Annabelle Lee

Electric Power Research Institute (EPRI)

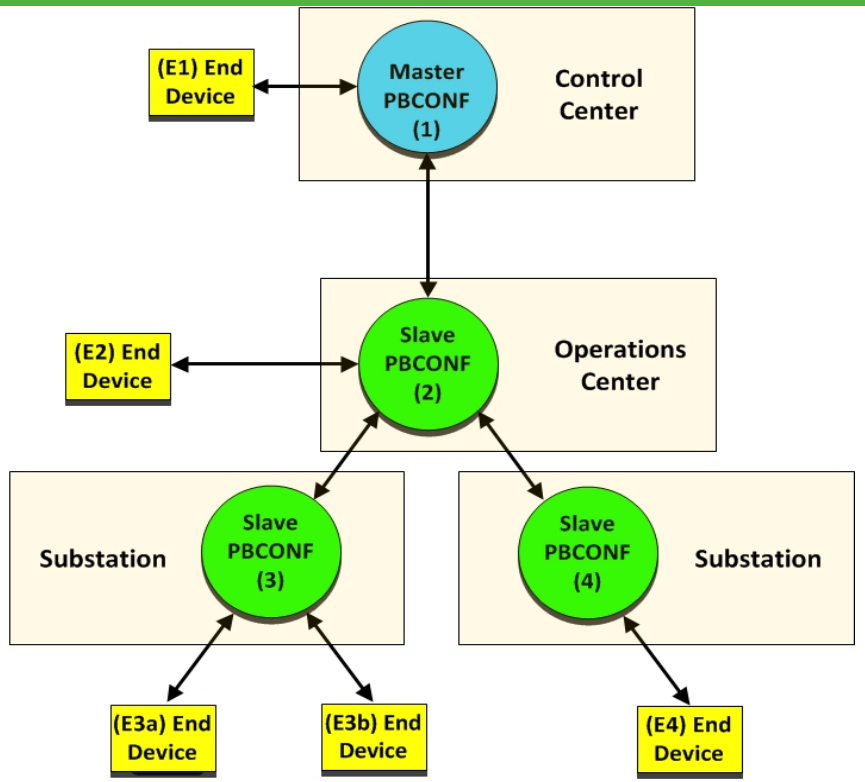
Secure Policy-Based Configuration Framework (PBCONF)

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

Summary: PBCONF

- **Objective**
  - The project will develop 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.
- **Schedule**
  - 10/2013 – 9/2016
  - Final PBCONF Detailed Design Completed – Month 9
  - Alpha version of PBFCONF – month 21
  - Beta version of PBCONF – month 28
  - Open source version 1.0 of PBCONF released – month 36
  - Capability: open-source remote access security configuration toolkit



- **Total Value of Award:** $2,054,343
- **% Funds expended to date:** 4%
- **Performer:** EPRI
- **Partners:** University of Illinois, Ameren, SEL

Advancing the State of the Art (SOA)

- **Incorrect or inconsistent security configuration of the multitude of energy sector devices in the field is a large potential attack vector**
- **Approach: apply uniform security policies across devices**
- **Why: both utilities and vendors have indicated the need for security configuration through remote access methods**
  - Uniform approach rather than through isolated applications (stovepipes)

Advancing the State of the Art (SOA) (2)

- **Benefits: 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
- **Advancement: the distributed architecture will enable both centralized and peer-based configuration of the devices to support scalability and resiliency**
  - Provides a model for implementation and deployment that is cost-effective

Challenges to Success

- **Challenge 1: ensuring the design addresses the electric sector's needs**

  Response - Work with the utility partner to define the scope

  Coordinate with utilities as the project progresses

- **Challenge 2: identifying the applicable security requirements and use cases**

  Response - Assess existing use case repositories, applicable guidelines, and standards

- **Challenge 3: addressing potential performance and scalability issues**

  Response - Ensure the design addresses electric sector constraints

Progress to Date

- **Major Accomplishments**
  - Selection of use case repositories and security requirements specifications
    - Used to develop security and application use cases for the PBCONF
  - Development of the design document
    - Conducted a review meeting with the entire team

