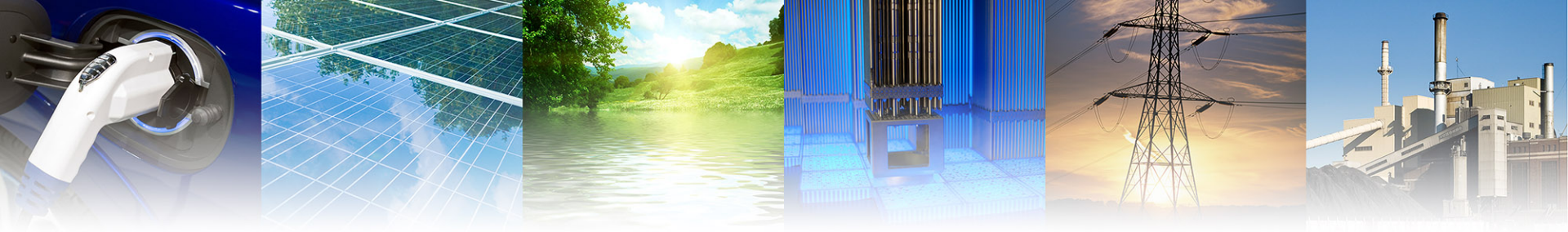


ELECTRIC POWER RESEARCH INSTITUTE

# Secure Remote Substation Access Solutions

## Supplemental Project - Introduction Webcast

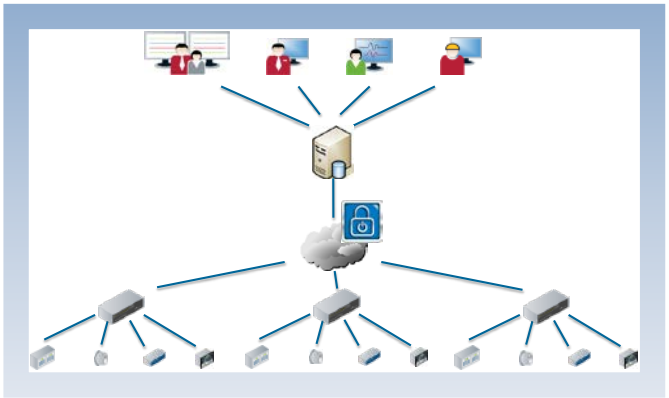
***October 16, 2013***


**Scott Sternfeld, Project Manager**
**Smart Grid Substation & Cyber Security Research Labs**

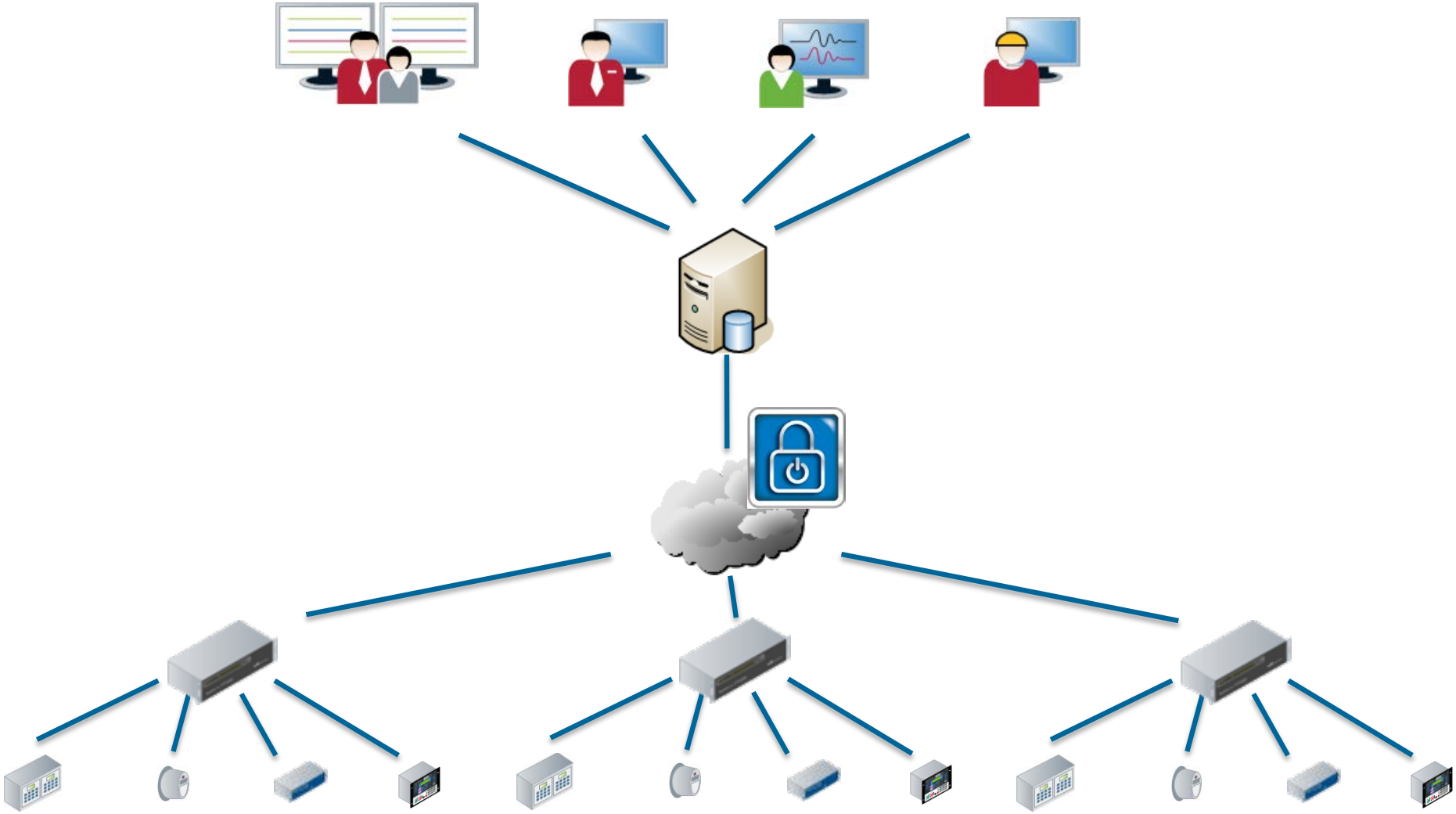
**ssternfeld@epri.com**
**(843) 619-0050**

# Agenda

- **What is a Secure Remote Substation Access System?**
- **History of EPRI's Remote Substation Access Research**
  - **2012 project and workshop**
  - **Interest Group**
  - **Supplemental project**
- **<u>Review of Top Challenges/Proposed Tasks</u>**
  - **Penetration Testing**
  - **Device compatibility testing**
  - **Password Vault Integration**
- **How <u>YOU</u> can get involved!**



# What is a Remote Substation (IED) Access System?

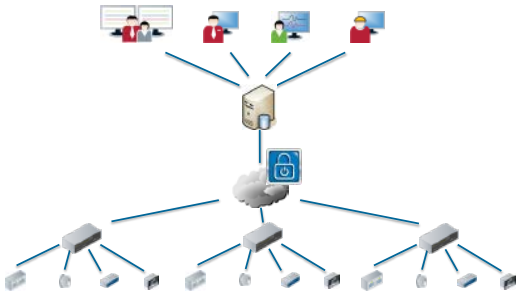






ELECTRIC POWER RESEARCH INSTITUTE

# Remote Substation Access System



- *What is it?*
  - Provides for remote “engineering” (manual) access to all substation (or field) devices (IEDs) in a secure fashion.
  - Optional: Integrated file extraction (automated) as part of an overall data integration solution.
  - Replaces a Terminal Server / “Jump Host“ solution.
  - Can be used as a tool to aid in NERC CIP compliance.
    - Provides technical controls
    - Reporting capabilities
  - May also include:
    - Password management
    - Configuration (change) management for IEDs
    - Asset management

# Cyber Security and Privacy 2012 Project: Assessment of Remote Access Solutions

**Purpose:**

Work with vendors and utilities to assess several products providing Interactive Remote Substation Access.

