

# **How Utilities are Handling (interpreting) NERC CIP Guidelines**

**Robert O' Reilly**  
**Senior Application Engineer**  
**Cooper Power Systems / Energy Automation Solutions**  
**Presented at South Dakota State University, Center for**  
**Power System Studies, October 2008**



**COOPER** Power Systems

# Presentation Overview

---

- > A review of the NERC – CIP requirements
- > Security in general
- > FERC - NERC
- > Utility # 1 and its interpretations
- > Utility # 2 with its approach
- > Conclusions

# Overview of key points in the NERC – CIP guidelines

# Relevance of NERC CIP for Substation Integration (SI)

---

- > Minor CIP002 (Asset identification)
- > Minor CIP003 (Security mgmt controls)
- > Moderate CIP004 (Personnel & training)
- > Major CIP005 (Electronic Security Perimeters)
- > Minor CIP006 (Physical Security Perimeters)
- > Major CIP007 (System Security Mgmt)
- > Minor CIP008 (Incident Reporting & Mgmt)
- > Major CIP009 (Recovery Plans & Procedures)

# NERC CIP-002-1

## Critical Cyber Asset Identification

---

...

For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

**R3.1.** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

**R3.2.** The Cyber Asset uses a routable protocol within a Control Center; or,

**R3.3.** The Cyber Asset is dial-up accessible.

# NERC CIP-005-1

## Electronic Security Perimeter(s)

---

...

**R1.** Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter...

**R2.** Electronic Access Controls — ... implement and document the organizational processes and technical and procedural mechanisms for control of electronic access ...

**R3.** Monitoring Electronic Access — ... implement and document an electronic or manual process(es) for monitoring and logging access at access points ...

# NERC CIP-007-1

## Systems Security Management

---

...

**R4. Malicious Software Prevention** — ... shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware...

# NERC CIP-007-1

## Systems Security Management

---

...

**R5.** Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

**R6.** Security Status Monitoring — ... shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

# Differences between IT and SI systems

---

- > Performance requirements(real-time, jitter, throughput,...)
- > Availability requirements (reboots, planned outage, testing,...)
- > Risk management (Safety, fault tolerance, impact,...)
- > Security focus (IT assets vs. utility assets).
- > Unintended consequences
- > Time-Critical Interaction
- > System Operation (IT systems vs DCS or SCADA systems)
- > Resource constraints
- > Communication protocols and media
- > Change impacts and management
- > Component lifetime
- > Physical component access

# Targeted Assets

---

- > Control centers performing functions of target entities
- > Backup control centers
- > Transmission/Distribution substations
- > Generation resources/stations
- > System facilities that are critical to system restoration
- > System facilities that are critical to automatic load shedding
- > Special protection systems
- > Automation controllers
- > Real-time inter-utility data exchange systems
- > Etc...

# Current IED deployment

---

- IEDs protect, control and report on critical resources (assets).
- IEDs can be critical substation cyber assets
- Current security relies on isolation:
  - > IEDs are installed for primary purpose (protection)
  - > Access is restricted to protection personnel
  - > All accesses must be local
  - > IEDs have simple passwords
  - > No permanent & no external connections are used

# IED Limitations

---

In general, IED's have most of the time some basic limitations, such as:

- > Stringent Real-Time Requirement
- > Insecure Communication Media
- > Open protocols
- > No (or little) Authentication/Authorization

# FERC - NERC

---

FERC indicated that NERC guidelines left to much room for interpretation.

**The overall security will only be as strong as the weakest link in the chain!**

Interpreted the guidelines in a very stringent fashion.

- Physical security at substations
- Continuous video surveillance
- Installed gateway at substation to isolate external communications from the communications within the substation which provided the following benefits:
  - Secured communication access
  - Encryption to and from higher level systems
  - Secured remote access to IED's from a central location using encryption

# Utility # 1 (cont'd)

---

- All IED's are provided basic protection by the use of the gateway
- All IED's capable of having password protection have it enabled (no default passwords used)
- All passwords are different (implementing special software to track all passwords for all IED's), this is a major effort

Interpreted the guidelines in a very different fashion in regards to the electronic perimeter:

- ❖ Implemented physical security
- ❖ Installed gateway at substation to isolate external communications from the communications within the substation, providing the following benefits:
  - ❖ Secured communication access
  - ❖ Encryption to and from higher level systems
  - ❖ Secured remote access to IED's using encryption

## Utility # 2 (cont'd)

---

- ❖ All IED's are provided basic protection by the use of the gateway
- ❖ Kept all default passwords or no passwords at all
- ❖ For this utility – if somebody got into the substation they can do ??????

# Conclusions

---

Security is a necessary and inconvenient evil

The interpretation can be very different between utilities

NERC CIP compliancy is not a simple matter

NERC CIP compliancy does not guarantee security

There is much more than just technology!

# Conclusion (Cont'd)

---

Success depends mostly on :

- > Sound technical choices
- > Global solutions
- > Homogeneous solutions
- > Simple solutions

Once more, success depends on VISION

**Make each small step count!**

**Thank you for your attention!**