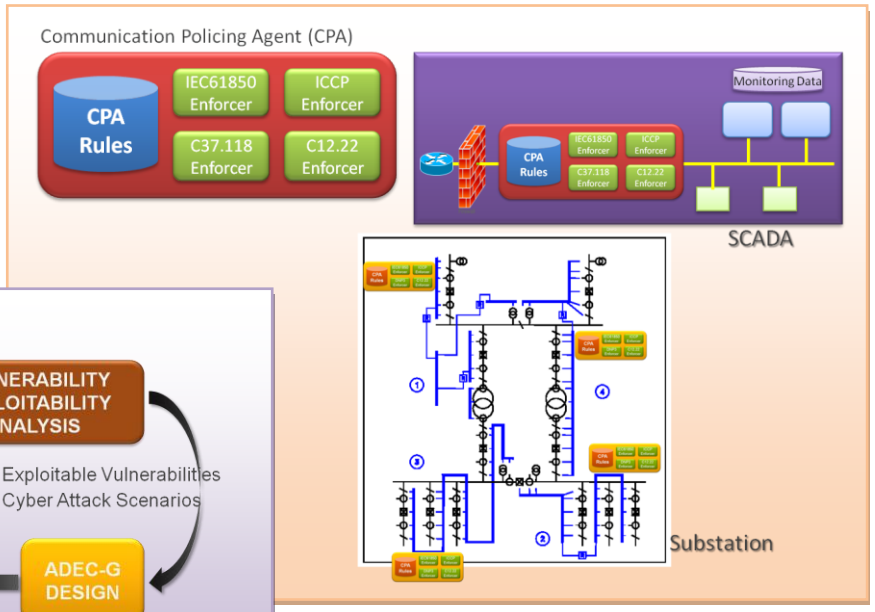
Benefits

- Improves the security of communication protocols used by the energy sector
- Enforces proper communication behavior by incorporating models of expected protocol behavior
- Provides more flexibility than data diodes or commercial firewalls

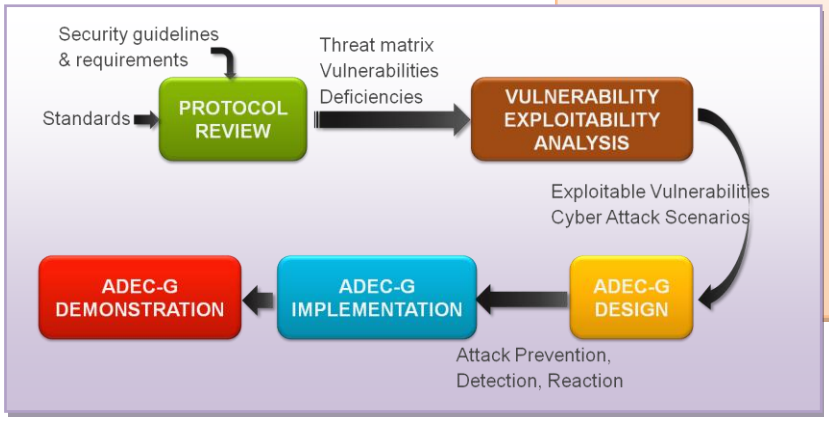
Partners

- Applied Communication Sciences
- The University of Illinois at Urbana-Champaign
- The Electric Power Research Institute
- DTE Energy

Communication Policing Agent use in substation



Development Process



Technical Objectives

The project will initially focus on the architectural design of the SMI, which involves substantial review and validation of security requirements and measures for energy delivery systems communications. The researchers will subsequently develop and integrate the ADEC-G solution, then complete the system integration, testing and demonstration. Commercialization efforts will occur alongside development activities.

Phase 1: SMI Architecture Design

- Gather security requirements
- Develop a threat matrix
- Design protocol validation tools and policy management architecture

Phase 2: SMI Component Development and Integration

- Develop communication protocol validation and policy management architecture
- Execute integration testing

Phase 3: SMI System Demonstration

- Conduct and analyze the results of demonstrations

End Results

Project results will include:

- An SMI to monitor and control perimeter security devices and policies
- More secure communication protocols for use by the entire energy sector
- A decrease in an adversary's abilities to exploit key protocols and launch cyber attacks

Content last updated: August 2012

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

Yow-Jian Lin
Senior Scientist
Applied Communication Sciences
908-748-2958
ylin@appcomsci.com

Current Contact as of Aug. 2020

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