**Approach:**

- Develop comprehensive list of requirements
- Develop use cases/scenarios
- Vendor deployment in Smart Grid Substation Lab
  - Some configuration/development required
- Vendor demonstrations of scenarios

Presenting utility requirements with a ‘unified voice’

# Cyber Security and Privacy 2012 Project: Assessment of Remote Access Solutions

- **Requirements workshops:**
  - May 23rd and June 13th, 2012
- **Product demonstration:**
  - Oct 24-25th, 2012 Knoxville, TN
  - Wide range of audience
  - Technical update: Document ID: 1024424 - Dec 2012

  *"Substation Security and Remote Access Implementation Strategies"*

**Utility Value:**

- Awareness of available products
- Common demonstration platform
- Vendor products improved

Vendors and utility collaboration for accelerated technology transfer





ELECTRIC POWER RESEARCH INSTITUTE

# EPRI's Cyber Security Research Lab Knoxville, TN

**Five vendors installed in the lab:**

- EnterpriseSERVER.NET by Subnet Solutions
- CrossBow by Ruggedcom, a Siemens Business
- SEL-3620 by Schweitzer Engineering Labs
- ConsoleWorks by TDi Technologies
- IED Manager Suite (IMS) by Cooper Power Systems
- Potentially others…

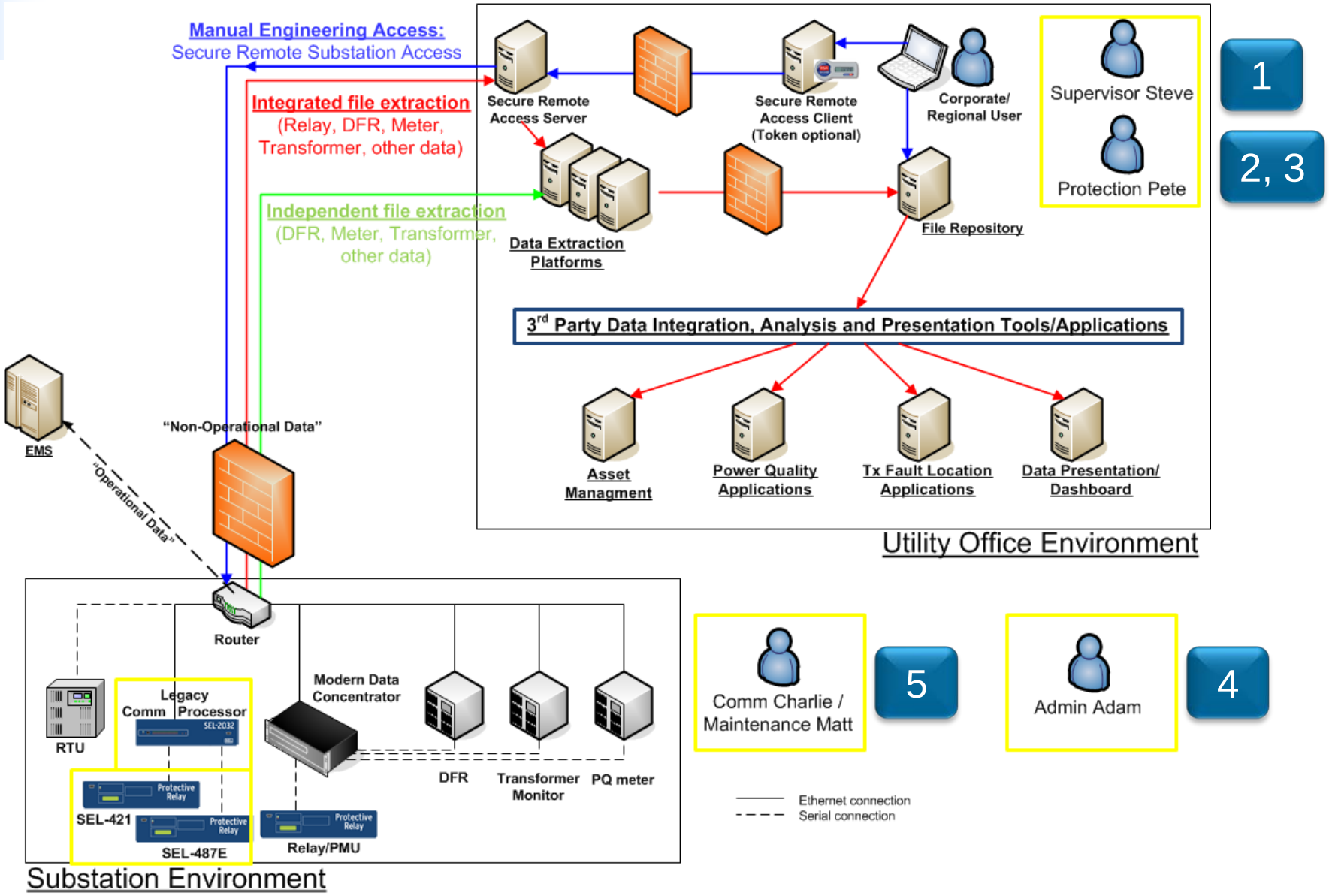
**Installation in a Common Demonstration Environment**





EPRI ELECTRIC POWER RESEARCH INSTITUTE

# Assessment of Remote Access Solutions: 2012 Remote Substation Access Scenarios








ELECTRIC POWER RESEARCH INSTITUTE

# EnterpriseSERVER.NET - Subnet Solutions

SUBNET EnterpriseSERVER.NET on localhost - Virtual Machine Connection

File Action Media Clipboard View Help

EnterpriseSERVER.NET Version 3.8.1 -- Logged in as Built-in account for administering the computer/domain [administrator] (Admin)

File Reports Administer Password Admin Help

Refresh IED Status | Launch Connection | Report General Error | Report Broken Connection...

- EPRI SGSL
  - Charlotte
  - Knoxville
  - Lenox

EPRI SGSL-Knoxville

| Device Name | Job Name | Device Type | Connection Name | Connection Type | Status | Available |
|---|---|---|---|---|---|---|
| 7SJ64 - KNX | Logon | Siemens 7SJ64 | 7SJ64 - KNX | TCPIP | Future | ☐ |
| DR E3 KNX | Logon | DR E3 | DR E3 connect | TCPIP | Available | ☑ |
| D60 HF - KNX | Logon | GE D60 | KNX D60 HF | TCPIP | Available | ☑ |
| D60 Line - KNX | Logon | GE D60 | KNX D60 Line | TCPIP | Available | ☑ |
| T60 - KNX | Logon | GE T60 | KNX T60 | TCPIP | Available | ☑ |
| SEL-421 - KNX | Logon Levl 2 | SEL-421 | KNX-SEL421 | TCPIP | Available | ☐ |
| SEL-421 - KNX | Level 2 Pas... | SEL-421 | KNX-SEL421 | TCPIP | Available | ☐ |
| SEL-421 - KNX | L | | | | Available | ☐ |
| P145 - KNX | L | | | | Disabled | ☐ |
| P546 - KNX | L | | | | Future | ☐ |
| P643 - KNX | L | | | | Future | ☐ |
| RED 670 - KNX | L | | | | | |
| REL 670 - KNX | L | | | | | |
| RSG2100 - KNX | L | | | | | |
| RSG2288 - KNX | L | | | | | |
| SEL-3351 - KNX | L | | | | | |
| SEL-3373 - KNX | L | | | | | |
| SEL-487E - KNX | L | | | | | |
| SEL-487E - KNX | L | | | | | |
| SEL-487E - KNX | L | | | | | |
| Webcam - KNX | L | | | | | |

Launch Connection

You

ESNETCOM5 - HyperTerminal

File Edit View Call Transfer Help

```
=>id0-
"FID=SEL-421-3-R123-V0-Z010010-D20070223","08FA"
"BFID=SLBT-4XX-R100-V0-Z001001-D20010703","0972"
"CID=6E74","0263"
"DEVID=K1SL2","0366"
```

