U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

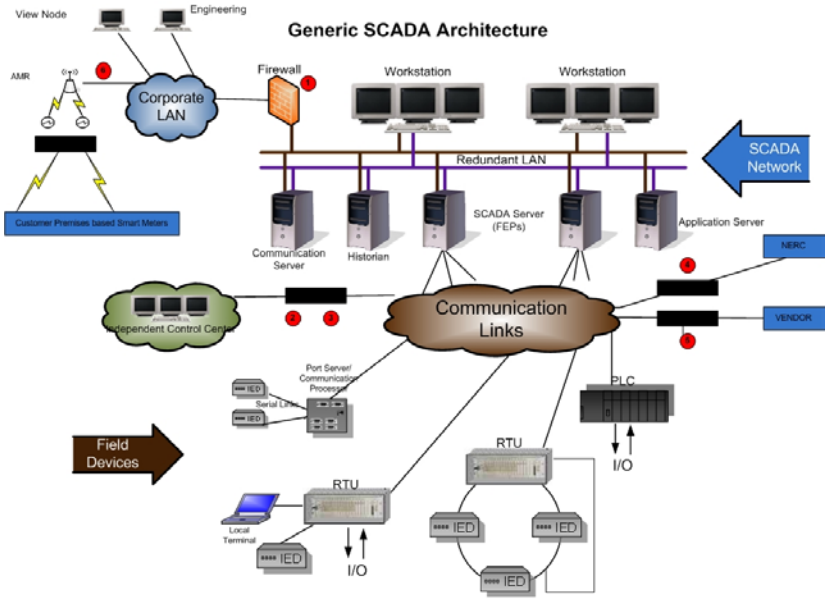
Philip A Craig Jr

Pacific Northwest National Laboratory

Field Device Management

Summary Slide: Field Device Management

- **Outcomes:** Feasibility study and final report, prototypical design specification for implementation of working prototype.
- **Roadmap Challenge:** Standardized test plans and upgrades for new technology are not widely available; complexity increases exponentially with an increase in number of nodes
- **Major Successes:** Outreach during study is identifying/addressing increasing interest from asset owners with regard to technical approach that meets assessment and audit criterion.



- **Schedule:** Feasibility Study/Report – FY10
- **Level of Effort:** $34K
- **Funds Remaining:** $25K
- **Performers:** PNNL
- **Partners:** BPA, ACS

Technical Approach and Feasibility

- **Approach**
  - Study of technical environment and identify gaps in existing solutions
  - Develop requirements for a prototype design leveraging available and proven COTS technology and integration API's that could provide a common open-source framework
  - Report feasibility and develop technical specification to build working prototype

Technical Approach and Feasibility

- **Metrics for Success**
  - Report industry interest and adaptability into current operational environments
  - Deliver specification to industry partners for advisory input
  - Demonstrate technical prototype and provide outreach (technical paper, conference participation)

Technical Approach and Feasibility

- **Challenges to Success**
  - Adaptation of technology to very broad and established technical environments
    - Leverages COTS currently used in many engineering, maintenance, operations environments today
    - Utilizes common API adaptable within an asset owners company to build commonality between IT/Engineering/Operations resources

Technical Approach and Feasibility

- **Technical Achievements to Date**
  - Identified strong technical (COTS) primary candidates and alternatives to provide the correct environment
  - Determined that common API approach would foster the best progression of adaptability for industry through open-source involvement
  - Drafted (in-work) specification that allows public dissemination without compromising the specific security attributes of a specific industry or asset owner
  - Performance tested small modules to ensure integration of the overall system will meet scalability requirements

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - What do you need (e.g., expertise, action, resources) from industry?
    - An industry partner willing to implement the design specification, document lessons learned, provide co-authored articles for industry best practice publication
  - What will you do/have you done to gain industry input and assistance?
    - Solicit and secure an active industry partner
    - PNNL has discussed this approach with BPA, Seattle Power & Light, Washington Natural Gas Company
  - What are the challenges to gaining this input?
    - Engineering and Information Technology (IT) organizational commitments for time and resources
    - Overcoming organizational boundaries between maintenance, engineering, operations

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - Who will use the technology or knowledge? How will they apply it? How should they not apply it?
    - Provides an efficient and effective solution for IT to provide secure architecture for engineering and maintenance organizations. IT would be able to meet many cybersecurity requirements while enabling capabilities for assessment and audit mechanisms that can be automated significantly reducing costs and recurring resource commitments.
    - End users should *not* change the fundamental technical approach, or specific details that have been already deemed “best practice”. Rather, end users should evaluate their environments to determine what policy and/or procedures are outdated, or unnecessary during implementation.

