ERO Enterprise CMEP Practice Guide:

Generation Segmentation
September 15, 2020

Background

In support of successful implementation of and compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, the Electric Reliability Organization (ERO) Enterprise[1] adopted the Compliance Guidance Policy.[2] The Compliance Guidance Policy outlines the purpose, development, use, and maintenance of guidance for implementing Reliability Standards. According to the Compliance Guidance Policy, Compliance Guidance includes two types of guidance – Implementation Guidance and Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.[3]

CIP-002-5.1a Attachment 1 Impact Rating Criterion (IRC) 2.1[4] provides this language for identifying medium impact BES Cyber Systems at generating stations [emphasis added]:

> **2.1** Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

This criterion permits a registered entity to reduce the impact rating of a BES Cyber System from medium impact to low impact by ensuring that the BES Cyber System cannot impact more than 1500 MW of generation. The process of reducing the impact rating of a BES Cyber System by reducing the amount of generation it can impact is known as "disaggregation" or "segmentation." Generation segmentation was a topic of the CIP Version 5 transition activities.[5]

[1] The ERO Enterprise consists of NERC and the Regional Entities.
[2] The ERO Enterprise Compliance Guidance Policy is located on the NERC website at: https://www.nerc.com/pa/comp/guidance/Documents/Compliance%20Guidance%20Policy.pdf.
[3] Implementation Guidance provides a means for registered entities to develop examples or approaches to illustrate how registered entities could comply with a Standard that are vetted by industry and endorsed by the ERO Enterprise. CMEP Practice Guides differ from Implementation Guidance in that they address how ERO Enterprise CMEP staff executes compliance monitoring and enforcement activities, rather than examples of how to implement the Standard.
[4] At the time of posting this CMEP Practice Guide, CIP-002-5.1a is subject to enforcement. However, as future revisions may be subject to enforcement, this CMEP Practice Guide remains relevant to assessments of IRC 2.1 if no revisions are made to the IRC language. Pending possible revisions, this Practice Guide may be inapplicable and/or subject to retirement.
[5] Lesson Learned CIP Version 5 Transition Program, CIP-002-5.1 Requirement R1: Impact Rating of Generation Resource, an ERO Enterprise-Endorsed Implementation Guidance, provides lessons learned for demonstrating compliance in generation resources.

Purpose

The purpose of this CMEP Practice Guide is to provide guidance to ERO Enterprise CMEP staff (CMEP staff) when assessing a registered entity's process to demonstrate the disaggregation of its generation BES Cyber Systems (BCS), in implementing IRC 2.1 and Requirement R2, Part 2.1. This Practice Guide outlines aspects that CMEP staff should consider in understanding how a registered entity has applied controls to isolate generation systems controlling a unit or multiple units at a single plant location. This information can be used to inform CMEP staff's understanding of a registered entity's security posture and commensurate Compliance Oversight (i.e., Compliance Oversight Plan, audit approach, etc.). Compliance determinations are to be made in consideration of specific facts and circumstances of the individual registered entities and the language of the Requirements.

Lessons Learned

When CMEP staff reviews evidence of effective segmentation for BES generation systems, they should include analysis of several key factors:

- Connected Systems: Applicable systems connected to any particular unit must be analyzed. Evidence must clearly differentiate one network segment from all others. Segment documentation such as walk-down reports, diagrams and network scanning tools may be used together to comprehensively define a network segment and all connections. The Lessons Learned documentation terms this "BES Cyber Systems protected by the segmented unit network(s)."
- Common Systems: Applicable systems shared (or common) between units must be analyzed. Fuel transfer systems, coal milling control systems, or water/cooling systems may introduce common points for failure or for potential misuse.[6] The Lessons Learned refers to this as "BES Cyber Systems shared by multiple generating units or group of units, and analysis that unavailability, degradation, or misuse of the BES Cyber Systems could not impact 1500 MW or more within 15 minutes."
- Access Controls: Access controls on network traffic between applicable systems of segregated units must be analyzed. For applicable systems that allow communication across routable protocols, access controls enforce segmentation of generation systems. The Lessons Learned details this as "Access restrictions on network interfaces between each generating unit or group of units and external networks (e.g., firewall rules)."
- Operational Processes: Operational processes over segregated applicable systems must be analyzed. Each process, especially those created for system change response, should avoid overreach to other segregated systems. The Lessons Learned describes this as "Generating plant operational processes shared by multiple generating units or group of units, and analysis that unavailability, degradation, or misuse of the shared BES Cyber Systems that operate those operational processes would not impact 1500 MW or more within 15 minutes."

Each of these key factors is discussed below.

[6] Refer to the interpretation in CIP-002-5.1a Appendix 1 for further clarification on shared BES Cyber Systems.

Connected Systems

A distributed control system (DCS) cannot solely use network partitioning to effectively segment a BES Cyber System due to its myriad interconnections in other communications domains, such as serial and analog. However, input and output (I/O) tag databases make control systems unique. The I/O tag database is a list of discrete variables for items found in the control system. In other words, a tag has objects with associated attributes/fields. The control system applies alarming parameters on these tags. CMEP staff may review such a database as evidence supporting segmentation of a DCS.