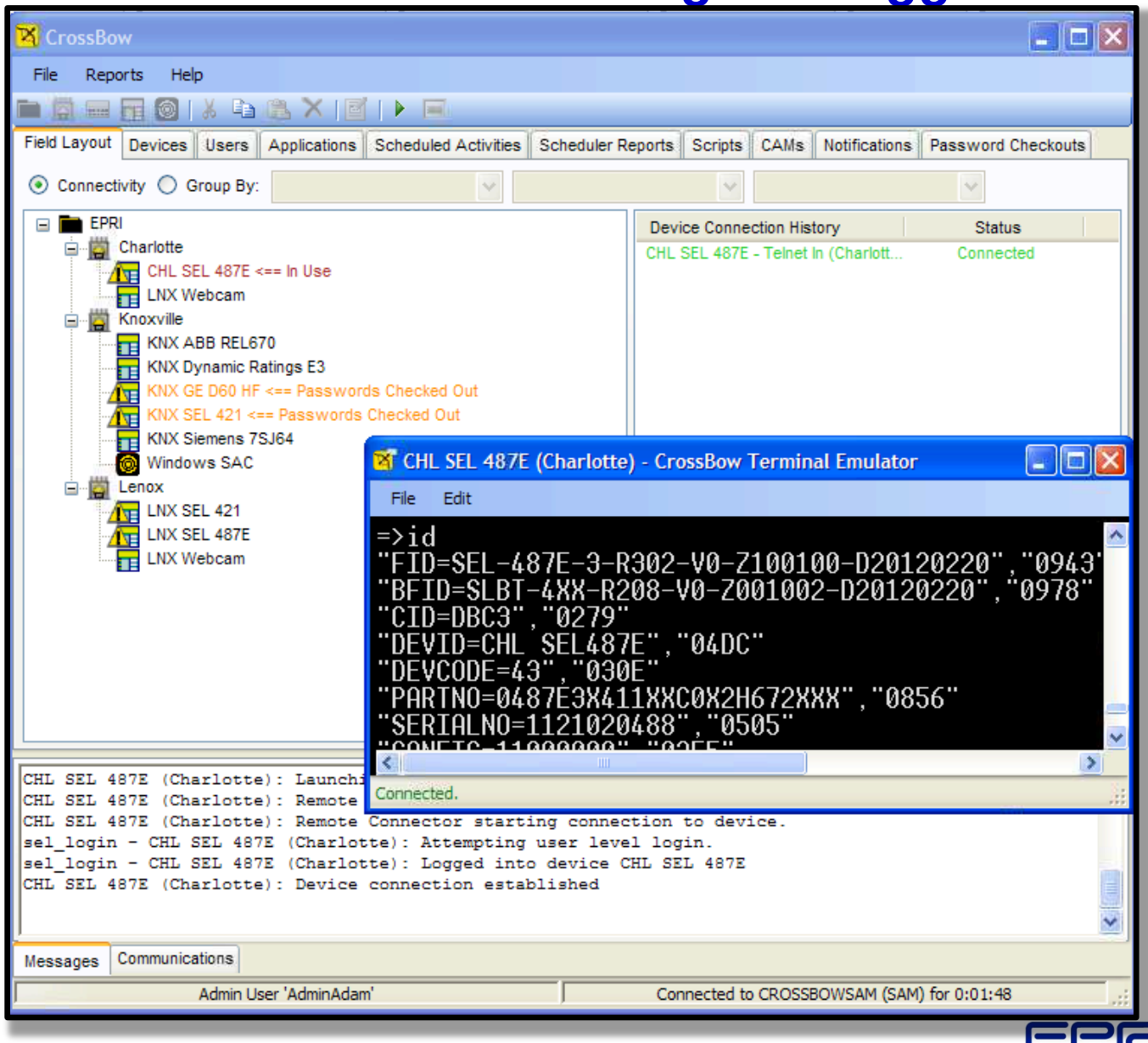
Status: Running





ELECTRIC POWER RESEARCH INSTITUTE

# CrossBow Secure Access Manager - Ruggedcom

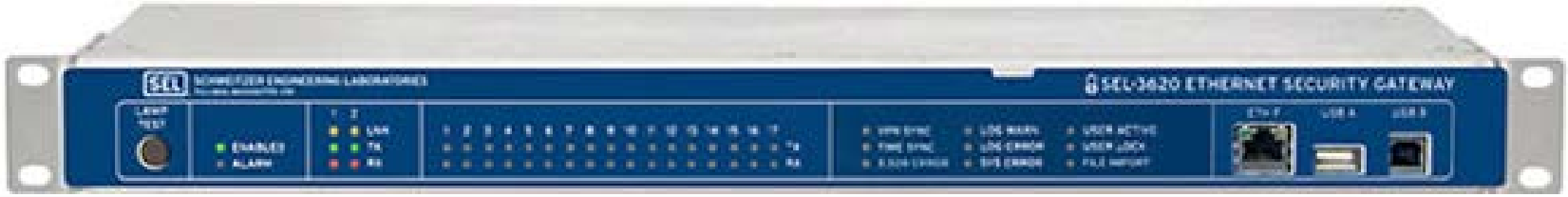







ELECTRIC POWER RESEARCH INSTITUTE

# SEL-3620 Secure Ethernet Gateway - SEL




SCHWEITZER ENGINEERING LABORATORIES

Device: EPRISEL-3620 | Rhett [ Logout ] | Server time: Fri, Sep 14, 2012 01:01 EDT

Dashboard
System
Date/Time
Usage Policy
File Management
Web Server
Device Reset
User
Accounts
LDAP Settings
Local Groups
Network
Network Settings
Static Routes
Syslog
Firewall
Hosts
Serial Ports
Port Settings
Port Profiles
Port Mappings
Security
X.509 Certificates
IPsec Connections
Allowed Clients
SSH Host Key
Password Management
Reports
System Logs
Diagnostics
Proxy Reports
Help

DASHBOARD

Network Interfaces: Eth F, Eth 1, Eth 2

Serial Ports: COM09, COM10, COM11, COM12, COM13, COM14, COM15, COM16, COM01, COM02, COM03, COM04, COM05, COM06, COM07, COM08, COM17

System Statistics

| | |
|---|---|
| IPsec Connections: | 0 |
| Web Users: | 1 |
| Uptime: | 0y 55d 9h 30m 38s |
| Hours: | 16910 |
| Power Cycles: | 290 |
| # of Firewall Rules: | 0 |
| Syslog Statistics | |
| # Messages: | 4428 |
| # Unacknowledged: | 4428 |
| Oldest Unacknowledged: | 184 days |

Light Indicators: VPN SYNC, LOG WARN, USER ACTIVE, TIME SYNC, LOG ERROR, USER LOCK, X.509 ERROR, SYS ERROR, FILE IMPORT

Ethernet Connections

| Alias | State | In | Out |
|---|---|---|---|
| Eth F | NO-CARRIER | 0 Bytes | 0 Bytes |
| Eth 1 | UP | 849.14 MB | 17.82 MB |
| Eth 2 | DOWN | 0 Bytes | 0 Bytes |

IPsec Connections: Alias, State, Out, In

Version Information

| | |
|---|---|
| Serial Number: | 1492000000 |
| Version: | R133 |
| FID String: | SEL-3620-R133-V0-Z003003-D20111014 |

Resource Usage: CPU, RAM, Disk (User), Disk (OS); 0, 10

Logs By Severity: 99%; Emergency (0), Alert (0), Critical (5), Error (0), Warning (44), Notice (4379), Informational (0)

PORT MAPPINGS

Add Group

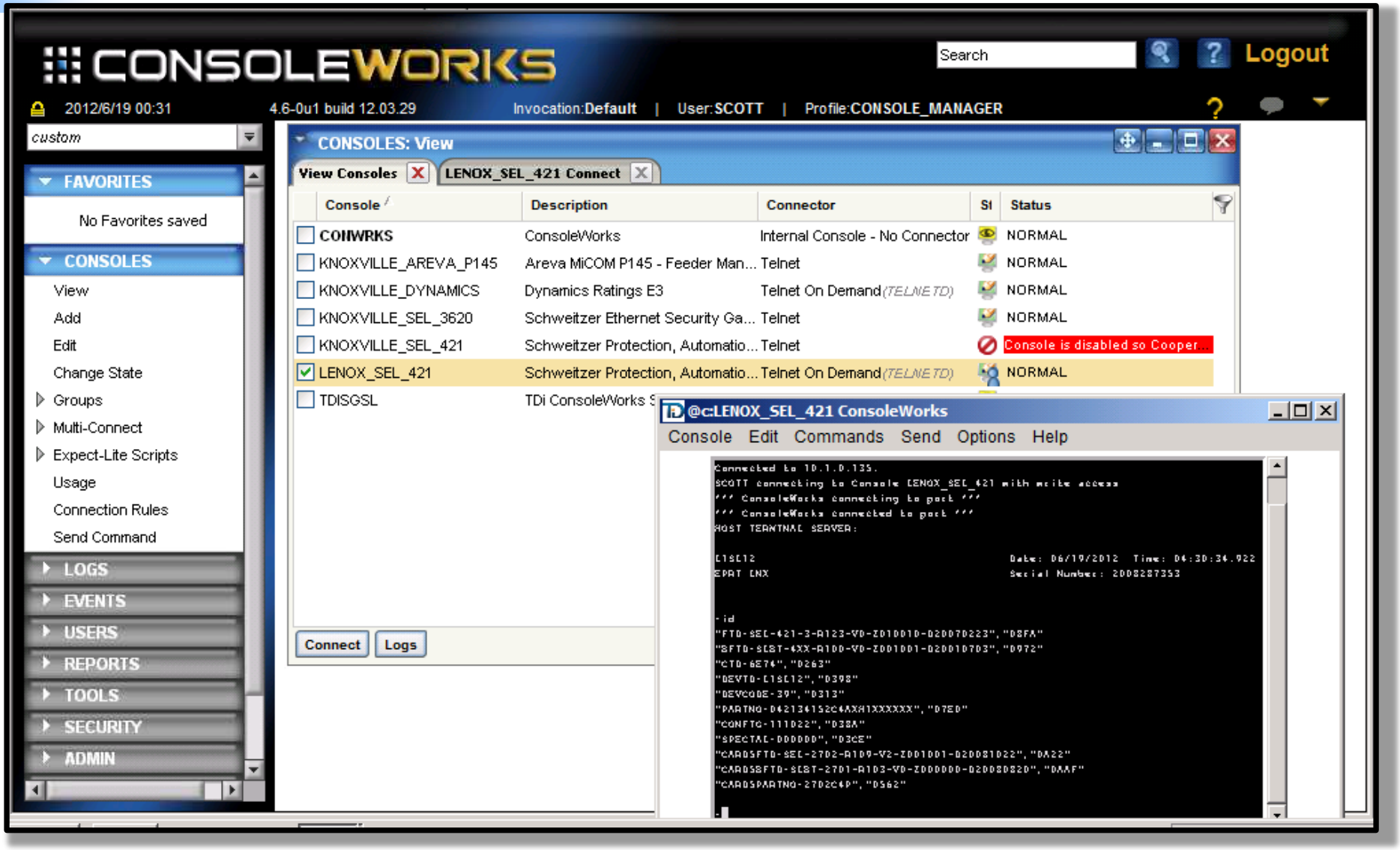
| Name | Action |
|---|---|
| scripted master port | Add Device, Rename, Disable, Delete |
| ALL:22 — SSH — master port | Update, Delete |
| Managed Devices: KNX-SEL-421 | Connected Via: COM01 |
| Telnet | Add Device, Rename, Disable, Delete |
| ALL:23 — Telnet — Telnet | Update, Delete |
| SSH — ALL — 192.168.1.2:22 — Remote Telnet | Update, Delete |





