ELECTRIC POWER RESEARCH INSTITUTE

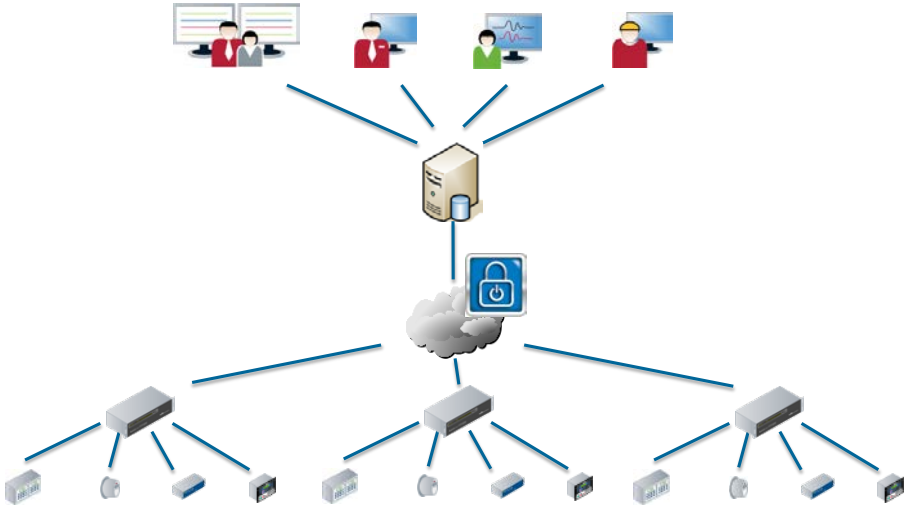
Secure Remote Substation Access Interest Group Kickoff Meeting

June 5, 2013

Scott Sternfeld, Project Manager
Smart Grid Substation & Cyber Security Research Labs
ssternfeld@epri.com

Utility co-chair:
John Stewart, PM Grid ICT
jwstewart@tva.gov

Agenda



EPRI background

Cyber Security Team/P183

2012 Remote Access Project Review

Interest Group Charter review

Topics of Interest for this Group

Password Management discussion

Schedule of next meetings

Outreach Efforts – Poll!

How did you first become aware of today's webcast?

- **EPRI member/advisor**
- **NATF member (N.A. Transmission Forum)**
- **EPRI + NATF**
- **Other (GIS int. group, etc…)**

Organization – Poll!

What organization do you represent?

- **Engineering**
- **SCADA/EMS Operations**
- **Protection**
- **CIP Compliance**
- **Field Organization**
- **Network/IT**
- **Other**

Introducing EPRI…

EPRI is a company that…

…brings together great people…

…with new and exciting ideas…

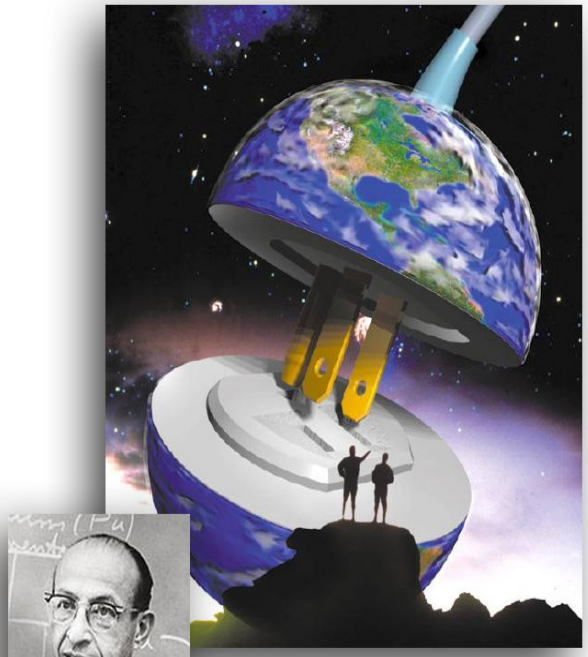
…to help energize the world!

"Together…Shaping the Future of Electricity"

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Our History…

- Founded in 1973
- Independent, nonprofit center for public interest energy and environmental research
- **Collaborative** resource for the electricity sector
- Major offices in Palo Alto, CA; Charlotte, NC; Knoxville, TN
  - Laboratories in Knoxville, Charlotte, and Lenox, MA