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - What are your plans to gain industry acceptance?
    - A functional demonstration must be presented in appropriate venues where hands-on experiences and discussion enables industry to fully appreciate the value of the system.
  - How does this solution fit into the existing paradigm of power systems technologies? How does it leverage (and avoid interference with) existing capability to protect the reliability of power systems?
    - This solution enables legacy systems to be included through protected virtual instances while also enabling the most current technologies in the same environments.
    - Significantly adds cybersecurity to “all” environments while also leveraging the needs of multiple responsible organizations to ensure consistent approach to managing revision planning through active state assessments.

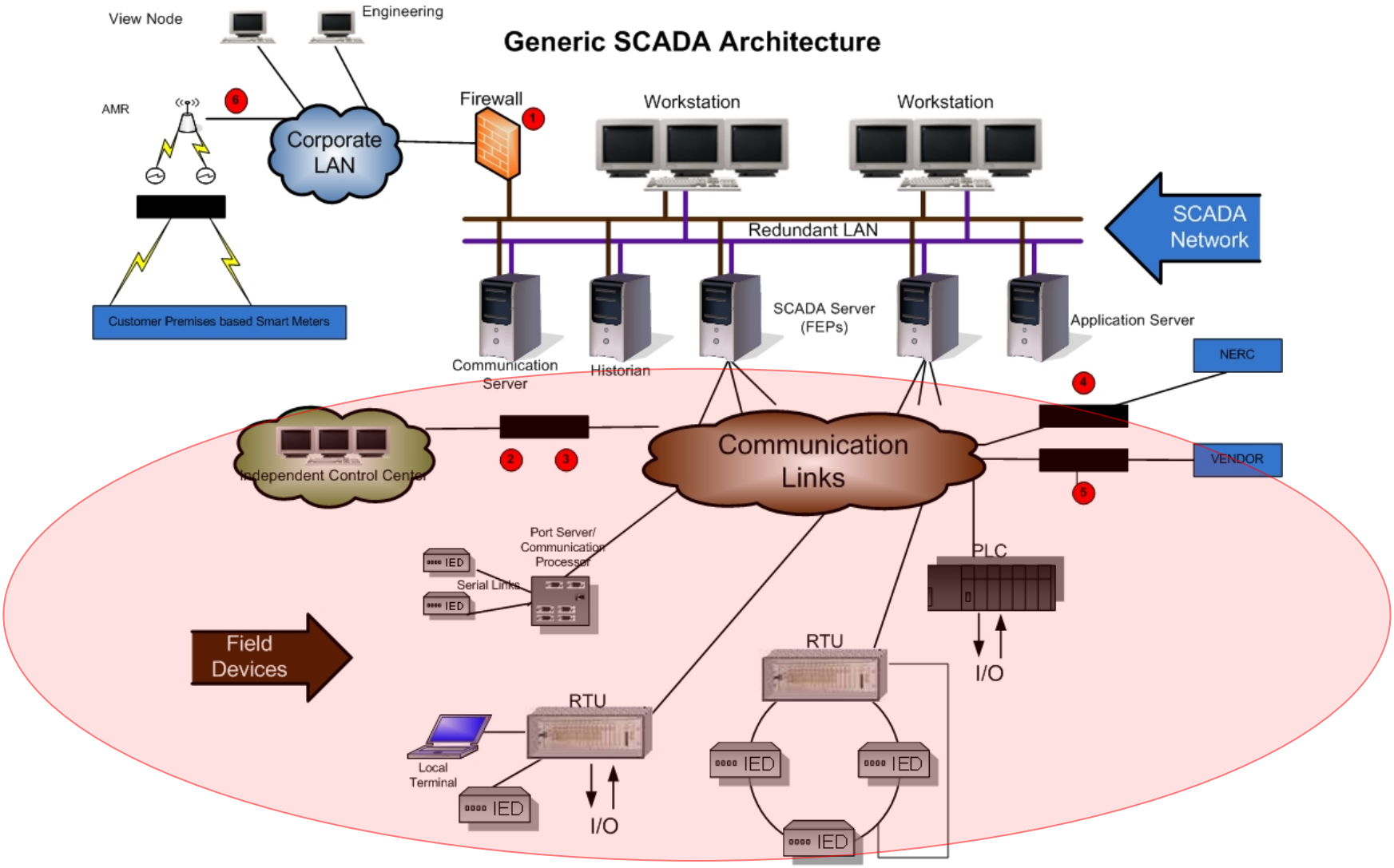
Next Steps

- **Approach For the Next Year**
  - Milestones to Accomplish
    - Identify and Secure an industry partner to act as an advisor to implement the technical specification.
    - Provide an appropriately sized demonstration capability to ensure all aspects of the system are present and functionally able to allow interaction with potential developers and users.
  - Risks Faced
    - This system is more “evolutionary” not “revolutionary” in nature. As such, it should enable industry to understand the benefits and overall effectiveness of the technical approach. There is little risk to educating the industry in the proper integration of these environments.

