Technical Rationale

Project 2021-03 CIP-002 | Reliability Standard CIP-002-8

CIP-002-8 – Cyber Security – BES Cyber System Categorization and Control Center Definition

Introduction

This document explains the technical rationale and justification for the proposed revisions to the Control Center Definition and Reliability Standard CIP-002-8. It provides stakeholders and the ERO Enterprise with a description of the technical requirements in the Reliability Standard. These are not Reliability Standards and should not be considered mandatory and enforceable.

Updates to this document include the Project 2021-03 CIP-002 Drafting Team's (DT's) intent in drafting changes to the requirements and definition.

Overview

Project 2021-03 proposes revisions to the Control Center definition and CIP-002-8 criterion 2.12 in Attachment 1. CIP-002-8 provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems (BCS) based on the impact to their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System (BES). The proposed revisions to Attachment 1 address the categorization of Transmission Owner Control Centers (TOCCs) performing the functional obligations of a Transmission Operator (TOP), specifically those that meet medium impact criteria, and clarifying the language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.

Rationale for Control Center Definition Modification

Rationale for Proposing Modifications to the Control Center Definition

During the CIP-002 TOCC Field Test[1], it was found that many Transmission Owners (TO)s struggled with how to interpret the Control Center definition. While the current Control Center definition does not specifically identify TOs, a TO may have a Control Center through its ability to monitor and control the BES in real-time to perform the reliability tasks of a TOP. This struggle surfaced in the following three manners:

- Lack of a common understanding of the term "control" versus "authority" as it relates to TOPs
- Lack of a common understanding of the term "perform the functional obligations of the TOP" as stated in Attachment 1 of CIP-002-5.1a.
- Lack of a common understanding of the term "associated data centers" versus TO BES Cyber Assets capable of controlling transmission Facilities.

Modifications to the definition have been proposed to eliminate ambiguity.

[1] The final field test report is available at https://www.nerc.com/pa/Stand/Project202103_CIP002_Transmission_Owner_Control_Ce/2021-03_CIP-002_TOCC_Field_Test_Final_Report_01262023.pdf.

Applicable Control Center Entities

Considering industry comments, the Control Center definition for Reliability Coordinator (RC), Balancing Authority (BA), TOP, and Generator Operator (GOP) was not revised. The industry felt the Control Center and data center definitions for these registered entities were well understood and is structured to explicitly identify the four different types of registered entities have gone through the scrutiny of compliance monitoring. Thus, no changes were made for these four registered entities that could have a Control Center.

The Control Center definition was expanded to incorporate the TO as follows: "One or more facilities of a TO that have the capability to control transmission Facilities at two or more locations in real-time using Supervisory Control and Data Acquisition (SCADA), including their associated data centers and excluding field Cyber Assets used for telemetry."

A TO is considered to have a Control Center if it has the capability to control transmission Facilities at two or more locations using SCADA. The concept of 'capability to control using SCADA' is specifically used to differentiate between control and monitor functions – i.e., clarify that a facility used by a TO to monitor Facilities without any capability to electronically control those Facilities using a SCADA system does not fall within the Control Center definition. For example, a TO who issues verbal instructions to field switching personnel but who does not have the 'capability to control using SCADA' would not be considered to have a Control Center.

The use of the NERC defined term "SCADA" is intended to exclude Cyber Assets used at a relay maintenance office to change relays setting, which may allow the capability to remotely operate a breaker. These Cyber Assets would not be considered a Control Center but may be required to be protected under other cyber security categories. Likewise, the use of the NERC defined term "SCADA" is intended to exclude Cyber Assets and Human Machine Interface (HMI) located at substations that have the capability to monitor and control transmission Facilities locally at the substation. These Cyber Assets would not be considered a Control Center but may be required to be protected under other cyber security categories.

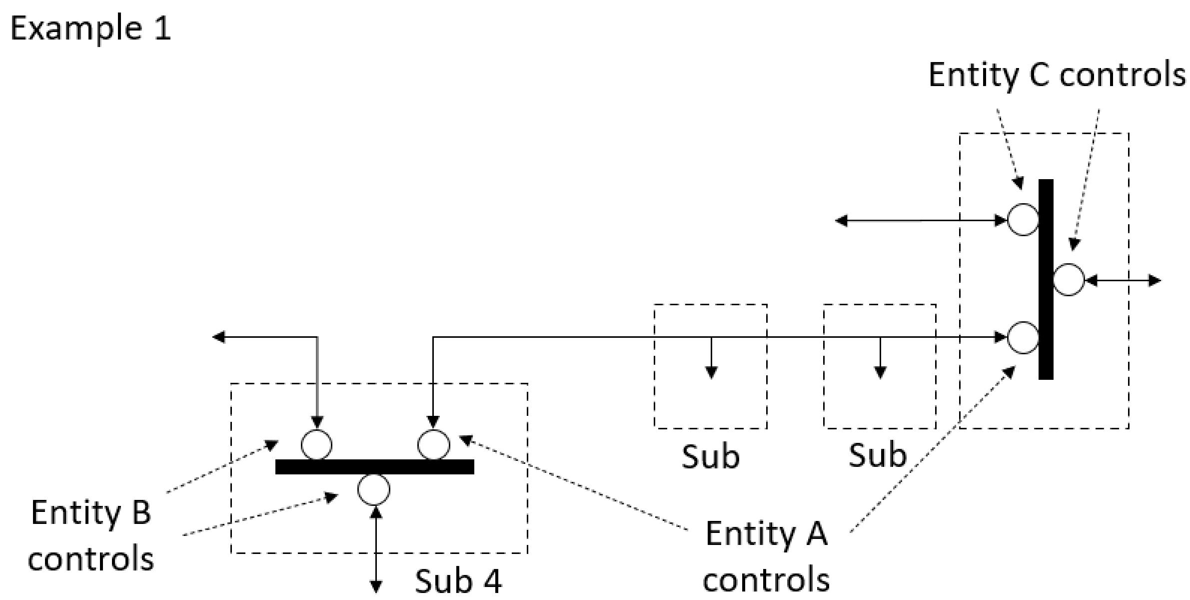
Because a SCADA system may include telemetry per the NERC defined term, the DT has crafted language to specifically exclude field Cyber Assets used for telemetry from being part of the Control Center and associated impact level determination. The impact level of field Cyber Assets, including telemetry, should be evaluated based on the location and associated impact level contained in Attachment 1.