Chauncey Starr
EPRI Founder

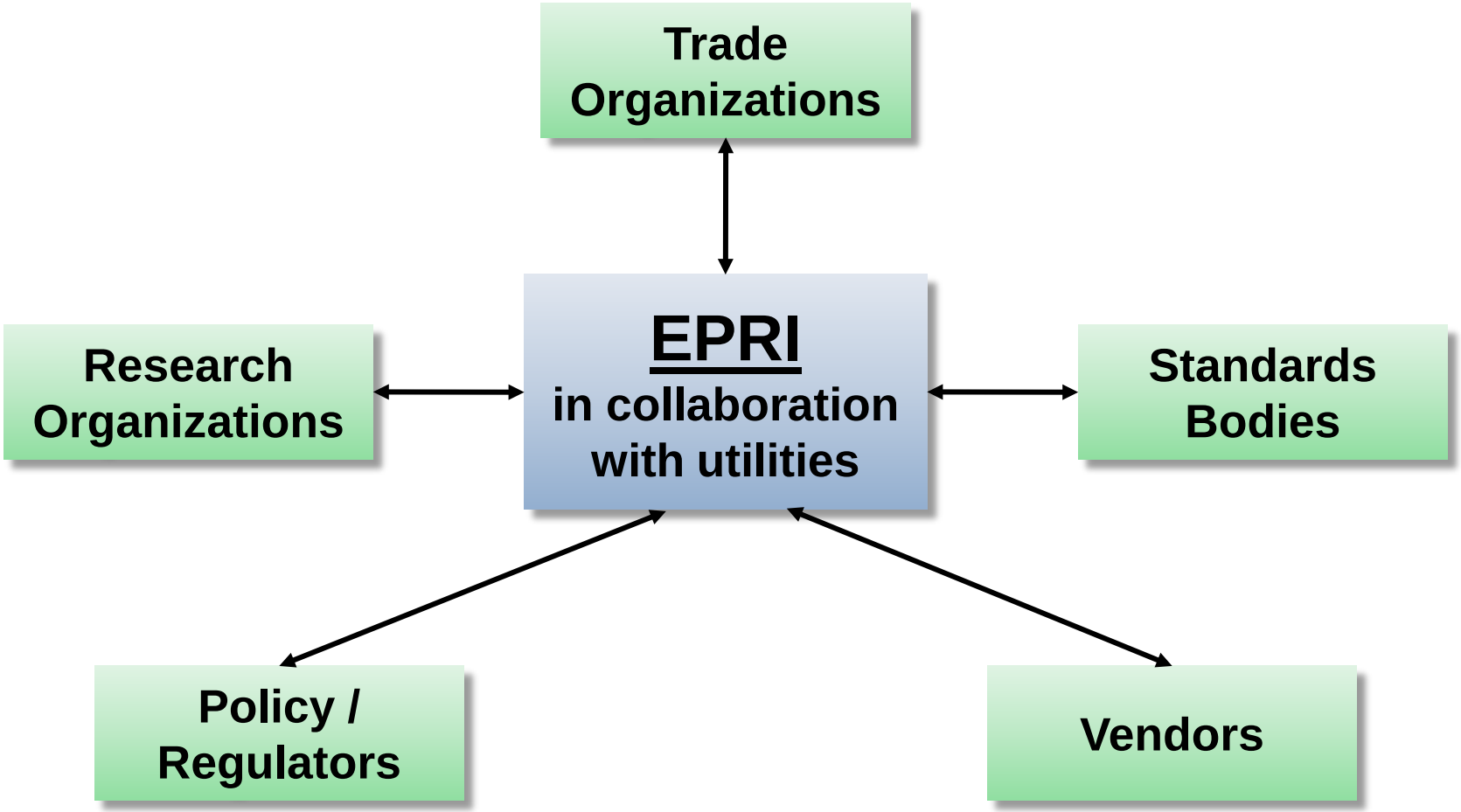
EPRI ELECTRIC POWER RESEARCH INSTITUTE

Our Members…

- 450+ participants in more than 30 countries
- EPRI members generate approximately 90% of the electricity in the United States
- International funding of nearly 25% of EPRI's research, development and demonstrations

EPRI ELECTRIC POWER RESEARCH INSTITUTE

EPRI Cyber Security Collaboration



Representing Utilities Through Coordination and Collaboration

ELECTRIC POWER RESEARCH INSTITUTE

EPRI Program 183: Cyber Security and Privacy Program Structure

Project Sets:

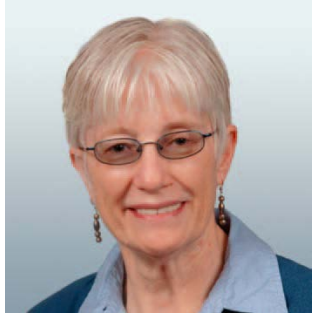
- P183A: Cyber Security and Privacy Technology Transfer and Industry Collaboration

- P183B: Security Technology for Transmission and Distribution Systems

- P183D: Cross-Domain Cyber Security Tools, Architectures, and Techniques

EPRI Cyber Security and Privacy Team

Galen Rasche
Technical Executive
P183 Program Lead
650-353-0336
grasche@epri.com



Annabelle Lee
Senior Technical Executive
202-293-6345
alee@epri.com

Eric Cardwell
Sr. Project Manager
865-218-8098
ecardwell@epri.com

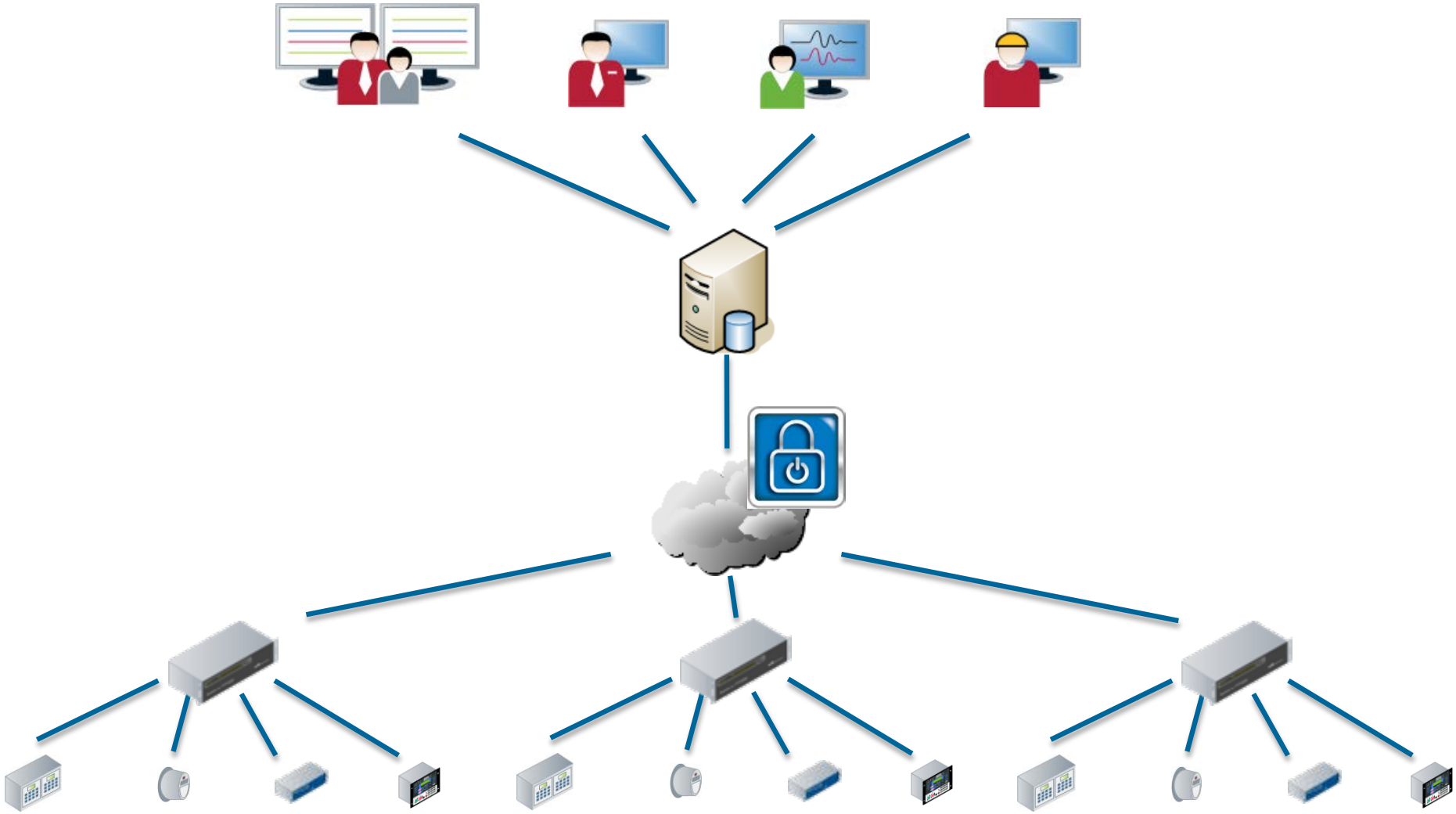
Glen Chason
Project Manager
865-218-8161
gchason@epri.com

