NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Reference Document CIP-002 Categorization Practices to Build on Lessons Learned

2020 FERC Report on CIP Audits | February 23, 2023

Purpose

The purpose of this document is to provide considerations related to categorization practices. This document expands on CIP-002 lessons learned from *FERC Staff Report Lessons Learned from Commission-Led CIP Reliability Audits* ("FERC Report").[1] It is not intended to establish new requirements under NERC's Reliability Standards, modify the requirements in any existing reliability standards, or provide an interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Introduction

This document provides background for considerations of CIP-002 categorizations resulting from the FERC Report Additional information was gathered from an August 2021 meeting with FERC, NERC, and Security Working Group (SWG) participants, where discussions focused on the scope, observations, and frequency of occurrence noted by FERC regarding entity categorization, processes used for categorization, defined systems, and risk potential within the CIP-002 categorization process. Specifically, the focus was related to the following report information:

While entities generally categorized the impact rating of Bulk Electric System (BES) Cyber Systems associated with substations effectively and accurately, in some cases entities did not properly consider the interdependency of relay schematics and configurations between control houses containing separate voltage levels. This can lead to the misidentification of a BES Cyber System located at a substation as low impact instead of medium impact. For example, 138 kV breaker failure relays can trip 345 kV buses, and as a result can impact 345 kV BES Cyber Systems classified as medium impact. In such circumstances, consider whether the Cyber Assets associated with the 138 kV breaker failure relays are also medium impact BES Cyber Systems.[2]

CIP-002 Categorization

[1] *See* 2020 Staff Report Lessons Learned from Commission-Led CIP Reliability Audits (Oct. 2, 2020), https://cms.ferc.gov/sites/default/files/2020-10/2020%20CIP%20Audits%20Report.pdf

[2] https://cms.ferc.gov/sites/default/files/2020-10/2020%20CIP%20Audits%20Report.pdf, page 9

NERC Reliability Standard CIP-002 and the Attachment 1 criteria[3] were developed to consider a variety of entity generation, transmission and Control Center equipment, systems, functions, organizations, processes, and technologies, as well as interactions between entity partners and neighbors. This includes modern facilities, legacy facilities, remedial action schemes, protection systems, communications systems, safety systems, software, and hardware used for managing reliable operation of the BES.

Because of the variety of equipment, functions, and impacts, CIP-002 provides latitude for entities to define impact to the BES, as well as the security controls necessary to maintain reliability. Apart from requirements in CIP-002 Attachment 1 criteria, there is not a single approach to CIP-002 categorizations for all entities. Some entities may choose a top-down or bottom-up method that identifies risk related to BES assets (control centers, substations, and generation), while another may choose to identify systems related to the operation of a given BES asset which meets the criteria of Attachment 1. Appropriately identifying impact is key to a successful CIP-002 categorization program, so entities may wish to consider the following situations in their CIP-002 categorization process.

Considerations

- Multiple BES impact levels (high/medium/low/non-BES) within the same substation, control center, or generating station.
- Contingency protection, such as breaker failure designs, with the ability for Cyber Assets at a lower voltage level to affect higher voltage elements.
- Interdependency of protection and control equipment installed in separate buildings (line and bus differential protection) and zones of protection associated with multiple voltage levels (transformer protection).
- Remedial Action Scheme (RAS), including elements that span multiple substations, generation stations, and Registered Entities.
- Facilities shared by multiple entities.
- A single BES Facility or BES Cyber Asset that may meet multiple CIP-002 Attachment 1 Criteria.
- Unintended compliance impacts from a change in classification or classification philosophy.

Suggestions

- Do not assume that any BES Cyber System associated with equipment <200kV does not meet BES Reliability Operating Service (BROS) criteria.
- Carefully evaluate entity assets which contain both low and medium elements for their overall impact.