The part of the Control Center definition that is applicable to the TO is not tied to the functional obligations of the TOP, nor is it tied to any TOP reliability tasks. Rather, it is tied to having a BES Cyber System or BES Cyber Asset, i.e., a SCADA system with the capability to control. It does not matter if the TO has a reliability task with pre-authorized authority from the TOP to control transmission Facilities or only receives operating instructions from the TOP. The cyber security risk that must be protected is access to the BES Cyber System or BES Cyber Asset(s), i.e., SCADA system that are able to control the transmission Facility.

When considering the language "transmission Facilities at two or more locations" and "generation Facilities at two or more locations," it is generally expected that the Facilities will have separate street addresses. Facilities located at a single street address would be associated with a single location. An entity must have more than one Facility and must have Facilities at two or more locations in order to have “transmission Facilities at two or more locations” or “generation Facilities at two or more locations.”

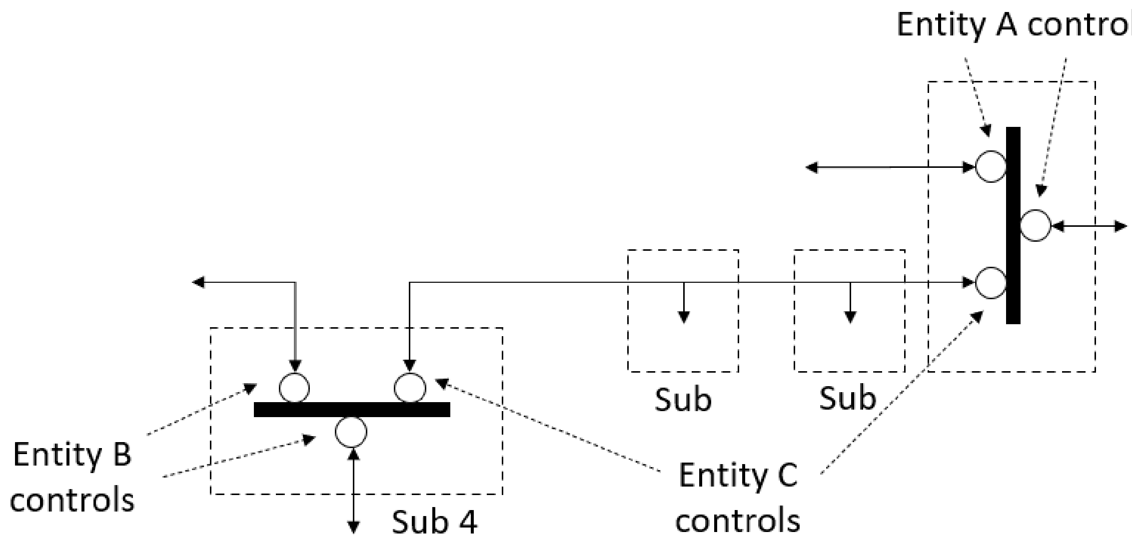
With respect to Transmission Owners who have facilities that are capable of controlling High Voltage Direct Current (HVDC) Facilities, each Responsible Entity will need to engage with their Regional Entity in order to determine how the language “transmission Facilities at two or more locations” should be applied based on the specific configuration. The current definition has not changed for Transmission Operators, and thus there is no expected change in applicability to classification of their operated HVDC Facilities.

The following examples differentiate between a single transmission Facility and two or more transmission Facilities at one location.



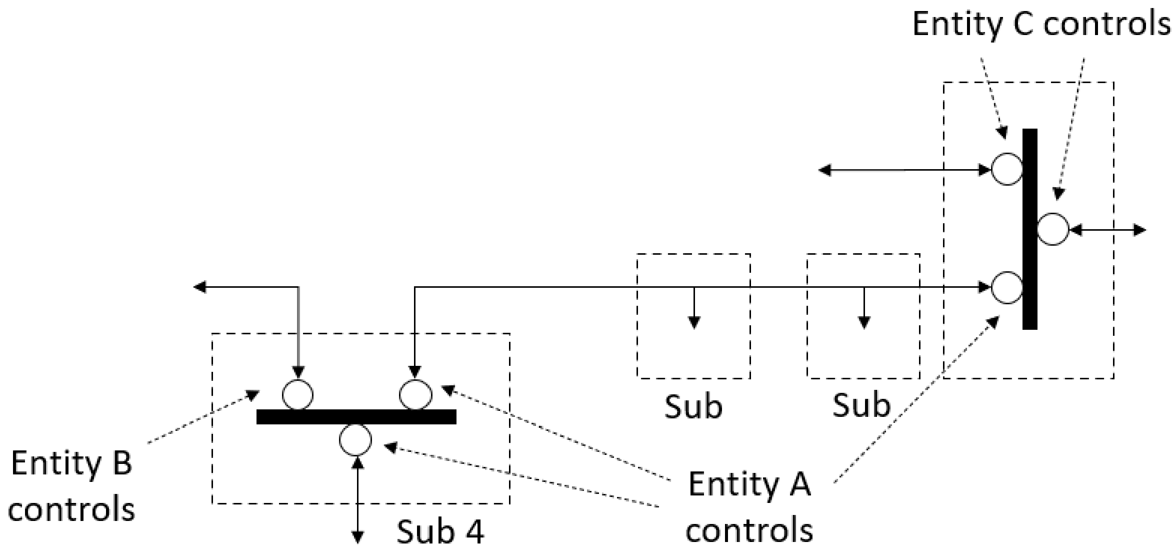
In Example 1, Entity A has control of breakers at both ends of a Transmission Line, which constitutes a transmission Facility. Because Entity A controls a single transmission Facility at 2 locations, Entity A does not meet the TO or TOP Control Center definition.