John McGuire
Project Manager
865-218-8018
jmcguire@epri.com

Scott Sternfeld
Project Manager
843-619-0050
ssternfeld@epri.com

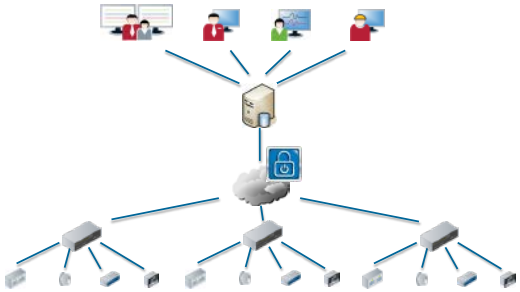
ELECTRIC POWER RESEARCH INSTITUTE

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



ELECTRIC POWER RESEARCH INSTITUTE

Remote Substation Access System



- *What is it?*
  - Provides for remote “engineering” (manual) access to all substation devices (IEDs) in a secure fashion.
  - Optional: Integrated with (automated) file extraction as part of an overall data integration solution.
  - Can be used as a replacement for a Windows Terminal Server (jump host).
  - Can be used as a tool to aid in NERC CIP compliance.
  - May also include:
    - Password management
    - Configuration (change) management for IEDs
    - Asset management

Remote Access Implementation – Poll!

Does your company allow remote access (dial-up or network) to remote devices?

- **No remote access allowed.**
- **Non-CIP sites only**
- **CIP sites only**
- **Both CIP and Non-CIP sites**

Remote Access Implementation – Poll!

If remote access is allowed, which methods are used to connect to remote devices?

- **Dial-up only**
- **Network only**
- **Dial-up and Network are both allowed**

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/development in Smart Grid Substation Lab
- Improved vendor products
- Vendor final demonstrations

Presenting utility requirements with a ‘unified voice’

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"

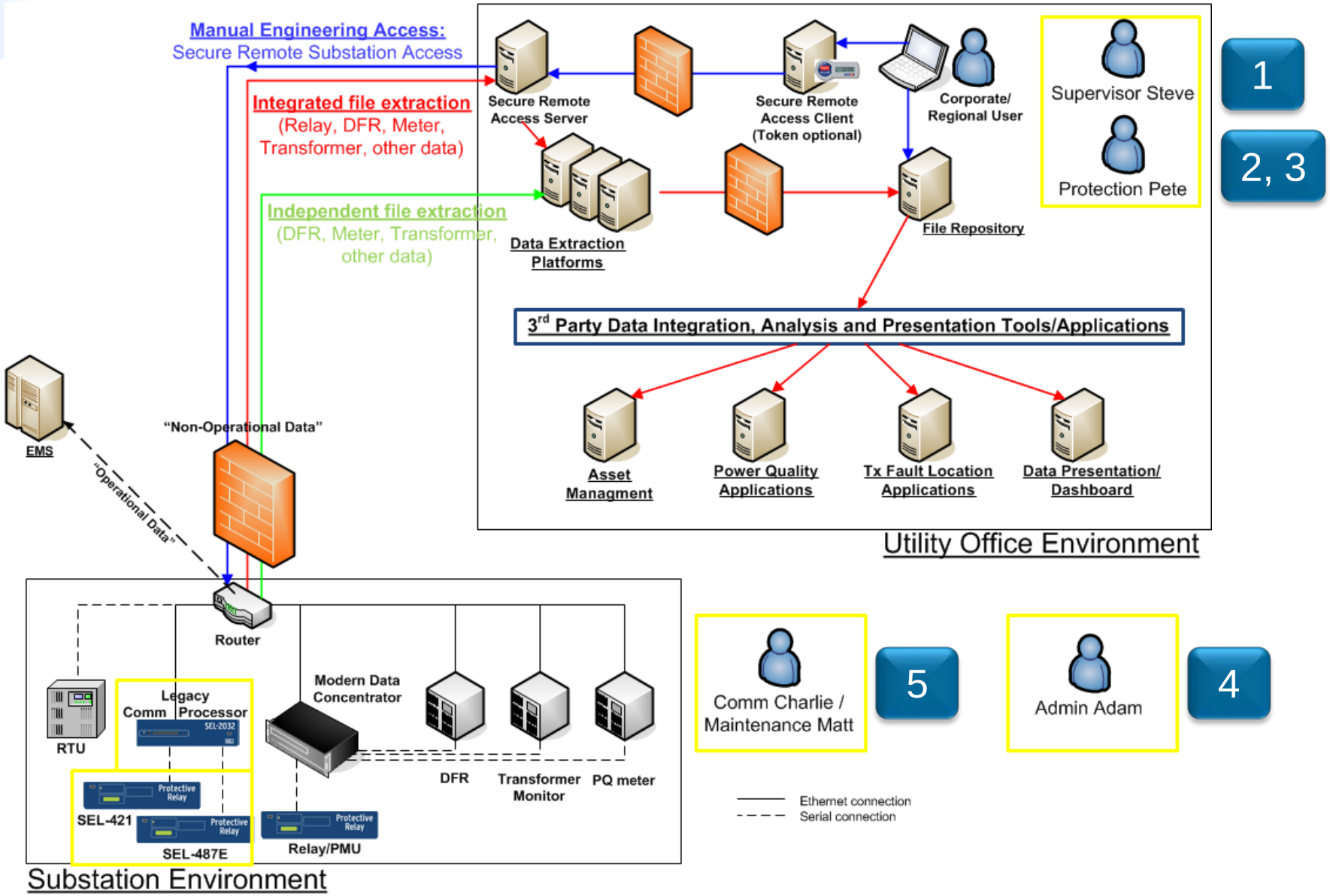
Utility Value:

