SIEGate

Secure Information Gateway for Electric Grid Operations

Background

In a modernized smart grid, there is an increasing need to share real-time data across organizational and functional boundaries. Systems to provide data exchange must be designed to ensure the security, efficiency and timely delivery of this data to support real-time electric system operations. These data exchange systems, or gateways, will serve as the points of real-time data exchange across a control center's electronic security perimeter. As such, when hardened, they offer the opportunity to significantly improve the protection of critical infrastructure.

Barriers

- Electric system data exchange is complex due to multiple regulated business processes, many entities, multiple protocols and numerous information systems
- Implementations of phasor measurement systems are rapidly increasing with a requirement for security compliance assurance
- Small time-delays (or latency) from data measurement to analysis are required for phasor measurement
- Mechanisms are needed to provide good security at low cost for data exchange among legacy systems

Project Description

The SIEGate project will develop a secure and flexible appliance that will serve as the gateway to exchange the multiple types of data required for real-time electric system operations.

SIEGate will resist cyber attacks, protect the confidentiality and integrity of a growing volume of real-time information being exchanged to assure the reliability of the bulk electric system, and inter-operate with existing and proposed data formats and networking technologies.

The project will develop gateway technology for adoption and deployment by the electric sector through an open source software commercialization approach. SIEGate will build upon open source components developed for the North American Electric Reliability Corporation's (NERC's) open phasor gateway (openPG).

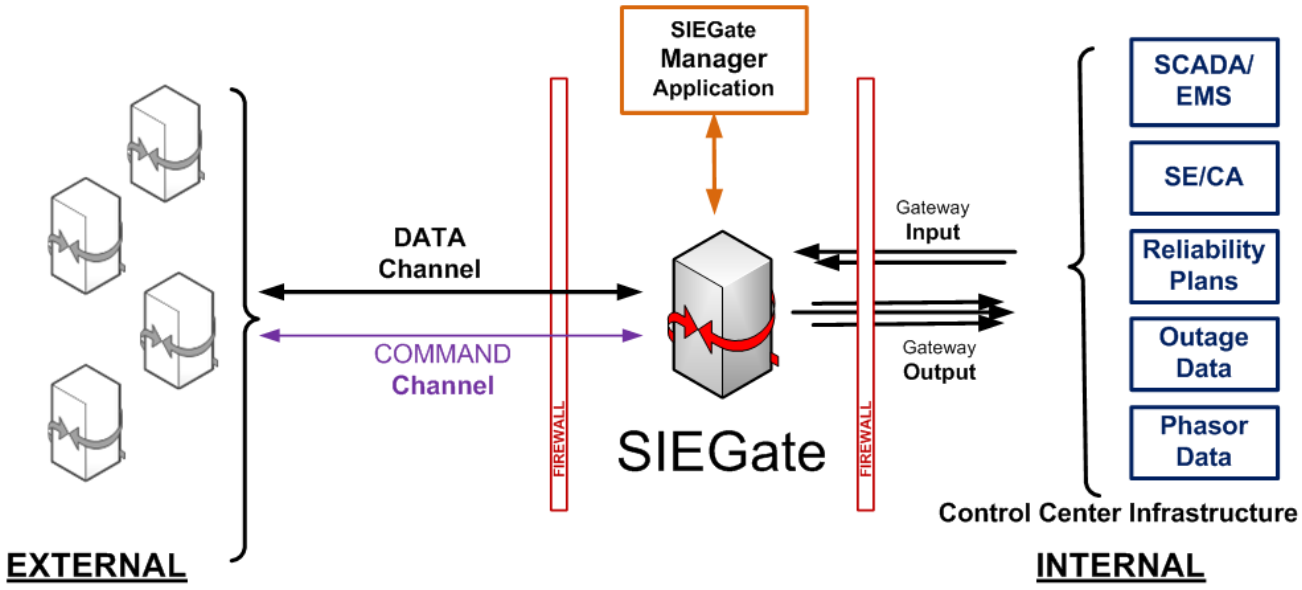
This open source commercialization approach results in low-product cost, allows commercialization by any vendor, and assures low technology risk as it jump starts commercialization by project partner Alstom Grid.

Benefits

- Enables flexible, real-time, reliable and secure information exchange among grid operating entities
- Easily integrates and interoperates with existing control room technology
- Consolidates data exchange to reduce the external attack surface and costs of maintaining multiple data exchange systems
- Provides a high-performance, low latency solution to securing data communication between control centers

Partners

- Grid Protection Alliance
- University of Illinois at Urbana-Champaign
- Pacific Northwest National Laboratory
- PJM Interconnection
- Alstom Grid



Technical Objectives

This project will develop a thoroughly vetted and demonstrably secure gateway appliance for inter-organizational data sharing in the electric sector. This gateway will be secure, interoperable, scalable, flexible with extensible protocol support, and able to support real-time operational needs of the modern power grid.

Phase 1: Project Setup and Gateway Design

- Gather use case information
- Develop functional, security and performance requirements
- Identify the practices and processes to facilitate utility adoption
- Design a secure, flexible and expandable gateway architecture
- Conduct a design review

Phase 2: Build and Test Gateway

- Complete alpha version of the SIEGate appliance, basing common components on NERC's openPG initiative
- Test and evaluate SIEGate and remediate problems as necessary

Phase 3: Demonstrate and Prepare for Commercialization of Gateway

- Develop and deploy demonstration systems and gateway performance reporting requirements
- Identify potential markets and market strategies
- Promote the use of SIEGate as a replacement for NERC's openPG
- Integrate into existing commercial product lines, such as Alstom Grid

End Results

Project results will include:

- Improved security posture for control centers by: 1) replacing the many devices used for exchanging power system data with a single, security-hardened gateway appliance, and 2) reducing the control center's external cyber attack surface
- Reduced cost and management overhead by maintaining and managing a single gateway
- Closing a technology gap by providing a gateway for sharing increasingly high volumes of high-frequency, real-time data, such as phasor data, in a secure and timely manner with significantly greater functionality and cybersecurity capabilities

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

Russell Robertson
VP, 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