Example 2



In Example 2, Entity A has control of breakers at one end of two transmission Facilities, but at a single location. Because Entity A controls two transmission Facilities at only 1 location, Entity A does not meet the TO or TOP Control Center definition.

Example 3



In Example 3, Entity A has control of breakers at one end of two transmission Facilities and a breaker at different location. Because Entity A controls two transmission Facilities at 2 locations, Entity A does meet the TO or TOP Control Center definition.

Associated Data Centers

The Control Center definition includes the phrase “associated data centers”. This phrasing is intended to ensure that Cyber Assets that are not co-located in the facilities that host operating personnel are included in the Control Center definition, and are thus included in the process of identifying and categorizing BCS.

Industry comments received during the standard drafting process indicate that lack of a NERC definition for data center has not been an issue in applying the Control Center definition. Therefore, the term “associated data center” was retained in the revised definition.

Rationale for CIP-002-8 Attachment 1 Modifications

Removal of Functional Obligation Language

Language throughout Attachment 1 of CIP-002-8 that referred to the “functional obligations” of the different Registered Entities has been replaced with references to the reliability tasks performed by those same Registered Entities. This change was incorporated given that the NERC Functional Model is no longer being actively maintained and to align with the language used in the Control Center definition. It also resolves an issue whereby an entity may be identified as performing functional obligations even though that entity is not currently registered with NERC. The proposed modifications ensure that the responsibility for entity registration precedes enforcement of CIP-002-8. Usage of ‘reliability task” is to provide flexibility to an entity when referring to activities performed by that entity to ensure resource adequacy and operational reliability of BES Elements and Facilities. Additional information on the BES reliability operating services that may be useful to entities when they are defining their reliability tasks can be found in the technical rationale document associated with CIP-002-7. Each entity is ultimately responsible for reviewing their obligations under the NERC Standards to identify their reliability tasks.

Calculating an Aggregate Weighted Value per Criteria 2.12

The total aggregate weighted value is used to account for the impact on the BES. The 6,000 aggregate weighted value threshold defined in criterion 2.12 provides sufficient differentiation for medium and low impact BCS associated with Control Centers that are operated by a registered TOP or owned by a registered TO. DT analysis of data obtained from the CIP-002 Transmission Owner Control Center Field Test[2] validated that those facilities that may have significant impact are categorized at an appropriate level commensurate with the associated risk.

The total aggregate weighted value of 6,000 was derived based on an entity with no single station or substation that meets criterion 2.5, but who has the capability or authority to control BES Transmission Lines with the equivalent weight of two stations or substations whose BCS would be classified as medium impact per criterion 2.5. This is ultimately derived from the "two or more locations" criteria that is documented in the Control Center definition.

For consistency with the existing Attachment 1 criteria, the weighted values for the various voltage classes of BES Transmission Lines were selected to align with the existing approved values in criterion 2.5. For BES Transmission Lines 200 kV to 299 kV and for BES Transmission Lines 300 kV to 499 kV, the weighted values per line are 700 and 1300, respectively. Similar average MVA line loadings based on kV rating were calculated for BES Transmission Lines less than 100 kV and for BES Transmission Lines 100 kV to 199 kV using Appendix A of NERC's Severity Risk Index Enhancements Report which result in weighted values of 100 and 250, respectively.

BES Transmission Lines that are energized at voltages of 500 kV and above have no contribution to the aggregated weighted value given that criterion 2.4 already includes BCS for any transmission Facilities at substations that are operated at 500 kV or higher as medium impact. Further, criterion 1.3 includes the BCS used by and located at Control Centers or backup Control Centers that monitor and control any BES Transmission Lines at substations that are operated at 500 kV or higher as high impact. During industry commenting periods, the drafting team received many inquiries into the use of zero (0) in the table for criterion 2.12, which was originally proposed to remain consistent with existing criteria 2.5. Pursuant to these comments, the DT elected to use "0 (N/A)" in both criterion 2.5 and criterion 2.12 to make it clear that these lines are not relevant for inclusion in the aggregate weighted value calculation.

For the purpose of identifying a Responsible Entity's BES Transmission Lines, a Transmission Line is typically defined by the Protection System(s) that would be used to isolate faults on the Transmission Line – which is generally defined by a boundary of fault interrupting devices (e.g., breakers) that are controlled by the line's Protection System(s). Transmission Lines can be single-ended, two-ended or three-ended.