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

Vendors and utility collaboration for accelerated technology transfer

ELECTRIC POWER RESEARCH INSTITUTE

Scenario Layout



ELECTRIC POWER RESEARCH INSTITUTE

Five Scenarios

Five vendor scenarios to be demonstrated:

- Scenario 1 – Serial connection to SEL relay with read/write access and A/D account – change a password
- Scenario 2 – Serial connection to SEL relay with read-only access and A/D account – with new relay password
- Scenario 3 – Unauthorized access – Valid A/D user with invalid password
- Scenario 4 – Auditing/Session Logs – user session analysis
- Scenario 5 – IED access from a substation – Network link to back-office is off-line

EPRI's Smart Grid Substation Lab
Knoxville, TN

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

Installation in a Common Demonstration Environment

EPRI 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

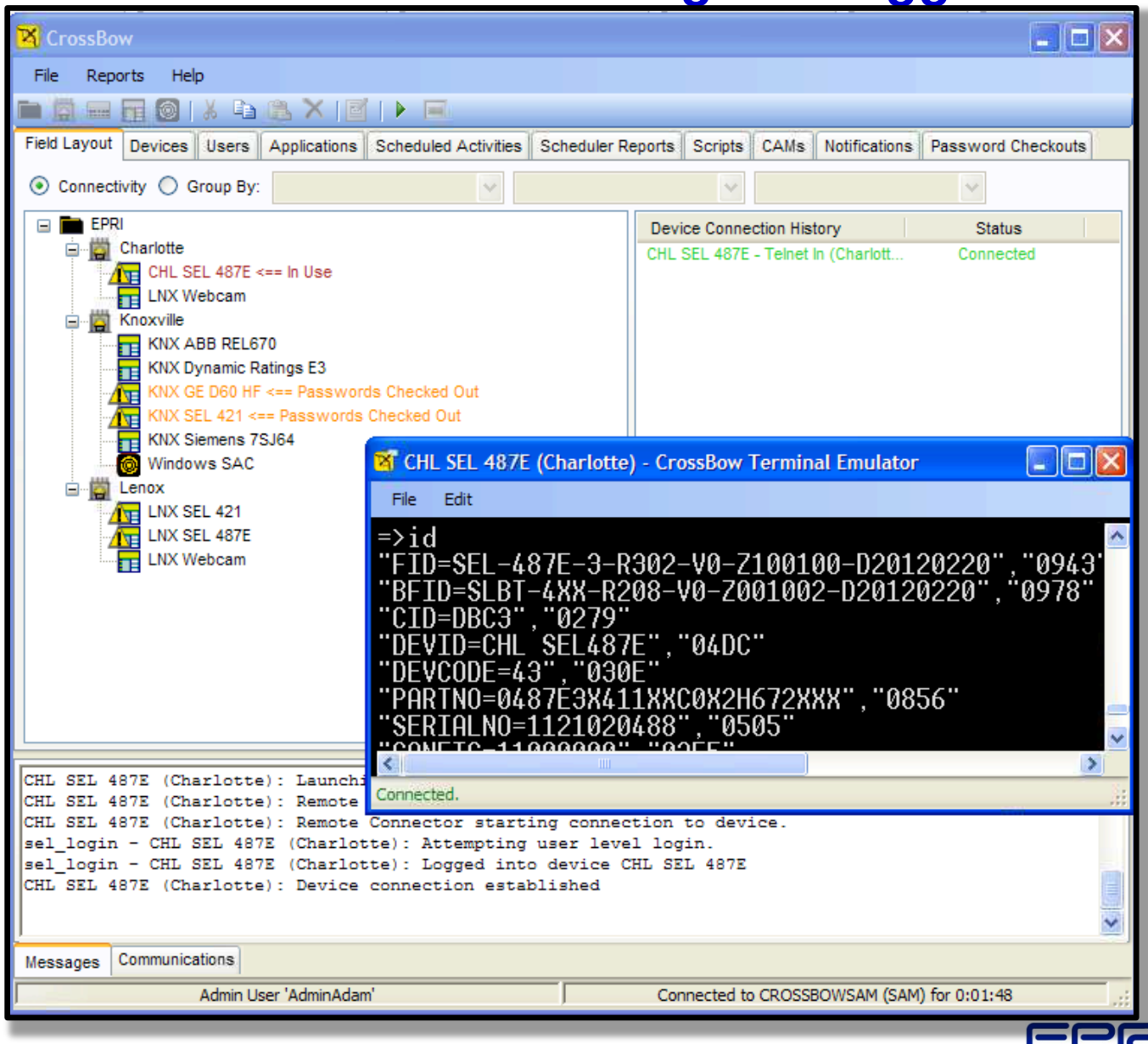
File Edit View Call Transfer Help

```
=>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

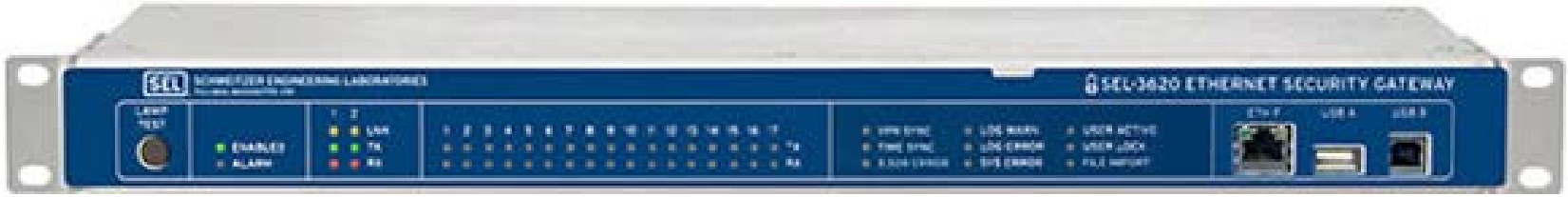
EPRI ELECTRIC POWER RESEARCH INSTITUTE

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 — Update, Delete
master port

Managed Devices: KNX-SEL-421 | Connected Via: COM01

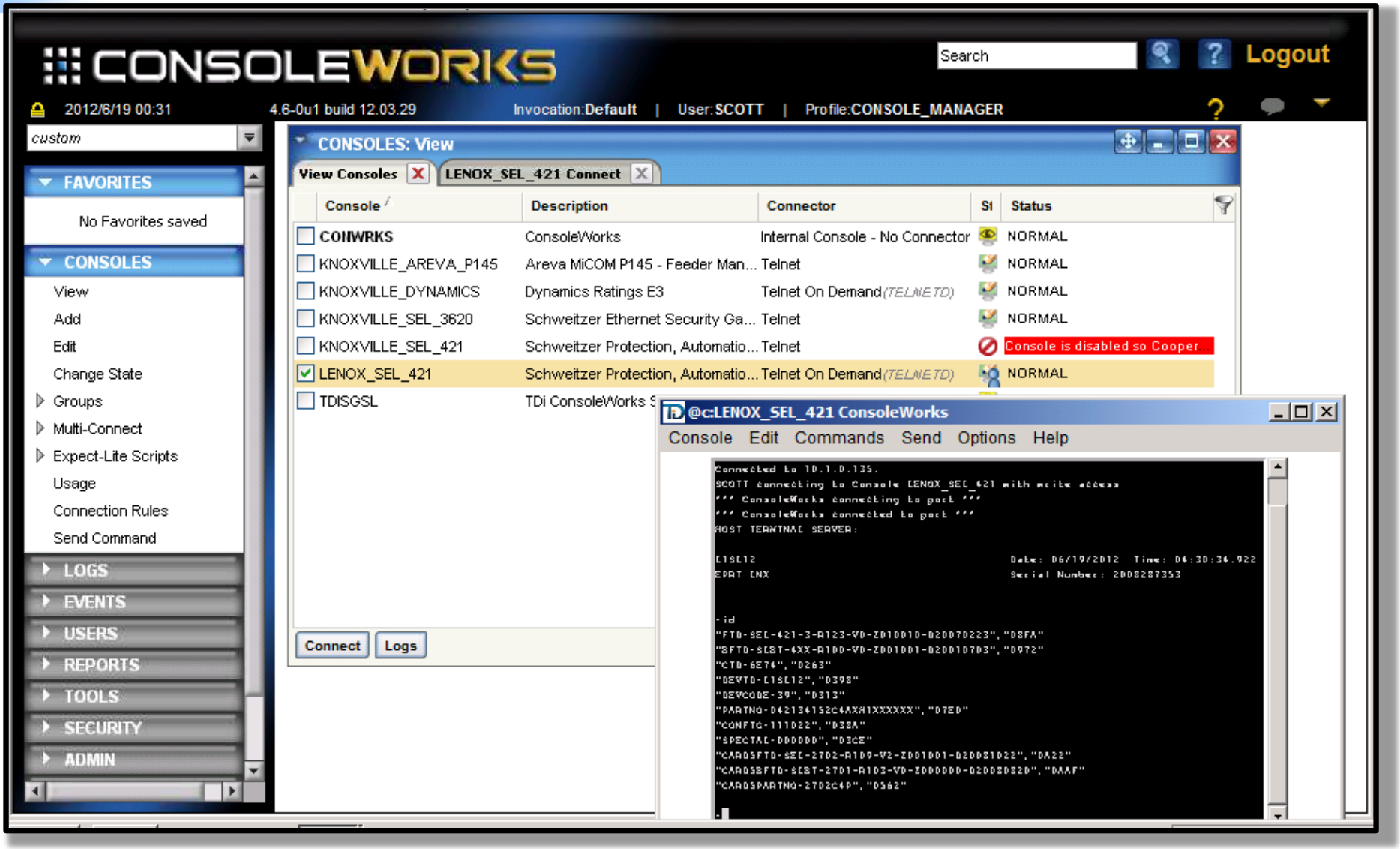
Telnet: Add Device, Rename, Disable, Delete

ALL:23 — Telnet — Update, Delete
Telnet

ALL — SSH — 192.168.1.2:22 — Update, Delete