The tag database is a central point to a control system. For example, a pump may have a Boolean tag of on/off. The same pump may have another tag that is analog for amperage. Alarming parameters may also be part of a tag. Types of tags may include string, analog, or digital (Boolean). Each tag must be unique in the tag database, as the tag database manages all new tags and any modifications to existing tags.

Evidence may locate and cite the I/O tag databases to demonstrate the entity possesses a comprehensive understanding of all associated systems. By contemplating and categorizing all possible associated systems, the entity may discover connections or risks that will either support or refute true segmentation. Effective evidence will generally demonstrate this effort and may include a list of tags, naming conventions, and definitions.

Common Systems

Any shared or common Cyber Assets (servers, workstations, PLCs, etc.) require extensive examination. CMEP staff should ensure there is sufficient detail included in the evidence to determine the extent to which common systems affect other applicable systems. As appropriate, CMEP staff should consider any shared compliance agreements detailing specific responsibilities when reviewing assessment of common systems.

- Example 1: A shared coal handling system may feed all units at a generation facility greater than 1500 MW. However, the entity may demonstrate the evaluation of the coal handling system do not meet the 15-minute criterion as the entity's storage capabilities of the coal silos can provide coal for a period exceeding 15 minutes.
- Example 2: If the fuel source is natural gas at a generation facility and a single BES Cyber System controls the fuel source(s) for greater than 1500 MW of generation, then that fuel handling system should be identified as a medium impact BES Cyber System if evaluation determined the system would meet the 15-minute criterion.
- Example 3: For a single plant location meeting IRC 2.1, Cyber Assets for each unit monitor for vibration on individual units, but these individual vibration monitoring Cyber Assets may also be part of a composite system for multiple turbines. This common composite system for vibration monitoring should be evaluated to determine if it meets the medium impact criteria for a BES Cyber System.

Access Control

CMEP staff should only accept claims of generation segmentation when individual DCS have no dependency on one another to function. A firewall separating an HMI from a backend server creates independent zones based on the rulesets. The firewall, router, or switch alone cannot fully "segment" all

control aspects of a DCS.

It is common to see more than one unit at generation facilities configured in identical (or equivalent) ways; in other words, each unit and individual components are duplicated to support the core functions. Compliance in such situations may prove challenging due to the similarities of Cyber Assets. To overcome these challenges, CMEP staff may begin with examining one-line diagrams or schematics of one unit and then proceed to evaluating the Cyber Assets of that unit. CMEP staff should be cautious when IP addressing is identical between units, as this may give the mistaken appearance of a common/single device. Effective evidence should clearly present how each Cyber Asset is unique and segmented from any "twins" in other units. Evidence examined may include:

- Asset management list of Cyber Assets
- Physical locations (buildings)
- MAC addresses (Note: If using NIC teaming or similar, a list of individual network adapters may be needed to get the physical MAC address)

Operational Processes

CMEP staff should analyze generating plant operational processes shared by multiple generating units or group of units to ensure that unavailability, degradation, or misuse of the shared BES Cyber Systems that support those operational processes would not impact 1500 MW or more within 15 minutes.

Facilities that require analysis include any group of generating units at a single plant location with a rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. Registered entities may determine net Real Power capability by analyzing nameplate ratings, MOD-025 results, FAC-008 Facility Ratings, or high sustainable limits (HSL) for each unit at the facility.

CMEP staff should seek an understanding of the operational components to establish any shared processes. BES Cyber Assets (BCAs) associated with those operational components could be considered shared and meet the 1500 MW or more within 15-minute criteria.

CMEP staff should analyze Cyber Assets (servers, workstations, remote terminal units (RTUs), and programmable logic controllers (PLCs), etc.) associated with common generation functions to identify potential BES Cyber Systems shared by multiple generating units. This analysis may include:

- Relationship of the number of DCSs to units
- Fuel handling system (combined system for facility of individual units, i.e., gas management system)
- Water (used for steam, cooling, and/or emissions)
- Startup functions
- Boiler
- Plant Air

- Lube Oil
- Plant Power
- Emissions
- Turbine
- Review of plant operational staff procedures in response to indicators or alarms from multiple units or common systems
- Communication to the GOP or BA Control Center (including RTUs or PLCs)
- Any other monitoring or alarming such as safety alarms or fire suppression systems
- Shared Ownership

Conclusion

In assessing a registered entity's generation segmentation, CMEP staff should consider whether all factors of segmentation have been analyzed by the entity. During this review, CMEP staff should consider connected systems, common systems, and controls for access in light of overarching operational processes.

The NERC Reliability Standards covered in this Practice Guide establish the minimum concepts for the segmentation of generation systems at a single plant. CMEP staff must gain understanding of how each of the registered entity's various CIP programs are applied, such as policies, procedures, access controls, training and periodic reviews. A review of the registered entity's efforts and evidence for segmentation may be included as part of any of the CMEP monitoring methods, as well as during a registration/certification activity.