Cyber Security and Substation Equipment Overview

Northeast Power Coordinating Council
Task Force on Infrastructure Security & Technology’s
Cyber Security Workshop
June 7 & 8, 2006

John Ciufo
Alfred Moniz
Agenda

• John
  • Cyber
  • Typical Assets
  • Cyber Security Assets
  • A Suggested To Do List
• AI
  • Typical Configurations & Security Perimeter

• All Q&A
Cyber

The new CIP standards include a larger scope of Cyber Assets - Substation Devices:

- Process Control Systems
- Distributed Control Systems
- Electronic protection Systems
- In a nutshell, Substation IEDs

What is Cyber

- Cyber infers communications, computers, internet, and information
- At the heart of cyber vulnerability of substations is the ability to remotely access IEDs
- Remote access is achieved through a communication link to the substation, from anywhere in the world.
- Once access is established, one can remotely control, manipulate, or initiate process actions similar to a local user.
Cyber

Cyber Asset and Power System Reliability
- CIP standards, like other NERC standards, exists to ensure reliable electrical power
- CIP standards apply to Critical Cyber Assets that if remote access is achieved, the cyber asset(s) can be manipulated to cause a BPS event.

Security Risks For Power Systems Utilities
- Risks associated with utilities relate to the use of information to control and or inhibit physical power system devices.
- Impacts of security breaches can have safety, power outages and equipment or system damage.
Some Potential breaches:

- **Protection Systems**
  - Denial of Fault Clearance
  - Non-protection operation of CBs and switchgear
  - Automatic Tripping of many CBs

- **Control**
  - Power system elements are operated
  - Voltage excursions beyond limits
  - False Alarms
  - Operators denied access

- **Monitoring Equipment**
  - False triggering and Analysis
Critical Cyber Assets

What Cyber Assets are Critical

- CIP Standards are flexible.
- We recommend that within NPCC, we interpret them the same.
- Some recommended principles that we should follow to determine Critical Cyber Assets:
  - The cyber asset has been engineered with remote access.
  - The cyber asset permits manipulating power system elements that would have disastrous consequences on the safety, and reliability of the power system if intruders were to gain access electronically.
  - Electronic intrusion could have an affect on the power system outside of the power system Area.
  - Electronic intrusion could prevent visibility and or lead to malicious actions that could effect a majority of the power system area.
Critical Cyber Assets

Cyber Assets

- Cyber Assets Employed at NPCC Defined Elements
  - The following family of cyber equipment can lead to the operation of BPS elements, or denial of clearance of system faults:
    - Protection measuring relays
    - Programmable Logic Controls
    - Teleprotection Equipment
    - RTUs
    - Control / protection Gateways

- SCADA/EMS Systems
  - Electronic intrusion could have disastrous consequences.

- Minimum Power System Restoration
  - NPCC Elements only – for discussion?
Critical Cyber Assets

A Suggested To Do List For Security Compliance

- Determine your critical Assets
- Determine your cyber assets used for these critical assets
- Determine which of these cyber assets are critical
- Define a electronic perimeter (s)
- Determine the access point (s) into the electronic perimeter
- Dial-In and/ or routable protocols?
- Plan to install appropriate Gateways / Telephone Switching devices, or the like, which provide authentication, supports user accounts, logging, etc.
- Documentation and more discipline approach.
- Ports and services reviews should apply only to the access points /device
High Level Overview

- Intelligent Electronic Devices
  - SCADA Communication
  - Engineering Communication
High Level Overview

- SCADA Communication
  - Real time status information
  - Current conditions that the relay is indicating and notification of
  - Alarm conditions
  - Control Commands
  - Can be two way
High Level Overview

- **Engineering Communication**
  - Settings
  - Profiles
  - Testing
  - How do you want the device to respond to conditions.
  - Enable/ disable ports.
  - Most devices will support only one engineering connection.
  - Can be 2 way.
Electronic Security Perimeter

- The logical border where access is controlled.
- Communications network not included in the Perimeter.
- Non-critical assets inside the perimeter shall be included.
Typical configuration
Electronic Security Perimeter

- Communication Processor w/Separate path engineering.
  - IED information focal point.
  - Must connect to the CP to communicate to IED

- Is it a Critical Cyber Asset
  1. Is it essential to the operation of the CRITICAL ASSET?
Typical configuration
Electronic Security Perimeter

- Communication Processor Network addressable IEDs.
  - Routable Protocol capable IED

- IED Network Device
  - Does it use routable protocol outside ESP.
Electronic Access Controls

- Deny access by default
- Enable only ports and services required for operations and monitoring.
- Secure dial up access to ESP.
  - Username/Password
  - Dial Back
  - SCADA enabled
- Interactive access
  - Strong Procedural or technical controls
- Banner
Electronic Security Perimeter

Substation A

Sub Station B

Non-Critical Asset

Critical Assets

Local Control / PC

Integrated Access Control

IED 1

IED 2

IED 3

IED 4

IED ...

IED N

Communications Network

Firewall

SCADA/EMS
Monitoring Electronic Access

- **Log access (Document monitoring)**
- **Detect & Alert attempts.**
Conclusion

- Understand the CIP.
  - Training, meetings, group effort.
- Know your Substation configurations
  - Document
  - How are the devices used
    - The same device used differently
- What are the configurations of the communication
  - RING
  - STAR
- Review capability of devices.
  - Password protection
  - Access logging capability
  - Engineering connections tunnel through to other devices?
  - Lock out conditions, i.e. 3 incorrect passwords.
  - Alarms when connection established