Remote Telnet

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

Deployment Status - Poll

What is your company's status regarding deploying a remote IED access system?

1) **Already implementing**
2) **Considering/Evaluating/RFP/Pilot**
3) **No interest at this time**

Vendor Selection - Poll

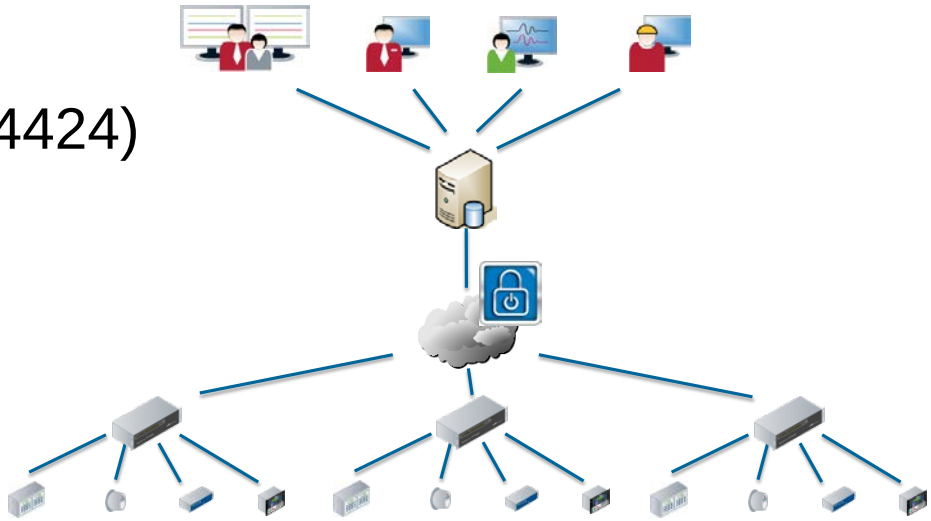
If deploying or evaluating, which vendor are you using?

1) **One of the 5 vendors deployed in EPRI lab**
2) **Other vendor**
3) **Internally developed solution**

Secure Remote Substation Access – Int. Group

Interest Group – open to all

- Follow-on to 2012 project (1024424) *"Substation Security and Remote Access Implementation Strategies"*



- Who?
- What?
- Why?

Kickoff Meeting: Wed, June 5th 2013 2:30-3:30pm EDT

Charter: Secure Remote Acc Int Group Cha

Identifying top Remote IED Access issues

ELECTRIC POWER RESEARCH INSTITUTE

What do you see as the biggest issue? What should this group address?

- **NERC CIPv5** – compliance to new or updated requirements (Serial vs Ethernet)

- Identification of **specific scenarios** or IEDs that do not easily integrate with RA solutions.
  - Protocol/Driver support: Universal IED tools/protocols vs. vendor proprietary tools/protocols
  - Impact of migration from command-line interfaces (CLI) on IEDs to web-based interfaces
  - Use of **multiple authentication devices**/gateways to proxy connections

- Remote Access System Management / **Links to other applications**
