Securing the Grid and Your Critical Utility Functions

April 24, 2017
Securing the Grid Effectively and Efficiently

• Recent threats to the Electric Grid and the importance of security
• Standards and Requirements set by the North American Electric Reliability Corporation (NERC)
• Leveraging resources of both Operations Technology (OT) and Information Technology (IT)
Introduction to Paper and Authors

• “Securing the Grid and Your Critical Utility Functions”
• Primary Author and Presenter:
  – William M. Bateman
    • Senior Project Manager, GDS Associates, Inc.
      – Manager of the NERC CIP Team
    • 19 years in the Electric Utility Industry
    • Experience in NERC Operations & Planning, NERC CIP Compliance, Transmission and Balancing Authority Operations
    • Serves as the NERC Compliance Manager and Senior CIP Manager for G&T Cooperative

• Additional Authors:
  – Alexander Amaya
    • CIP Project Engineer, GDS Associates, Inc.
    • Experience with Physical Security at a major BA/TOP in the western United States
    • Expertise in Transmission Planning and Protection Systems
  – James Fenstermaker
    • CIP Analyst, GDS Associates, Inc.
    • Expertise in electronic security and cyber vulnerability assessments
Importance of Security

Recent NERC Alerts
- Substation Sabotage
- Ukraine Cyber Attack
- Internet of Things (IoT) Distributed Denial of Service (DDoS) Attack

Recent Cyber Attacks outside of NERC
- Cyber Security Attack on Dallas Emergency Alert System
- Ransomware Attacks
- Yahoo Data Breach
NERC Requirements

Critical Infrastructure Protection (CIP) Standards

• Applicability
  – Bulk Electric System (BES)
  – Specific to Operations Technology (OT)

• Impact Levels
  – High
  – Medium
  – Low – Most smaller entities fall here

• Requirements based on Impact Level
Low Impact Requirements

Entities must create a Cyber Security Plan that addresses the following:

- Cyber Security Awareness
- Physical Security Controls
- Electronic Access Controls
- Cyber Security Incident Response
IT and OT Working Together

Evolution of OT

• Paradigm Shift from traditional OT systems
• Increased use of IT equipment on the operations side

Changes

• Facilitate the sharing of resources
• Encounter similar problems
• Benefits of integration
• NERC Standards can be used as guidelines for Information Technology (IT) Security
Components of Cyber Security protection

1. Human Resources and Human Factors
   – Training
   – Resource Use

2. Technical and Electronic Security
   – Firewalls
   – Intrusion Detection

3. Physical Security
   – Control Rooms
   – Data Centers
   – In the field
IT/OT Teams and Human Factors

Reasons for Unification of Teams
• Similar Training is needed for bot Teams
• Cost savings associated with employing full time staff
• Overlapping knowledge and skills
• Overlapping of job functions
• Operate as a single unit

Possible Hurdles
• Need for additional training
• May require restructuring different teams
• Need to promote the idea of teamwork
Sample Traditional IT/OT Organization
Traditional Labor Allocation and Cost

Separate Team 24/7 Coverage

- 2- Manager
  - $300,000
- 4- Supervisors
  - $500,000
- 8 Techs
  - $800,000

Total Staff and Costs:

- 14 Total Employees
  - 2 completely separate teams
  - 8 Techs would be a minimum level for 24/7 coverage for 2 Teams

- Total Labor Cost:
  - $1.6 Million

Estimate based on IEEE-USA Salary & Benefits Survey 2016 Edition
Unified Labor Allocation and Cost

IT/OT Team with 24/7 Coverage

• 1- Manager
  – $150,000

• 2- Supervisors
  – $250,000

• 5 Joint Use Techs
  – $500,000

Total Staff and Costs:

• 8 Total Employees
  – Combined Teams
  – 5 Techs can overlap doing IT and OT support

• Total Labor Cost:
  – $900,000
  – Savings of $700,000 with the additional support Tech

Estimate based on IEEE-USA Salary & Benefits Survey 2016 Edition
Technical and Electronic Security

OT and IT Convergence

• Evolution of OT Infrastructure
  – Electromechanical to microprocessor (OT)
  – Serial to IP