[3] https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

- Documented procedures for defining risk and potential impact can be valuable for Cyber Assets that are used for transformer protection, breaker failure protection, and protection systems which deploy Cyber Assets across multiple physical locations.
- Entities may consider both top-down and bottom-up approaches for categorization to help further define risks to the BES, with considerations for substation engineering and operations, information technology, network, transmission/generation operations and compliance in the development of categorization approaches.
- Pay special attention to categorizations for substations, generation, and control center locations with multiple, shared, or combined asset owners or operators. Entities may review and agree on categorization processes and identified levels of categorizations. Consider roles and responsibilities and/or contractual agreements to the operation, categorization, and risk of assets.
- Cyber Assets that are connected to the same logical network are typically part of the same BES Cyber System. For example, 500kV line protection and 500kV capacitor protection have the same classification even if the reactive resource does not meet the Impact Rating Criteria of Attachment 1 to CIP-002[4]. This example assumes there is not a separate communication network for the Cyber Assets associated with the line and capacitor protection.
- Ensure integrity of change and asset management during construction or modification at substations and when onboarding equipment and systems. Evaluate categorization levels by onboarding assets and systems through the categorization process.
- Ensure changes to classification of assets, Cyber Assets, and classification philosophies align with compliance requirements. For example, de-classification (or increasing classification) of a BES Cyber Asset may require reclassification or de-classification (or increased classification) of other systems.

Example Scenarios

While many scenarios may challenge an entity's classification practices, this paper will consider two hypothetical configurations. **Scenario A** considers a transformer low-side breaker failure protection scheme associated with a ring bus. **Scenario B** illustrates two transformer low-side breaker failure protection schemes associated with a double bus.

Scenario A

Ring Bus Transformer Low Side Breaker Failure Protection

Scenario A is a 500 kV ring bus with four circuit breakers and three 500 kV lines. A 500/138kV transformer is connected to the fourth ring position. 138kV circuit breaker CB A uses a breaker failure scheme for contingency protection.

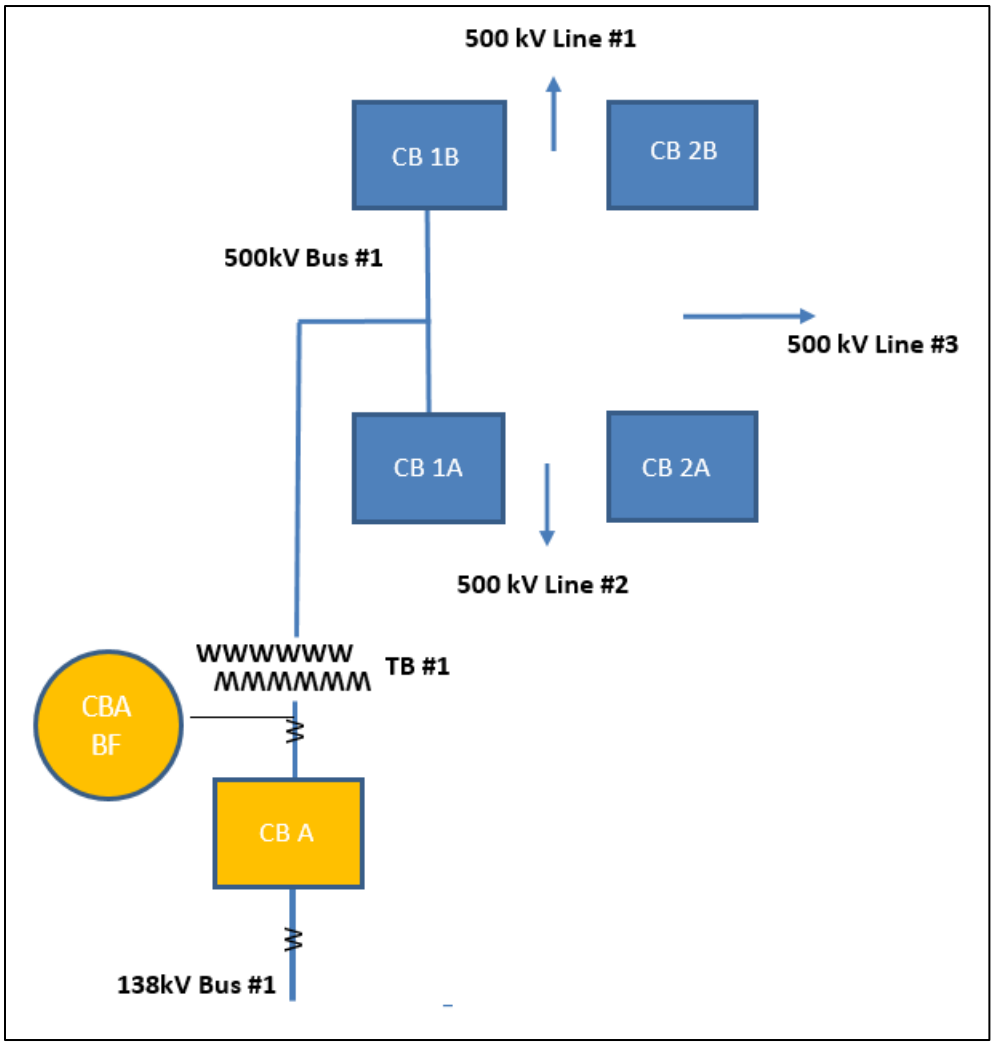
During a breaker failure condition of circuit breaker CB A, relay CBA BF trips 500kV circuit breakers 1A and 1B. In this case, Cyber Asset CBA BF can be misused to operate circuit breakers 1A and 1B. It is important