  - **Ownership** issue: Multiple user groups vs. single organizational "owner"
  - Security operations/compliance with Remote Access – integrating RA logs with EMS logs
  - Asset management and maintenance – integrating file retrieval to A.M. with RA systems

What do you see as the biggest issue? What should this group address? – (Continued)

- Access policy/methods from outside the substation vs. inside the substation (local)
- Coordination of access with operations for **safety** and situational awareness
- Management and tracking of IED **configurations**
- **Patch** management of IEDs
- IED **password management**

Interest Group Topics - Poll!

What are the top issues to address?

1. NERC CIP (v3/v5)
2. Challenging scenarios/ unique IEDs
3. Multiple authentication gateways
4. Links to other applications
5. Ownership issues
6. Safety related issues
7. Other

Schedule of next meetings – Remote Access (Tentative topics)

Discussion topics. 1 hr session each. 2-3pm EDT? Each session should review and add test scenarios if appropriate.

- **July 12th** – Unique IEDs / Development of test scenarios
- **August 8th** – NERC CIP changes, Password Management
- **Sept 4th** – Ownership / Multiple authentication gateways
- **October 3rd** – Links to other applications / Safety coordination
  - Vendor presentation/discussion?
- **October 31st** – TOPIC / DEMO
  - Vendor presentation/discussion?
- **November 21st** – TOPIC / DEMO