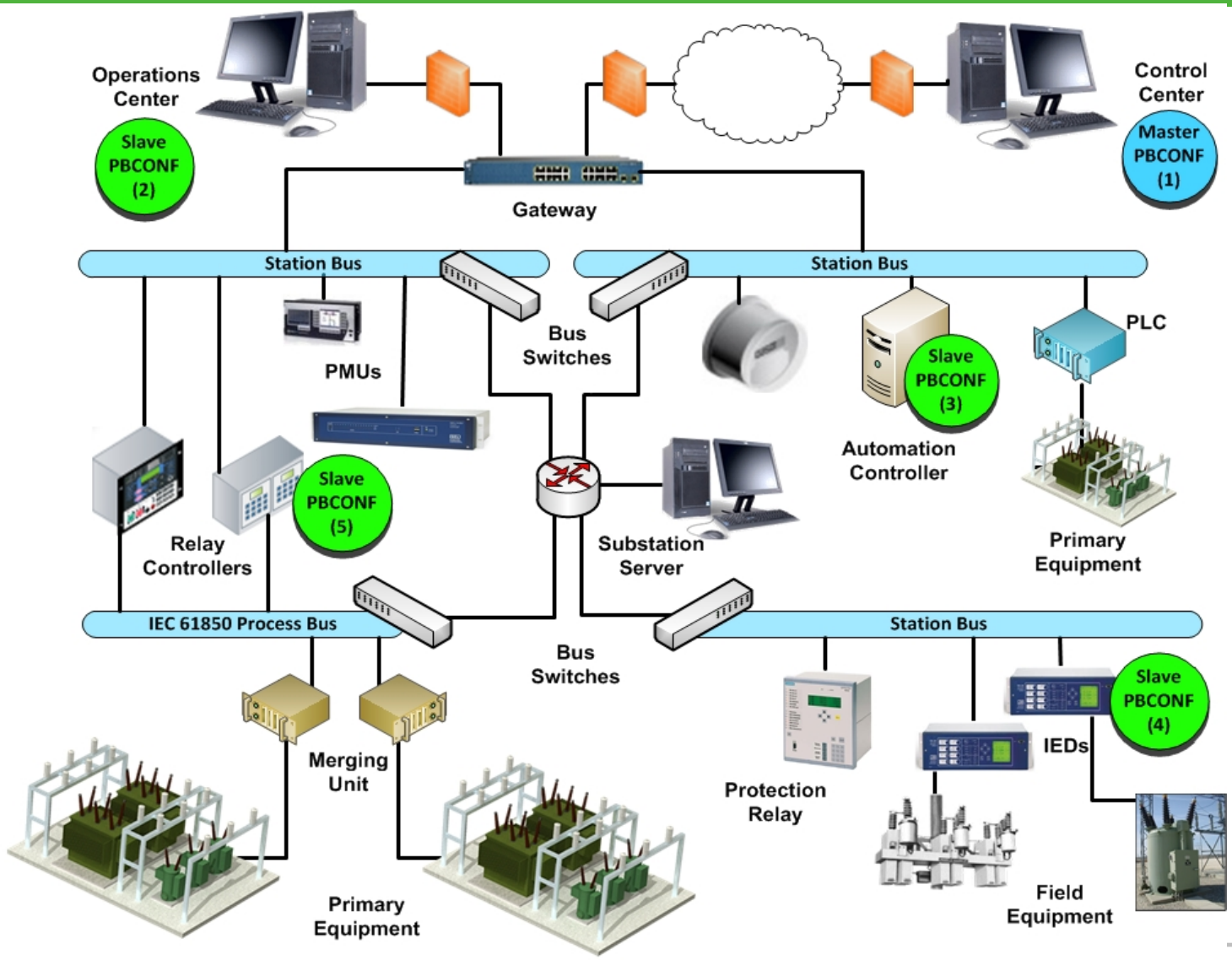
Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end users**
  - The end users for this technology are utilities and vendors
    - Includes utilities of all sizes – from small to large
    - Vendors will develop the translation modules
  - What are your plans to gain industry acceptance?
    - EPRI will conduct an outreach workshop near the end of the project for all interested utilities and vendors
    - One of the team members is a utility – and they will be used to test the alpha and beta versions of the technology
    - As the project continues, other utilities will be briefed on the technology

