SIEGate

Secure Information Exchange Gateway
for Electric Grid Operations

GRID PROTECTION ALLIANCE

SIEGate is a hardened security appliance used to exchange real-time electric grid operating information.

Application Profile
SIEGate is a back office system that is designed to securely send and receive data required for operation of the Bulk Electric System.

Required Hardware
SIEGate is open source software that can execute on standard server hardware.

Required OS and Services
SIEGate is a Microsoft .net application and is intended for deployment using Windows Server Core 2008. However, SIEGate will run under other Windows operating systems.

Availability
SIEGate is available for free download, installation and production use.

http://siegate.codeplex.com

Background
In a modernized smart grid there is an increasing need to share real-time data across organizational boundaries. Energy accounting data exchanged using the Inter-Control Center Communications Protocol (ICCP) over the NERC Inter-regional Security Network (ISN) and synchrophasor data using Phasor Data Concentrators over Wide Area Networks (WANs), are two examples of data sharing needs among bulk electric system control centers.

Systems must be designed to ensure the security, efficiency and delivery timeliness of data necessary to support real-time electric system operations. These gateway systems 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 as they provide greater assurance of the integrity and availability of information.

SIEGate Project Objectives
1. To improve the security posture and minimize the cyber-attack surface of electric utility control centers
2. To reduce the cost of maintaining current control-room-to-control-room information exchange

These objectives will be met by replacing current practices for utility information exchange with a single security-hardened appliance. 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 data formats and networking technologies.

SIEGate Software Features
- Support for three data classes:
  - — Real-time data, such as phasor or SCADA data
  - — File-based data, such as SDX files
  - — Alarm and notification data
- High-trust relationship among gateways
- Encrypted communication
- Change and operational logging
- Meta-data naming services that facilitate data sharing without a requirement for naming rules
- Easy point-level publication and subscription configuration
- Implementable as a high-availability solution
- Modularized and adaptable

SIEGate Performance Features
- High performance, low latency
- Efficient and scalable
- Reliable and resilient

Sponsored by DOE Office of Electricity Delivery and Energy Reliability
Cybersecurity for Energy Delivery Systems Program

