PBCONF is an extensible, policy-based configuration framework that will 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 for their power delivery devices.

**PROJECT SCOPE**

- The development of an open-source, policy-based configuration framework wherein energy sector devices can be securely configured for access control, authorization, and authentication (AAA) to enable secure remote access.
- The development of a means by which utilities may define a remote access policy and apply it to heterogeneous devices while providing in-depth information detailing any deviations from that policy.
- The development of a method for securing remote access to a variety of devices.
- The development of a common framework that may be used for both legacy and modern equipment.

**PBCONF NODE**

The system is composed of several functional components or subsystems that are contained within a PBCONF node. These nodes combine to provide the functionality of the PBCONF system. A node consists of a Web Interface and a Service Container. The Service Container is segmented into subcomponents, which include the:

- SSH connection broker,
- HTTPS server hosting Web-based API,
- Policy Engine,
- Change Management Engine, and
- Translation Engine hosting the device-specific vendor modules.

**USE CASES**

Operations IT group would select the policy through the web interface. A compliance check is run by the system which will securely connect to each remote device, verify the current configuration and determine if it is in compliance with the selected policy.

1. Secure change management: Each node maintains a Git repository that contains configuration information for all devices under its control. Any changes are compared and tracked by Git, and includes an audit log and time stamping.
2. Monitoring for security configuration changes: Every node sends configuration changes of a device to its upstream node. The operating mode determines the scope of propagation. The device’s configuration is validated against the stored configuration before and after any changes. Any noncompliance is reported.
3. Auditing and reporting: Alarm and notification system via emails and logging mechanism. Custom logging levels can be set.
4. Secure remote access: Development of secure remote access protocols to a variety of transmission and distribution substation devices.
5. Global policy application: Heartbeat communication among nodes to indicate status and policy revision.
6. Authorization and non-repudiation: Will leverage X.509 identity certificates to validate communication between nodes. Identity verification required to access the API.

**ONTOLOGIES FOR SECURITY POLICIES**

One of the goals is the development of a well-specified and open ontology that represents the concepts and relationships of the security policy. The ontology will provide the basis for mapping the deploying organization’s security policy to the device-specific configurations. The policy rules will define constraints that a security configuration must meet. These can include user credentials, identity certificates and access control information.

**PBCONF SYSTEM OVERVIEW**

- Will leverage distributed architecture concepts to support both centralized and peer-based configuration of the devices to support scalability and resiliency.
- The system is a tree-like hierarchy. The master node can direct and control the nodes directly below it. It may directly configure end devices through remote access, direct subordinate instances, or it may do both.
- Communication is chained. Policy changes flow down the tree, security configuration changes propagate up the tree.