In the terms of applicable BES Transmission Lines, the following should be considered:

- All BES Transmission Lines that are energized at voltages less than 100 kV, are monitored and controlled by a Control Center, and have been specifically designated as part of the BES via the

[2] The final field test report is available at https://www.nerc.com/pa/Stand/Project202103_CIP002_Transmission_Owner_Control_Ce/2021-03_CIP-002_TOCC_Field_Test_Final_Report_01262023.pdf.

NERC Rules of Procedure (ROP) Exception Process.

- All BES Transmission Lines that are energized at voltages between 100 kV and 499 kV, connect to another Transmission station or substation, and are monitored and controlled by a Control Center. This includes BES Transmission Lines that connect to neighboring entities.
- Multiple-point BES Transmission Lines (e.g., two-ended or three-ended lines) are considered to contribute a single weight value per line. For any fault on the line, all line breakers located at the terminals are expected to operate to clear the fault. For example, a single 230 kV three-ended line would contribute an aggregate weighted value of 700 based on the criterion 2.12 table.

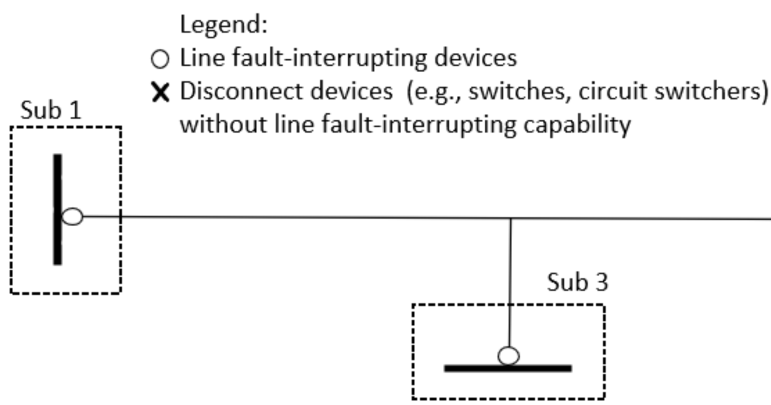


Figure 1: A 230 kV three-terminal Transmission Line contributes an aggregate weighted value of 700

- Multiple-taps BES Transmission Lines (including various implementations such as loop-in-loop-out) are considered to contribute a single weight value per line. For example, a two-ended 230 kV line with two substations tapped on the line where the substations do not have any 230 kV line fault-interrupting devices would contribute an aggregate weighted value of 700 based on the criterion 2.12 table.

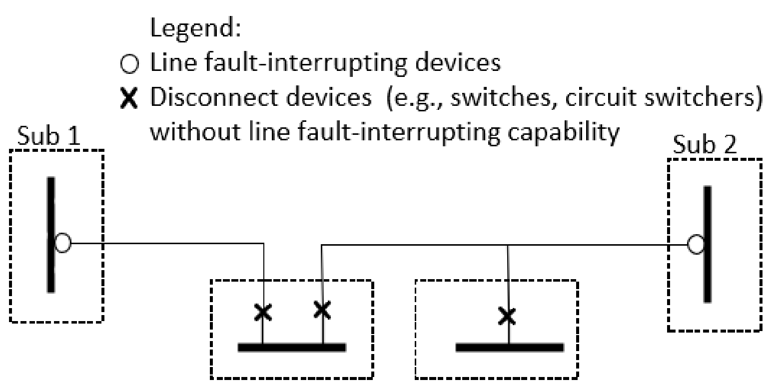


Figure 2: A 230 kV two-terminal Transmission Line with two tapped substations contributes an aggregate weighted value of 700

- Multiple lines between two transmission stations or substations are considered to contribute multiple weight values per line. For example, two two-ended 345 kV lines that connect between the same two transmission stations or substations would contribute an aggregate weighted value of 2,600 based on the criterion 2.12 table.

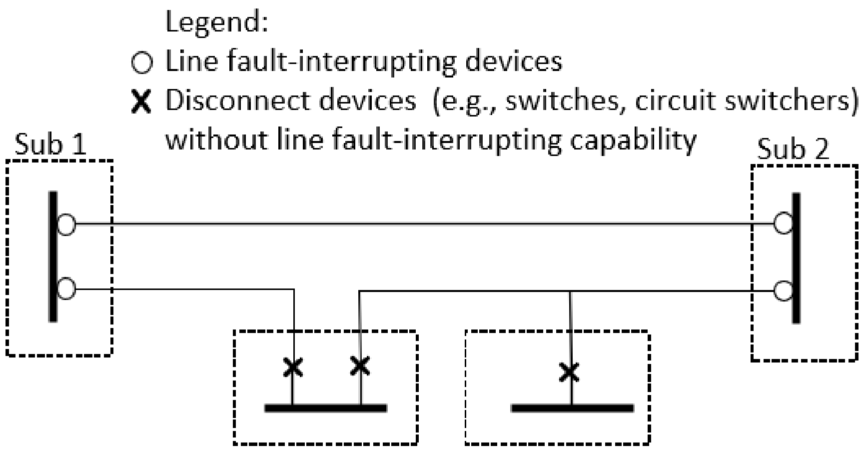


Figure 3: Two 345 kV two-terminal Transmission Lines that connect between the same two Transmission stations or substations contribute an aggregate weighted value of 2,600

Applying the Exclusion Clause per Criterion 2.12

An exclusion clause has been provided to allow Responsible Entities to appropriately categorize their BES Cyber Assets at Control Centers at a level that is commensurate with the associated risk for local systems having limited flow-through or generation export, and are primarily designed to serve load.