Project Team

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

ILLINOIS UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

GRID ALSTOM

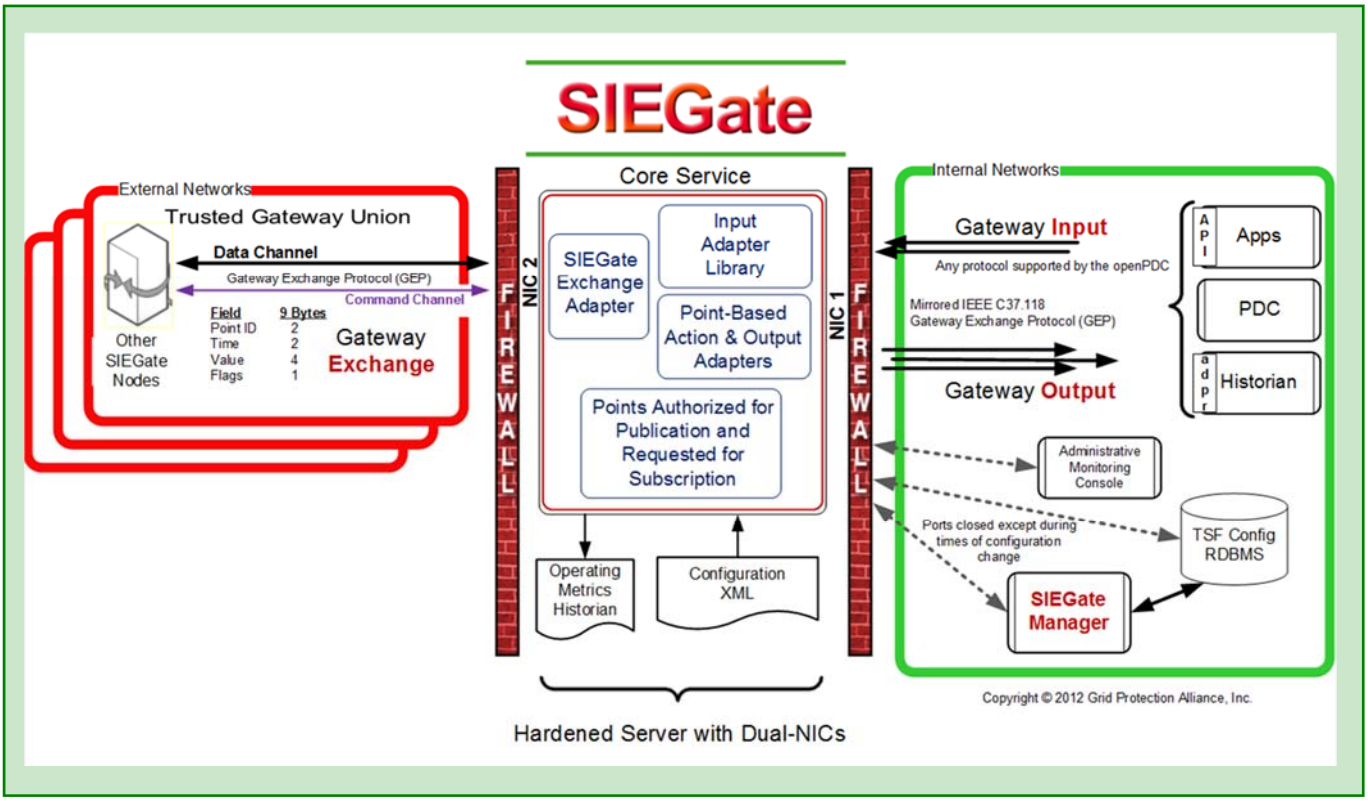
pjm

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

SIEGate - Secure Information Exchange Gateway

DOE - Cybersecurity for Energy Delivery Systems Program

RECOMMENDED IMPLEMENTATION

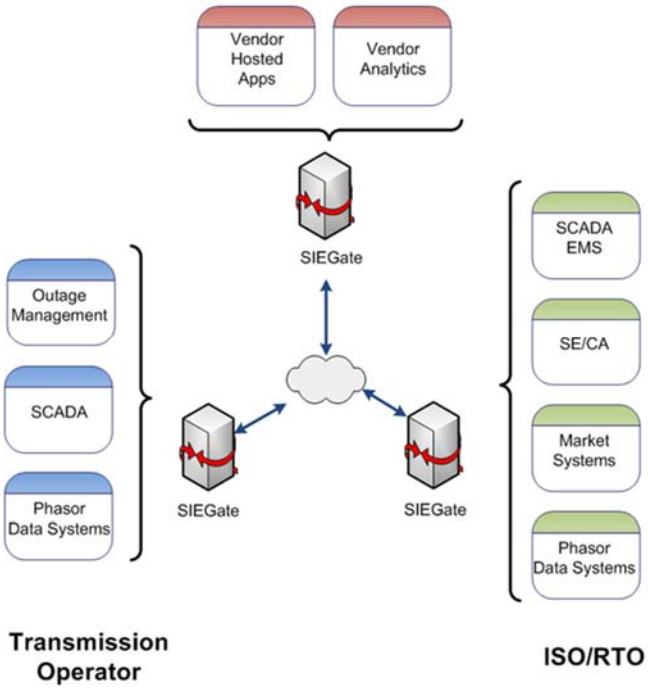


Open Source.

SIEGate is an open source project with the source code made publically available under the Eclipse Public License.

Open source:

- Accelerates innovation and removes barriers to commercialization.
- Increases the quality of product and puts "many eyes" to work assuring security
- Lowers development cost and total cost of ownership
- Provides freedom from vendor lock in Improves agility to quickly adapt system to new threats or changing electric grid requirements



Security Design Features.

The SIEGate system will be secure by default. It will be trustworthy and be deployable in a hostile environment. SIEGate provides:

- Defense in depth with multiple layers of protection
- Hardened OS configured with application white listing
- Data encryption with NIST approved algorithms
- Code reviewed and segmented to improve security
- Encrypted logging
- Cryptographic key lifecycle management
- Role based access control