  - Vendor presentation/discussion?

IED Password Management
Through remote substation access systems

Approach:

- Identify the requirement, benefits and challenges associated with implementing IED password management

Value:

- Support CIP compliance and documentation for password change requirements
- Reduce risk of unauthorized access attempts by obscuring the password
  - No more default or ‘utility standard’ passwords
- Reduce the frequency of password updates
- Reduce inefficiencies and costs through automated password changes.

IED Password Management:

Report outline:

1. What is IED password management?
2. Requirements
3. Benefits
4. Risks
5. Central vs. Distributed architecture
6. IED p/w capabilities and limitations
7. Password complexity issues
8. Deep-dive scenario
9. Alternatives to passwords

Password Management – Poll!

When would you consider the use of randomized passwords for IEDs?

1) **Already implementing**
2) **6 mo-2 years**
3) **2-5 years**
4) **I would never consider it**

Discussion of topics

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

Deployment considerations

ELECTRIC POWER RESEARCH INSTITUTE

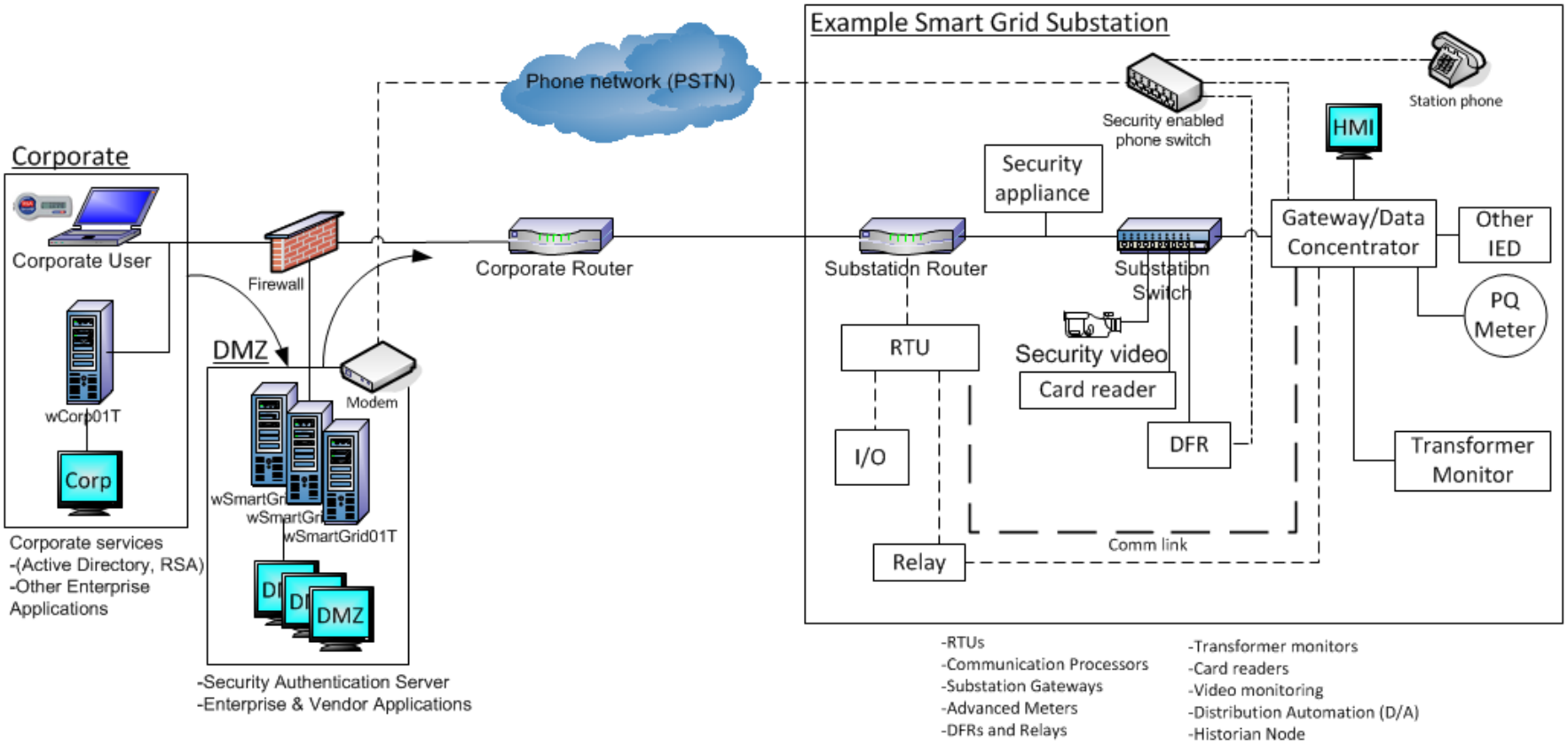
System Ownership

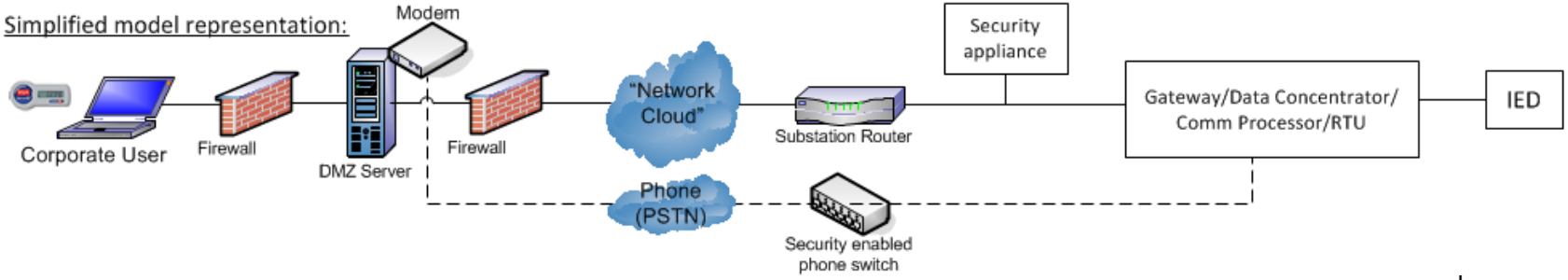
- Who will assume overall ownership of the system?
  - Single POC or group needed (champion)
  - Provides coordination between other users
- Many, many groups involved that can be considered "owners":