The exclusion clause applies to TOPs and TOs where the initial calculated aggregated weighted value (AWV) is less than 12,000. In such cases, the TOP/TO may calculate a revised AWV that excludes those BES Transmission Lines that are contained in a single group of contiguous Elements (GCE[3]) operated at or greater than 69 kV but less than 300 kV, as defined by the Responsible Entity. The hourly integrated gross export from the GCE must not exceed 75 MWh during the preceding 12 calendar months during non-Energy Emergency Alert (EEA) conditions. Gross exports from the GCE during an EEA condition that exceed 75 MWh are allowed to enable the Responsible Entity to provide support to neighboring entities during EEA conditions without any compliance impact.

Entities that choose to pursue an exclusion under criterion 2.12 are responsible for documenting the process whereby they will calculate the hourly integrated gross export from the defined GCE. The concept of an hourly integrated value was selected to avoid requiring entities to use an instantaneous value. There is no requirement that entities install meters specifically for the purpose of calculating the hourly integrated gross export; however, they may do so if they choose. Alternatively, entities may choose to use SCADA data for the purposes of calculating the hourly integrated value.

An entity is responsible to clearly define the GCE and to monitor flows across the interfacing equipment

[3] The concept of a "group of contiguous Elements" will be referred to as a GCE throughout the remainder of this document for simplicity. The acronym is solely used in this document and is not included as a defined term in the NERC Glossary of Terms.

in order to demonstrate compliance with CIP-002. Interfacing equipment is not limited to BES Transmission Lines, provided that the entity is able to collect the necessary data to demonstrate gross export from the GCE remains below 75 MWh. The GCE may contain Elements that the Control Center is not able to control, provided that the GCE boundary encompasses a transmission network that is primarily designed to serve load. The GCE specifically excludes Transmission Lines 300kV and above, as they are generally intended for the bulk transfer of power and not for local load serving purposes. A restriction to allow the responsible entity to define only one GCE is established to prohibit the ability of the entity to segment off multiple areas within a larger geographic area.

An initial calculated AWV of 12,000 is established to avoid application of the exclusion to large control areas. The AWV of 12,000 corresponds to an entity with no single station or substation that meets criterion 2.5, but who has the capability or authority to control BES Transmission Lines with the equivalent weight of four stations or substations whose BES Cyber Systems would be classified as medium impact per criterion 2.5. During the Field Test performed by the DT, entities with AWV between 500 and 11,300 were evaluated and no reliability risks to the BES were identified for any entities.

The bright line of 75 MWh is selected to align with pre-existing criteria including (1) the registration criteria for a Distribution Provider (DP) and (2) the registration criteria for a GO. Establishing a threshold is intended to differentiate between non-impactful load serving areas and areas that are more likely to have an impact on the interconnected BES. It was selected to be conservative and is below other established thresholds such as the reporting requirement for uncontrolled loss of firm load resulting from a BES Emergency and firm load shedding resulting from a BES Emergency as documented in EOP-004. EEA conditions were specifically excluded to ensure a Responsible Entity is not disincentivized from providing all available assistance during emergency conditions due to future compliance considerations.

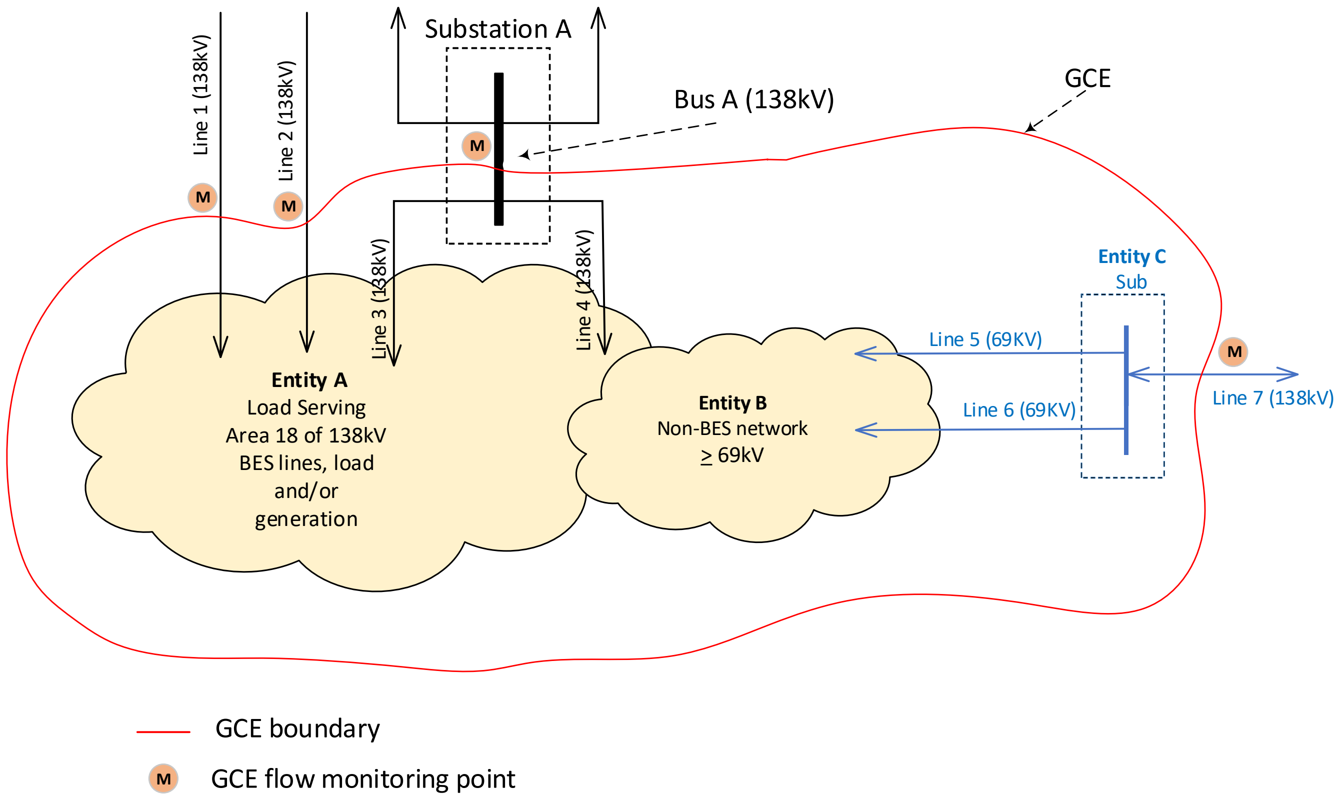
The DT has intentionally constructed the exclusion clause to require an entity to measure gross export from their defined GCE. This accounts for both generation output and flow-through the GCE. It ensures that an entity is unable to define a GCE that contains significant generation that supports the BES or with significant flow-through that impacts the BES.