EPRI ELECTRIC POWER RESEARCH INSTITUTE

# ConsoleWorks – TDi Technologies








ELECTRIC POWER RESEARCH INSTITUTE

# IED Manager Suite - Cooper Power Systems

Enterprise Management Console [Lab_EPRI]

Server Context View Tools Help

Configure:
- Server Characteristics
- Event Classification
- Password Policies
- Passthrough
- Supported Device Types
  - IED Families (13)
- Regions, Substations and IEDs (1)
  - EPRI (1)
    - Region: Tennessee (3)
      - Subst: Charlotte (1)
        - IED: Gateway_3_0_56
      - Subst: Knoxville (1)
        - IED: Gateway_1_0_65
      - Subst: Lenox (1)
        - IED: Gateway_2_0_56
- Users and Groups
  - Active Directory Users and Groups (1)
  - Local Users (3)
  - Groups (5)
- SMP Gateway Local Users and Group
- IED Polling Settings (1)
  - EPRI (1)
    - Region: Tennessee (3)
      - Subst: Charlotte (1)
      - Subst: Knoxville (1)
      - Subst: Lenox (1)

Show:
- IED Status

Configure: \ Regions, Substations and IEDs (1) \ EPRI (1) \ Region: Tennessee (3) \ Subst: Knoxville (1) \ IED: Gateway_1_0_65

**Define IEDs that are behind the selected device.**

IED and Connection Definition | IED Info | Password Management

| IED Name | IED Type | LinkType | Conx Address | IED Description |
|---|---|---|---|---|
| LD_HF_1_0_69 | UR-D60 | TCP/IP | "UR69" | Line Distance Relays (HF) |
| LD_Line_1_0_70 | UR-D60 | TCP/IP | "GED60" | Line Distance Relays (Line) |
| LD_Line_1_0_70_Web | Web | TCP/IP | "GED60Web" | |
| LP_1_0_71 | SEL-421 | TCP/IP | "SEL421" | High-Speed Line Protection,... |
| TR_1_0_72 | SEL-487 | TCP/IP | "SEL72" | Transformer Protection Relay |
| TR_1_0_74 | UR-T60 | TCP/IP | "UR74" | Transformer Protection Syste... |

Ready | Editing: Lab_EPRI | Operational: Lab_EPRI | Connected





EPRI ELECTRIC POWER RESEARCH INSTITUTE

# Remote Access Timeline

| 2012 | 2013 | 2014 |
|---|---|---|

2012 project:

Oct Workshop

Features

***Vendor product maturity***





ELECTRIC POWER RESEARCH INSTITUTE

# Interest Group (Free!)



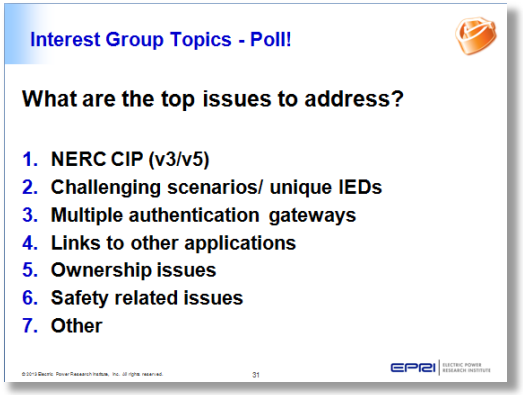



ELECTRIC POWER RESEARCH INSTITUTE

# Secure Remote Substation Access Interest Group

## Interest Group – open to all utilities!

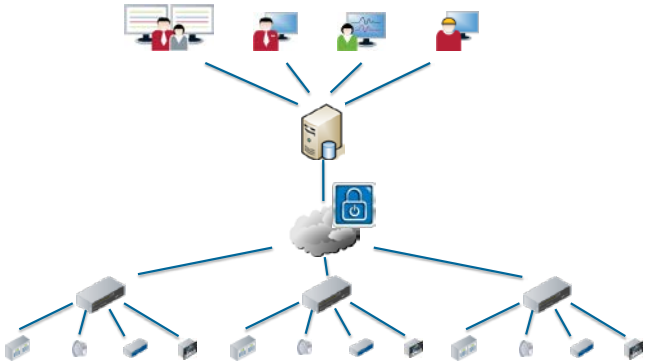
- Webcasts to develop additional scenarios for testing
  - Identify top “challenging”, “unusual” or “difficult” IEDs, protocols or implementation challenges
- Can be discussion topics or working sessions
  - Ex. Mapping NERC CIP v5 requirements to Remote Access System capabilities or RFP requirements
- Discussions amongst peers
- Develop community of users



# Secure Remote Substation Interest Group

Discussion topics with both EPRI and utility guest presenters:

- Implementation Challenges/Proposed Tasks
- Unique IED vendor integration challenges
  - *IED Compatibility Matrix*
- Password management issues and concepts
  - *Integration with Password Vault*
- NERC CIP v3 and v5 mapping
- Requirements review (one-on-one effort)



**Identifying top Remote IED Access issues**

# Review of Top Challenges/ Proposed Tasks






ELECTRIC POWER RESEARCH INSTITUTE

# List of Remote Access Challenges/Tasks

1. **Penetration Testing**

2. **Remote Access Vendor ←→ IED interoperability / compatibility tests**

3. **Integration with a "Password Vault"**

**<u>Others:</u>**

- **Password, Configuration, Change Management**
- **Alarm Correlation / Incident Management**
- **Coordination with Operations**

**These top items are planned to be addressed in our supplemental project, with additional items as time and funding permit.**

# Scenario 1: Penetration Testing

Remote Substation Access Systems can manage our IED passwords, with role based access control and supporting CIP compliance…

...But are they SECURE?

Utilities have requested through the Interest Group for independent penetration tests to be performed on remote access systems.

We are now planning on including this task for 2014.

# Scenario 1: Penetration Testing

## Vulnerability Identification

- Databases
  - CVSS
  - CVE
- Configuration
  - CCE
  - CPE

A search on “SQL” and “passwords” in the NIST NVD CVSS produces 472 matches. These matches range from 1998 to 2013.

## NESCOR Testing Guides

- Guide to Penetration Testing
- Guide to Vulnerability Scanning


## Tools

- Scanning
- Exploitation

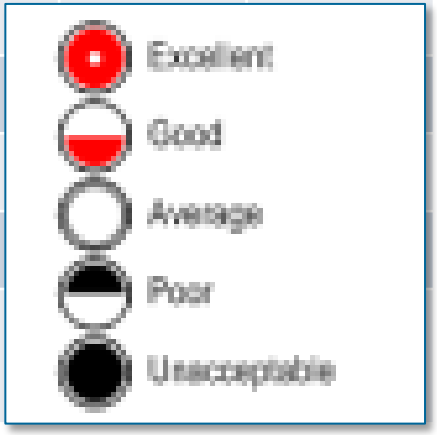




ELECTRIC POWER RESEARCH INSTITUTE

# Scenario 2: Remote Access Vendor ←→ IED interoperability / compatibility tests

| RA system / IEDs | SEL relay | GE UR relay | ABB Relay | Siemens Relay | PQ meter | DFR | Other |
|---|---|---|---|---|---|---|---|
| Crossbow | | | | | | | |
| ESNET | | | | | | | |
| Cooper | | | | | | | |
| SEL-3620 | | | | | | | |
| TDI | | | | | | | |
| Vendor X (example) | ✓ | ✗ | ✗ | ✓ | ◐ | | |




- Tests would be broken down into <u>specific</u> tasks such as:
  - Intelligent vs. Passive proxy
  - Ability to manage passwords
  - File/Event retrieval
- Could include gateway products (RTAC, SMP, 2020, D20, SSNET)

