Overview of NERC CIP Compliance Report

SCOTT R. MIX, CISSP

PNNL

Fall 2017 NASPI Meeting
PNNL-SA-129369

Overview of NERC CIP Compliance Document

- Document Outline
- Overview of NERC CIP Terms
- BES Cyber Asset Determination
- BES Asset Level Determination
- Implementation Recommendations

Document Outline

- Introduction
- Background
  - Development History
  - Impact Rating Criteria
  - Categorization Examples
- Implementation Recommendations
- Conclusions

Document Outline – Implementation Recommendations

- Implementation Recommendations
  - Impact Level Determination
  - BES Cyber Asset Determination
  - Low Impact, non BES Cyber Asset
  - Low Impact, BES Cyber Asset
  - Medium Impact, non-BES Cyber Asset, non-Protected Cyber Asset
  - Medium Impact, non-BES Cyber Asset, Protected Cyber Asset
  - Medium Impact, BES Cyber Asset
  - PDC at Medium Impact Control Center
  - PDC at High Impact Control Center
  - Communication Links
  - Applications using Synchrophasor data
  - Distribution Locations

Currently Approved NERC CIP Terms

- Cyber Asset
- BES Cyber Asset
- BES Cyber System
- Electronic Security Perimeter
- Protected Cyber Asset

NERC Terms

- **Cyber Asset**: Programmable electronic devices, including the hardware, software, and data in those devices.
- **BES Cyber Asset**: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber System.
- **BES Cyber System**: One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

NERC Terms

- **Electronic Security Perimeter**: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
- **Protected Cyber Asset**: One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

- Note – these terms only apply at high and medium impact levels

NERC Terms

- The CIP Standard requirements are written to address BES Cyber Systems
- Significant deference is given to utilities for determining what constitutes a BES Cyber System
  - Each individual BES Cyber Asset could be its own BES Cyber System
  - BES Cyber Assets can be grouped into BES Cyber Systems by location or function
  - BES Cyber Systems can be different for different requirements, for example:
    - An EMS can be a BES Cyber System
    - The HMIs in an EMS can be a BES Cyber System
    - All protective relays at a single station can be a BES Cyber System
    - All medium impact Vendor X Model Y protective relays using firmware version Z (across all stations) can be a BES Cyber System
  - BES Cyber Systems are not created by circumstance
    - Relay coordination between two ends of a line does not require both relays to be in the same BES Cyber System

BES Cyber Asset Determination

- Analyzes the function performed by either the Cyber Asset, or the data produced by the Cyber Asset (data is included in the definition of Cyber Asset)
- If the Cyber Asset meets the qualifications from the definition of a BES Cyber Asset (e.g., has a 15 minute impact on operations), it is a BES Cyber Asset
  - A protection relay meets the definition
  - An RTU meets this definition
- All BES Cyber Assets associated with the Bulk Electric (Bulk Power) System must be afforded some level or protections
- Also refer to the NERC Functional Model description for obligations
  - For example, the Transmission Operator is obligated to “[provide] Real-time operations information to the Reliability Coordinator and Balancing Authority.”

BES Asset Level Determination

- BES Impact levels are determined by applying the criteria in Attachment 1 of CIP-002
  - Criteria describes power system characteristics (e.g., number and voltage of lines leaving a transmission station)
- Impact levels are assigned to BES Cyber Assets based on their location
- Only Control Centers have an impact level of high
  - Field locations (transmission stations & generating plants) exist at medium and low impact levels
  - Control Centers (generation and balancing) also exist at medium and low impact levels
- If a PMU or PDC is determined to be a BES Cyber Asset, its impact level is based on its location, not the location of the user of the data

Implementation Recommendations

- Ten examples provided
- All focus on Synchrophasor Cyber Assets (PMUs and PDCs)
- Range from low impact scenario to medium impact scenario for PMU; medium impact and high impact for PDC or PMU
  - Includes brief discussion of PMUs outside of transmission stations
  - Includes discussion of communications networks carrying Synchrophasor data
- Assumes that the PMUs and PDCs communicate (externally at least) using a “routable protocol”
- Provides an overview of the NERC CIP requirements
  - Also includes several suggested security practices beyond minimum required for NERC CIP compliance
  - Exceeding the requirements is always an option, and has no compliance down-side

Implementation Recommendations

- Low Impact:
  - Includes governance requirements (policy, CIP Senior Manager)
  - Minimal set of requirements, including:
    - Cyber security awareness
    - Physical security controls
    - Electronic access controls
    - Cyber security incident response
    - Transient Cyber Assets and Removable Media protections*
    - CIP Exceptional Circumstances*
  - Recommended for all synchrophasor devices at low impact locations, even if not BES Cyber Assets, specifically if on the same LAN as BES Cyber Assets
  - Also recommended for synchrophasor devices at non-BES locations (e.g., distribution)

* - submitted to FERC but not approved

Implementation Recommendations

- Medium Impact
  - Requires compliance with nearly all CIP standard requirements
  - If the PMU is on the same LAN as a BES Cyber Asset, it is a Protected Cyber Asset (PCA) regardless of its use, and must comply with the CIP standard requirements as a PCA

Medium Impact example

- CIP-007 requirement R2 – Patching
  - Requires a “patch management program” to assess patches that have been released from a designated patch source, that are applicable to the BES Cyber Asset (i.e., the PMU)
  - Every month (35 days) the source needs to be queried to determine what patches have been released, determine if they are “security patches”, and determine their applicability to the utility’s environment
  - If the patch is applicable, within another month (35 days), either install the patch, or develop and implement a plan to mitigate the issue addressed in the patch
    - The mitigation plan should address when the patch will be installed, even if installation must be deferred due to operational considerations
    - Document the mitigations and implementation timeframes, including the expected timeframe to install the patch and remove any unneeded temporary mitigations

High Impact

- PDCs at Control Centers
- Follow all medium requirements discussed for PMUs
  - Some additional requirements
  - Some substitute requirements for high impact

Synchrophasor Data

- Data is used by applications
- Applications execute on a Cyber Asset
- That Cyber Asset is analyzed to determine if it is a BES Cyber Asset, and then its impact level is determined by its location
- Requirements attach to the BES Cyber Asset based on its level determination
  - Could be at a Control Center
  - Could be in an autonomous substation automation or Remedial Action Scheme in a transmission station

Communication Networks

- Currently, no NERC CIP requirements exist for communication networks
- Work underway to define requirements for “Control Center to Control Center” networks (e.g., subset of PDC to PDC communications)
- NASPInet (even if used for station communications) should follow best practices for security, and should be reviewed once the Control Center to Control Center communication requirements are completed

Other Locations

- PMUs in distribution stations
  - Out of scope – not Bulk Electric System (transmission)
  - Recommend following low impact requirements
- PMUs at Control Centers
  - Probably either test (out of scope) or located on distribution network (out of scope)

Open Q&A

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*