GCE Example

The GCE must be a contiguous system. It may contain non-BES assets that are operated at 69kV or above and it may contain assets owned/operated by another entity. In the event that a non-BES element is part of the GCE interface, it will need to be included in the gross export calculation.

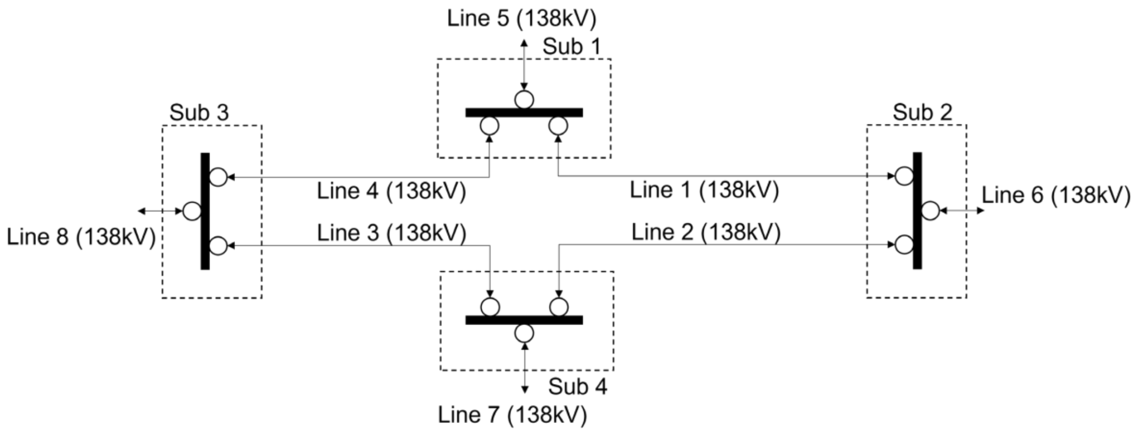
In this example, Entity A defines a GCE that contains all equipment shown in the red boundary below. The GCE interface consists of the flow through Bus A, Line 1, Line 2, and Line 7. The GCE contains equipment owned and operated by Entities A, B and C. To demonstrate compliance with the exclusion clause, Entity A must be able to obtain the necessary data from Entity C for Line 7 to calculate the gross export to demonstrate compliance with CIP-002. The entity must also be able to determine the relevant flow through Bus A, Line 1, Line 2, and Line 7 to demonstrate that gross export from the GCE does not exceed 75 MWh.

In this particular example, Entity A may not have the capability to measure the flow through Bus A; however, the entity may be able to utilize existing measurement points that exist on the four lines that terminate on Bus A to determine the flow as necessary to calculate the hourly integrated gross export from the GCE.



Criterion 2.12 Example 1: Aggregate Weighted Value below 6,000

In example 1 below, BCS are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in criterion 2.12 and sum the weighted values for each BES Transmission Line.



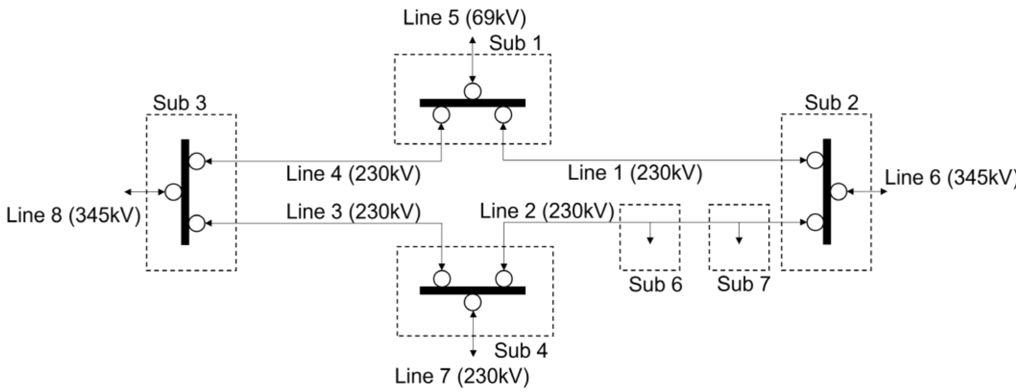
Note: Substation equipment (e.g., transformers) is not shown for simplicity. Circles represent fault interrupting devices.