[4] https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

to consider that relays used to protect and control the 500kV circuit breakers could potentially have more significant impact than CBA BF.

For Scenario A, consider the following questions when determining the impact rating of the associated BES Cyber System(s):

- Can the 138kV protection and control systems impact power flow through the 500kV transmission system?
- Does the loss of the transformer impact the 500kV system?
- Is the 138kV system a source to the 500kV system (for example, nearby generating resources on the 138kV system)?
- Will permanent or extended outage configurations of the ring bus create a more significant impact from a Cyber Asset associated with the 138kV system or the transformer protection?



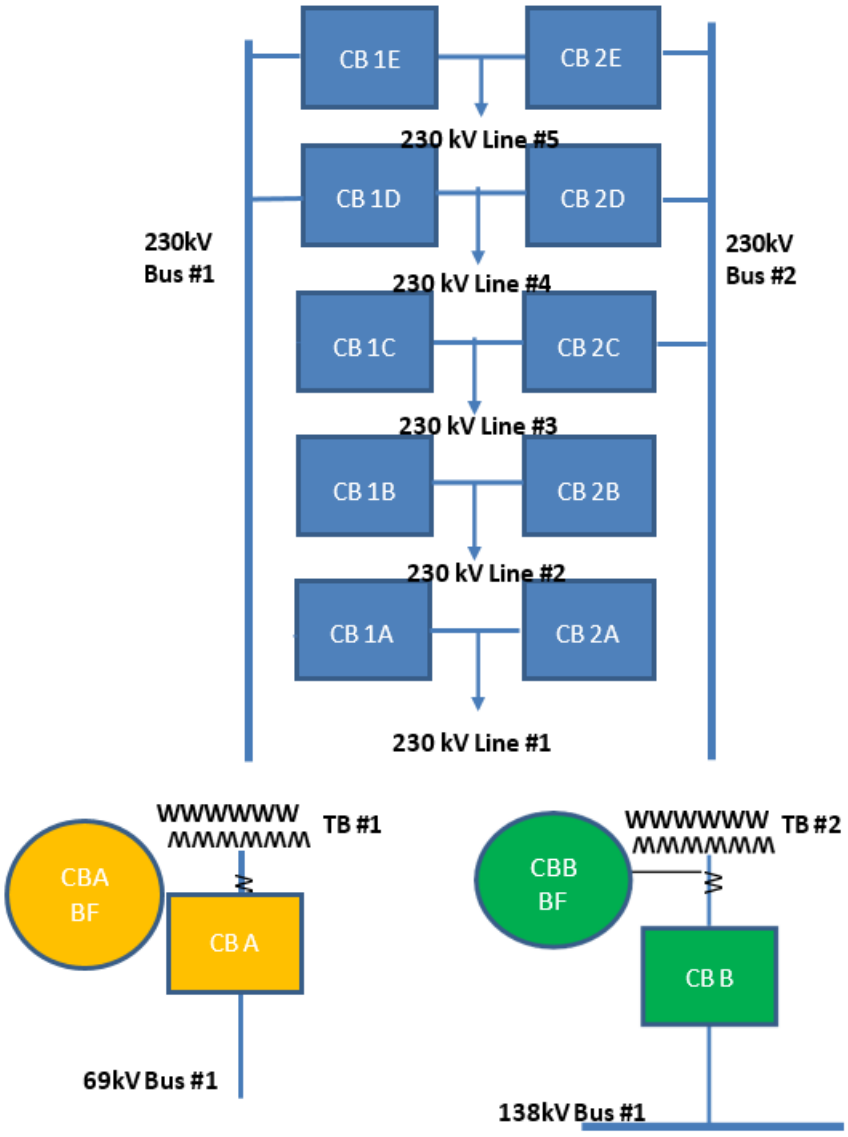
Scenario A: Ring Bus Transformer Low Side Breaker Failure Protection