  - Group that specifies and procures equipment?
  - Group that provides initial configuration?
  - Group that maintains equipment in the field?
  - IT: System upgrades, patching, disaster recovery, deployment to users
- Other considerations to determine ownership:
  - Frequency of use: Who manages the configurations of the devices?
  - Volume: What is the quantity of IEDs to be managed?
  - Criticality: What is the criticality of these devices?
  - Availability: Is there 24/7 support from any of the organizations?

Architectures

ELECTRIC POWER RESEARCH INSTITUTE

Sample Network Environment

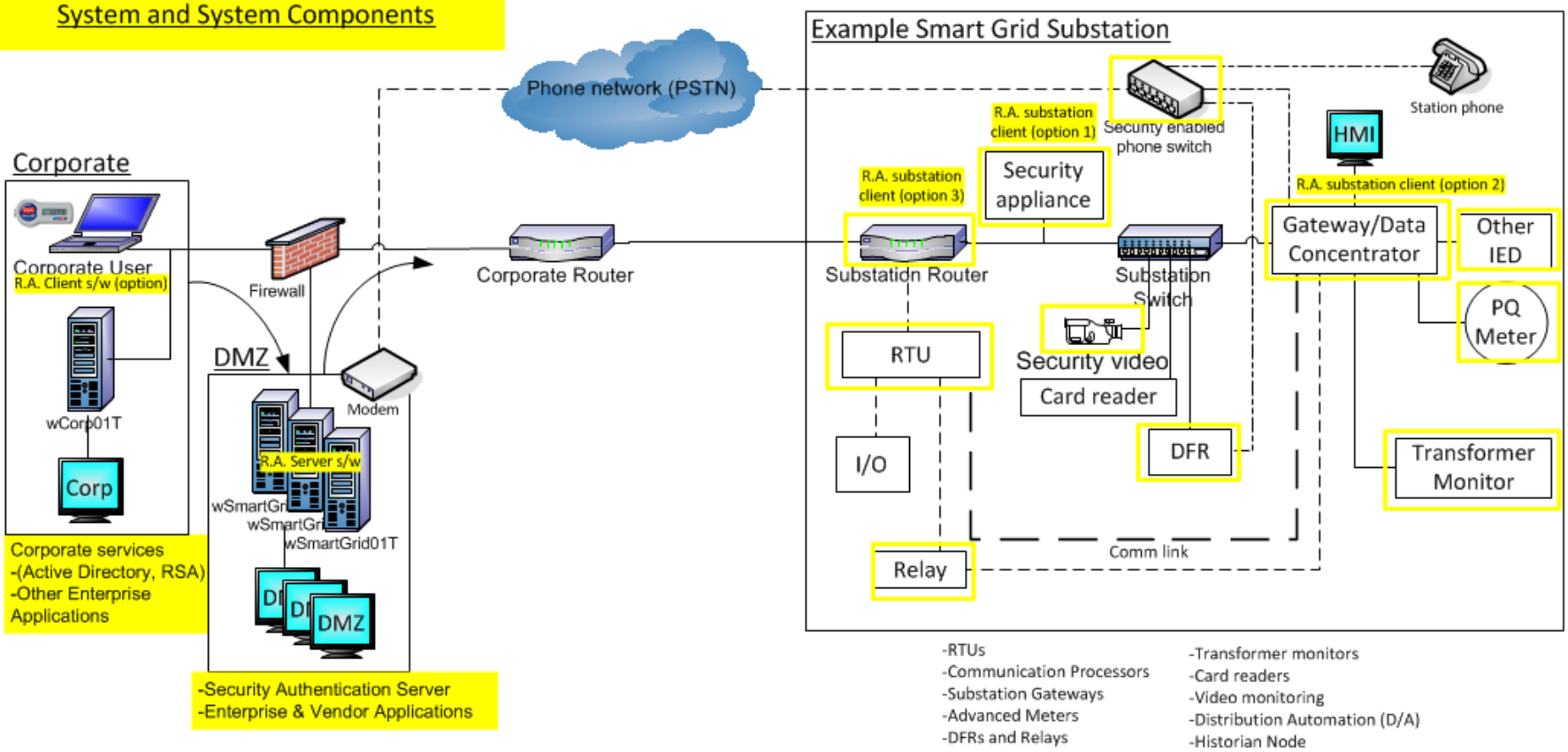


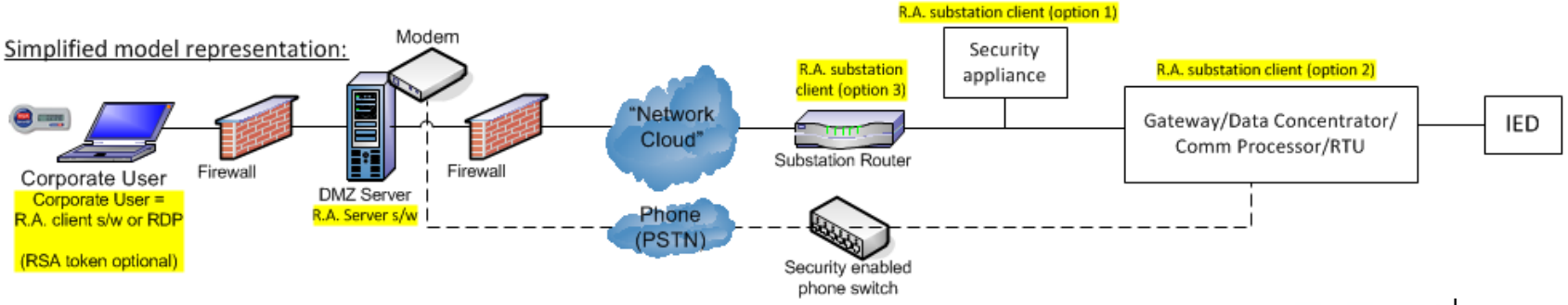


ELECTRIC POWER RESEARCH INSTITUTE

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

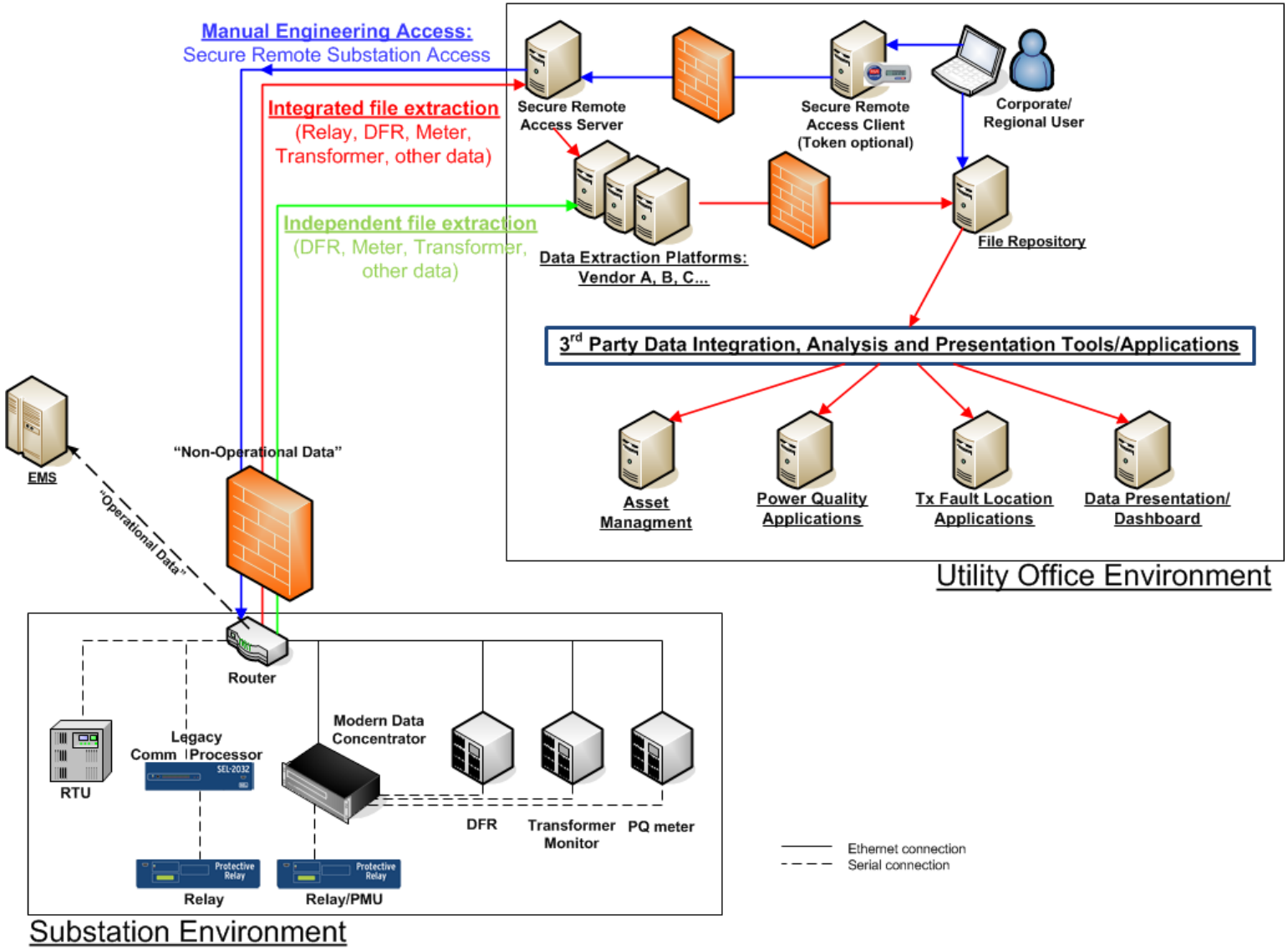
Sample Network Environment





EPRI ELECTRIC POWER RESEARCH INSTITUTE

Engineering Access and File Extraction



ELECTRIC POWER RESEARCH INSTITUTE

Active Directory Groups and Users

Remote-Admin	Security Group - Global
Remote-Comm	Security Group - Global
Remote-Maint	Security Group - Global
Remote-Meter	Security Group - Global
Remote-Protection	Security Group - Global
Remote-ProtectionSupervisor	Security Group - Global
Remote-RTU	Security Group - Global
Remote-Tech	Security Group - Global

AdminAdam	User
CommCharlie	User
MaintenanceMatt	User
ProtectionPete	User
RTURalph	User
SupervisorSteve	User
TechTom	User