IED Device Matrix





EPRI ELECTRIC POWER RESEARCH INSTITUTE

# Scenario 2: Specific Task function examples

| General | | | | |
|---|---|---|---|---|
| Type | IED | Remote Access Protocol | Data Acquisition Protocol | Priority |

| Advanced/ Automated Functions | | | | | | |
|---|---|---|---|---|---|---|
| Login and Logout | | Passwords | | Configurations | | |
| Automated login | Automated logout | Change Device Password in gateway | Change Password | Backup config | Restore Config | Get Config summary |

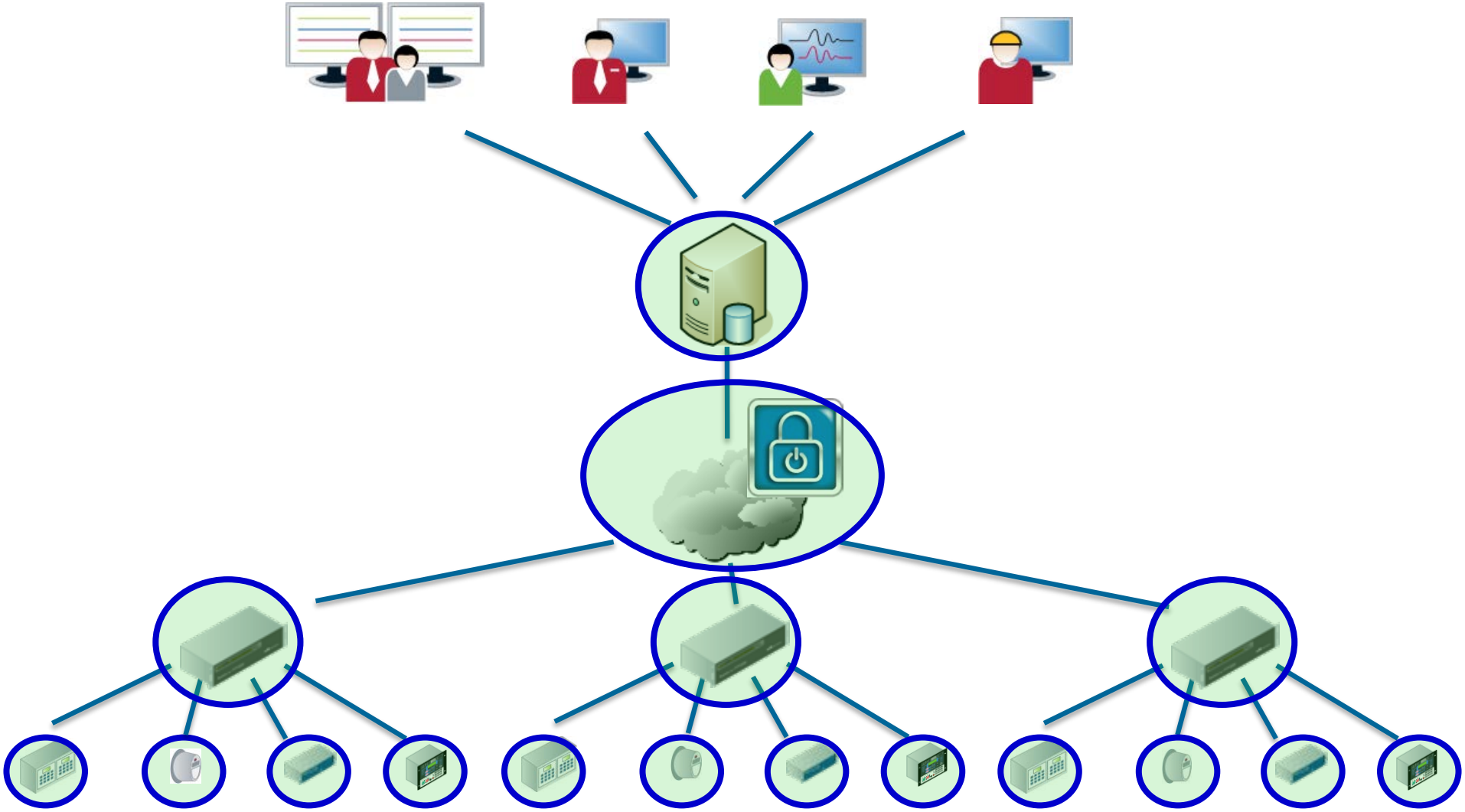
| Advanced/ Automated Functions | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Firmware | | | Events | SOE | Logs | Discover | Faceplate | Data |
| Retrieve firmware version | Compare firmware | Update firmware | Retrieve new event files | Retrieve SOE files | Retrieve device logs | Discover Connected devices | Refresh Faceplate LEDs | Retrieve device data |





ELECTRIC POWER RESEARCH INSTITUTE

# BYOD! (Bring your own device!!)







ELECTRIC POWER RESEARCH INSTITUTE

# Scenario 3: Integration with a "Password Vault"

# What is a "Password Vault"?

Benefits of a password management solution:

- Regular password changes improve security and compliance
- Control which users have access to passwords
- Allow detailed auditing of each use of these passwords

Some solutions offer advanced functionality including:

- Password Changes
- Password Verification
- Password Reconciliation

Automatic password management of service accounts either through 'push' or 'pull' approach

# Scenario 3: Integration with a “Password Vault”

- Problem statement:
  - Multiple password vaults, different security or logging levels for various systems, makes difficult for auditing/compliance
  - Current IT Enterprise password vault products do not interact with substation IEDs

- Ideal end state:
  - Single integrated password vault to manage all shared/service account passwords.
  - Remote Access solution would connect to IEDs using passwords stored in Password Vault solution

- Potential solutions:
  - Integrate products via API

# NERC CIP considerations:

"How do we be achieve remote access and remain compliant without being intrusive to the operational and maintenance activities??"

# Remote Access to CIP v5 mapping exercise:

Guide to **Medium** Substation Assets

- Credit: MidAmerican Energy and FirstEnergy
- DRAFT standards as of November 2012 Recirculation ballot

| Std | R | Full Text | Medium Impact BES Cyber Systems (MIBCS) | Medium Impact BES Cyber Systems (MIBCS) with Routable Connectivity | Remote Access Tool? |
|---|---|---|---|---|---|
| 007 | 5.1 | Have a method(s) to enforce authentication of interactive user access, where technically feasible. | - | Yes + PCA | n |
| 007 | 5.2 | Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). | Yes | Yes + PCA | y |
| 007 | 5.3 | Identify individuals who have authorized access to shared accounts. | - | Yes + PCA | y |
| 007 | 5.4 | Change known default passwords, per Cyber Asset capability | Yes | Yes + PCA | y |
| 007 | 5.5 | For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset. | Yes | Yes + PCA | y |
| 007 | 5.6 | Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months. | - | Yes + PCA | y |
| | 5.7 | Limit unsuccessful attempts or generate alerts of unsuccessfull authentication attempts | | control centers only | y |





ELECTRIC POWER RESEARCH INSTITUTE

# Remote Access Timeline

| 2012 | 2013 | 2014 |
|---|---|---|

2012 project:

Oct Workshop

June 2013

Secure Remote Access **Interest Group**

- Discussions
- Develop Test Scenarios

Features

***Vendor product maturity***





EPRI ELECTRIC POWER RESEARCH INSTITUTE

# Exciting Supplemental Plans!





ELECTRIC POWER RESEARCH INSTITUTE

# Secure Remote Substation Access Solutions Supplemental Project

This project will investigate and address implementation challenges for secure remote substation access security solutions, including:

- "Hands-on" workshop allows system familiarization and understanding of implementation challenges, best practices, and technology gaps

<u>Areas of focus may include:</u>

- Specific devices not easily integrated with existing solutions
  - Vendor proprietary IED tools/protocols
  - Use of multiple authentication devices/gateways

- Remote Access System Management of IEDs
  - Management and tracking of configurations
  - Patch management
  - Password management

# Secure Remote Substation Access Solutions Research Drivers

- Remote Access products are still maturing
  - Require support for legacy, current and future devices
  - Products must provide features to support changing cyber security and compliance requirements.