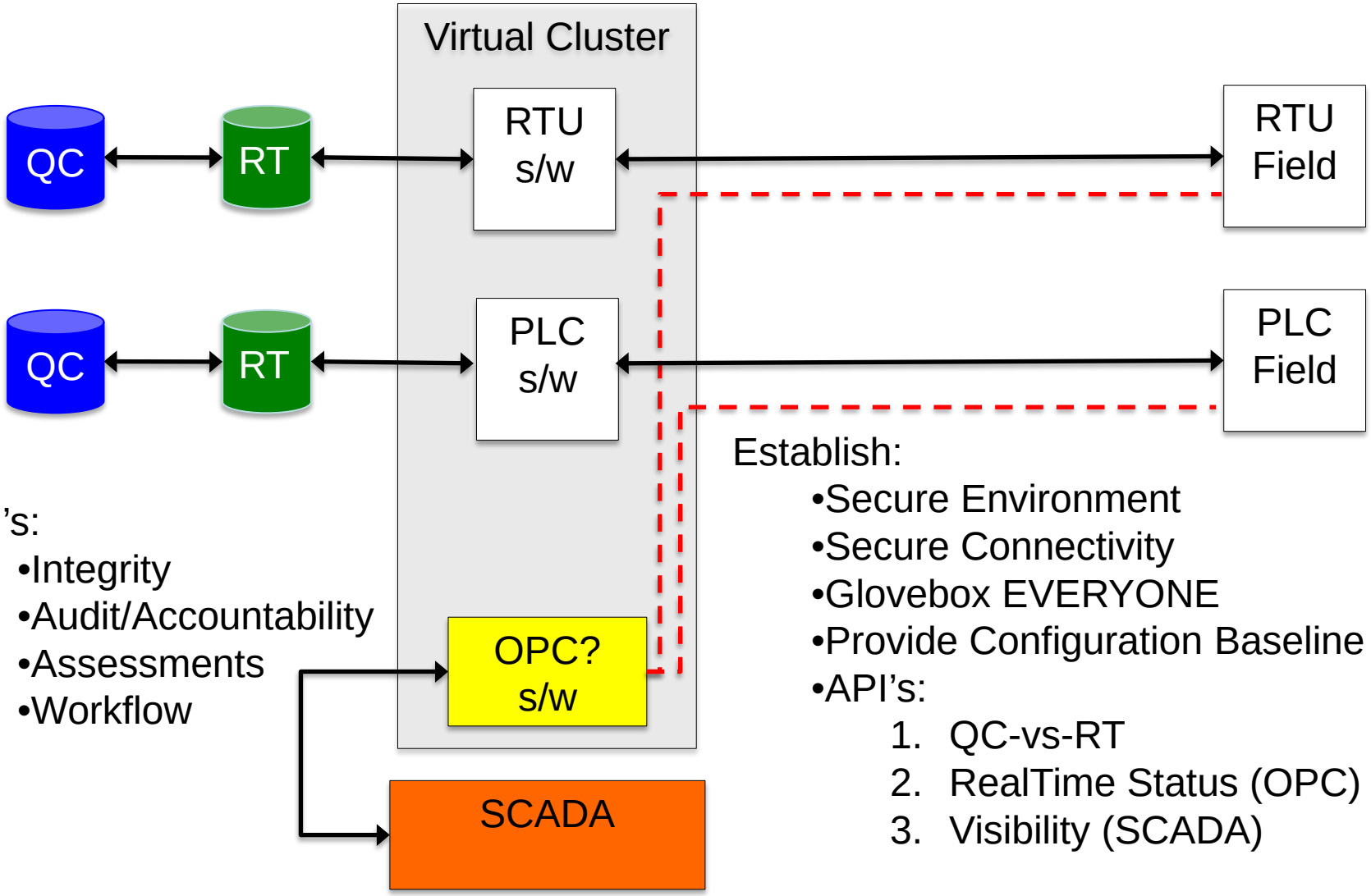
Next Steps

- **Project results that may form the basis of future control systems security work or link to other programs/organizations**
  - Information systems and control systems are trending towards much higher dependencies and interconnectivity. A successful implementation will push cross-organizational coordination where security expectations are shared and *organizational interconnectivity* must also provide a common security framework for the overall system, and not just an individual department.

Field Device Management



Virtual-Field Device Management



API's:

- Integrity
- Audit/Accountability
- Assessments
- Workflow

Establish:

- Secure Environment
- Secure Connectivity
- Glovebox EVERYONE
- Provide Configuration Baseline
- API's:
  1. QC-vs-RT
  2. RealTime Status (OPC)
  3. Visibility (SCADA)

QUESTIONS?

Philip A Craig Jr.

PNNL

509-375-4464