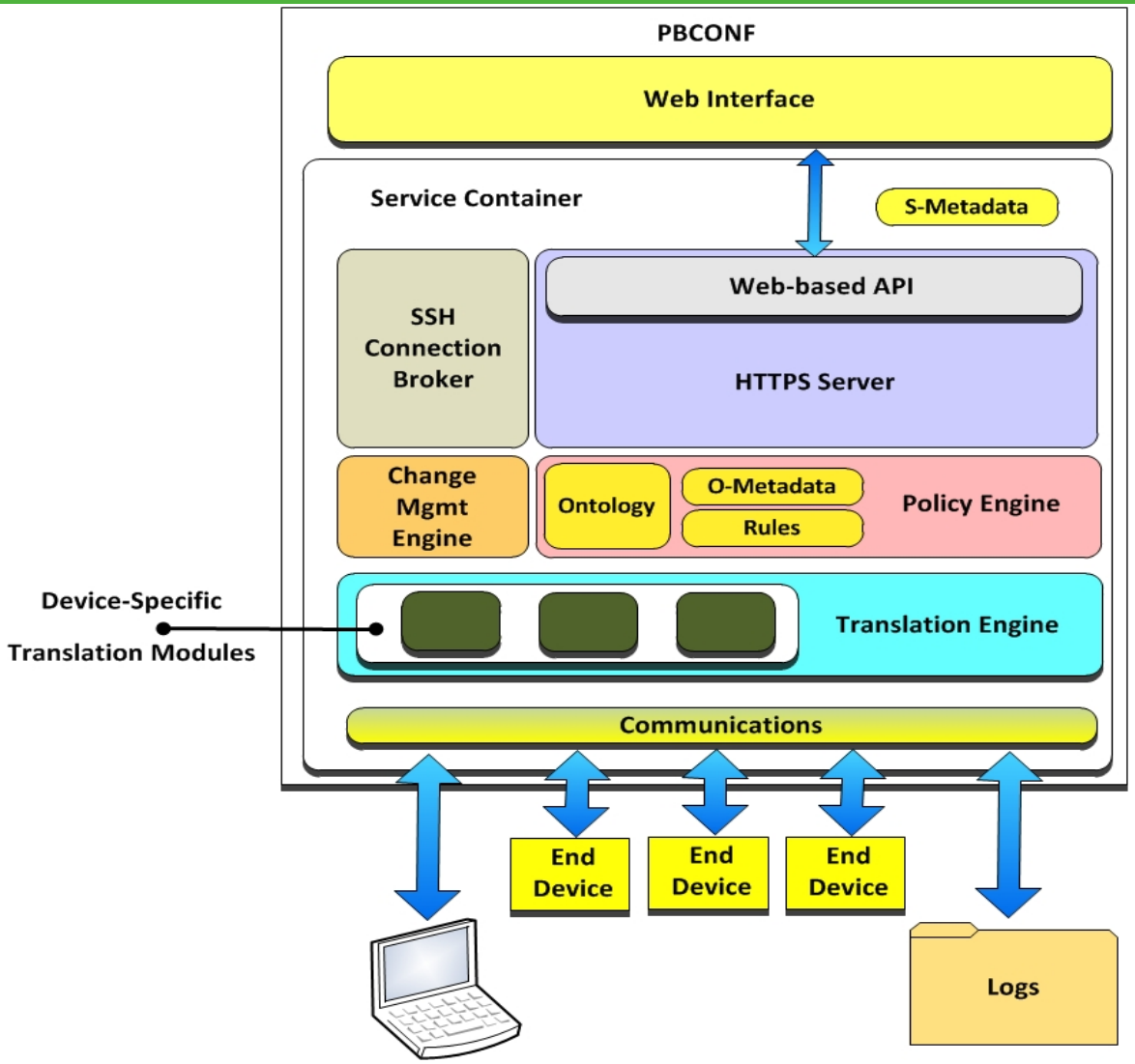
Next Steps for this Project

- **Approach for the next year or to the end of project**
  - Continue to refine the design document and develop applicable use cases
  - Develop a test plan
  - Key Milestone 2: Alpha version of PBFCONF – month 21
  - Key Milestone 3: Beta version of PBCONF – month 28
  - Develop a transition plan
  - Key Milestone 4: Open source version 1.0 of PBCONF released – month 36

PBCONF Illustrative Example



PBCONF Component Architecture



Composed PBCONF System Overview