- Remote access to substations can provide new opportunities for data integration solutions such as fault location, asset optimization, and power quality monitoring.
  - Leads to improved asset monitoring

- Remote access can also reduce “windshield time” to reach field IEDs
  - Leads to improved restoration time

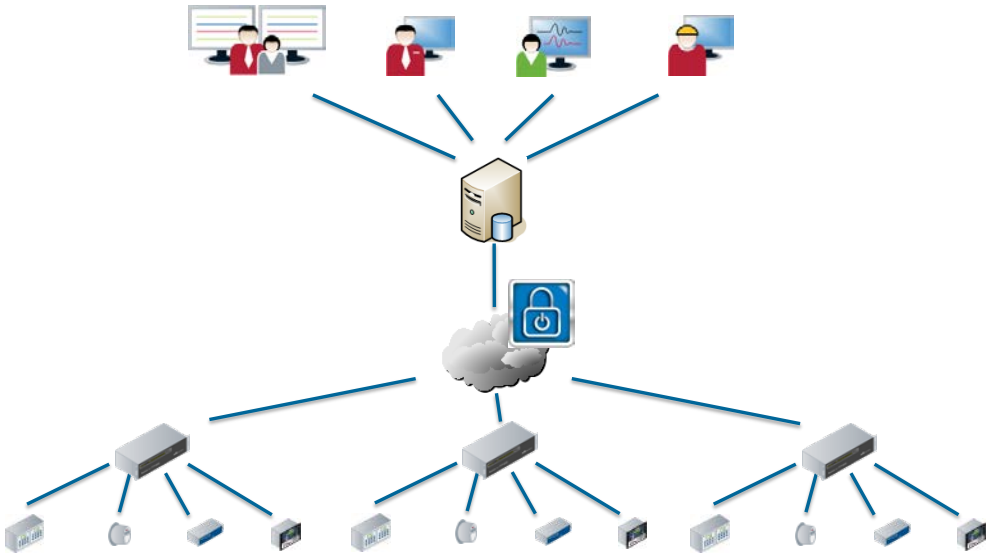
Value:

- This project is valuable to any utility that has or desires to implement secure remote access to substations, IEDs, and field equipment. The topics covered can be applied to both transmission and distribution substations.

# Secure Remote Substation Access Solutions Expected Key Results

Through participation in this supplemental, members will be able to :

- Learn about emerging technologies and solutions while gaining visibility into existing best practices
- Identify challenges unique to Remote Access systems
- Study implementation options, best practices and capabilities/limitations regarding the challenge.
- Share challenges, solutions and lessons learned with peers







ELECTRIC POWER RESEARCH INSTITUTE

# Reasons to Participate

- Changes to NERC CIP may necessitate new features and new tests to be performed on remote access systems
  - Previous discussions with members highlighted NERC CIP as major focus with remote access systems.

- Side-by-side comparison of Remote Access Vendors in common environment
  - Unbiased visibility into vendor-based remote access solutions

- Demonstration and Workshop with individual presentations by remote substation access solution vendors.

# Even More Reasons to Participate

## EPRI's Cyber Security Research Lab

- Take advantage of EPRI's lab as **YOUR** resource!
  - Labs are difficult to maintain
  - Variety of multi-vendor substation equipment
    - Able to introduce other equipment as requested
    - OR… "Bring your own device"
  - Utility labs may not include "end-to-end" architecture
    - EPRI's reconfigurable lab allows modeling and testing with **YOUR** substation architecture.
  - "Try before you buy"
    - Remote access to EPRI lab for "hands-on" testing from your office!

# Remote Access Timeline

2012 | 2013 | 2014

2012 project:

Oct Workshop

June 2013

Secure Remote Access **Interest Group**

Scenarios

Scenarios

Scenarios

- Discussions
- Develop Test Scenarios

Remote Access Solutions **Supplemental**

- Develop/Enhance Features
- Applying Test Scenarios
- Penetration Testing

Features

Feature

Feature

Feature

**Solving Implementation Issues!**

***Vendor product maturity***



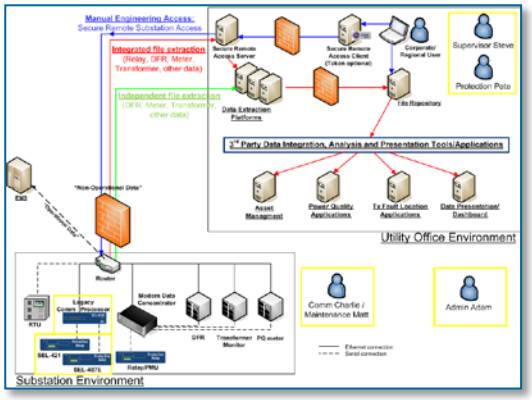


EPRI ELECTRIC POWER RESEARCH INSTITUTE

# Key Take-Aways:

- Remote Substation Access products are still in their infancy.
  - You are not the first one to implement these products or run into challenges.
- We need to build and strengthen a community of users now!
  - Challenge: Users span multiple organizations
  - Work together to share technical approaches to NERC CIP
- Developing <u>unified</u> utility requirements and test scenarios can improve the market offerings.
- <u>Together, we can accelerate the maturation process!</u>

# Secure Remote Substation Access Solutions 2014 plans




## Interest Group

Free to participate, open to all utilities:

- Remote Access *Interest Group:*
  - Discussion of challenges
  - Presentations on related topics by peers
  - Utility only (no vendor) participation

## Supplemental

- Webcasts
  - Presentation by vendors
- Development/Integration efforts
  - Translate Interest Group challenges into testing scenarios
- On-site workshop with vendors at EPRI labs. Knoxville, TN
  - Live demonstrations, interaction with vendors
  - Share challenges, solutions and lessons learned by peers





EPRI ELECTRIC POWER RESEARCH INSTITUTE

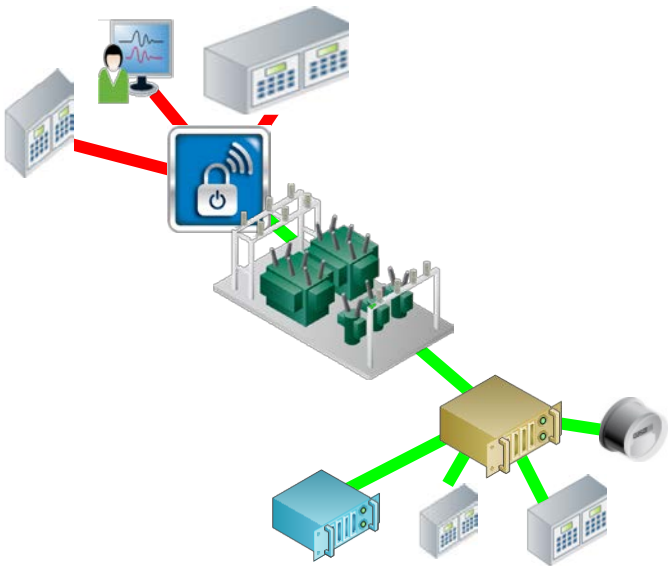
# Secure Remote Substation Access Solutions

## Objectives and Scope

- Address implementation challenges identified by the Secure Remote Access Interest Group such as:
  - Scalability
  - Management and tracking of IED configurations
  - Use of multiple authentication devices/gateways
- Provide implementation options and best practices
- Conduct a Secure Remote Access Workshop

## Value

- Gain new knowledge and practical guidance on a variety remote access solutions and scenarios
- Coordinate with vendors to advance the capabilities of remote access solutions



### Details and Contact

- Price: $40,000
- Qualifies for TC and SDF


***Scott Sternfeld***

- ssternfeld@epri.com
- 843-619-0050


***SPN Number: 3002001767***

**Advanced Implementation Guidance for Secure Remote Access Solutions**





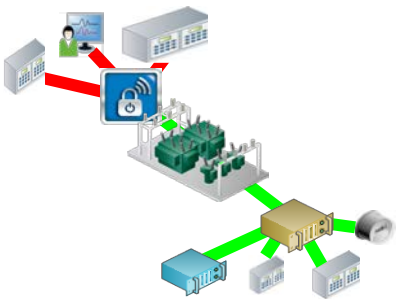
EPRI ELECTRIC POWER RESEARCH INSTITUTE

# Key meeting reminders and links

**<u>Secure Remote Substation Access Solutions</u> – Introductory Webcast**

**October 16th Webcast - NOW**

***SPN Number: 3002001767***



**<u>Remote Access Interest Group Calls</u>**

**Quarterly: Nov 2013; Feb, May, Aug, Nov 2014**

**<u>NERC CIP Tools and Techniques</u> - Introductory Webcast**

**October 17th Webcast 11-12pm EST**

**<u>Add to Calendar</u>**

***SPN Number: 3002001768***

**For questions, please contact: Scott Sternfeld**

- ssternfeld@epri.com
- 843-619-0050





ELECTRIC POWER RESEARCH INSTITUTE

# NERC CIP Tools and Techniques

## Objectives and Scope

- Provide guidance for transitioning to NERC CIP Version 5
- Project may focus on:
  - Configuration change management
  - Patch management
  - Identity access management
  - Determination of BES cyber assets and BES Cyber Systems

## Value

- Identify gaps in current tools that have been deployed to address the CIP requirements
- Provide guidance and techniques for complying with CIP requirements