The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 2,000, which is below the minimum threshold for the medium impact rating required in criterion 2.12. The BCS associated with the Control Center in this example should be categorized as low impact BCS pursuant to criterion 3.1.

Voltage Value of a BES Transmission Line	Weight Value per BES Transmission Line	Applicable Lines	Weighted Value
< 100 kV	100	None	0
100 kV to 199 kV	250	Line 1, Line 2, Line 3, Line 4, Line 5, Line 6 Line 7, Line 8	2000
200 kV to 299 kV	700	None	0
300 kV to 499 kV	1300	None	0
500 kV and above	0	None	0

Criterion 2.12 Example 2: Aggregate Weighted Value exceeds 6,000 with no Exclusion

In example 2 below, BCS are associated with a Control Center that monitors and controls seven BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in criterion 2.12 and sum the weighted values for each BES Transmission Line.



Note: Substation equipment (e.g., transformers) is not shown for simplicity. Circles represent fault interrupting devices.

The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 6,100, which is above the minimum threshold for the medium impact rating required in criterion 2.12. Given that the calculated aggregated weighted value is less than 12,000, the Responsible Entity would be eligible to consider calculating a modified aggregate weighted value that excludes a single GCE in accordance with the exclusion clause; however, in this example, the Responsible Entity either did not choose to pursue an exclusion or did not meet the exclusion criteria. In accordance with criterion 2.12, the BCS associated with the Control Center should be categorized as medium impact BCS.

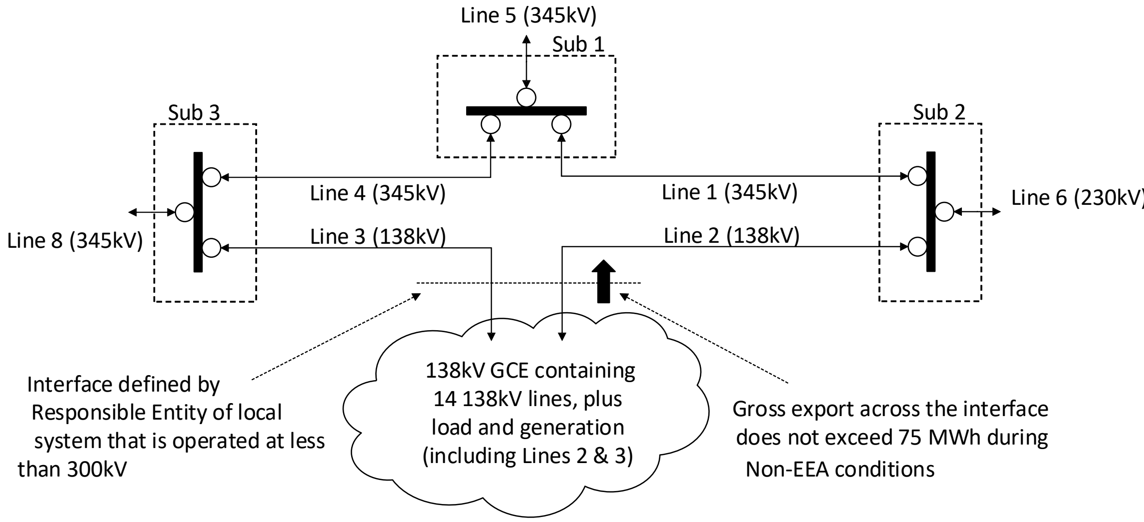
The circles on the diagram indicate the presence of fault-interrupting devices. There are two substations shown (Sub 6 and Sub 7) that are tapped on Line 2 for load serving purposes; however, these substations do not have line fault-interrupting devices that will operate for a fault on Line 2. Therefore, the BES Transmission Line is defined between Sub 2 and Sub 4.

Voltage Value of a BES Transmission Line	Weight Value per BES Transmission Line	Applicable Lines	Weighted Value
< 100 kV	100	None	0
100 kV to 199 kV	250	None	0
200 kV to 299 kV	700	Line 1, Line 2, Line 3, Line 4, Line 7	3500
300 kV to 499 kV	1300	Line 6, Line 8	2600
500 kV and above	0	None	0

*Line 5 is less than 100 kV; however, no exception has been obtained through the NERC ROP Exception Process and therefore, the line is not BES.

Criterion 2.12 Example 3: Aggregate Weight Value below 6,000 after Applying GCE Exclusion

In example 3 below, BCS are associated with a Control Center that monitors and controls nineteen BES Transmission Lines, of which 14 are to be excluded from the calculation using the GCE exception. The entity should first calculate its aggregate weighted value, referencing the table located in criterion 2.12. The entity is eligible to calculate a modified aggregate weighted value if the original aggregate weighted value is less than 12,000. In order to calculate the Control Center's modified aggregate weighted value, the Responsible Entity should reference the table located in criterion 2.12, and the exclusion language, and sum the weighted values for each BES Transmission Line that is not part of a single GCE that was defined by the entity in accordance with the exclusion clause.



Note: Substation equipment (e.g., transformers) is not shown for simplicity.

Circles represent fault interrupting devices.

The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 9,400, which is above the minimum threshold for the medium impact rating required in criterion 2.12. Given that the calculated aggregated weighted value is less than 12,000, the Responsible Entity is eligible to calculate a modified aggregate weighted value that excludes a single GCE in accordance with the exclusion clause.

