# Challenges of Implementing Substation Hardware Upgrades for NERC CIP Version 5 Compliance to Enhance Cybersecurity

J. Matt Cole, PE
Power Delivery Services
Sargent & Lundy LLC
Chicago, IL, USA
Joesph.m.cole@sargentlundy.com

***Abstract*—To minimize the vulnerability of the electric power grid to cyberattacks the NERC enacted and enforced cybersecurity standards that continue to evolve as technology and the nature of these threats advance. These Critical Infrastructure Protection (CIP) standards require utilities to meet an aggressive timeline for regulatory compliance. This paper discusses major design challenges faced when upgrading substation equipment for cybersecurity enhancements and, specifically, the hardware improvements implemented for the NERC CIP V5 conversions.**

## Recent Cyber Attacks and Threats (Ukraine)

- Spear phishing email received with malware 9 months before attack
- All breakers opened at 27 substations
- 103 cities blacked out with another 189 partially out

## NERC CIP Version 5 Regulatory Standards

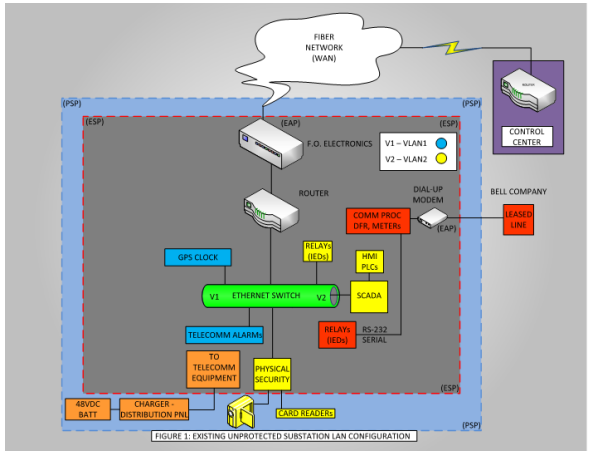
- V5 Deadline delayed from April 1 to July 1, 2016

## V5 Substation design Challenges

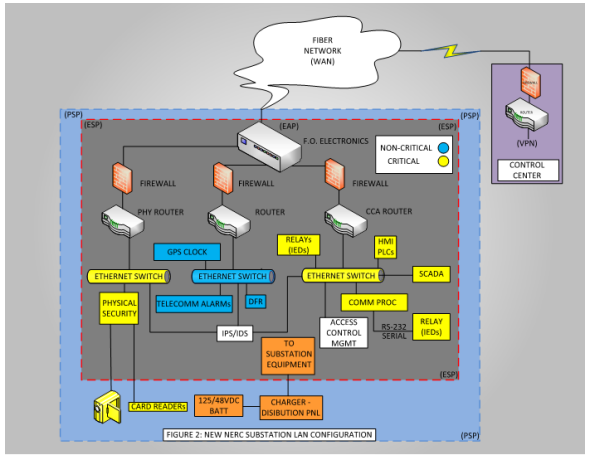
- VLANs not recommended for CCAs and Non-CCAs
- Installing Firewalls, IPS/IDS and EACMS
- Upgrading legacy and obsolete equipment
- Security risks for unsecure dial up devices
- Unanticipated costly equipment upgrades
    - Incompatibility issues/security vulnerabilities with legacy equipment
    - Telecomm Transport Systems
    - Battery/Charger Systems

| NERC CIP STANDARDS | TITLE |
|---|---|
| CIP-002-5.1 | BES Cyber System Categorization |
| CIP-003-5 | Security Management Controls |
| CIP-004-5.1 | Personnel & Training |
| CIP-005-5 | Electronic Security Perimeter(s) |
| CIP-006-5 | Physical Security of BES Cyber Systems |
| CIP-007-5 | System Security Management |
| CIP-008-5 | Incident Reporting and Response Planning |
| CIP-009-5 | Recovery Plans for BES Cyber Systems |
| CIP-010-1 | Configuration Change Management and Vulnerability Assessments |
| CIP-011-1 | Information Protection |
| CIP-014-1,2 | Physical Security |

*NERC CIP V5 Standards*




*Unprotected Substation LAN Configuration*




*New NERC Substation LAN Configuration*

## Construction

- V5 Implementation without service disruptions
- Additional unanticipated upgrades of DC and transport systems had to remain on schedule

## Conclusion

Upgrading substation hardware for NERC CIP V5 conversions has been complicated by the discovery of legacy and obsolete equipment that must be replaced to enable the required cybersecurity improvements. Another challenge is lack of up to date as-built documentation not adequately representing the current design configuration. Also, the increase in DC power loads from additional substation equipment that is required for V5 may result in the need to upgrade, some batteries, chargers and distribution panels to handle larger capacities. It is recommended that contingencies be included in resource plans, budgets and schedules when beginning the process of modifying substation hardware for NERC CIP standards.