• Availability vs Security
  – OT systems uptime requirements

• Integrated Systems
  – IT issues on the operations side
  – Commonalities in equipment
Technical and Electronic Security

Security Vulnerabilities in OT Networks without Cyber Security Protection

- Publicly accessibility
- Insecure remote connectivity
- Missing security updates
- Poor password practices
- Insecure firewall configuration and management
- OT systems on IT networks

- Weak protection of the corporate IT network from OT systems
- Lack of network segmentation
- Unrestricted outbound internet access from OT networks
- Insecure encryption and authentication on wireless networks
Physical Security

Securing IT systems similar to OT

• NERC standards have requirements in place to protect OT assets, but not the IT system.

• If entity has an interconnected IT and OT network, they run the risk of having an IT cyber attack migrate to the OT system.

• A physical hack can occur if an individual decides to clone an ID card from the IT network, to gain access to the OT system.

• Security experts suggest entities to protect their IT systems with the same rigor as their OT systems.
Physical Security

Defense in Depth Strategy

• The more layer of security a utility has, the harder it is to penetrate the system.

• Example:
  • One of the most common ways is to separate locked critical assets, both IT and OT, within a separately locked room or cabinet.
Case Studies

Utility A

- Generation and Transmission cooperative
  - Serving 10 distribution members with over 300,000 customers
  - Multiple BES Generation facilities
  - Multiple 138 kV Transmission Facilities
  - Data Center with both IT and OT systems

- Low Impact rating
Case Studies

Utility A

• Human Factors
  – Multiple Members with combined IT/OT Teams or contractors

• Physical Security
  – Locking OT assets behind a key-locked gate at Transmission Facilities
  – Locking IT and OT assets behind a keypad door at Data Center
  – Escorting Visitors at all times

• Electronic Security
  – Separate IT and OT networks
  – Firewalls to control communication to Data Center
  – Switches at Substations
Case Studies

Utility B

• Transmission and Distribution cooperative
  – Serving over 70,000 customers
  – Multiple 138 and 69 kV Transmission Facilities
  – Primary/Backup Control and Data Centers, hosting both IT and OT systems

• Low Impact rating
Case Studies

Utility B

- **Human Factors**
  - Single IT/OT Team made up of in-house staff
  - Field personnel work with the IT/OT Team

- **Physical Security**
  - Locking IT and OT assets behind Card Access entry points
  - Individuals are given Card Access after passing applicable training classes
  - Up-to-date master access list
  - Separate IT and OT cabinets with unique keys at Substations

- **Electronic Security**
  - Firewalls to control communication to Data Center
  - Strong password policy
  - Secured Remote Access
  - Ability to monitor network through IDS/IPS modules, installed on firewalls
Case Studies

Utility C

• Generation and Distribution cooperative
  – Serving over 280,000 customers
  – Multiple Generation Facilities in two different grids
  – Primary/Backup Data Colocation Centers, hosting both IT and OT systems

• Medium Impact rating
Case Studies

Utility C

• Human Factors
  – Single IT/OT Team
  – Team manages all updates at the Collocation Centers
  – Field staff coordinates with the IT/OT Team

• Physical Security
  – IT and OT assets at Colocation Center with multi-level access
  – Individuals are given Card Access after passing applicable training classes
  – Up-to-date master access list

• Electronic Security
  – Firewalls to control communication into and out of the IT and OT Networks
  – IT and OT Networks are separate
  – Strong password policy
  – Secured Remote Access
  – Ability to monitor network through IDS/IPS
## Conclusions

<table>
<thead>
<tr>
<th>IT Systems vs OT Systems</th>
<th>Combined Resources increase efficiency</th>
<th>NERC Standards can be used as a starting point for IT Security</th>
<th>Similar IT and OT Systems</th>
</tr>
</thead>
</table>
| • Differences are becoming less clear  
• Both are Critical to Utility functions | • Less labor cost  
• Additional IT and OT support coverage | • Required for OT Systems  
• Good practice for IT Systems | • Increases security  
• More efficient |
Thank you for the opportunity to present at the 2017 IEEE REPC