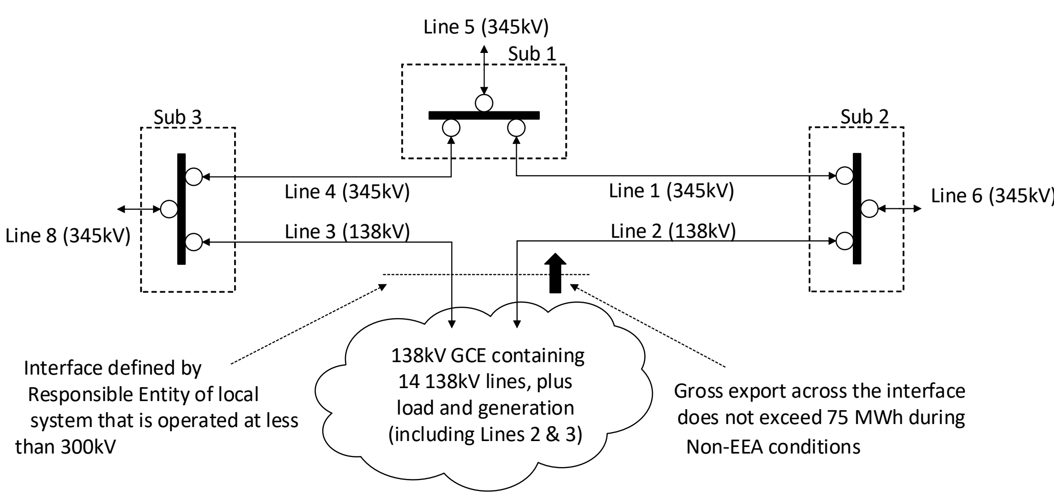
Voltage Value of a BES Transmission Line	Weight Value per BES Transmission Line	Applicable Lines	Weighted Value
< 100 kV	100	None	0
100 kV to 199 kV	250	Line 2, Line 3, 12 additional lines	3500
200 kV to 299 kV	700	Line 6	700
300 kV to 499 kV	1300	Line 1, Line 4, Line 5, Line 8	5200
500 kV and above	0	None	0

The calculation of the modified aggregate weighted value is demonstrated below and equates to an aggregate weighted value of 5,900, which is below the minimum threshold for the medium impact rating required in criterion 2.12. The BCS associated with the Control Center in this example should be categorized as low impact BCS pursuant to criterion 3.1.

Voltage Value of a BES Transmission Line	Weight Value per BES Transmission Line	Applicable Lines	Weighted Value
< 100 kV	100	None	0
100 kV to 199 kV	250	None	0
200 kV to 299 kV	700	Line 6	700
300 kV to 499 kV	1300	Line 1, Line 4, Line 5, Line 8	5200
500 kV and above	0	None	0

*Lines 2 and 3 (along with the 12 additional lines located in the 138 kV GCE) are excluded from the calculation because the Responsible Entity has defined an interface to a GCE that is operated at less than 300kV, where the gross export across the interface does not exceed 75 MWh during non-EEA conditions.

Example 4: Aggregate Weight Value above 6,000 after Applying GCE Exclusion
In example 4 below, BCS are associated with a Control Center that monitors and controls 19 BES Transmission Lines, of which 14 are to be excluded from the calculation using the GCE exception. The entity should first calculate its aggregate weighted value, referencing the table located in criterion 2.12. The entity is eligible to calculate a modified aggregate weighted value if the original aggregate weighted value is less than 12,000. To calculate the Control Center's modified aggregate weighted value, the Responsible Entity should reference the table located in criterion 2.12, and the exclusion language, and sum the weighted values for each BES Transmission Line that is not part of a single GCE that was defined by the entity in accordance with the exclusion clause.



Note: Substation equipment (e.g., transformers) is not shown for simplicity.

Circles represent fault interrupting devices.

The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 10,000, which is above the minimum threshold for the medium impact rating required in criterion 2.12. Given that the calculated aggregated weighted value is less than 12,000, the Responsible Entity is eligible to calculate a modified aggregate weighted value that excludes BES Transmission Lines contained in a single GCE in accordance with the exclusion clause.

Voltage Value of a BES Transmission Line	Weight Value per BES Transmission Line	Applicable Lines	Weighted Value
< 100 kV	100	None	0
100 kV to 199 kV	250	Line 2, Line 3, 12 additional lines	3500
200 kV to 299 kV	700	None	0
300 kV to 499 kV	1300	Line 1, Line 4, Line 5, Line 6, Line 8	6500
500 kV and above	0	None	0

The calculation of the modified aggregate weighted value is demonstrated below and equates to an aggregate weighted value of 6,500, which is above the minimum threshold for the medium impact rating required in criterion 2.12. In accordance with criterion 2.12, the BCS associated with the Control Center should be categorized as medium impact BCS.

Voltage Value of a BES Transmission Line	Weight Value per BES Transmission Line	Applicable Lines	Weighted Value
< 100 kV	100	None	0
100 kV to 199 kV	250	None	0
200 kV to 299 kV	700	None	0
300 kV to 499 kV	1300	Line 1, Line 4, Line 5, Line 6, Line 8	6500
500 kV and above	0	None	0

*Lines 2 and 3 (along with the 12 additional lines located in the 138kV GCE system) are excluded from the calculation because the Responsible Entity has defined an interface to a GCE that is operated at less than 300kV, where the gross export across the interface does not exceed 75 MWh during non-EEA conditions.