**Details and Contact**

- Qualifies for TC and SDF


***Scott Sternfeld***

- ssternfeld@epri.com
- 843-619-0050


***SPN Number: 3002001768***

**Guidance for Efficiently Meeting NERC CIP v5 Requirements**





ELECTRIC POWER RESEARCH INSTITUTE

# Together…Shaping the Future of Electricity





ELECTRIC POWER RESEARCH INSTITUTE

# Legal Notices

**Please observe these Antitrust Compliance Guidelines:**

- Do not discuss pricing, production capacity, or cost information which is not publicly available; confidential market strategies or business plans; or other competitively sensitive information
- Be accurate, objective, and factual in any discussion of goods and services offered in the market by others.
- Do not agree with others to discriminate against or refuse to deal with a supplier; or to do business only on certain terms and conditions; or to divide markets, or allocate customers
- Do not try to influence or advise others on their business decisions and do not discuss yours except to the extent that they are already public

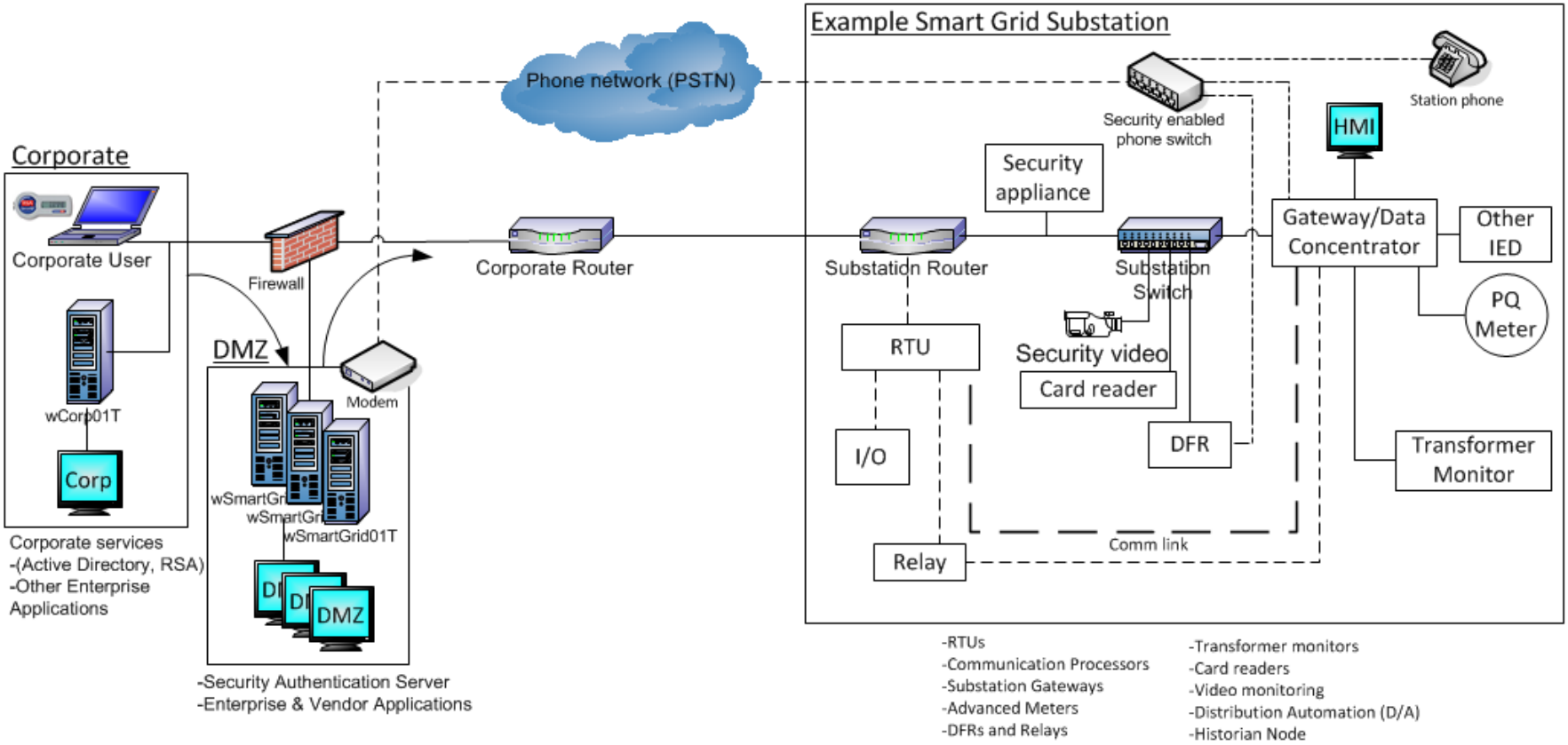
# Architectures

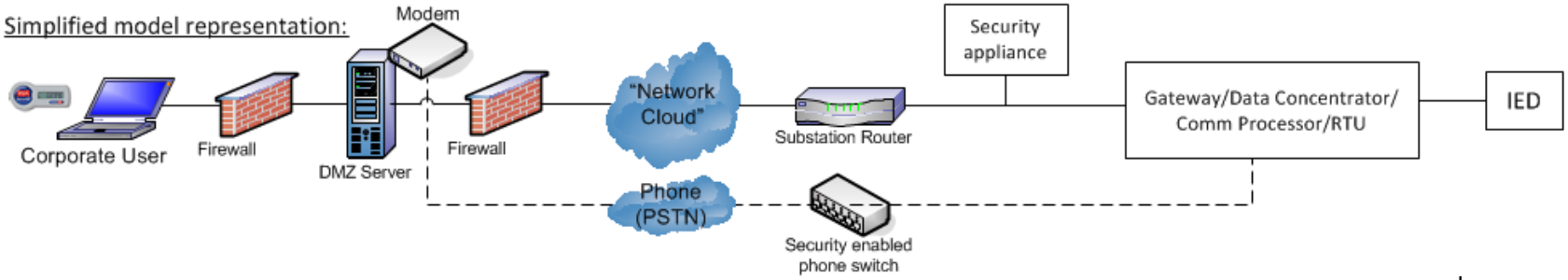





ELECTRIC POWER RESEARCH INSTITUTE

# Sample Network Environment



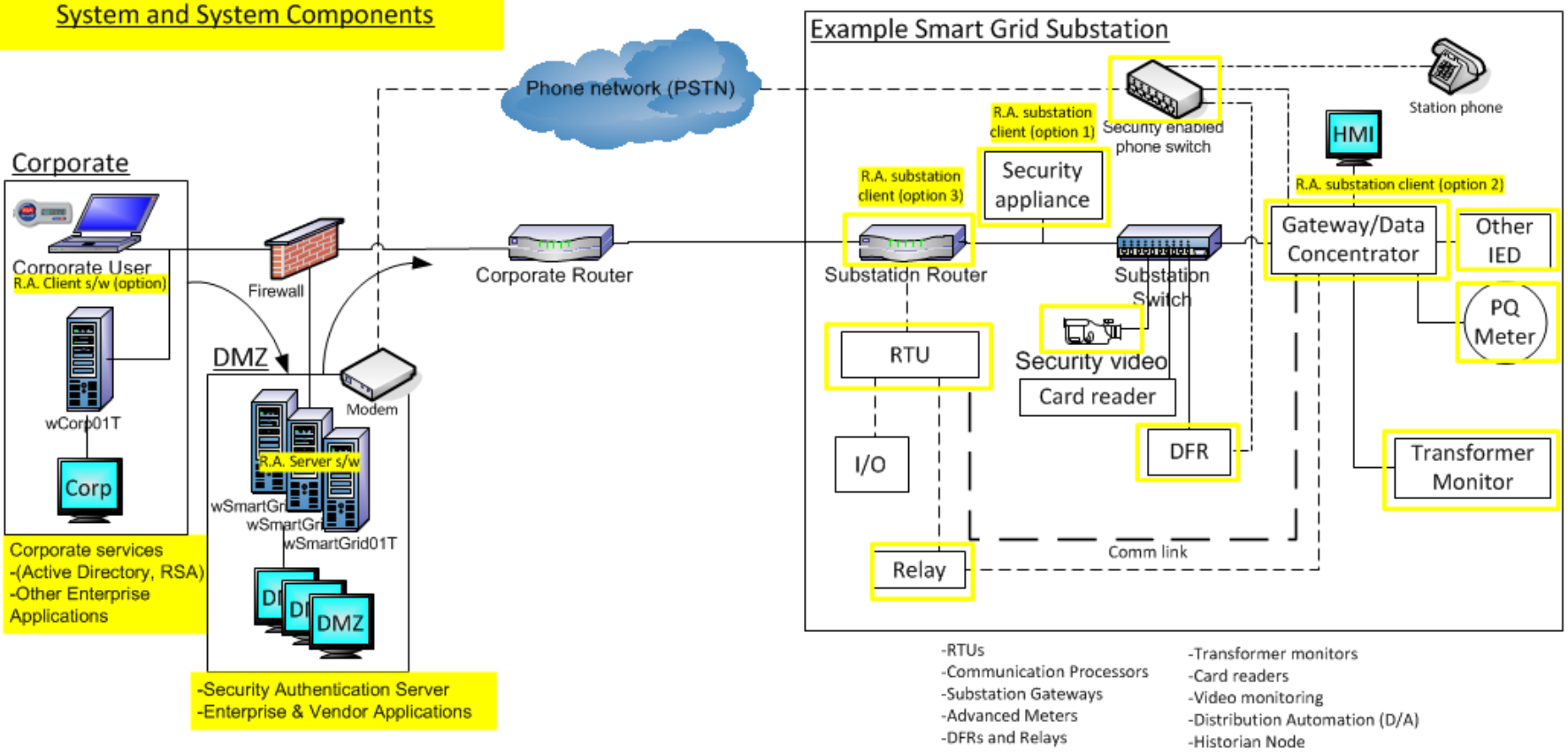


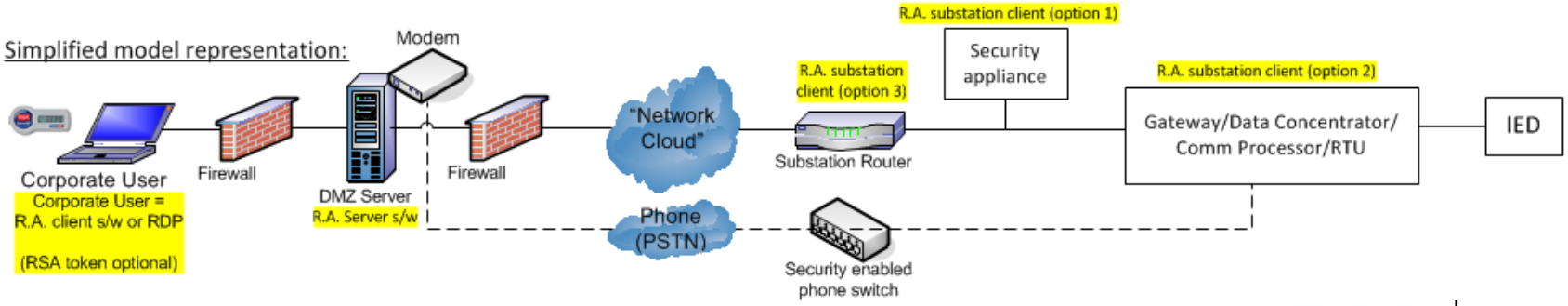



ELECTRIC POWER RESEARCH INSTITUTE

Example devices that can be accessed/ managed with a Remote Substation Access System and System Components

# Sample Network Environment



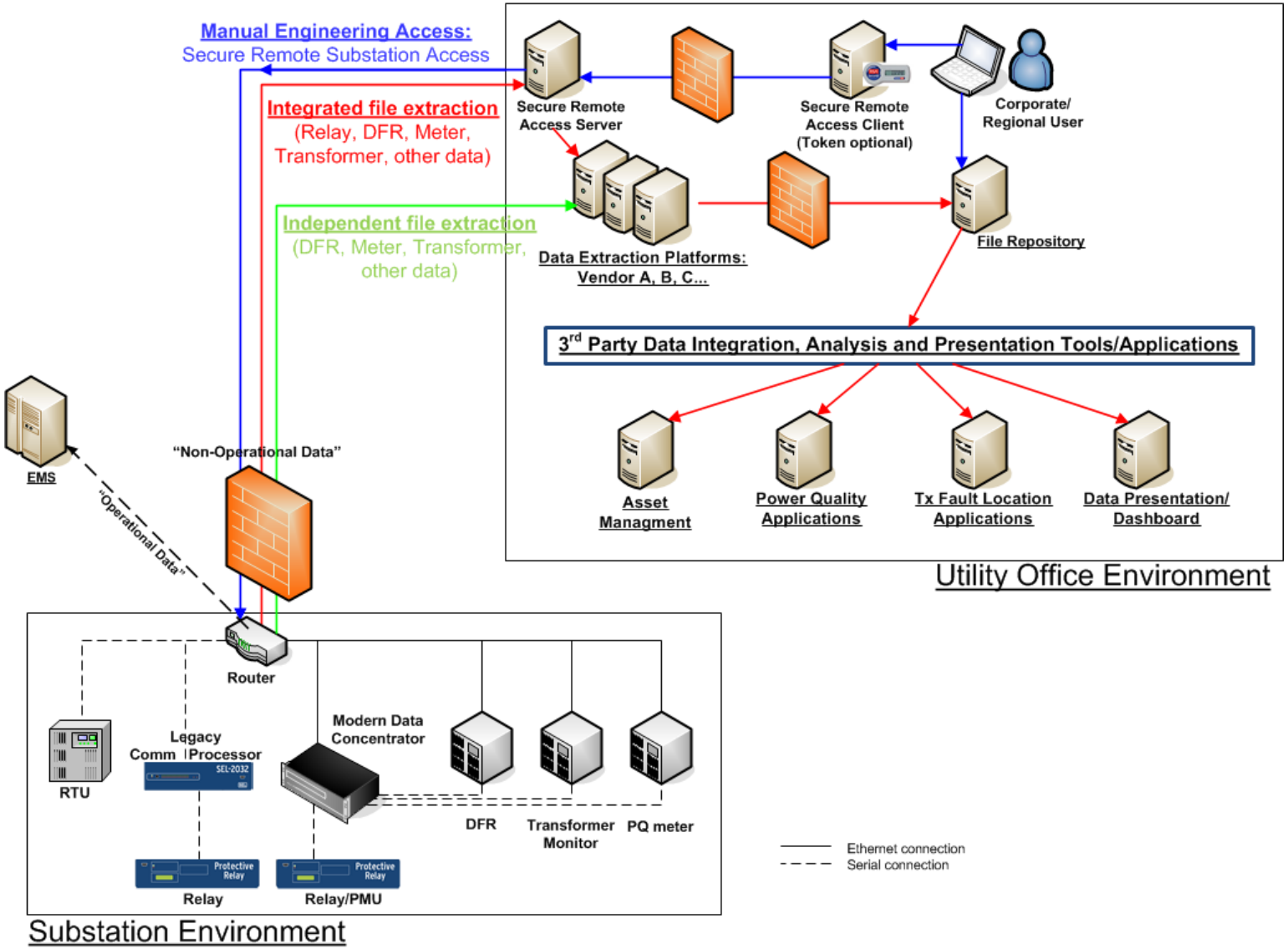








ELECTRIC POWER RESEARCH INSTITUTE

# Engineering Access and File Extraction








ELECTRIC POWER RESEARCH INSTITUTE

# Remote Substation Access Interest Group homepage: http://www.smartgrid.epri.com/SRSA.aspx

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

EPRI.com | Contact Us

## Smart Grid Resource Center

Home | EPRI Research | Resources | Interest Groups | Events Calendar | Newsletters

- Interest Groups
- GIS Interest Group
  - Webcast Archive
- **Secure Remote Substation Access Interest Group**
- Smart Grid EA Interest Group
- Metering & AMI Interest Group
- Communications Interest Group
- Roadmap Interest Group

