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”
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
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 Cyber Security Collaboration

EPRI in collaboration with utilities

- Trade Organizations
- Research Organizations
- Policy / Regulators
- Standards Bodies
- Vendors

Representing Utilities Through Coordination and Collaboration
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
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 24-25\textsuperscript{th}, 2012 Knoxville, TN
  – Wide range of audience
    “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
Scenario Layout

Manual Engineering Access:
Secure Remote Substation Access

Integrated file extraction
(Relay, DFR, Meter, Transformer, other data)

Independent file extraction
(DFR, Meter, Transformer, other data)

Data Extraction Platforms

Secure Remote Access Server

Corporate/Regional User

Protection Pete

File Repository

3rd Party Data Integration, Analysis and Presentation Tools/Applications

Asset Management

Power Quality Applications

Tx Fault Location Applications

Data Presentation/Dashboard

Utility Office Environment

Substation Environment

Comm Charlie/Maintenance Matt

Admin Adam

SEL-421

SEL-487E

Legacy Comm Processor

Modern Data Concentrator

DFR

Transformer Monitor

PQ meter

Router

EMS

“Non-Operational Data”
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
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
EnterpriseSERVER.NET - Subnet Solutions
CrossBow Secure Access Manager - Ruggedcom
## IED Manager Suite - Cooper Power Systems

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

<table>
<thead>
<tr>
<th>IED Name</th>
<th>IED Type</th>
<th>Link Type</th>
<th>Conx Address</th>
<th>IED Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LD_HF_1_0_69</td>
<td>UR-D60</td>
<td>TCP/IP</td>
<td>&quot;UR69&quot;</td>
<td>Line Distance Relays (HF)</td>
</tr>
<tr>
<td>LD_Line_1_0_70</td>
<td>UR-D60</td>
<td>TCP/IP</td>
<td>&quot;GED60&quot;</td>
<td>Line Distance Relays (Line)</td>
</tr>
<tr>
<td>LD_Line_1_0_70/Web</td>
<td>Web</td>
<td>TCP/IP</td>
<td>&quot;GED60Web&quot;</td>
<td></td>
</tr>
<tr>
<td>UP_1_0_71</td>
<td>SEL-421</td>
<td>TCP/IP</td>
<td>&quot;SEL421&quot;</td>
<td>High-Speed Line Protection...</td>
</tr>
<tr>
<td>TR_1_0_72</td>
<td>SEL-487</td>
<td>TCP/IP</td>
<td>&quot;SEL72&quot;</td>
<td>Transformer Protection Relay</td>
</tr>
<tr>
<td>TR_1_0_74</td>
<td>UR-T60</td>
<td>TCP/IP</td>
<td>&quot;UR74&quot;</td>
<td>Transformer Protection System</td>
</tr>
</tbody>
</table>
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 Ch;

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

Sample Network Environment

Example Smart Grid Substation

Simplified model representation:
Engineering Access and File Extraction
Active Directory Groups and Users

<table>
<thead>
<tr>
<th>Group</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote-Admin</td>
<td>Security Group - Global</td>
</tr>
<tr>
<td>Remote-Comm</td>
<td>Security Group - Global</td>
</tr>
<tr>
<td>Remote-Maint</td>
<td>Security Group - Global</td>
</tr>
<tr>
<td>Remote-Meter</td>
<td>Security Group - Global</td>
</tr>
<tr>
<td>Remote-Protection</td>
<td>Security Group - Global</td>
</tr>
<tr>
<td>Remote-ProtectionSupervisor</td>
<td>Security Group - Global</td>
</tr>
<tr>
<td>Remote-RTU</td>
<td>Security Group - Global</td>
</tr>
<tr>
<td>Remote-Tech</td>
<td>Security Group - Global</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminAdam</td>
<td>User</td>
</tr>
<tr>
<td>CommCharlie</td>
<td>User</td>
</tr>
<tr>
<td>MaintenanceMatt</td>
<td>User</td>
</tr>
<tr>
<td>ProtectionPete</td>
<td>User</td>
</tr>
<tr>
<td>RTURalph</td>
<td>User</td>
</tr>
<tr>
<td>SupervisorSteve</td>
<td>User</td>
</tr>
<tr>
<td>TechTom</td>
<td>User</td>
</tr>
</tbody>
</table>