Securing the Electric Grid with Common Cyber Security Services

Jeff Gooding

TCIPG Seminar
April 4, 2014
Southern California Edison (SCE) is committed to safely providing reliable and affordable electricity to its customers.

On an average day SCE provides power to:

- Nearly 14 million people
- 180 cities in 50,000 square miles of service area, encompassing 11 counties in central, coastal and Southern California
- Commercial industrial and nonprofit customers, including:
  - 5,000 large businesses
  - 280,000 small businesses
The electric utility system is facing fundamental changes

**CURRENT**
- Grid stability thru rotational inertia
- Dispatchable generation
- Passive/predictable loads
- Human-in-the-loop grid management
- Rigid and centralized system control

**EMERGING**
- Reduced stability due to generation mix change
- Stochastic generation
- Transactive loads
- Faster system dynamics by orders of magnitude
- Flexible and resilient distributed systems

**Drivers**
- Policies
- Technologies
- Customers
- Competition

**CURRENT** vs. **EMERGING**
- Rigid and centralized system control
- Faster system dynamics by orders of magnitude
- Flexible and resilient distributed systems
System stability through technology

Basic capability
Mechanical controls
Stability through physics

Advanced capabilities
Fly by wire
Stability through technology
Smart grid design goals

• **More** – increased capabilities
  – More capabilities at the edge and enterprise, pervasive automation

• **Better** – faster, more reliable & secure
  – The electric grid is more resilient
  – Dynamic control of all security elements allows the system to adapt to evolving threats

• **Easier** – usability (convergence, unified control, visualization, information on demand)
  – Tens of Millions of nodes are manageable
  – Situational awareness
  – Common Services allow for easier integration of new capabilities and technologies
Smart Grid System of Systems (SoS) Research

Four evolutions of Smart Grid SoS Architectures

1. Current-state
2. Typical SI Approach
3. DoD-style approach
4. Standards –based Internet-style
A holistic strategy is needed to serve customers better

- Inform policy
- Manage operational costs
- Serve customers through improved operations and services
- Mitigate reliability impact of variable energy resources
- Mitigate risk of technology obsolescence and stranded assets
- Secure our system from cybersecurity threats
- Integrate and adapt to disruptive technologies
SCE developed a structured approach for modernization strategies and technologies.
There are already a number of smart grid projects in flight to meet policy and changing customer needs.
SCE evaluates the safety and operability of new technologies in a controlled environment first

Integrated platform for evaluating the safety and operability of smart grid technologies in a controlled environment before being deployed on the grid.
Goals of Information Security

**Goals:**

- Make data visible
- Make data accessible
- Enable data to be understandable
- Enable data to be trusted
- Enable data interoperability

**Actions:**

- Secure data assets to ensure reliable operations through:
  - Authentication
  - Authorization
  - Accounting
  - Peer to Peer
  - Quality-of-Trust
  - Dynamic security posture awareness
- Make system data and processes available to the Enterprise by protecting:
  - Availability
  - Integrity
  - Confidentiality

To make the right decisions at the right time

Courtesy DOD office of CIO
High Assurance Capability

Using DoD cybersecurity methods to enhance system resiliency

Networked Battlefield

Networked Utility Operations

CIP owners/operators facing transition that DoD started 10+ years ago
Common Cyber Security Services (CCS)

• An advanced security system for the energy sector
  – Next generation utility technologies
  – DoD technology transfer
  – Best practices from many sectors
  – Modern SOA style architecture

• A standards compliant security system
  – NERC CIP Version X
  – All Federal Processing Standards (DHS, FIPS)
  – NIST Compliant (NISTIR, SP)

• An extremely scalable and dynamic security system
  – Supports Grid Applications (control & monitoring)
  – Supports current and next generation networking (MPLS)
  – Supports major protocols used on the Grid (61850-90-5, DNP3, etc)

• “Build-to” specifications supports multi-vendor adoption
## Cybersecurity System Capabilities

<table>
<thead>
<tr>
<th><strong>Authentication</strong></th>
<th>• Integrated Operational Public Key Infrastructure (PKI), Identity Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authorization</strong></td>
<td>• Role and Group Based Access Control (RBAC)</td>
</tr>
<tr>
<td><strong>Accounting</strong></td>
<td>• Security Information and Event Management (SIEM)</td>
</tr>
</tbody>
</table>
| **Peer to Peer**   | • Authenticated communication  
                      • Defense in Depth                                                             |
| **Quality-of-Trust** | • Continuous device to device trust monitoring  
                         • Cyber & Physical alerts, device health, operator actions                   |
| **Integrity**      | • Trusted Boot, Trusted Network Connect  
                      • Device Bill-of-Health                                                         |
| **Dynamic Scalable GUI** | • Central operations security visualization GUI accessed via web browser  
                             • Multi-Tier Security Operations Capability  
                             • Large scale System Planning and Test Capabilities |

© 2013 Southern California Edison  
© 2013 ViaSat, Inc.
CCS Enabled ESP

- Separation based on Application (e.g., EMS, DMS, CRAS) not physical network
- Access Controls at entry points into application (discrete ESP)
- Client Access is simplified (Single IPSEC Operational Tunnel)
- User Access Control should be in Protected Security Space
- Entry points into network only at Application Access Points
COI (Key Group Management)
Common Cybersecurity Service Concept

Security Policy Enforcement & Status based on device and function

Status:
- Trusted
- Questionable
- Untrusted
- Unknown
Real-time Operational Grid Security Posture
Common Cyber Security Services (CCS)

- CCS operational in production environment since mid-2013.
- Various federal and state agencies are supportive of CCS and are open to supporting a variety of industry adoption acceleration approaches.
- Key vendors such as GE and others have developed and delivered CCS enabled clients.
- SCE has installed CCS in the McArthur substation and is working to scale up to BES subs over the next several years.
- CCS Specifications are available under NDA upon request.
Questions?

Jeff Gooding  
Southern California Edison  
jeff.gooding@sce.com  
+1-714-895-0254