### Secure Remote Substation Access Interest Group

*A Technology Transfer Outreach Effort of the EPRI Cyber Security Program*

**Purpose of the SRSA Interest Group**

The SRSA Interest Group is a forum for utilities to share experiences and best practices, discuss the tools and techniques, and exploring research topics for the advancement of secure remote substation access.

There is an established need for remote substation access solutions that provide support for a wide range of IEDs including current, legacy, and future devices, and also deliver the required level of cyber security and compliance support. Remote communications access to substations can provide new opportunities for data integration solutions such as fault location, asset optimization, and power quality monitoring. It may also reduce the number of times field personnel are required to visit substations to retrieve IED configuration or event files for analysis. However, balancing this level of access with cyber security and potential regulatory compliance requirements can be very difficult. This balance can be achieved through proper preparation, procedure implementation, and organizational support.

The objectives of this interest group are to identify implementation challenges for secure remote access functionality, advance the state-of-the-art of secure remote access systems for the power delivery domain, and build a community of end users to socialize secure remote substation access concepts and best practices.

Key activities for the interest group include:

**Additional Resources**

**July 18th, 2013**
**Secure Remote Access Interest Group Webcast**
Recording (17.7 MB)
Presentation (2 MB)

**June 6th, 2013**
**Secure Remote Access Interest Group-kickoff Webcast**
Recording (12 MB)
Presentation (3 MB)
EPRI Secure Remote Substation Access Interest Group Charter - May 2013 (71 KB)

For more information, contact Scott Sternfeld at EPRI.





EPRI | ELECTRIC POWER RESEARCH INSTITUTE

# EPRI's Smart Grid Substation Lab Knoxville, TN


**Product testing and demonstration site: Common environment for all vendors**





EPRI ELECTRIC POWER RESEARCH INSTITUTE