Secure Policy-Based Configuration Framework (PBCONF)

Interoperable, open-source framework for secure remote configuration of modern and legacy devices

Background

Energy delivery devices are dispersed throughout the electric grid and are an integral part of real-time power transmission and distribution. As today's cyber threats continue to advance, ensuring the security and resiliency of these digital devices is critical to ensuring the continuous delivery of power to consumers. Incorrect or inconsistent configuration of these devices in the field could present a potential attack vector. However, this attack vector can be mitigated by applying a uniform security policy across devices, providing consistency and visibility.

Both utilities and vendors have indicated an increased need for configuration through remote access methods. While some vendors have standardized their device configurations to address this issue, those solutions are typically only for that vendor's devices. A vendor-neutral framework for secure configuration and remote access is needed to solve these problems for the energy sector.

Barriers

- Many utilities use legacy devices for energy delivery, posing a challenge for interoperability and upgradability.
- The distributed nature of utility systems requires secure remote access, which is often achieved through mutually isolated applications (stovepipes).
- Utilities use energy delivery devices from multiple vendors.

Project Description

The PBCONF project is developing an extensible, open-source, policy-based configuration framework to support the secure configuration and remote access of modern and legacy devices from a variety of vendors. The open-source framework will combine a policy engine with a translation engine to address the interoperability challenges of various remote access control methods and provide utilities with a single organization-wide view of the security configuration of their power delivery devices.

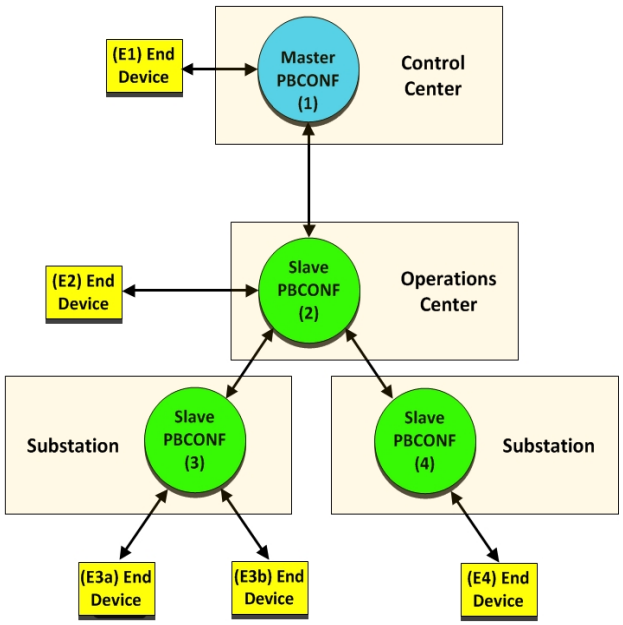
By building this framework in a modular way and starting from an ontology that represents the concepts and relationships of the configuration policy, the framework will have the necessary flexibility and adaptability for both legacy and new devices. This is particularly important for the electric sector, which features legacy devices that may be 40 years old. The system will leverage distributed architecture concepts to enable both centralized and peer-based configuration of the devices to support scalability and resiliency.

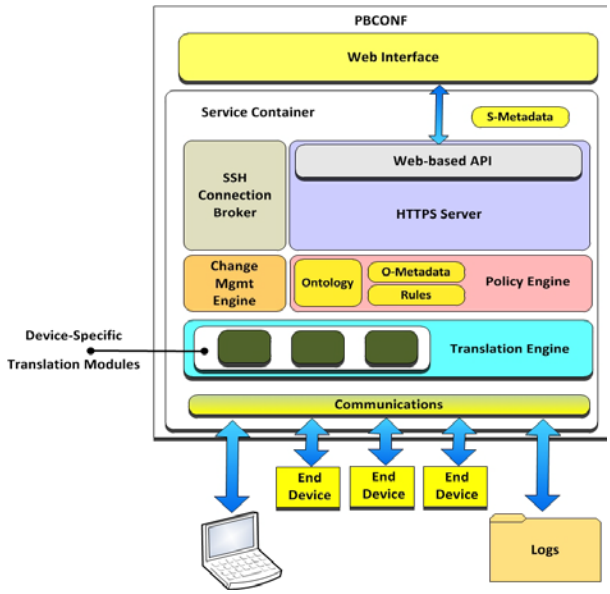
Benefits

- Provides the necessary flexibility and adaptability for both legacy and new devices
- Leverages distributed architecture concepts to support both centralized and peer-based configuration of devices
- Offers a cost-effective solution that supports scalability and resiliency
- Allows for consistent global policy application across vendor products
- Enables efficient inquiry and security/compliance checks against current policies

Partners

- **Electric Power Research Institute (EPRI)**
- University of Illinois at Urbana-Champaign (UIUC)
- Schweitzer Engineering Laboratories (SEL)
- Ameren





The PBCONF system is composed of several functional components or subsystems that are contained within a PBCONF node. The PBCONF node comprises a web interface and a service container. The service container is made up of subcomponents: the SSH connection broker, an HTTPS server that hosts a web-based API, a policy engine, a change management engine, and a translation engine that hosts the device-specific vendor modules.

Technical Objectives

The project consists of research, development, and demonstration activities to build an interoperable common framework for secure remote configuration of a utility's energy delivery devices. Commercialization efforts will occur alongside development activities.

Phase 1:

- Develop an open-source implementation of PBCONF, a supporting graphical user interface (GUI), an open-source ontology for describing the security policy and device capabilities, a secure remote access method, and an open application programming interface (API)
- Map, verify, and validate applied remote access, configuration, change management and analysis, auditing and alerting, and core functionality

Phase 2:

- Test PBCONF in a demonstration environment using EPRI, UIUC, and utility testbeds to ensure that the implemented functionality performs as expected
- Iterate development as necessary with feedback from vendors and utility partners

Phase 3:

- Open-source release and technology transfer

End Results

Project results will include the following:

- A policy-based configuration framework that combines the policy engine with the translation engine
- A peer-based architecture that leverages a master/slave relationship between nodes to allow the system to operate under disconnected conditions or when circumstances dictate localized actions
- A fully demonstrable architecture for secure remote access configuration, auditing, change management, and support

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

Annabelle Lee
Senior Technical Executive
Electric Power Research Institute
202-293-6345
alee@epri.com

Current Contact as of Aug. 2020

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