Scenario B
Double Bus Transformer Low Side Breaker Failure Protection

Scenario B is a 230kv double bus and double breaker substation configuration. A 230/69 kV transformer is connected to 230kV Bus 1 and a 230/138 kV transformer is connected to 230kV Bus 2. The 69kV and 138kV systems both use circuit breaker failure protection that can trip each 230kV bus individually. CBA BF and CBB BF relays can be simultaneously misused to de-energize the 230kV system. This is a scenario where an entity could carefully consider the impact to the 230kV system based on the capability of the Cyber Assets associated with the 69kV, 138kV, and transformer protection systems.

For Scenario B, consider the following questions when determining the impact rating of the associated BES Cyber System(s):

- Are there any systems under 100kV or not part of the BES that may have been overlooked?
- Can the 138kV or 69kV protection and control systems impact power flow through the 230kV transmission system?
- Does the loss of either transformer impact the 230kV system?
- Is the 138kV system or the 69kV system a strong source to the 230kV system?
- Will permanent or extended outage configurations create a larger impact from a Cyber Asset associated with the 138kV system, the 69kV system, or any of transformer protection systems?
- How is simultaneous misuse of CBA BF and CBB BF prevented?
- What security controls are in place for these relays?
- Are the 69kV and 138kV relays in separate cyber systems?
- Are the relays located in the same physical location?
- Do the relays support interactive remote access?
- Are the relays installed outside the physical security perimeter (cabinets in the switch yard)?
- If someone has access to one, is it easy to access the other (same network, same password, same security controls)?



Scenario B: Double Bus Transformer Low Side Breaker Failure Protection

Additional Recommendations

Entities may consider reviewing their CIP-002 categorization processes to include power flow from lower-rated to higher-rated elements. For example, a sub-process step could perform power flow, load, or modeling studies for elements whose combined lower to higher KV potential may adversely impact reliability. An entity could choose a use case focused on loss of lower rated elements (such as 138kV sources) to determine the adverse impacts to the reliability of in-scope higher KV elements and assets. Entities may also consider cross referencing their FAC-008 processes while determining such elements and equipment as they may find best practice opportunities and efficiencies between assessing and identifying elements in FAC-008 and the categorization processes in CIP-002.

Conclusion

CIP-002 Attachment 1 criteria[5] provide latitude for entities to identify risks at various levels. It is important to gain a thorough understanding of the facilities, equipment, and systems that operate, maintain, and protect the reliability of the BES. Documented classification procedures and philosophies help to ensure entities consistently categorize and protect BES Cyber Systems to maximize the reliable operation of the BES.

[5] https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx